LSM 3.5 SP3 Business + Prof.

Manuale

24.01.2024

SimonsVoss technologies

Sommario

1. Indicazioni generali ... 6
1.1 Avvisi di sicurezza generali ... 6
1.2 Avvertenze di sicurezza specifiche del prodotto ... 7
1.3 Avvisi legali ... 7
1.4 Requisiti di sistema ... 8
1.5 Informazioni sul manuale ... 9
1.6 Protezione dei dati nel sistema 3060 ... 9
1.6.1 Protezione base IT ... 10
1.6.2 Codifica ... 10
2. Utilizzo conforme ... 11
3. Significato della formattazione del testo ... 12
4. Installazione ... 13
4.1 Software ... 13
4.1.1 LSM Business/Professional ... 13
4.1.2 VNHost ... 22
4.1.3 CommNode ... 24
5. Primi passi dopo la nuova installazione ... 26
5.1 Gestione consigliata delle password ... 26
5.2 Registrazione di LSM ... 26
5.3 Creazione di un impianto di chiusura ... 31
5.3.1 Panoramica della generazione di protocolli ... 34
5.3.2 Impianto di chiusura G1 ... 36
5.3.3 Impianto di chiusura G2 ... 36
5.3.4 Impianto misto G2+G1 ... 36
5.3.5 Modalità Overlay ... 36
5.4 Backup automatico della banca dati ... 37
6. Dispositivi di programmazione ... 40
6.1 Riconoscimento e corretto utilizzo dei dispositivi di programmazione ... 40
6.1.1 SmartCD.G2 ... 40
6.1.2 SmartCD.MP ... 41
6.1.3 SmartCD.HF ... 41
6.1.4 SmartStick AX ... 42
6.2 Distanze di programmazione ... 42
6.2.1 Programmazione di chiusure ibride ... 44
6.3 Controllo del collegamento ... 44
7. Interfaccia utente ... 45

7.1 Barra del menu ... 46
7.1.1 File ... 46
7.1.2 Database ... 46
7.1.3 Vista ... 47
7.1.4 Procedure guidate ... 54
7.1.5 Modifica ... 54
7.1.6 Report ... 105
7.1.7 Programmazione ... 115
7.1.8 Opzioni ... 118
7.1.9 Rete ... 123
7.1.10 Finestre ... 124
7.1.11 Guida ... 124
7.2 Barra multifunzione ... 125
7.3 Impianto di chiusura ... 126
7.4 Gruppi e settori ... 126
7.5 Matrice ... 128
8. Conoscenze generali sull'LSM ... 130
8.1 Autorizzazioni di gruppo ... 130
8.1.1 Riserve gruppo (solo G1) ... 131
8.1.2 Eredità ... 131
8.2 Autorizzazioni nel protocollo G2 ... 131
8.3 Programmi delle fasce orarie ... 132
8.4 Livello di chiusura trasversale ... 133
8.5 Crittografia (WaveNet) ... 135
9. Funzioni base ... 136
9.1 Creazione di un nuovo impianto di chiusura ... 136
9.2 Creazione di un nuovo gruppo transponder ... 136
9.3 Creazione di un nuovo transponder ... 136
9.4 Assegnazione successiva di un transponder ad un gruppo transponder ... 137
9.5 Creazione di un nuovo settore ... 137
9.6 Creazione di una nuova chiusura ... 137
9.7 Creazione del tastierino PinCode ... 137
9.7.1 Configurazione del tastierino PinCode ... 138
9.7.2 Creazione del tastierino PinCode nel piano di chiusura ... 138
9.7.3 Programmazione del tastierino PinCode ... 139
9.8 Assegnazione di una chiusura ad un settore ... 139
9.9 Assegnazione/ritiro dell'autorizzazione ... 139
9.10 Configurazione di componenti DoorMonitoring ... 140

9.11 Livello di chiusura trasversale ... 140
9.11.1 Creazione di un livello di chiusura trasversale ... 140
9.11.2 Associazione delle chiusure ... 141
9.11.3 Associazione dei transponder ... 142
9.11.4 Autorizzazione dei transponder ... 143
9.12 Creazione dei transponder per i Vigili del fuoco ... 143
9.13 Backup manuale della banca dati ... 144
9.14 Metodi di lavoro conformi alla protezione dei dati secondo il RGPD ... 145
9.14.1 Esportazione dei dati personali ... 145
9.14.2 Cancellazione dei dati ... 147
9.14.3 Quali dati personali vengono memorizzati nel software? ... 149
9.14.4 Per quale finalità i dati personali vengono memorizzati nel software? ... 150
9.14.5 Per quanto tempo i dati personali sono memorizzati nel software? ... 150
9.14.6 I dati personali memorizzati nel software sono protetti dall'accesso di terzi? ... 150
9.14.7 Può essere messa a disposizione una copia dei dati memorizzati? ... 150
9.14.8 I dati personali possono essere cancellati dal software? ... 150
9.15 Ricerca all'interno della matrice ... 151
9.16 Esecuzione di azioni di gruppo ... 151
9.17 Programmazione del transponder ... 152
9.18 Programmazione della chiusura ... 152
9.19 Programmazione tramite LSM Mobile ... 153
9.19.1 Con laptop, netbook o tablet ... 153
9.20 Definizione programma fasce temporali (con giorni festivi e ferie aziendali) ... 154
9.21 Reset dei componenti ... 156
9.22 Sostituzione della chiusura difettosa ... 156
9.23 Blocca transponder ... 157
9.23.1 Blocca permanente il transponder e crea un transponder sostitutivo ... 158
9.23.2 Blocca temporaneamente il transponder ... 161
9.24 Controllo e valutazione dello stato batteria delle chiusure ... 162
9.25 Reset della modalità magazzino nelle chiusure G1 ... 164
9.26 Reset della modalità Freeze nelle chiusure G2 ... 164
9.27 Amministrazione degli elenchi accessi ... 165
9.27.1 Elenchi degli accessi ... 166
9.28 Gestione utenti ... 167
9.29 Gestione schede ... 167
9.29.1 Modifica della configurazione ... 168
9.29.2 Tabella ... 169

9.30 Inoltro dei dispositivi di programmazione USB ai terminal server (LSM Professional) 171
9.30.1 SmartCD.G2 / SmartCD2.G2 171
9.30.2 SmartCD MP / HF 176
9.30.3 SmartStick AX 188

10. Esecuzione di attività correnti basate su WaveNet in LSM 195

10.1 Creazione di una rete radio WaveNet e integrazione di una chiusura 195
10.1.1 Preparazione del software LSM 195
10.1.2 Prima programmazione dei componenti di chiusura 195
10.1.3 Preparazione dell'hardware 196
10.1.4 Creazione del nodo di comunicazione 197
10.1.5 Configurazione della rete e importazione nell'LSM 197

10.2 Messa in funzione del chiusure DoorMonitoring 199
10.2.1 Possibili stati (porta) 199
10.2.2 Integrazione di chiusure DoorMonitoring nella rete 200
10.2.3 SmartHandle DoorMonitoring 201
10.2.4 Cilindri DoorMonitoring 203
10.2.5 Valutazione degli input del controller 204
10.2.6 Trasferimento della configurazione WaveNet 206
10.2.7 Assegnazione del LockNode a una chiusura 206
10.2.8 Attivazione degli eventi di input della chiusura 206

10.3 Configurazione del RingCast 207
10.3.1 Preparare RouterNode per RingCast 207
10.3.2 Creazione del RingCast 209
10.3.3 Test di funzionamento RingCast 212

10.4 Configurazione dell'Event management (eventi) 215
10.4.1 Configurazione del server e-mail 216
10.4.2 Impostazione del servizio task 216
10.4.3 Inoltro degli eventi di input tramite il RouterNode2 216
10.4.4 Inoltro degli eventi di input tramite il sistema SREL3-ADV 216
10.4.5 Creazione di una reazione 218
10.4.6 Creazione di un evento 219

10.5 Gestione della rete virtuale (VN) 225
10.5.1 Rete virtuale con SmartRelè 3 Advanced 226
10.5.2 Rete virtuale con SmartRelè 2 G2 232

10.6 Lettura della chiusura 251

11. Glossario & Acronimi 256

12. Supporto e ulteriori informazioni 259

1. Indicazioni generali

Questo manuale descrive le funzioni del software Locking System Management 3.5 SP3. Il software Locking System Management, in breve software LSM, è stato sviluppato per gestire impianti di chiusura complessi dotati di componenti SimonsVoss.

Ad integrazione del presente manuale sono disponibili altri documenti:

- *Manuale WaveNet*

  Descrive l'uso della rete radio WaveNet.

- *SimonsVoss SmartUserGuide*

  Illustra l'esecuzione delle funzioni base con il software LSM.

- *Manuale Aggiornamento LSM*

  Descrive la procedura di aggiornamento dalle versioni precedenti.

1.1 Avvisi di sicurezza generali

Parola segnale: Possibili effetti immediati di non conformità
AVVERTENZA: Morte o lesioni gravi (possibili, ma improbabili)
ATTENZIONE: Lesione minori
AVVISO: Danni materiali o malfunzionamento
NOTA: Basso o no

AVVERTENZA

Accesso bloccato

Con componenti montati e/o programmati in modo difettoso, l'accesso attraverso una porta può restare bloccato. La SimonsVoss Technologies GmbH non risponde delle conseguenze di un accesso bloccato, per esempio nel caso si debba accedere a persone ferite o in pericolo, di danni a cose o altri danni!

Accesso bloccato tramite manipolazione del prodotto

Se si modifica il prodotto da solo, possono verificarsi malfunzionamenti e l'accesso attraverso una porta può essere bloccato.

- Modificare il prodotto solo quando necessario e solo nel modo descritto nella documentazione.

NOTA

Uso conforme

I prodotti SimonsVoss sono concepiti esclusivamente per l'apertura e la chiusura di porte e oggetti simili.

- Non utilizzare i prodotti SimonsVoss per altri scopi.

Tempi diversi per chiusure G2

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

Qualifiche richieste

L'installazione e la messa in servizio richiedono conoscenze specialistiche.

- Solo personale qualificato può installare e mettere in servizio il prodotto.

Non si escludono modifiche o perfezionamenti tecnici, anche senza preavviso.

La versione in lingua tedesca è il manuale di istruzioni originale. Altre lingue (redazione nella lingua del contratto) sono traduzioni delle istruzioni originali.

Leggere e seguire tutte le istruzioni di installazione, installazione e messa in servizio. Passare queste istruzioni e tutte le istruzioni di manutenzione all'utente.

1.2 Avvertenze di sicurezza specifiche del prodotto

ATTENZIONE

Perdita della password dell'impianto di chiusura

La password dell'impianto di chiusura è la componente centrale del concetto di sicurezza. La perdita della password dell'impianto di chiusura ne limita il funzionamento e costituisce un rischio per la sicurezza.

1. Conservare la password dell'impianto di chiusura in un luogo sicuro (ad es. in una cassaforte)!
2. Rendere sempre visibile la password dell'impianto di chiusura alle persone autorizzate!

1.3 Avvisi legali

Si avvisa espressamente l'acquirente che l'uso di un sistema di chiusura (ad es. con registrazione degli accessi e funzioni DoorMonitoring) può essere soggetto a obblighi legali di autorizzazione, in particolare in materia di tutela della privacy, e diritti di compartecipazione dei dipendenti. La responsabilità dell'uso a norma di legge del prodotto è dell'acquirente o cliente e dell'utente finale.

L'uso non conforme agli accordi o inconsueto, che non corrisponda cioè espressamente ad interventi di riparazione o modifiche autorizzati da SimonsVoss Technologies GmbH o ad un'assistenza non corretta, può causare malfunzionamenti ed è pertanto vietato. Qualunque modifica non autorizzata da SimonsVoss Technologies GmbH determina la perdita di qualunque richiesta di responsabilità e garanzia, inclusi eventuali diritti di garanzia specificamente pattuiti.

1.4 Requisiti di sistema

Per lavorare senza problemi con LSM SimonsVoss consiglia sempre di utilizzare un hardware potente e aggiornato che superi i requisiti di sistema.

Al fine di visualizzare chiaramente anche impianti di chiusura di grandi dimensioni con molti componenti SimonsVoss raccomanda un monitor widescreen ad alta risoluzione da 21" o più.

Informazioni generali

- Diritti di amministratore locale per l'installazione
- TCP/IP (NetBios attivo)

  (L'uso di EventAgent richiede NetBios.)
- LAN (min. 100MBit/s)
- Domini Windows (non necessario in caso di installazioni per utente singolo)
- Risoluzione dei nomi (non necessario in caso di installazioni per utente singolo)
- .NET-Framework 4.0 o più recente
- Interfaccia/e USB
- Nessun supporto per i processori ARM in System 3060

Client PC

- Monitor: min. 48 cm (19")
- Risoluzione del monitor: min. 1024x768, raccomandata 1280x1024 o più
- Processore: min. 2,66 GHz con 2 o più core (Intel/AMD)
- Memoria di lavoro: min. 4 GB
- Dimensioni del disco rigido: a seconda delle dimensioni dell'impianto, min. 500 MB

  (durante l'installazione circa 1 GB)
- Sistema operativo Windows:
  - Windows 11 Professional, 64 bit
  - Windows 10 Professional, 64 bit

Server

- Processore: min. 2,66 GHz con 2 o più core (Intel/AMD)

  (rete virtuale con SmartRelè 3 Advanced e VNHost: min. 4 core, il clock dipende dal numero di gateway)
- Memoria di lavoro: min. 4 GB

- Dimensioni del disco rigido: applicazione ca. 500 MB
  (durante l'installazione circa 1 GB)
  Database a seconda della quantità di dati trattati
- Windows Server:
  - Windows Server 2022
  - Windows Server 2019
- Ambienti virtuali:
  - VMware ESXi (versione 7.0 U2) con Windows Server 2022 e 2019
  - VMware ESXi (versione 6.5.0) con Windows Server 2019
- Se si utilizza il server CommNode: .NET Framework 4.0 o più recente
- Se l'applicazione viene utilizzata su base server. Abilitazione su Advantage Database Server per una directory database

NOTA

Consultate le Release Notes del software LSM per sapere quale versione di LSM Mobile utilizzare.

1.5 Informazioni sul manuale

Questo manuale descrive le funzioni del software LSM. L'utente sarà pertanto in grado di programmare i componenti di chiusura SimonsVoss e gestire l'impianto di chiusura.

NOTA

Il manuale non tratta il montaggio dei singoli componenti di chiusura SimonsVoss. A tale scopo, osservare tassativamente le guide brevi e i manuali dei vari componenti!

Transponder

Nel software LSM, tutti i supporti di identificazione (transponder, tag, scheda ecc.) vengono considerati transponder. Nel manuale, pertanto, il termine "transponder" si applica anche a tutti gli altri supporti di identificazione, quali tag e schede.

1.6 Protezione dei dati nel sistema 3060

Vedi *Metodi di lavoro conformi alla protezione dei dati secondo il RGPD [▸ 145]*.

1.6.1 Protezione base IT

1.6.1.1 Quali sono i requisiti di protezione dei dati elaborati nel sistema?

In generale, nel software vengono elaborati e memorizzati solo dati non critici con requisiti di protezione cosiddetti normali. In altre parole, dati la cui ipotetica perdita non danneggerebbe la reputazione di una persona o l'immagine di un'azienda. E nemmeno un danno finanziario elevato.

1.6.1.2 Quali sono i requisiti raccomandati per l'infrastruttura IT?

Secondo l'Ufficio federale per la sicurezza informatica (BSI), una protezione informatica di base come concetto di sicurezza è sufficiente per un sistema di chiusura SimonsVoss ed è considerata il requisito minimo raccomandato per la vostra infrastruttura informatica.

1.6.2 Codifica

1.6.2.1 I dati del Sistema 3060 sono criptati?

Sì. All'interno della comunicazione del sistema, i pacchetti di dati sono criptati end-to-end. Le versioni più recenti dei nostri prodotti garantiscono un incremento del livello di sicurezza, perché sono sempre all'avanguardia. Vengono utilizzati metodi di crittografia a più livelli (AES, 3DES).

1.6.2.2 Quali dati vengono criptati durante il processo?

Nessun dato personale viene trattato nell'ambito della comunicazione del sistema, ma viene pseudonimizzato con l'aiuto di numeri di identificazione. Anche senza crittografia, non è possibile attribuire il nome a una persona reale.

1.6.2.3 Anche i percorsi di trasmissione, ad esempio via radio, sono criptati?

No. Con la crittografia end-to-end utilizzata non è necessaria un'ulteriore crittografia dei percorsi di trasmissione.

2. Utilizzo conforme

LSM 3.5 SP3 sta per Locking System Management ed è un software supportato da database. Potete usarlo per creare, gestire e controllare i piani di chiusura.

3. Significato della formattazione del testo

Questa documentazione utilizza la formattazione del testo e gli elementi di progettazione per facilitare la comprensione. La tabella spiega il significato delle possibili formattazione del testo:

Esempio	Tasto
☑ Esempio ☐ Esempio	Casella di controllo
◉ Esempio	Opzione
[Esempio]	Scheda di registro
"Esempio"	Nome della finestra visualizzata
| Esempio |	Barra superiore del programma
Esempio	Voce nella barra del programma superiore aperta
Esempio	Voce del menu contestuale
▼ Esempio	Nome del menu a discesa
"Esempio"	Opzione di selezione in un menu a discesa
"Esempio"	Area
Esempio	Campo
Esempio	Nome di un servizio (Windows)
Esempio	Comandi (ad es. comandi CMD di Windows)
Esempio	Voce di banca dati
[Esempio]	Selezione del tipo di MobileKey

4. Installazione

Il presente capitolo descrive la prima installazione del software LSM in un sistema nel quale non siano installate precedenti versioni dell'LSM. In genere è possibile anche eseguire l'aggiornamento da precedenti versioni dell'LSM alla versione 3.5 SP3 attuale. In questo caso, tenere presente che l'LSM 3.5 SP3 non può essere installato in parallelo con precedenti versioni dell'LSM.

LSM Business e LSM Professional richiedono anche il server Advantage Database Server in versione 12.x o superiore.

Il manuale di aggiornamento LSM descrive la procedura di aggiornamento del software LSM.

4.1 Software

4.1.1 LSM Business/Professional

L'installazione dell'LSM Professional è simile.

4.1.1.1 Installazione e configurazione del server ADS

Advantage Database Server è un componente fondamentale per l'uso di LSM Business. Esso garantisce che più utenti possano accedere simultaneamente ai piani di chiusura del database e che lo scambio dati sia sicuro.

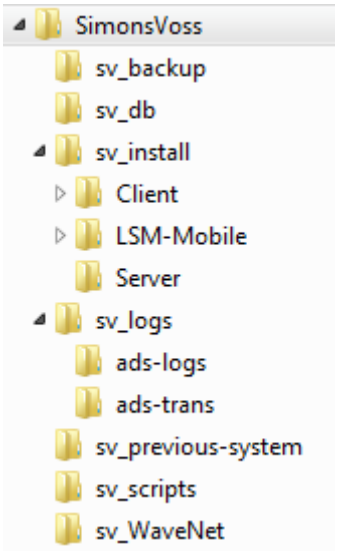
Questo capitolo mostra tutti i passi necessari da eseguire sul server.

NOTA

L'installazione del server ADS presuppone il possesso di una chiave di licenza valida *(Validation Code e Replication Code)*. Qualora non si possieda ancora un codice di licenza, rivolgersi al proprio referente con la bolla di consegna SimonsVoss del software LSM Business. Su tale documento è riportato un certificato con numero di serie e codice di validazione con cui viene registrata la licenza ADS.

Creazione della struttura delle cartelle

Durante l'installazione, creare la seguente gerarchia di cartelle nella directory principale (ad esempio `C:\SimonsVoss`):



Cartella	Contenuto
sv_backup	File di backup locali per riportare un impianto di chiusura ad uno stato precedente
sv_db	Piano di chiusura
sv_install	File di installazione (se necessario)
sv_logs	File di log del server ADS
sv_previous_system	File di vecchie versioni LSM
sv_scripts	Script di backup che viene aggiunto all'Utilità di pianificazione di Windows
sv_WaveNet	File di WaveNet Manager

Installazione del server ADS

Installare il server ADS sul server:

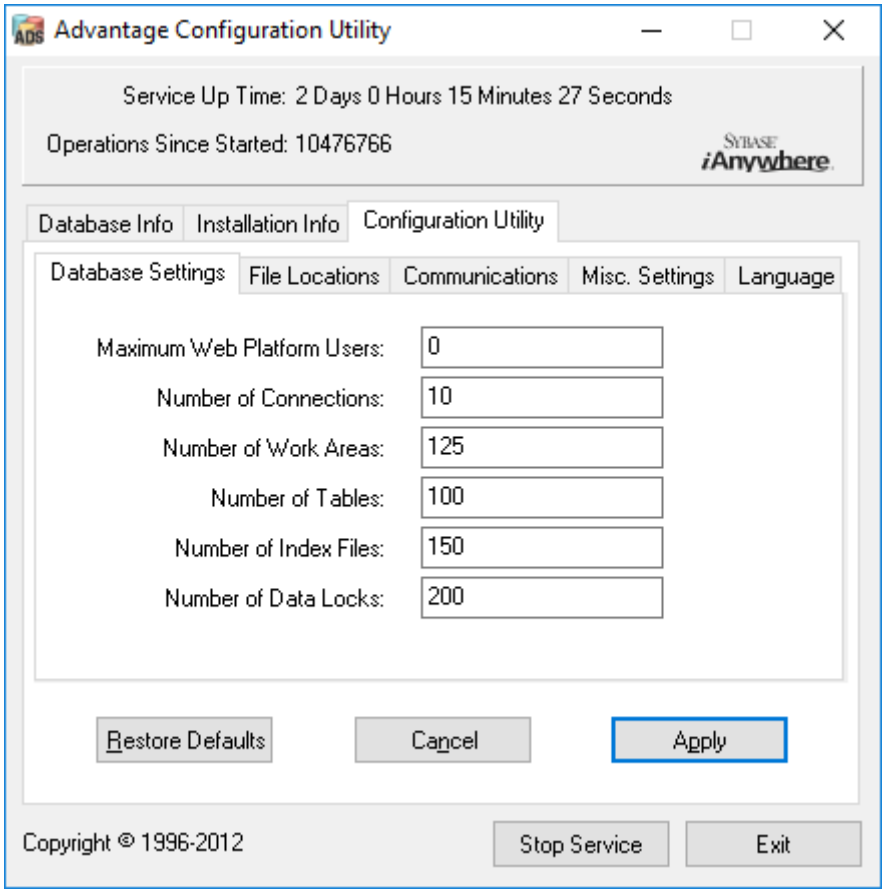
1. Lanciare il file di installazione in qualità di amministratore.
2. Seguire le istruzioni per l'installazione.
   ↳ Accettare le condizioni di licenza per eseguire l'installazione.
   ↳ Per registrare correttamente il server ADS, inserire i codici necessari quando compare l'apposita richiesta.

Configurazione del server ADS

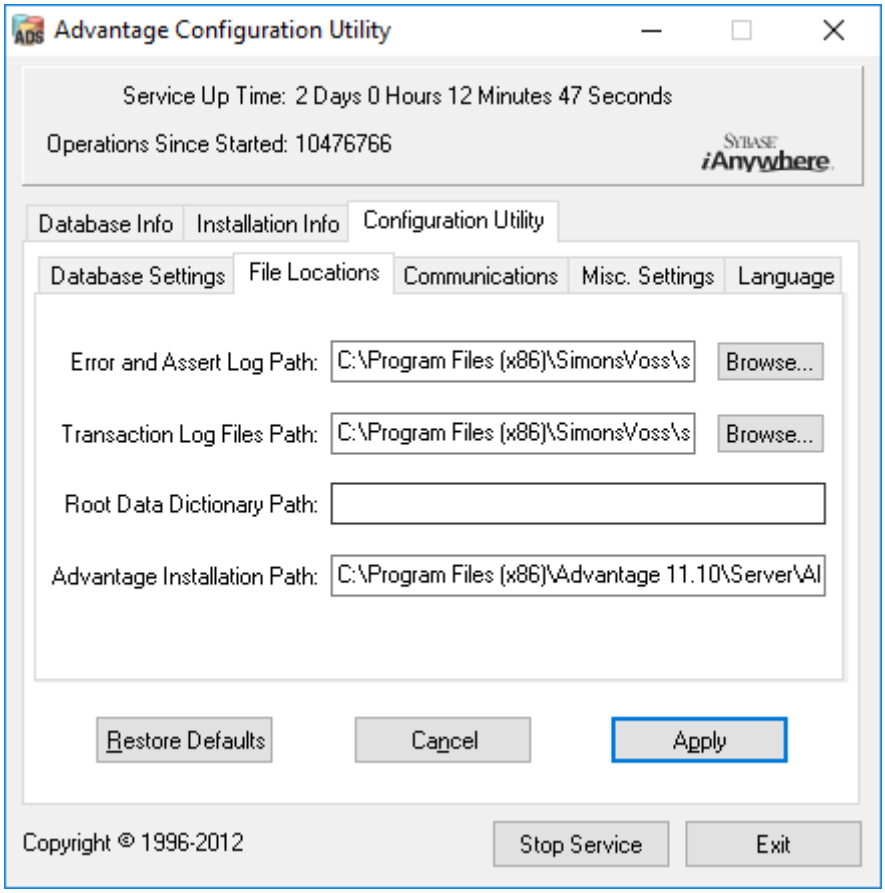
Configurare il server ADS con l'Advantage Configuration Utility:

1. Avviare l'Advantage Configuration Utility, ad es. tramite *Start/Programmi/Advantage Database Server/Advantage Configuration Utility* (la configuration utility potrebbe essere già avviata).
2. Selezionare la scheda "Configuration Utility".

3. Modificare le seguenti proprietà della scheda "Database Settings" e salvarle con il pulsante "Apply":

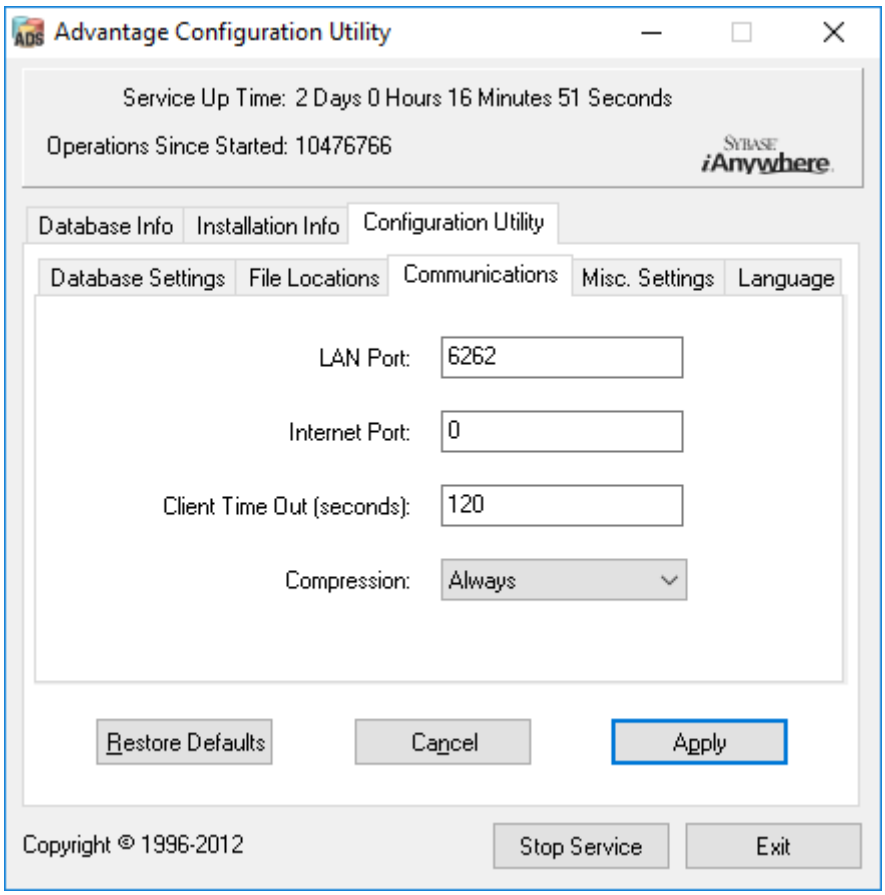


4. Modificare le seguenti proprietà della scheda "File Locations" e salvarle con il pulsante "Apply":

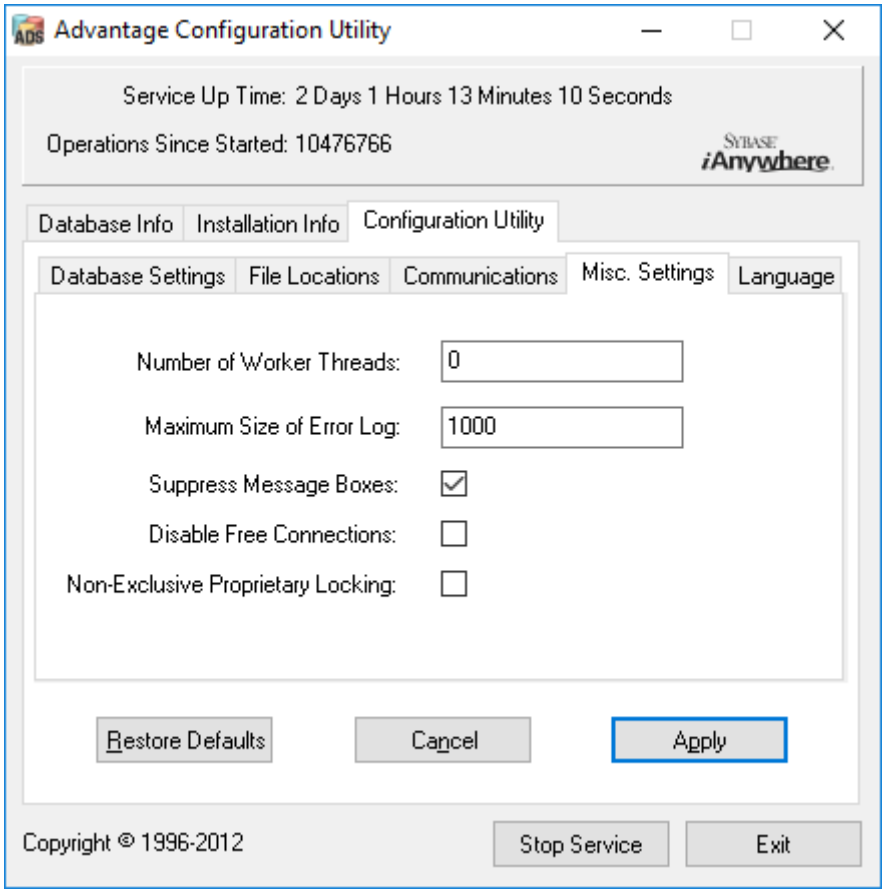


↳ Fare attenzione che l'unità (qui C:) può essere diversa da quella del server!

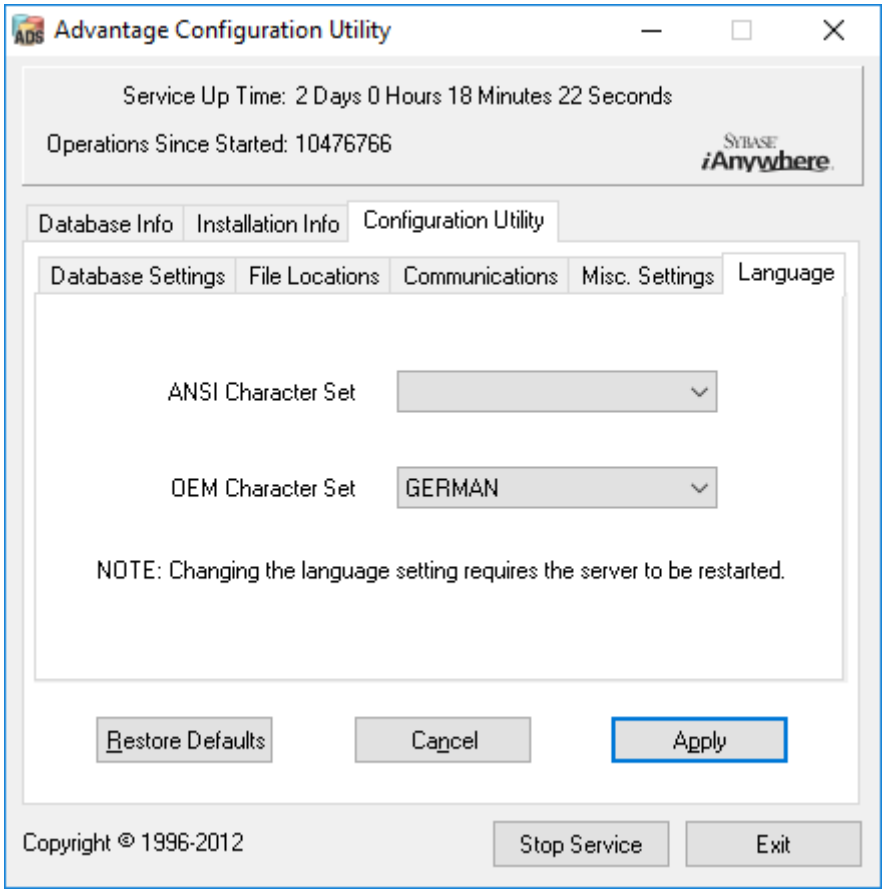
5. Modificare le seguenti proprietà della scheda "Communications" e salvarle con il pulsante "Apply":



6. Modificare le seguenti proprietà della scheda "Misc. Settings" e salvarle con il pulsante "Apply":



7. Modificare le impostazioni lingua della scheda "Language" secondo le necessità e salvarle con il pulsante "Apply":



Controllo del servizio server ADS

Controllare se il servizio del server ADS viene eseguito automaticamente come servizio di sistema:

1. Aprire il pannello di controllo, ad es. tramite *Start/Pannello di controllo*.
2. Aprire la cartella "Gestione".
3. Aprire la cartella "Servizi"
4. Controllare se il servizio "Advantage Database Server" possiede lo stato "Avviato" e il tipo di avvio è impostato su "Automatico".
   ↳ Modificare i valori facendo doppio clic sul servizio ADS per applicare le eventuali modifiche.

Abilitazione del database nella rete

La directory del database "sv_db" deve essere approvata nella rete. Configurare l'abilitazione con diritti di lettura. Si consiglia di configurare una "Abilitazione nascosta". *Le abilitazioni possono essere nascoste aggiungendo il carattere $ alla fine del percorso di abilitazione.*

4.1.1.2 Installazione e configurazione di LSM Business

ATTENZIONE

Installazione del VNHost dopo l'LSM

L'VNHost non può accedere al database se l'LSM non è ancora installato e l'impianto di chiusura non è stato configurato. Se l'VNHost durante l'installazione non rileva alcun database a cui accedere si potrebbero verificare dei problemi.

1. Installare l'LSM prima del VNHost.
2. Creare un impianto di chiusura.
3. Installare il VNHost.

Installazione di LSM Business

LSM Business viene installato sui computer client desiderati. Quest'ultimi accedono nella rete al server ADS che gestisce i piani di chiusura.

NOTA

Si consiglia di installare il software LSM direttamente in un account amministratore locale! *Effettuare il login con account Amministratore; non è sufficiente selezionare "Esegui come amministratore" accedendo con un normale account utente.*

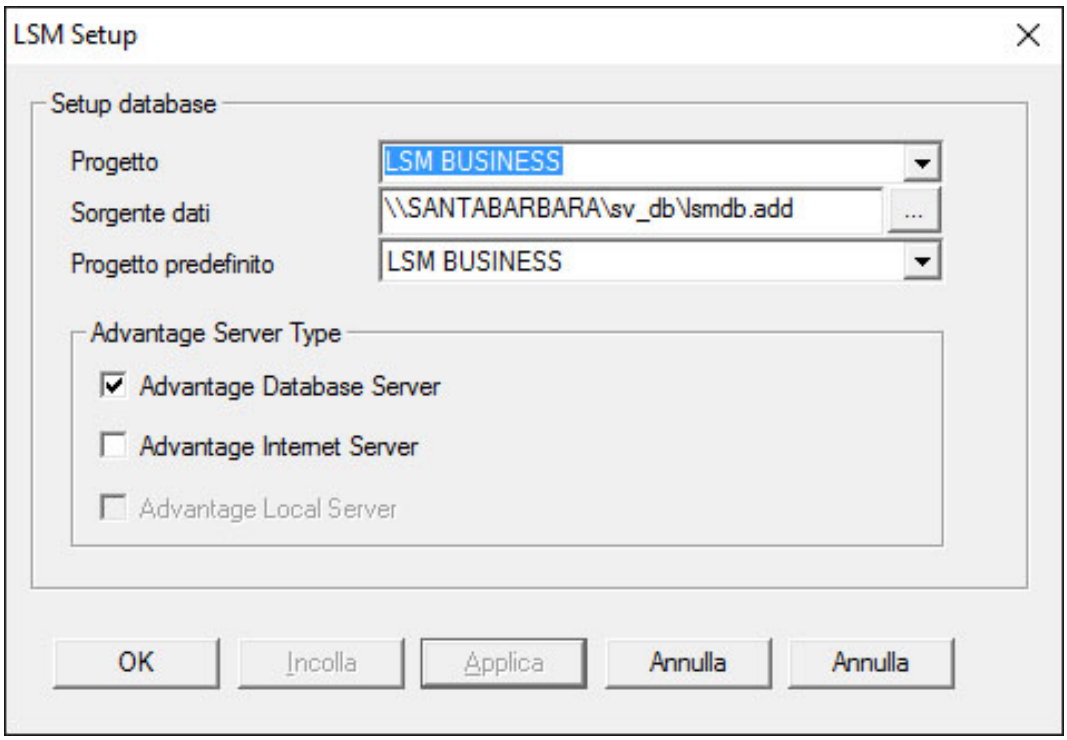
1. Lanciare il file di installazione in qualità di amministratore.
2. Seguire le istruzioni per l'installazione.
   ↳ Accettare le condizioni di licenza per eseguire l'installazione.
3. Avviare LSM Business *(icona sul desktop o da Start/Programmi/SimonsVoss/LSM BUSINESS)*

Configurazione di LSM Business

LSM Business va configurato un'unica volta. In questa fase, si copia un piano di chiusura vuoto sul server e si configura l'LSM Business in modo che possa accedere a tale piano di chiusura.

1. Estrarre il piano di chiusura salvato nella directory di installazione dell'LSM Business (ad es. C:\Programmi (x86)\SimonsVoss\LockSysMgr_3_5\db) nella directory "sv_db".
2. Avviare l'LSM Business (ad es. tramite *Start/Programmi/SimonsVoss/LSM Business)*.
3. Selezionare "Setup".

4. Alla prima esecuzione, comparirà una finestra in cui si imposta il percorso per il salvataggio del database.



   - ↳ Assegnare il nome desiderato al progetto.
   - ↳ Con il pulsante "...", selezionare il percorso sul server e indicare direttamente il file lsmdb.add. In caso di abilitazioni nascoste, il percorso al file lsmdb.add va inserito direttamente con caratteri $; ad es..: \\<SERVER>\sv_db$\lsmdb.add
   - ↳ *In LSM Business non è possibile scegliere una directory locale!*
5. Applicare le impostazioni.

4.1.1.3 Installazione dell'hotfix Crystal Reports

Crystal Reports viene utilizzato in background come strumento di reporting. Il tool si installa automaticamente nel corso dell'installazione di LSM Basic Online, Business e Professional. Per il corretto funzionamento, è necessario installare l'ultima versione dell'hotfix.

1. Lanciare l'hotfix con formato .exe.
2. Seguire le istruzioni per l'installazione.
   - ↳ Accettare le condizioni di licenza per eseguire l'installazione.

NOTA

Installazione senza componenti Java

I componenti Java (JCE) della hotfix non sono necessari per il funzionamento dell'LSM.

- Disattivare la casella di controllo ☐ JCE durante la routine di installazione.

4.1.2 VNHost

VNHost accede al database LSM e fornisce varie funzioni senza che l'LSM stesso venga eseguito (compreso il gateway).

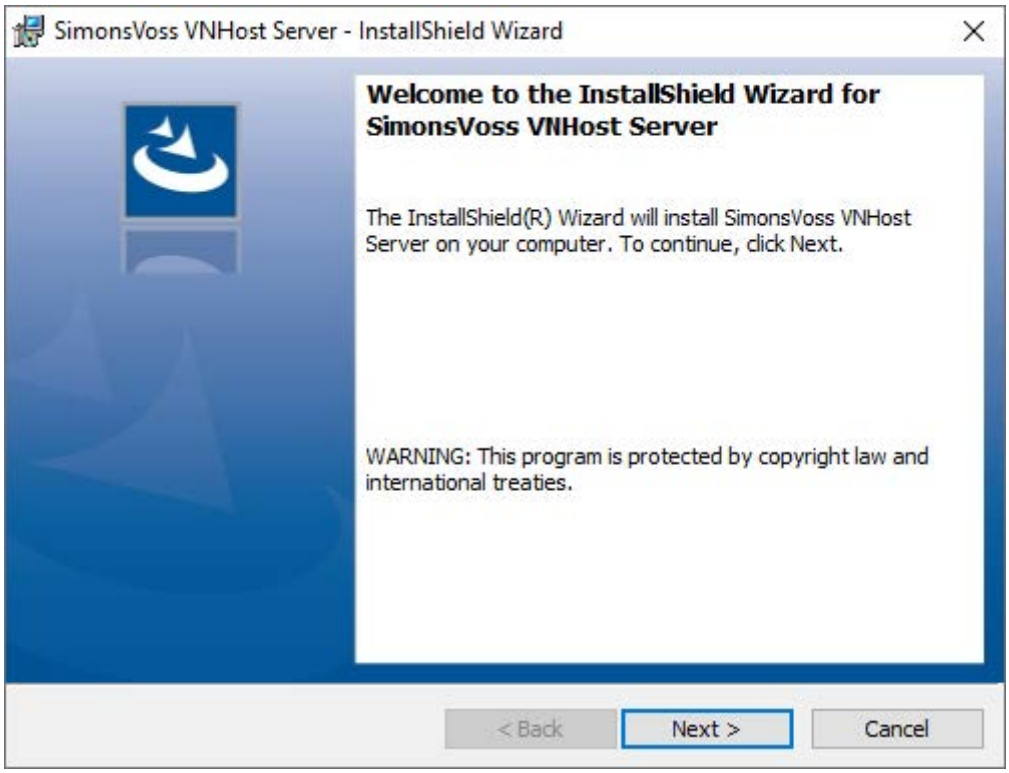
ATTENZIONE

Installazione del VNHost dopo l'LSM

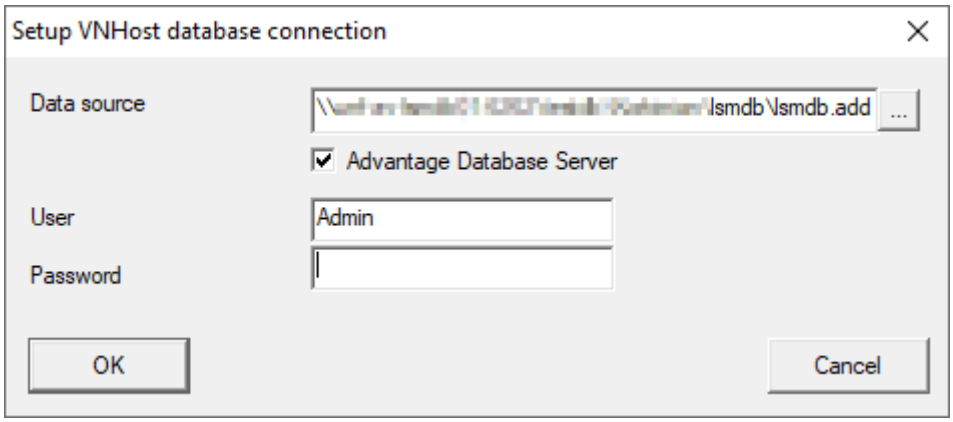
L'VNHost non può accedere al database se l'LSM non è ancora installato e l'impianto di chiusura non è stato configurato. Se l'VNHost durante l'installazione non rileva alcun database a cui accedere si potrebbero verificare dei problemi.

1. Installare l'LSM prima del VNHost.
2. Creare un impianto di chiusura.
3. Installare il VNHost.

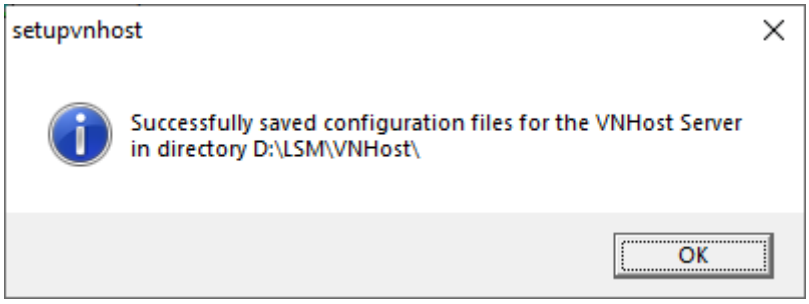
1. Eseguite il file Setup (vnhost_setup_3_5_sp3.exe).



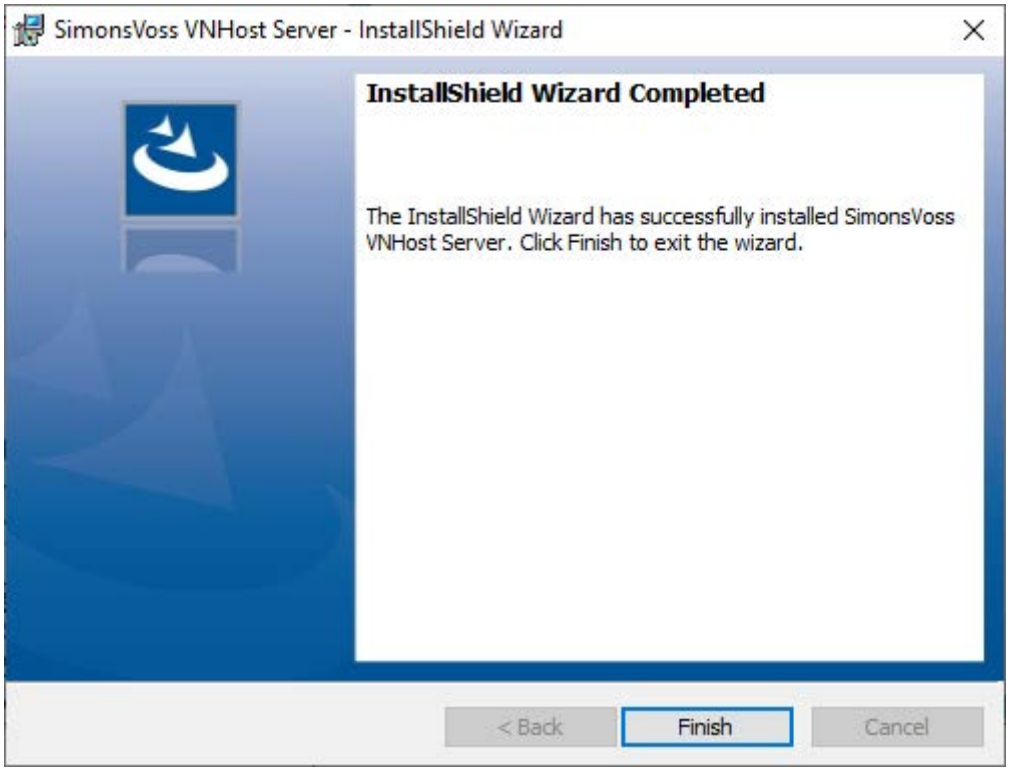
2. Seguite le istruzioni di installazione e installate il VNHost sul server.
3. Nella finestra "Setup VNHost database connection" inserite il percorso UNC al vostro lsmdb.add (può essere copiato dalla finestra di login di LSM).



4. Inserite il nome utente LSM e la vostra password utente LSM.
5. Se il vostro lsmdb.add è installato localmente: disattivate la casella di controllo ☐ Advantage Database Server.
6. Fare clic sul pulsante OK.
   ↳ La connessione tra VNHost e il database è stabilita.



↳ Installazione completata.



4.1.3 CommNode

È possibile installare il server CommNode utilizzando il file di installazione. Se il servizio CommNode non viene successivamente elencato nei servizi di Windows (server CommNode di SimonsVoss), è necessario eseguire l'installazione con un file batch.

1. Richiamare la directory di installazione del server CommNode (`C:\Program Files (x86)\SimonsVoss\CommNodeSvr_3_5`).
2. Eseguire il file batch install_CommNodeSvr con i diritti di amministratore.
   ↳ La riga di comando si apre.
   ↳ Il server CommNode viene installato.

↳ Il server CommNode è installato ed elencato nei servizi di Windows.

4.1.3.1 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.

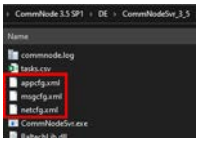
1. Aprire il software LSM.
2. Selezionare | Rete |/ Nodi di comunicazione .
3. Compilare le informazioni "Nome", "Nome PC" e "Descrizione".

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

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

   ↳ *Ad es. UNF-AL-18KJ793; UNF-AL-18KJ793.ALLEGION.COM; Nodo di comunicazione per la rete radio WaveNet 123.*

4. Fare clic sul pulsante File di configurazione .
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 Esci .

5. Primi passi dopo la nuova installazione

5.1 Gestione consigliata delle password

Due tipi di password vengono utilizzati in linea di principio nel software LSM:

- **Password utente**

  Per accedere al piano di chiusura o alla banca dati è necessaria la password utente.

- **Password del sistema di chiusura**

  La password del sistema di chiusura viene programmata in tutti i componenti SimonsVoss. Questa password del sistema di chiusura viene memorizzata nel piano di chiusura o nella banca dati in un'area criptata e non può essere letta. I componenti programmati di SimonsVoss possono essere riprogrammati solo se la banca dati conosce la password del sistema di chiusura!

Di seguito sono riportate due raccomandazioni per gestire le password in modo sicuro:

- Per una maggiore sicurezza dell'intero sistema di chiusura, la password del sistema di chiusura deve essere divisa in almeno due parti, che vengono assegnate individualmente dalle singole persone.
- Si raccomanda vivamente di annotare la password dell'amministratore e del sistema di chiusura e di conservarla al sicuro in luoghi diversi e inaccessibili a terzi!

Il gestore dell'impianto di chiusura dovrebbe sempre tenere presente una domanda: cosa succede se l'unica persona che conosce la password del sistema di chiusura (o parte di essa) improvvisamente non è più disponibile.

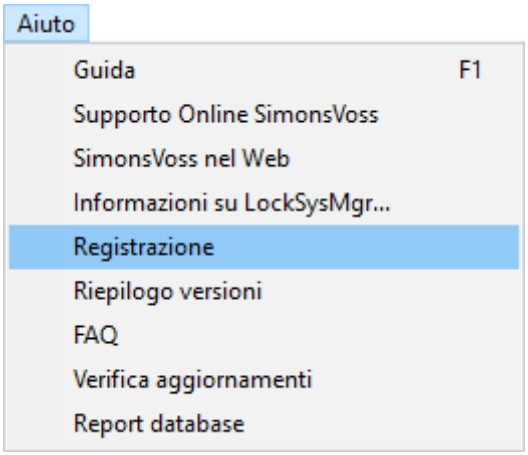
5.2 Registrazione di LSM

Registrare l'LSM. A tale scopo, viene creato un file di registrazione, che viene inviato a un apposito indirizzo e-mail. Si riceverà una risposta automatica con allegato il file di licenza personale. Con questo file di licenza è possibile registrare l'LSM con i moduli ordinati.

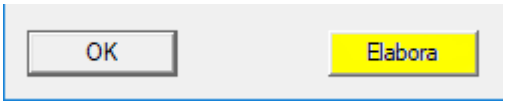
Procedura

- ✓ L'installazione dell'LSM è eseguita.
- ✓ Si dispone della bolla di consegna con le informazioni per la registrazione.
- ✓ Invio e-mail possibile.

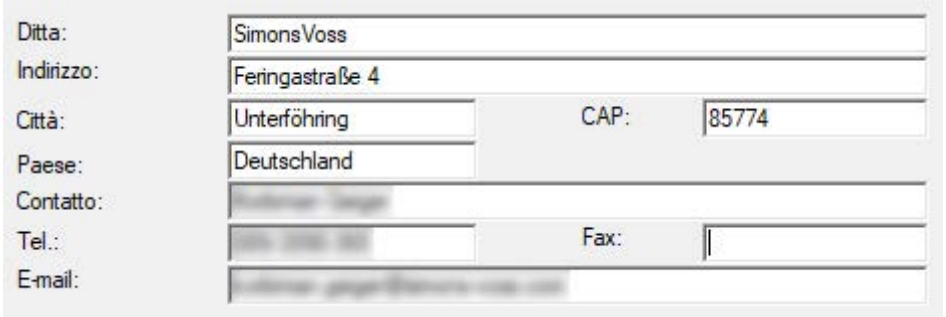
1. Nella scheda | Aiuto | fare clic sul Registrazione.
   ↳ Si apre la finestra "Registrazione".



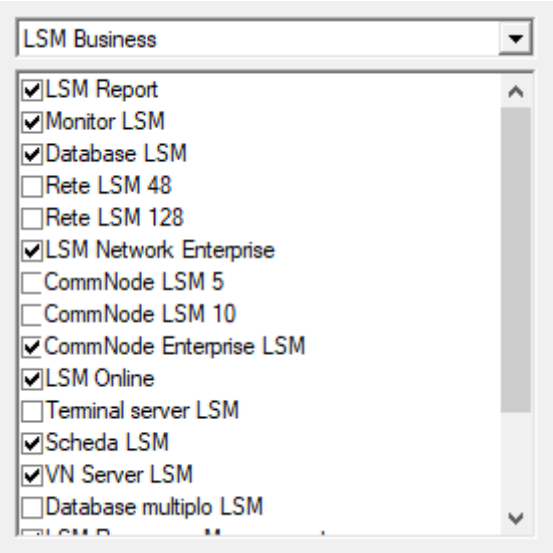
2. Fare clic pulsante Elabora.



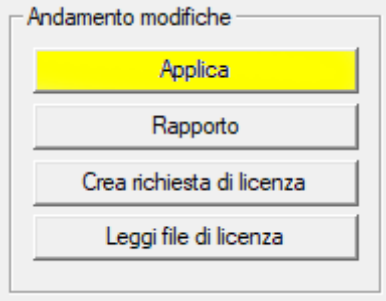
   ↳ Si apre la finestra "Modificare registrazione".
3. Compilare il modulo.



4. Assicurarsi che sia selezionata l'edizione corretta (esempio: Business).

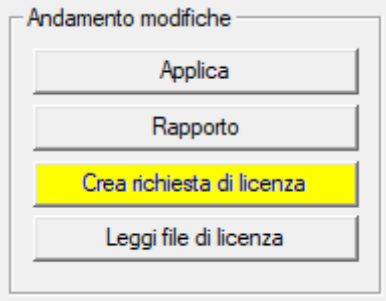


5. Fare clic pulsante Applica.

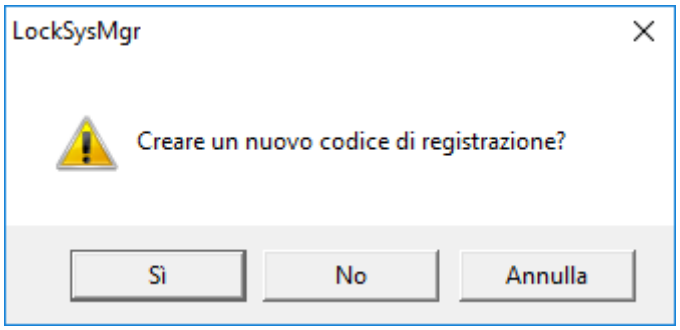


↳ Il record dati è salvato.

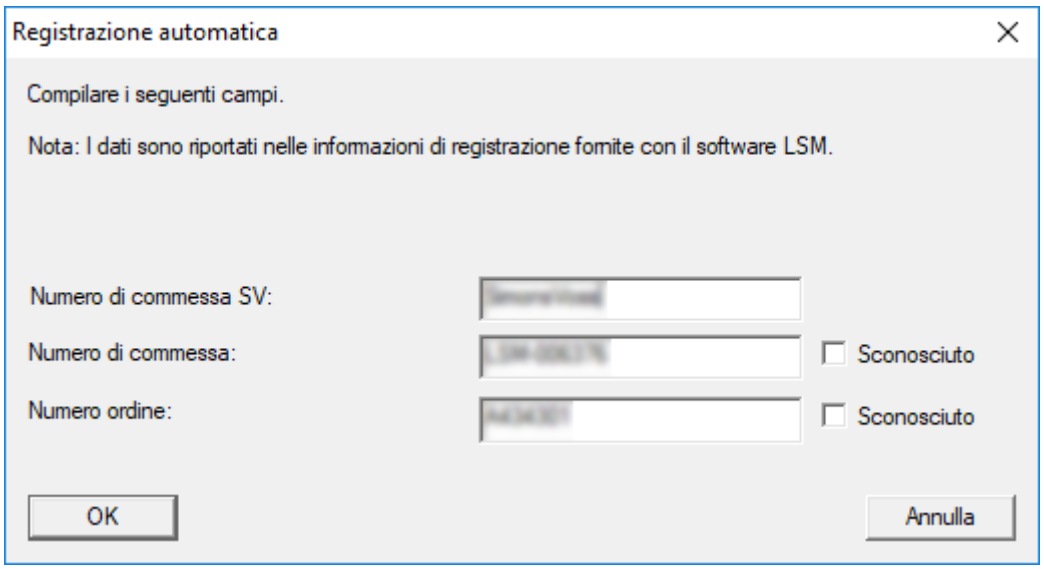
6. Fare clic pulsante Crea richiesta di licenza.



7. Fare clic pulsante Sì per confermare la richiesta.

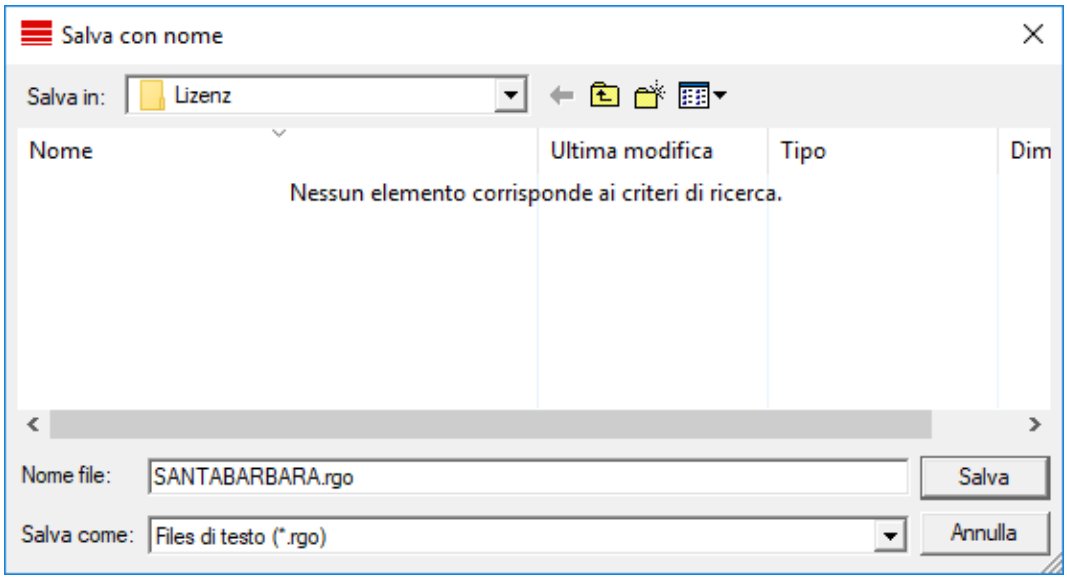


8. Compilare il modulo (numero di commessa LSM in formato LSM-xxxx-xx, numero ordine in formato Axxxxxx).

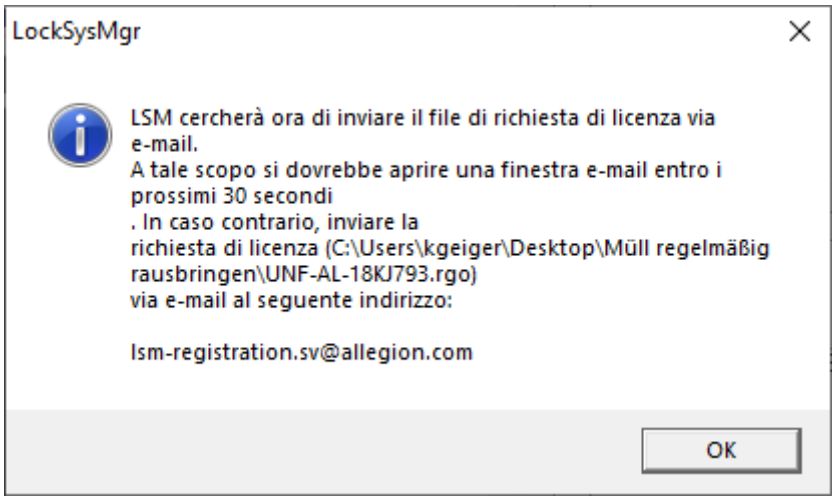


9. Fare clic sul pulsante OK.
   ↳ Viene creato il file RGO.
   ↳ Si aprirà la finestra Esplora risorse.

10. Salvare il file RGO in una directory di propria scelta.



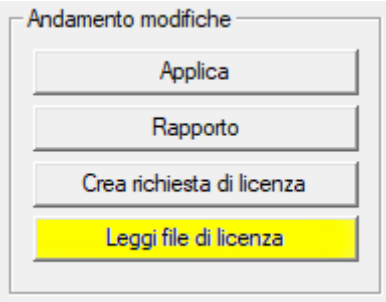
11. Fare clic sul pulsante OK.



    ↳ Si aprirà il client di posta elettronica predefinito. È già precompilata un'apposita e-mail con il file RGO allegato.

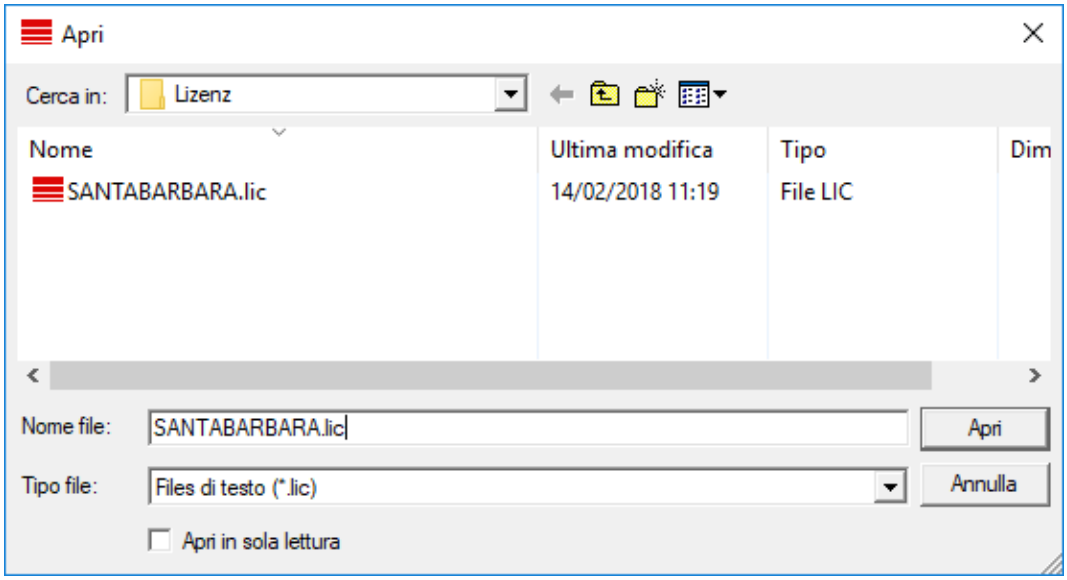
12. Se il file RGO non è allegato, eseguire l'operazione manualmente.
13. Inviare un'e-mail con il file RGO a lsm-registration.sv@allegion.com.
    ↳ La risposta con il file LIC allegato arriverà automaticamente.
14. Salvare il file LIC in una directory di propria scelta.
15. Ritornare all'LSM.

16. Fare clic pulsante Leggi file di licenza.



↳ Si aprirà la finestra Esplora risorse.

17. Selezionare il file LIC.



18. Fare clic pulsante Apri.
19. Fare clic pulsante OK" per confermare l'avviso.
20. Riavviare l'LSM.

↳ La registrazione è stata eseguita.

5.3 Creazione di un impianto di chiusura

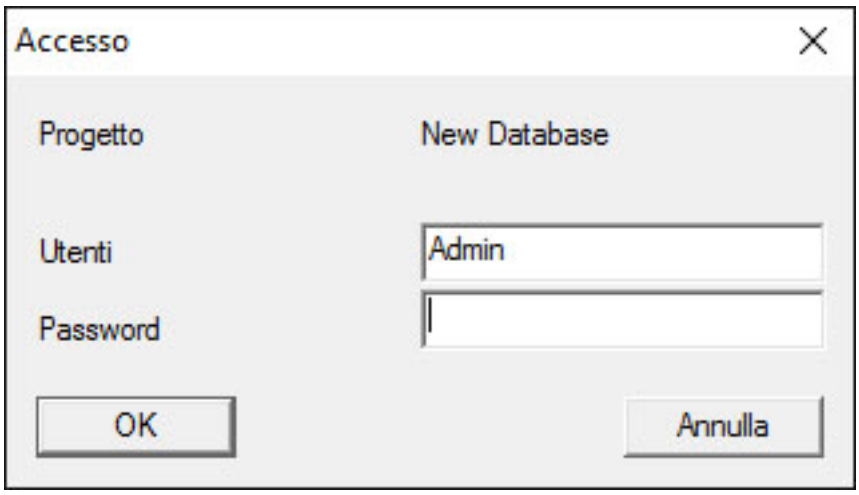
Definire la password

Se è già stato creato un progetto, ora è possibile creare un impianto di chiusura.

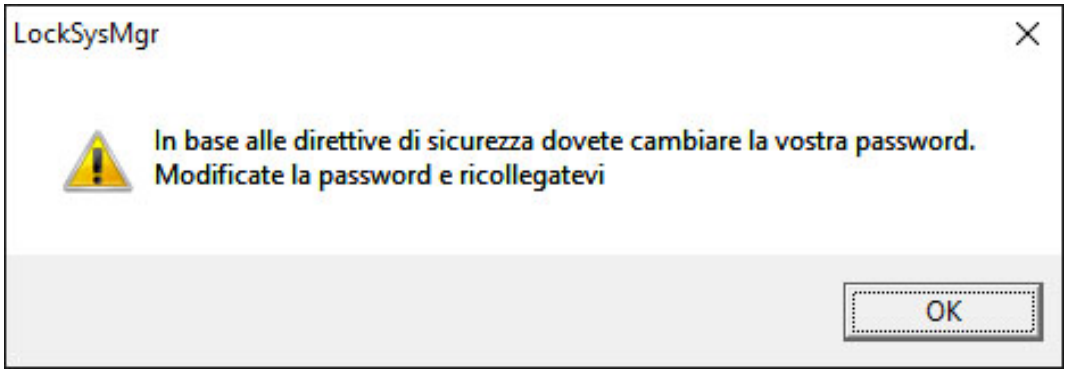
NOTA

Durante la creazione del primo piano di chiusura in LSM BUSINESS o LSM PROFESSIONAL, la procedura viene interrotta dal processo di assegnazione della licenza. Il processo di assegnazione della licenza per altri moduli è opzionale in LSM BASIC.

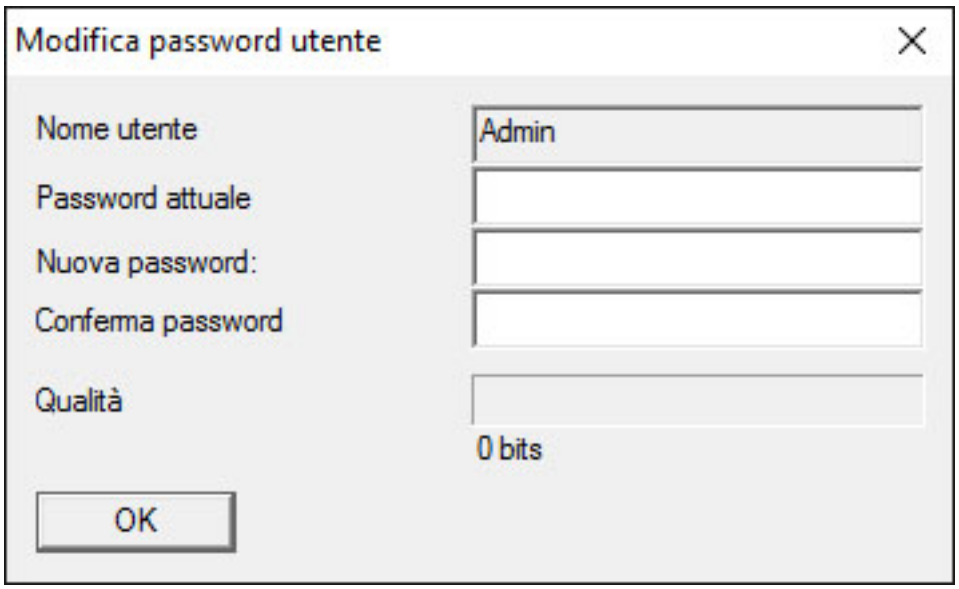
1. Fare clic su "Login" nel menu principale del software LSM. Alla voce "Setup", assicurarsi eventualmente che sia stato selezionato il progetto giusto.
2. Inserire la password predefinita "system3060".



3. Confermare l'avviso facendo clic su "OK".



4. Inserire nuovamente la password predefinita "system3060" e quindi specificare una nuova password utente.

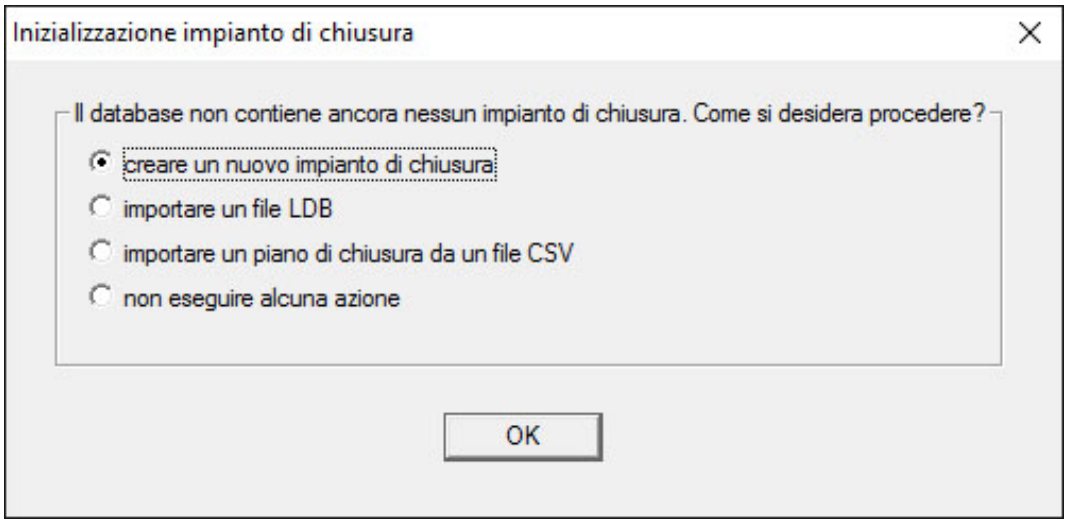


NOTA

La password utente viene richiesta ad ogni tentativo di accesso al database. In LSM Business si possono creare più utenti con password e diritti diversi.

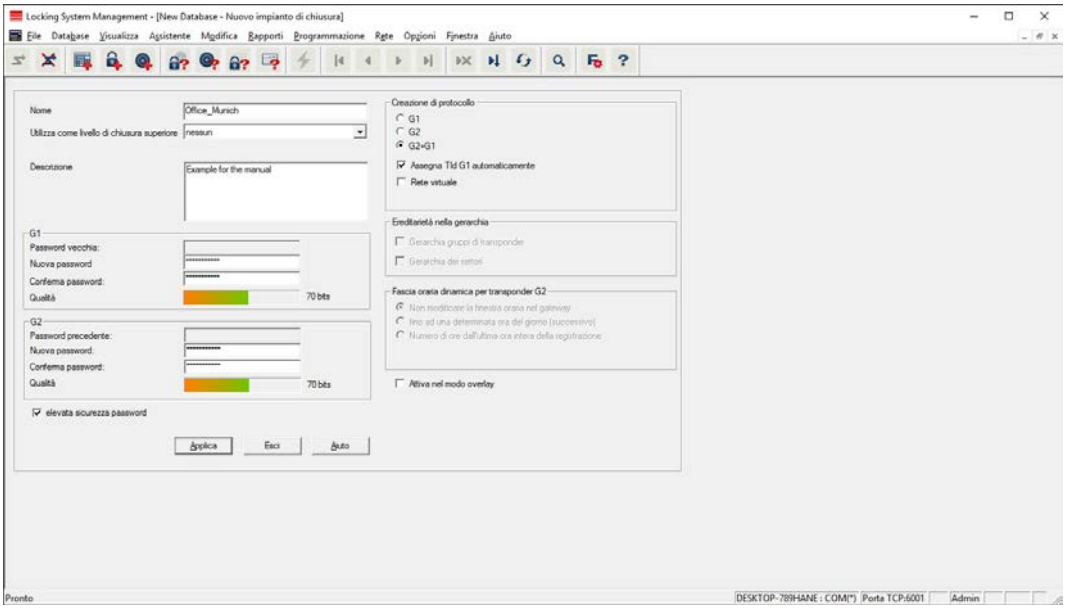
Creazione dell'impianto di chiusura

1. Subito dopo l'assegnazione di una nuova password, si aprirà una procedura guidata di configurazione:



2. Selezionare "Creare nuovo impianto di chiusura" per creare un impianto di chiusura completamente nuovo. Confermare con "OK".

3. Definire le proprietà del nuovo impianto di chiusura e assegnare una password sicura. *Sebbene sia sempre possibile apportare modifiche successive, tale operazione risulta particolarmente complessa dopo la prima programmazione dei componenti a causa delle elevate necessità di programmazione.*



4. Creare il nuovo impianto di chiusura facendo clic su "Applica".
5. Fare clic su "OK" per accedere direttamente al nuovo impianto di chiusura.

NOTA

La password dell'impianto di chiusura viene programmata in tutti i componenti SimonsVoss e viene gestita con il software LSM! Senza questa password non è possibile apportare alcuna modifica ai componenti programmati, come mostra anche il software LSM. *Osservare il capitolo Gestione consigliata delle password [▸ 26] per un uso corretto dell'impianto di chiusura.*

Se la password dell'impianto di chiusura viene modificata, tutti i componenti programmati dovranno essere riprogrammati!

5.3.1 Panoramica della generazione di protocolli

	G1	G2
Gestione dei diritti d'accesso:	Chiusure	Chiusura e supporto di identificazione (VN solo supporto di identificazione)
Numero di chiusure:	16.000	64.000

	G1	G2
Numero di transponder:	8.000	64.000
Numero di SLA su un transponder:	3	4 x G2 + 3 x G1
Gruppi di fasce orarie:	5+1	100+1
Accessi memorizzabili in una chiusura:	Cilindro 1.000	Cilindro 3.000 SmartRelè 3.600 (200 come gateway)
Elenco accessi su transponder:	No	1.000 per piano di chiusura G2 (incl. data, ora e ID chiusura)
Procedura di gestione dei gruppi:	Impostabile; il numero viene definito nel gruppo	Nessuna preimpostazione necessaria; diritti e deroghe vengono immessi nel TRA
Transponder sostitutivo:	7 TRA sostitutivi via modalità Overlay	Nessuna preimpostazione necessaria
Capacità di rete:	Sì	Sì
Rete virtuale:	No	Sì, assegnare ID di blocco in VN
Durata di accoppiamento:	5 sec. o 10 sec.	Da 1 sec. a 25 sec.; il tempo di accoppiamento nel TRA può essere raddoppiato singolarmente, max. 25 sec.
Autorizzazione limitata nel tempo:	Sì	Sì
Avviso batteria:	Livello 1; livello 2; modalità magazzino	Livello 1; livello 2; modalità Freeze
Sostituzione delle batterie:	SmartCD	TRA per sostituzione batteria insieme al TRA autorizzato o SmartCD
LSM/LDB:	Tutte le versioni	A partire da LSM3.0
Attivo / Passivo:	Sì / Sì	Sì / Sì

5.3.2 Impianto di chiusura G1

G1 Standard rappresenta la prima generazione di protocolli di SimonsVoss. Questo standard è compatibile con il predecessore del software LSM, ossia il software LDB Locking Database.

NOTA

Utilizzare questo prodotto ormai obsoleto solo per gestire impianti di chiusura di tipo G1 già esistenti. Per impianti di chiusura moderni, si consiglia l'uso di protocolli G2 con componenti G2.

5.3.3 Impianto di chiusura G2

G2 è l'attuale generazione di protocolli per i componenti SimonsVoss. Il protocollo G2 offre numerosi miglioramenti rispetto al precedente G1.

NOTA

Se possibile, utilizzare sempre il protocollo G2. Solo con questo protocollo e i componenti G2 abbinati è possibile realizzare e gestire un impianto di chiusura conforme agli attuali standard tecnici.

5.3.4 Impianto misto G2+G1

I vantaggi di un impianto misto *(per l'utilizzo contemporaneo di componenti G1 e G2 nello stesso impianto di chiusura)* sono accompagnati da piccoli svantaggi *(scarsa visione generale dei componenti utilizzati, nessuna vera esperienza G2)*.

Gli impianti misti sono principalmente di tipo G1. L'unico vantaggio di un impianto misto è dato dalla possibilità di utilizzare contemporaneamente componenti G2. L'impianto misto limita, tuttavia, l'uso dei componenti G2.

In generale, l'uso contemporaneo di componenti G1 obsoleti e componenti G1 aggiornati può essere reso possibile da un impianto misto. Il supporto di componenti obsoleti consente un uso efficiente di componenti già esistenti o utilizzati. Questa funzione è concepita proprio per tali casi particolari. Tuttavia, ciò implica che si debba rinunciare ad alcune caratteristiche utili dei componenti G2.

5.3.5 Modalità Overlay

La modalità Overlay può essere attivata solo nella generazione di protocollo "G1" o "G1+G2".

La modalità Overlay consente una funzione molto comoda nella pur limitata generazione G1, ossia il fatto che i nuovi transponder programmati possono essere utilizzati direttamente senza riprogrammare la chiusura. Questa caratteristica funziona soltanto per un massimo di 7 nuovi transponder creati.

Nella generazione di protocollo G2 si possono eseguire le programmazioni indifferentemente tramite transponder o la chiusura.

Con modalità Overlay attivata, per ogni ID transponder vengono creati altri 7 ID transponder:

Gli ID transponder iniziano dall'ID 64

- Transponder 1 con ID transponder 64: Vengono riservati gli ID transponder 65 - 71 aggiuntivi.
- Transponder 2 con ID transponder 72: Vengono riservati gli ID transponder 73 - 79 aggiuntivi.
- Transponder 3 con ID transponder 80: Vengono riservati gli ID transponder 81 - 87 aggiuntivi.
- (ecc.)

Esempio - transponder sostitutivo: Per il transponder 2 con ID transponder 72 va programmato un transponder aggiuntivo in caso di perdita o furto. A questo transponder sostitutivo viene assegnato l'ID transponder 73 riservato. Se il nuovo transponder sostitutivo programmato viene azionato in una chiusura autorizzata, la chiusura si accoppia e il "vecchio" transponder 2 con ID transponder 72 viene bloccato nella chiusura. La procedura può essere terminata tramite un apposito feedback nel software LSM.

Complessivamente si possono riservare in questo modo fino a 1.000 transponder.

5.4 Backup automatico della banca dati

Creare o modificare lo script batch con un editor di testo per eseguire automaticamente il backup della banca dati. In alternativa, utilizzare il toolbox di installazione LSM.

I comandi e il timeout per Smart.XChange e il terminale del transponder sono opzionali:

- net stop Smart.XChangeService /y o net start Smart.XChangeService /y
- net stop TransTermSvr /y o net start TransTermSvr /y

Sono richiesti solo se si utilizzano questi servizi. Quindi salvare lo script batch con estensione .bat nella cartella SimonsVoss. Questo script batch opera come segue:

1. Interrompe l'accesso dei servizi alla banca dati
2. Rimuove il vecchio backup
3. Copia la banca dati nella directory di backup
4. Riavvia i servizi

Contenuto dello script batch:

```
net stop VNHostSvr /y
timeout /t 30
net stop SVCommNodeSvr /y
timeout /t 30
net stop TransTermSvr /y
timeout /t 30
net stop Smart.XChangeService /y
timeout /t 30
net stop Advantage /y
timeout /t 30
rmdir /s /q C:\SimonsVoss\sv_backup\
md C:\SimonsVoss\sv_backup\
xcopy C:\SimonsVoss\sv_db\*.* C:\SimonsVoss\sv_backup\ /s /c /e
net start Advantage /y
timeout /t 30
net start VNHostSvr /y
timeout /t 30
net start SVCommNodeSvr /y
timeout /t 30
net start TransTermSvr /y
timeout /t 30
net start Smart.XChangeService /y
```

Al posto dei percorsi *C:\SimonsVoss\sv_backup* e *C:\SimonsVoss\sv_db*.** inserire i propri percorsi o i percorsi di rete nella banca dati o nella directory di backup, se necessario.

È possibile utilizzare questo script batch per eseguire backup regolari (idealmente: giornalieri) tramite l'utilità di pianificazione di Windows. Selezionare lo script creato. Non sono necessari ulteriori parametri.

Prestare attenzione a quanto segue:

Impostazioni predefinite per le opzioni di sicurezza

- Esecuzione tramite l'account "System" e non tramite un login di amministratore
- Enable: Eseguire indipendentemente dal login dell'utente

- Enable: Non memorizzare la password
- Enable: Eseguire con i più alti privilegi

Parlate con il vostro dipartimento IT. In qualità di proprietario del sistema, è responsabile della corretta esecuzione dei backup pianificati e dell'archiviazione sicura.

6. Dispositivi di programmazione

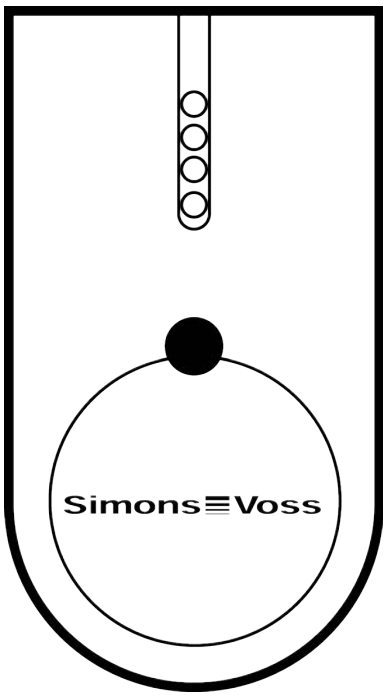
Ad ogni PC con software LSM installato è possibile collegare un dispositivo di programmazione. A tale scopo, il PC deve disporre di un'interfaccia USB. Il dispositivo di programmazione consente di trasferire le impostazioni effettuate e le autorizzazioni ai componenti di chiusura SimonsVoss. Inoltre, è possibile effettuare comodamente la lettura di tutti i componenti. Per i componenti già programmati, è possibile eseguire tale operazione anche tramite LSM Mobile Edition o tramite la rete WaveNet di SimonsVoss.

6.1 Riconoscimento e corretto utilizzo dei dispositivi di programmazione

I dispositivi di programmazione SimonsVoss sono disponibili nelle seguenti versioni:

6.1.1 SmartCD.G2

SmartCD.G2 è il dispositivo di programmazione standard per i componenti attivi e ibridi. Con SmartCD.G2 è possibile programmare tutti i componenti SimonsVoss attivi. Questo dispositivo di programmazione è dotato di un modulo Bluetooth e una batteria. È così possibile utilizzarlo comodamente anche con LSM Mobile in abbinamento ad un PDA/PocketPC. SmartCD.G2 è riconoscibile dal logo SimonsVoss.



NOTA

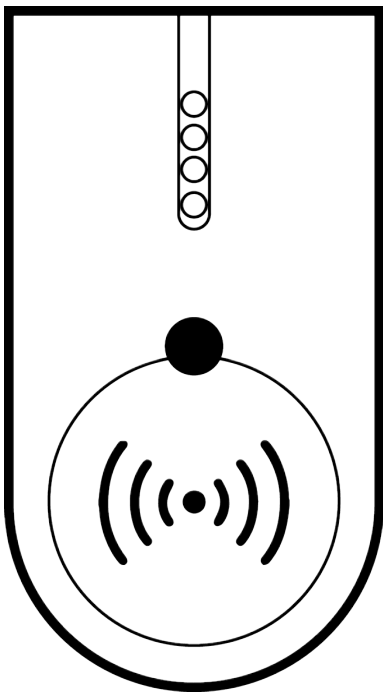
Caricamento iniziale delle batterie incorporate.

Le batterie incorporate sono scariche alla consegna.

- Caricare il dispositivo di programmazione per almeno tre ore prima di utilizzarlo.

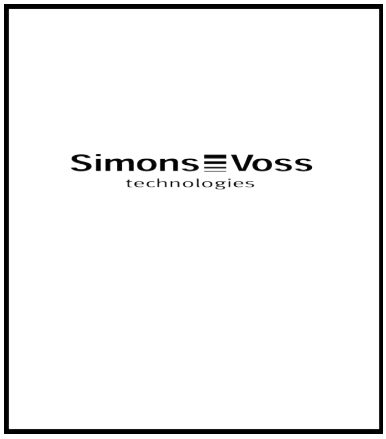
6.1.2 SmartCD.MP

Con il dispositivo di programmazione SmartCD.MP è possibile programmare e leggere i componenti passivi. A differenza del dispositivo attivo SmartCD.G2, SmartCD.MP è riconoscibile dal simbolo del lampo. SmartCD.MP può essere utilizzato solo tramite un collegamento USB diretto.



6.1.3 SmartCD.HF

I tag e le schede passive possono essere programmate e lette anche con il dispositivo di programmazione schede SmartCD.HF.



6.1.4 SmartStick AX

Lo SmartStick AX è il dispositivo di programmazione standard per tutti i componenti con interfaccia BLE. Tutti i componenti SimonsVoss AX possono essere programmati con lo SmartStick AX.

Questo dispositivo di programmazione è collegato tramite un cavo USB e viene alimentato.

Prima della programmazione, i componenti AX da programmare devono essere toccati con lo SmartStick AX per risvegliare l'interfaccia BLE. I componenti AX vengono quindi riconosciuti dallo SmartStick AX per circa 30 secondi e possono essere programmati.

6.2 Distanze di programmazione

Per corrette procedure di programmazione e lettura, è necessario attenersi a determinate distanze fra il dispositivo di programmazione e i componenti.

SmartStick AX

Dopo il risveglio della serratura, SmartStick AX ha un raggio d'azione fino a 300 cm.

SMARTCD.G2

- La distanza fra SMARTCD.G2 e il componente attivo (ad es. cilindri di chiusura o transponder) deve essere di circa 20 cm.
- Fare attenzione che durante la procedura di programmazione o lettura non vi siano altri componenti attivi nelle immediate vicinanze (raggio di circa 1,5 m da SMARTCD.G2).

NOTA

La distanza di programmazione fra SMARTCD.G2 e lo **SmartRelais 1 o 2 o il lettore biometrico** deve essere di 40 cm!

SMARTCD.MP

- Il pomolo della parte elettronica del cilindro di chiusura *(anello nero fra pomolo e alloggiamento del cilindro profilato)* deve essere tenuto direttamente sul simbolo dell'antenna dello SMARTCD.MP.
- Tenere il cilindro di chiusura sul simbolo dell'antenna durante l'intera procedura.
- SMARTCD.MP permette anche di programmare schede appoggiandole direttamente sul dispositivo di programmazione.

SMARTCD.HF

- Posizionare la scheda o la tag a filo sul margine inferiore sinistro di SMARTCD.HF.

6.2.1 Programmazione di chiusure ibride

Le chiusure ibride sono programmate con SmartCD.G2. Per la programmazione deve essere collegato (e installato) contemporaneamente anche uno SmartCD.MP o SmartCD.HF.

Eccezione: lo SmartHandle AX può essere programmato anche con lo SmartCD.MP.

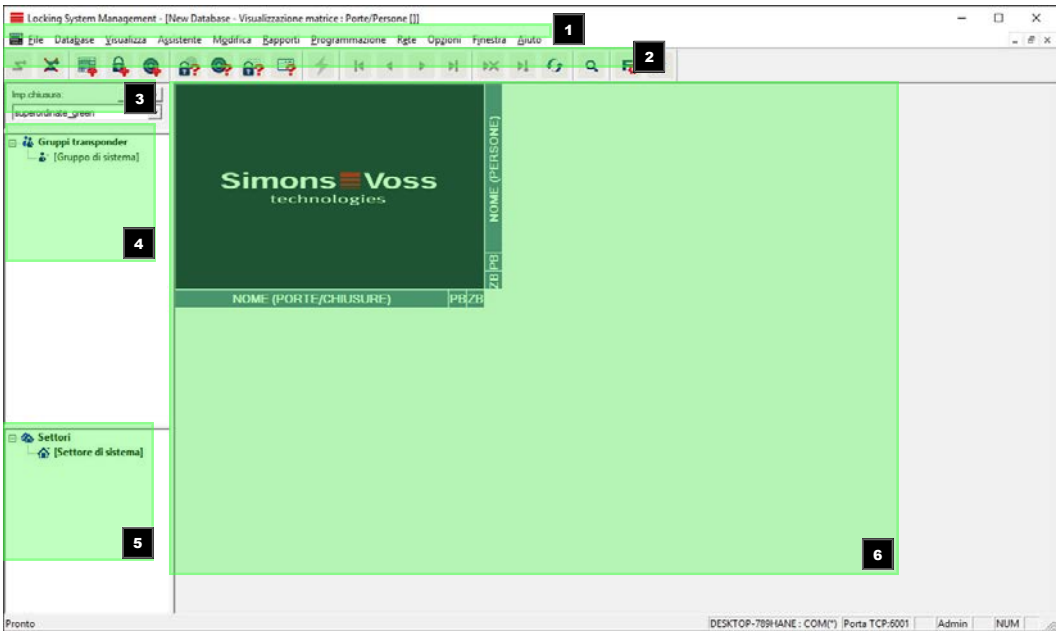
6.3 Controllo del collegamento

Per controllare nel software LSM se il dispositivo di programmazione è stato collegato e installato correttamente, procedere come segue:

1. Nella barra del menu, selezionare la voce "Programmazione".
2. Selezionare il dispositivo di programmazione da controllare, ad es. "Test SmartCD Aktiv" per eseguire il controllo di SMARTCD.G2.
   ↳ Il test verrà avviato immediatamente.

7. Interfaccia utente

L'interfaccia utente del software LSM è suddivisa nelle seguenti aree:



1. **Barra del menu**

   Utilizzare la barra del menu per richiamare le principali funzioni.

2. **Barra multifunzione**

   Nella barra multifunzione si possono richiamare direttamente le funzioni più importanti e utilizzate.

3. **Impianto di chiusura**

   Qui è possibile passare rapidamente da un impianto di chiusura all'altro all'interno del progetto.

4. **Gruppi**

   Per una migliore gestione, riunire gli utenti in gruppi.

5. **Settori**

   Per una migliore gestione, riunire le chiusure in settori.

6. **Matrice**

   La matrice mostra una panoramica dell'impianto di chiusura selezionato.

NOTA

A seconda del software LSM utilizzato, alcune funzioni/voci potrebbero non essere disponibili.

7.1 Barra del menu

7.1.1 File

7.1.1.1 Stampa matrice

Stampa dell'impianto di chiusura selezionato.

7.1.1.2 Pagina intera

Prima della stampa, mostra la matrice come anteprima.

7.1.1.3 Impostazioni di stampa

Definizione delle opzioni di stampa avanzate, ad es. le dimensioni pagina.

7.1.1.4 Modifica password utente

Qui è possibile modificare la password dell'utente al momento connesso.

7.1.1.5 Termina

Logout dal progetto e uscita dal software LSM.

7.1.2 Database

7.1.2.1 Login

Effettuare il login ad un progetto. *Questa funzione è disponibile solo se al momento non si è effettuato il login a nessun progetto.*

7.1.2.2 Logout

Si esce dal progetto in corso facendo clic su "Logout".

7.1.2.3 Setup

Qui è possibile gestire i progetti o i database. Sono disponibili le seguenti possibilità:

- Modifica di un progetto attuale.
- Eliminazione di un progetto attuale.
- Creazione di un nuovo progetto.
- Come preimpostazione è possibile aprire un progetto predefinito che viene caricato automaticamente.

7.1.2.4 Backup

Con questa funzione è possibile creare un backup del database e ripristinare i database salvati come backup.

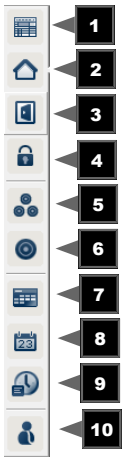
7.1.3 Vista

7.1.3.1 Barra di stato

Mostra e nasconde la barra di stato sul bordo inferiore dello schermo. Per impostazione predefinita, la barra di stato è visualizzata. Nella barra di stato, vengono mostrati, fra l'altro, lo stato attuale dell'impianto di chiusura, il nome del computer e il collegamento del dispositivo di programmazione.

7.1.3.2 Modifica

Tramite *Vista/Modifica* è possibile visualizzare un'altra barra multifunzione, che consente l'accesso rapido alle seguenti funzioni:



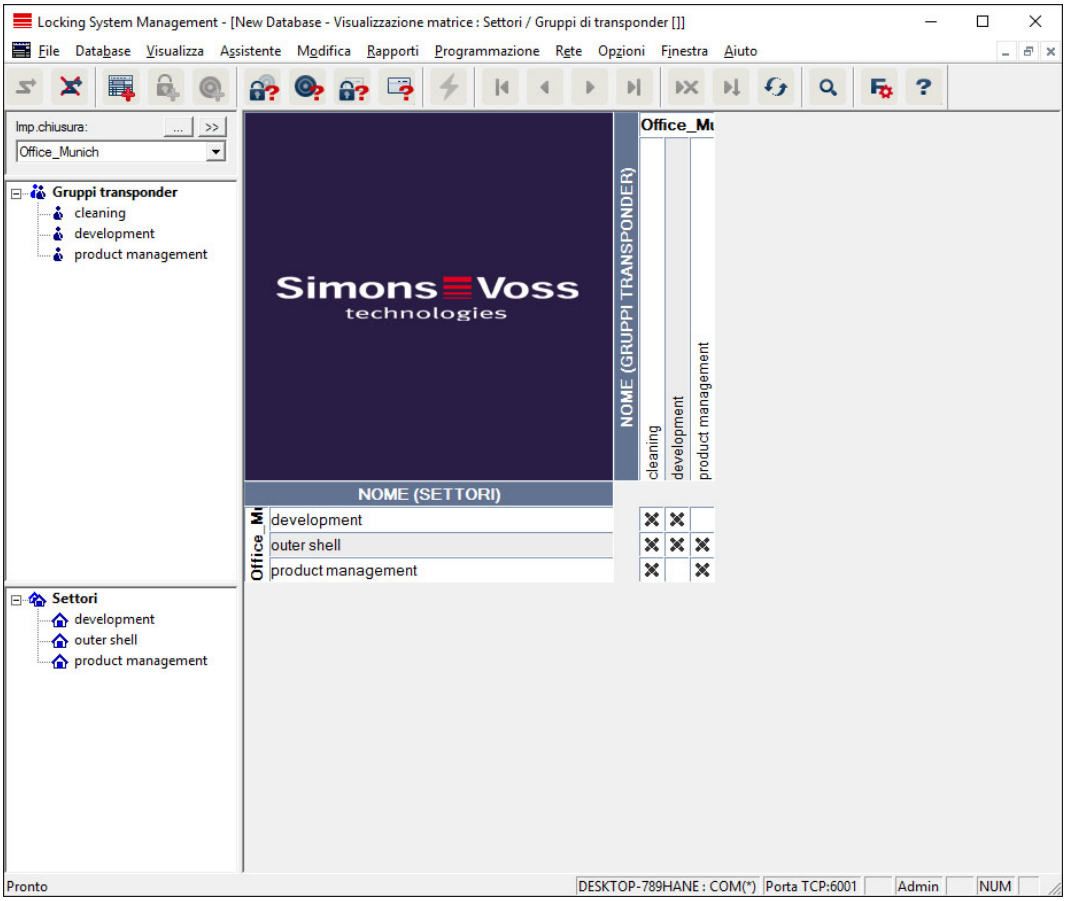
1. **Proprietà dell'impianto di chiusura**
2. **Settore**
3. **Porta**
4. **Chiusura**
5. **Gruppo transponder**
6. **Transponder**
7. **Elenco giorni festivi**
8. **Giorno festivo**
9. **Fasce orarie**
10. **Persona**

7.1.3.3 Aree/Gruppi di transponder

Questa schermata rappresenta una matrice, che visualizza le strutture gerarchiche di personale e ambienti , ma è anche in grado di autorizzare gruppi completi di transponder verso intere aree. In questa matrice diventa così possibile creare facilmente e rapidamente le autorizzazioni basilari. Dovendo assegnare autorizzazioni di altro tipo, come autorizzazioni individuali allargate o ristrette, lo si potrà fare nella schermata Porte/ Persone.

Se si lavora nell'impianto di chiusura con gruppi di transponder e aree, questa opzione offre, tra l'altro, i seguenti vantaggi decisivi:

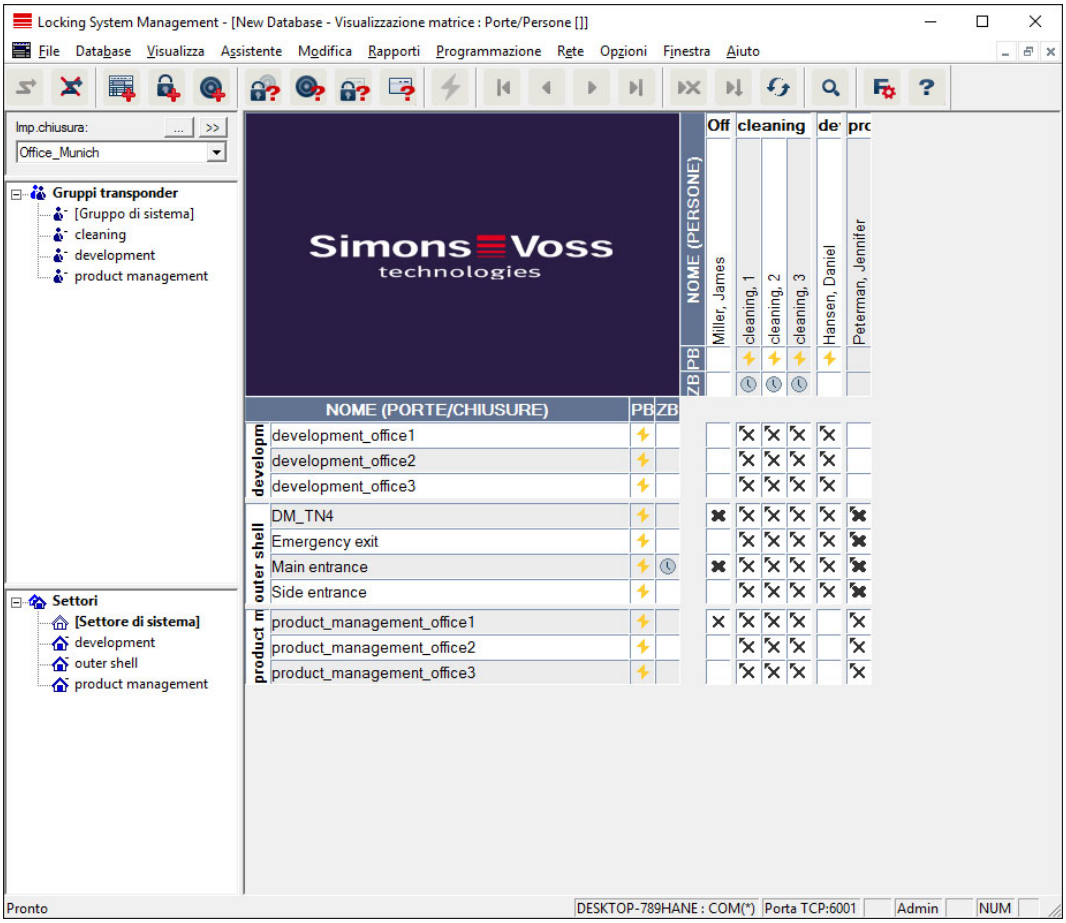
- Riduzione della schermata, perché continuano a essere visualizzati soltanto gruppi di transponder e aree. Ciò permette di semplificare l'individuazione nella matrice.
- Conferimento o ritiro di autorizzazioni di interi gruppi per intere aree.
- I soggetti che vengono aggiunti in un secondo momento a un gruppo, ottengono automaticamente tutti i diritti del gruppo.



7.1.3.4 Porte/Persone

In questa schermata vengono visualizzate le singole autorizzazioni di tutte le persone per singole porte. Ovviamente, la matrice diventa così conseguentemente ricca, però permette di impostare in modo preciso

diritti eccezionali, potendo estendere o anche restringere autorizzazioni di gruppi impostate in precedenza. Questa schermata è pertanto indicata per procedere, ad esempio, a estensioni o restrizioni individuali, dopo aver prima definito la struttura base sotto *Schermata Aree/Gruppi di transponder* .



7.1.3.5 Tutti i settori inferiori/Apertura gruppi

In questa impostazione vista, vengono aperti tutti i settori e gruppi, visualizzando perciò tutte le chiusure anche se in precedenza erano stati nascosti singoli settori.

7.1.3.6 Protocollo

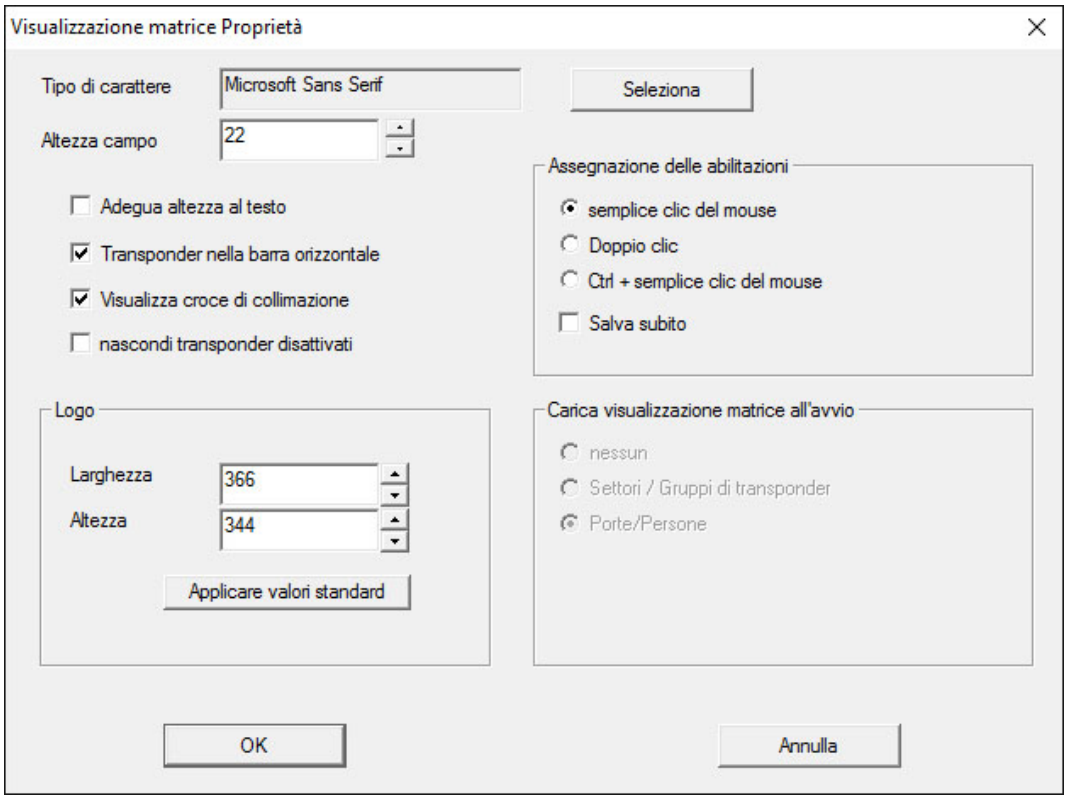
Tramite il protocollo, è possibile visualizzare tutte le azioni eseguite sul database. Allo stesso modo, è possibile tracciare l'utente che ha creato o modificato una determinata chiusura o risalire alle operazioni di login al database.

- I protocolli possono essere limitati a piacimento, ad es. in base ad un intervallo, un utente o un'azione.
- L'elenco può, a sua volta, essere ordinato con un semplice clic a seconda del titolo della colonna , ad es. in base alla data, l'ora o il nome.

7.1.3.7 Impostazioni matrice

Ogni utente ha la possibilità di configurare la propria vista preferita come vista predefinita, che verrà visualizzata dopo il login. Inoltre, qui si possono effettuare diverse impostazioni di base.

Le impostazioni relative alla vista standard possono essere adattate mediante la barra menu alla voce *Vista/Impostazioni vista matrice*.



- **Carattere**

  È possibile scegliere il tipo di carattere preferito.

- **Altezza campo**

  Si può adattare l'altezza dei campi in punti.

- **Adattamento dell'altezza al carattere**

  Adattamento automatico all'altezza del carattere.

- **Transponder nella barra orizzontale**

  Per impostazione predefinita, i transponder vengono visualizzati in orizzontale. Questa impostazione può essere modificata qualora si desideri, ad es., gestire più chiusure come transponder.

- **Visualizza reticolo**

  Visualizza un reticolo che agevola la navigazione.

- **Nascondi transponder disattivati**

  Nasconde i transponder disattivati.

- **Logo**

  Modifica le dimensioni del logo.

- **Assegnazione delle autorizzazioni**

  Negli impianti di chiusura più grandi, sussiste il rischio di fare clic inavvertitamente con il mouse. In questi casi si consiglia di modificare questa impostazione.

  Attivare "Salva subito" se si desidera applicare le modifiche alle autorizzazioni immediatamente dopo un singolo clic del mouse.

7.1.3.8 Colonne supplementari

Nella barra orizzontale e nella barra verticale della matrice possono essere aggiunte ulteriori colonne che forniscono all'utente utili indicazioni aggiuntive. Le impostazioni prescelte valgono solo per la rispettiva vista in cui sono state effettuate. A seconda del tipo di vista, sono disponibili varie informazioni. Anche la sequenza dei dati visualizzati può essere personalizzata e salvata in modo specifico per l'utente (utente Windows).

Per visualizzare le colonne supplementari nella matrice, procedere come segue:

1. Nella barra del menu scegliere *Vista/Colonne supplementari* e quindi la rispettiva vista, ad es. *Transponder/Persone.*
2. Selezionare tutte le informazioni aggiuntive da visualizzare.
3. Ordinare la sequenza con "In alto" o "In basso".
4. Fare clic sul pulsante OK.

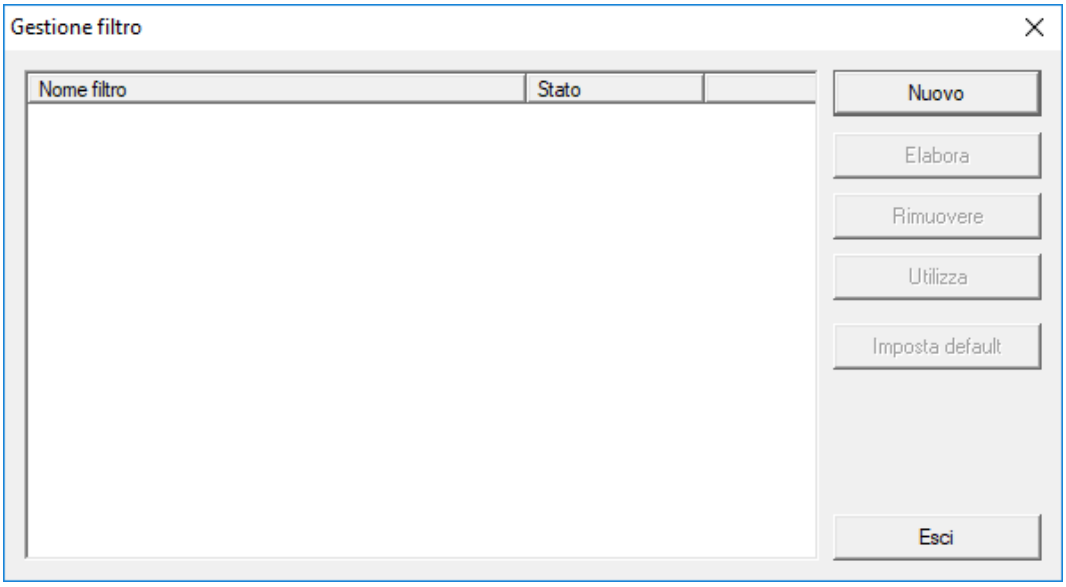
7.1.3.9 Aggiorna

Aggiorna la vista matrice.

Negli impianti di chiusura più grandi o con impostazioni particolari, può essere necessario aggiornare eccezionalmente la matrice in modo manuale.

7.1.3.10 Gestisci filtri

In seguito all'introduzione dei filtri, è diventato ancora più facile amministrare un impianto di chiusura. È possibile selezionare molte opzioni filtro diverse e metterle a disposizione delle persone o dei gruppi di persone più vari. Oltre a ottenere maggiori informazioni tramite la visualizzazione di colonne supplementari, con la funzione filtro le viste risulteranno sempre estremamente chiare e comprensibili.



- **Nuovo**

  Creazione di un nuovo filtro

- **Modifica**

  Modifica del filtro selezionato

- **Rimuovi**

  Rimozione del filtro selezionato

- **Applica**

  Applicazione del filtro selezionato. Se si applica un filtro, il pulsante cambierà, passando alla dicitura "**Disattiva**".

- **Applica standard**

  È il filtro applicato per impostazione predefinita

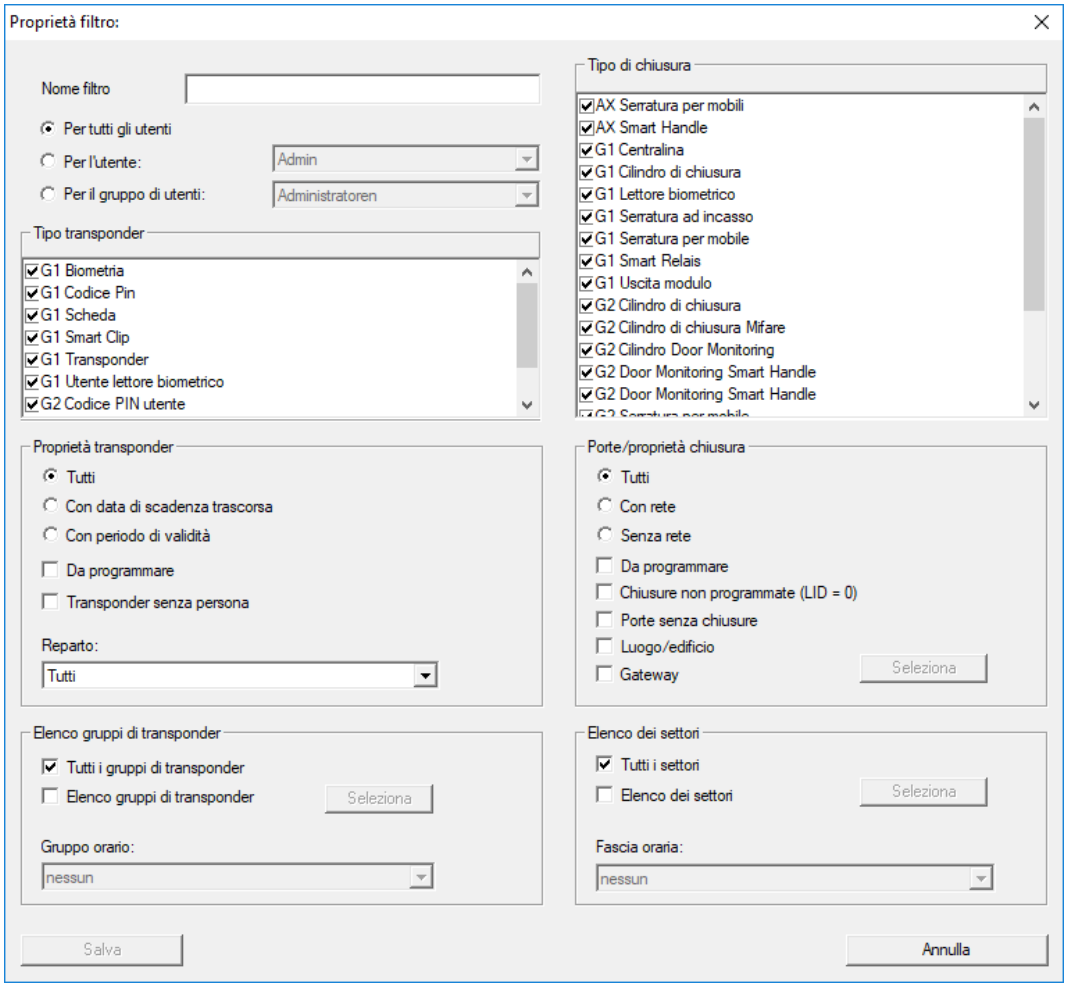
- **Termina**

  Termina la gestione filtri e ritorna alla matrice

NOTA

Il filtro rimane attivo finché non viene disattivato!

Con il pulsante "Nuovo" è possibile creare un nuovo filtro:



- **Nome filtro**

  Attribuire qui un nome significativo al nuovo filtro.

- **Limitazione utenti**

  Utente o gruppo di utenti autorizzati ad utilizzare il filtro.

- **Tipo transponder**

  Tipo di transponder che deve essere visualizzato.

- **Proprietà transponder**

  Limitazioni delle proprietà del transponder (ad es. intervallo di validità o necessità di programmazione).

- **Elenco gruppi transponder**

  Limitazioni dell'appartenenza del transponder (ad es. gruppo transponder "Amministrazione").

- **Tipo di chiusura**

  Tipo di chiusura che deve essere visualizzata.

- **Porte/proprietà impianto di chiusura**

Limitazioni delle proprietà della chiusura (ad es. con rete o necessità di programmazione).

- **Elenco settori**

  Limitazioni dell'appartenenza della chiusura (ad es. settore "Portoni").

7.1.4 Procedure guidate

Le procedure guidate facilitano il primo approccio al software LSM per i nuovi utenti, ma risultano utili anche agli utenti esperti, in quanto consentono di effettuare tutte le impostazioni centralmente un'unica volta.

7.1.4.1 Procedure guidate/Porta

Con queste procedure guidate è possibile creare una nuova porta.

7.1.4.2 Procedura guidata/Persona

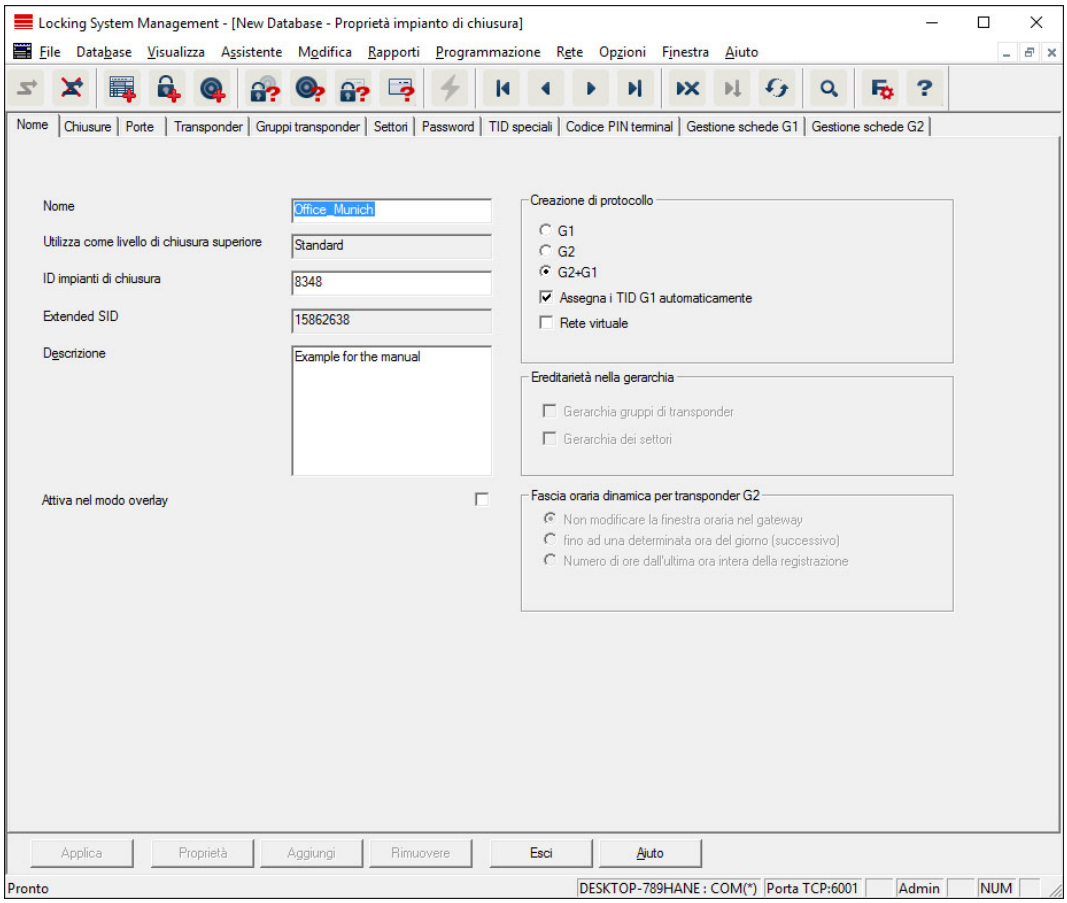
Con queste procedure guidate è possibile creare una nuova persona.

7.1.5 Modifica

7.1.5.1 Proprietà: Impianto di chiusura

Impostazioni dell'impianto di chiusura selezionato al momento.

Nome



- **Nome**

  Denominazione dell'impianto di chiusura

- **Utilizza come livello di chiusura trasversale**

  Definizione del livello di chiusura trasversale

- **ID impianto di chiusura**

  Numero di sistema dell'impianto di chiusura

- **Extended SID**

  Ulteriore caratteristica distintiva dell'impianto di chiusura

- **Descrizione**

  Campo libero per la descrizione dell'impianto di chiusura

- **Funzionamento in modalità Overlay (solo G1)**

  Attiva la modalità Overlay. *Questa funzione deve essere già attivata al momento della creazione dell'impianto di chiusura. Non è possibile modificare tale impostazione successivamente.*

- **Generazione protocollo**

  Selezione della variante di espansione dei componenti hardware

- **Eredità nella gerarchia [LSM BUSINESS]**

  Selezione dei settori di eredità

- **Fascia oraria dinamica per transponder G2**

  Impostazioni orarie avanzate per l'uso con gateway:

  - **Non modificare fascia oraria nel gateway**

    La validità di tutti i transponder G2 che si registrano nel gateway non viene limitata temporalmente.

  - **Fino ad una determinata ora del giorno (successivo)**

    La validità di tutti i transponder G2 che si registrano nel gateway viene limitata temporalmente fino ad una determinata ora.

  - **Numero ore dall'ultima ora piena di registrazione**

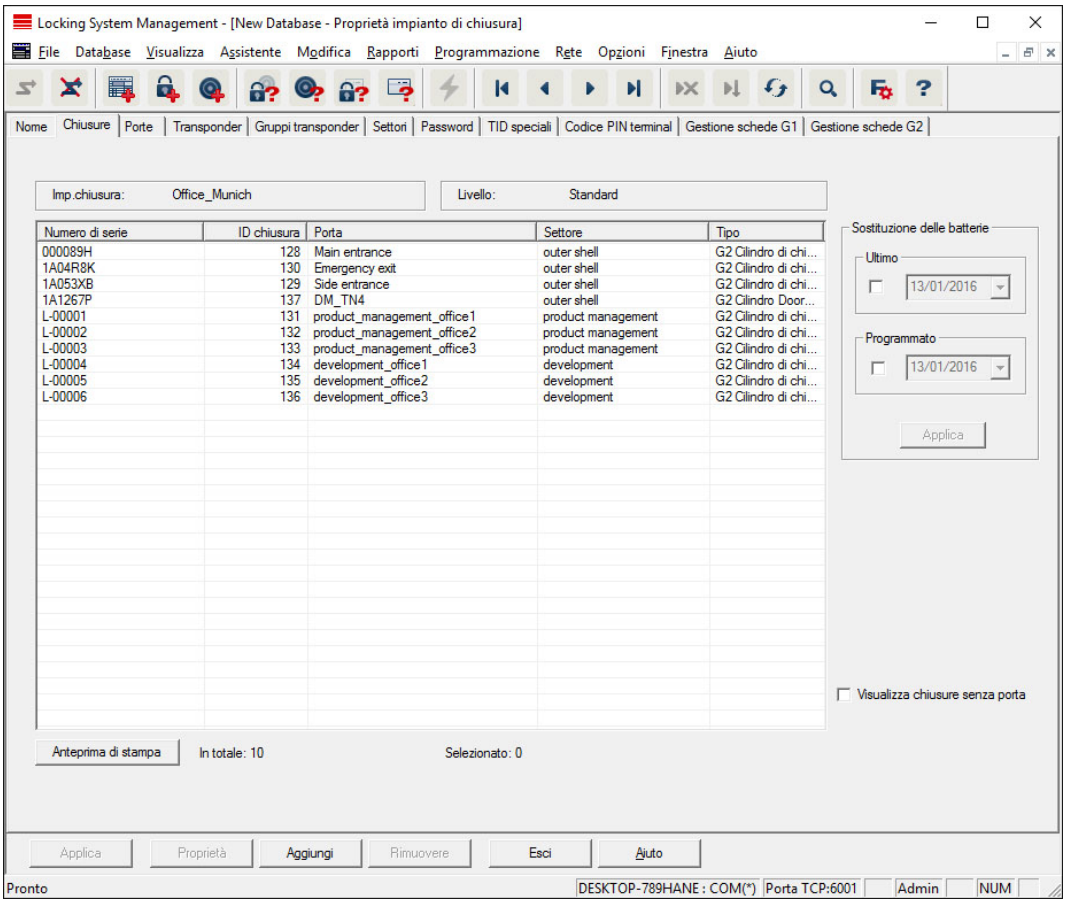
    La validità di tutti i transponder G2 che si registrano nel gateway viene prolungata della durata in ore stabilita.

NOTA

Rete virtuale non necessaria

La configurazione di una rete virtuale non è strettamente necessaria per l’uso di un gateway ai fini della gestione delle fasce orarie.

Chiusure

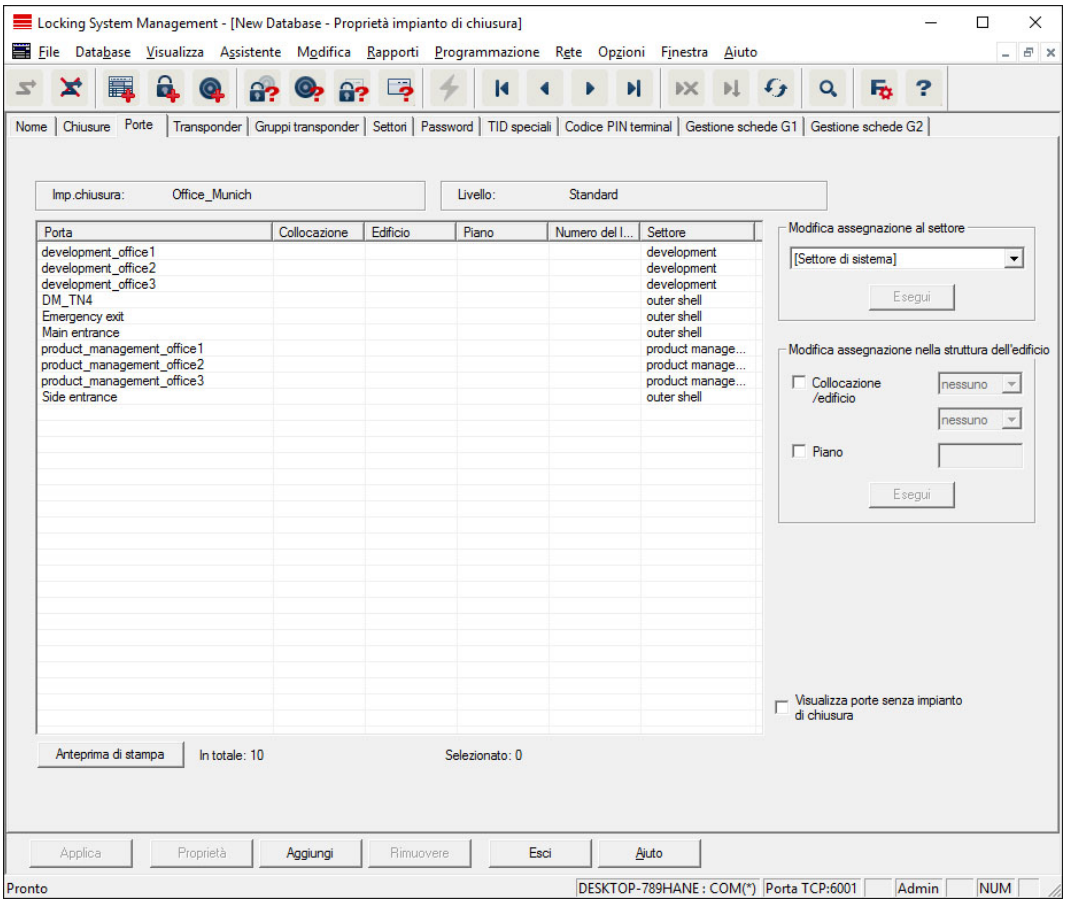


Questa scheda fornisce una panoramica generale delle chiusure utilizzate nell'impianto, che sono visualizzate dettagliatamente all'interno di una tabella.

Si possono inoltre specificare avvisi sul cambio della batteria:

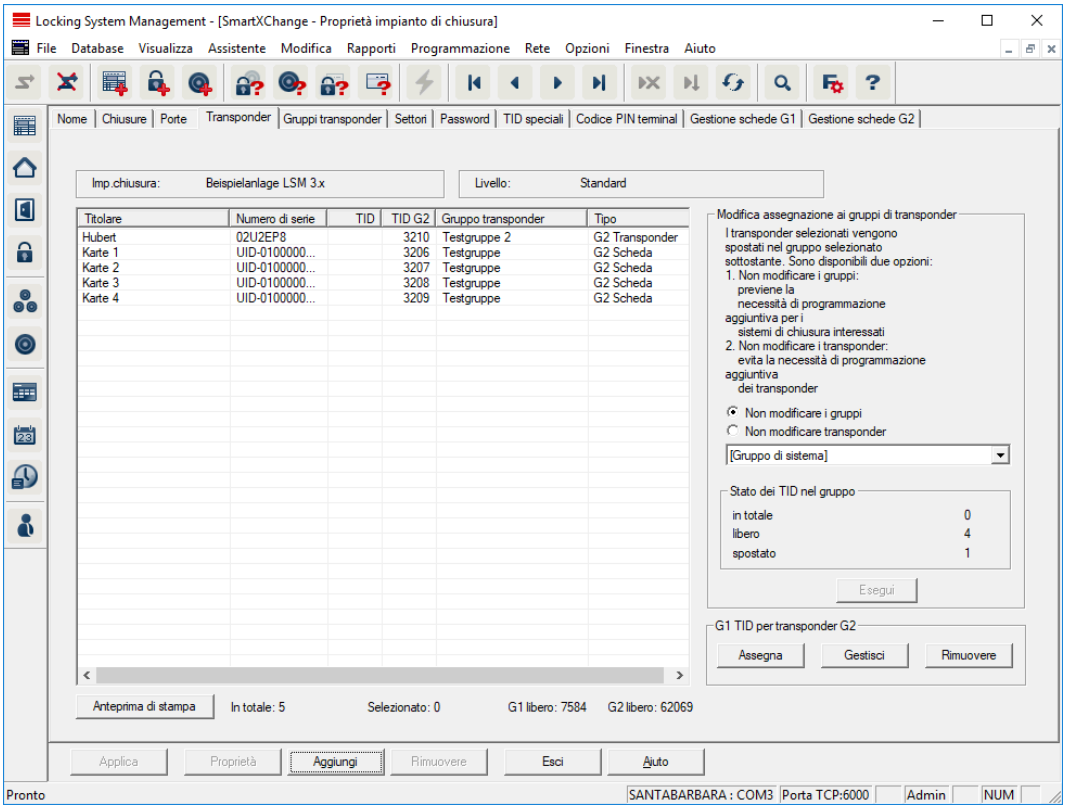
La sostituzione programmata della batteria viene visualizzata nel monitor avvisi e nell'elenco azioni della rispettiva chiusura. Inoltre, esiste la possibilità di inserire il cambio batteria programmato nell'elenco azioni della rispettiva chiusura per più chiusure contemporaneamente. Alla voce "Ultimo" è possibile inserire il cambio batteria eseguito per una o più chiusure.

Porte



Questa scheda mostra la relazione fra i settori assegnati e le porte contenute nell'impianto di chiusura, che sono visualizzate dettagliatamente all'interno di una tabella. È possibile selezionare una o più porte e assegnarla/e ad un settore, luogo o piano specifico. Tenere presente che i settori, luoghi e piani devono essere già stati creati.

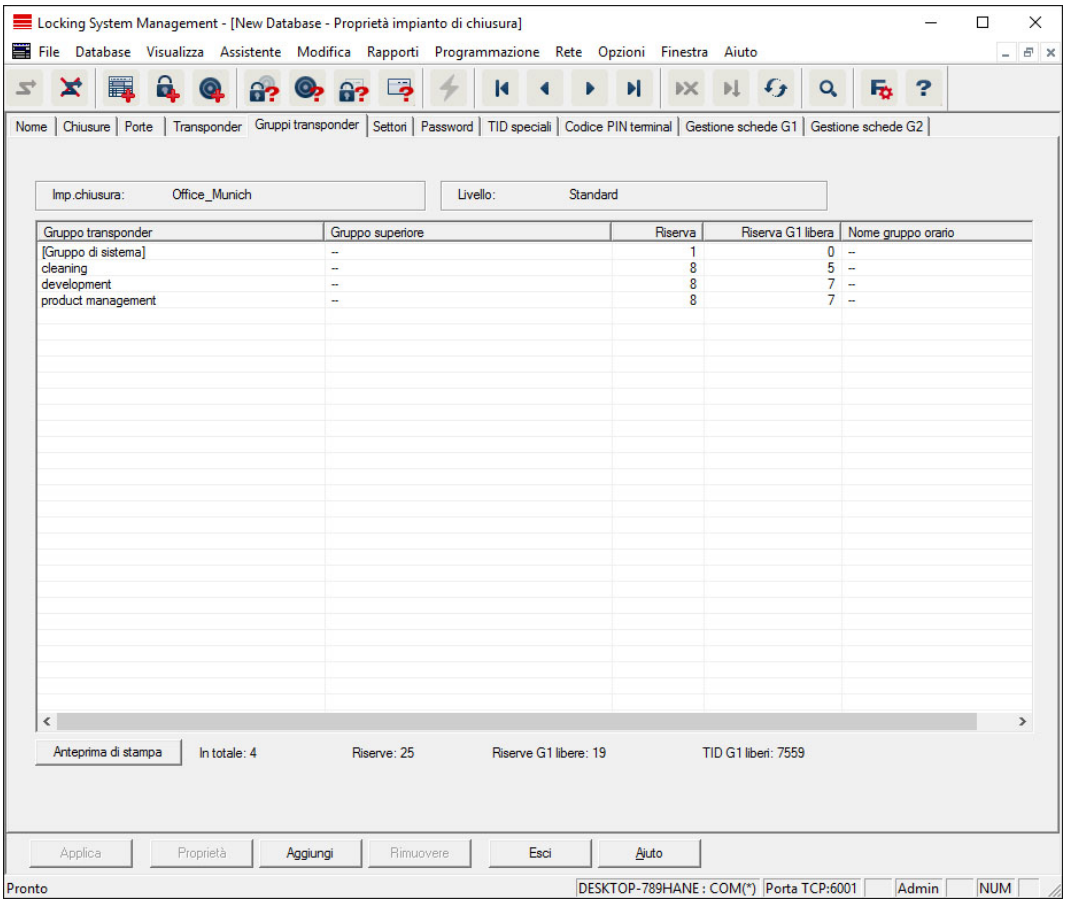
Transponder



Questa scheda fornisce una panoramica generale dei transponder utilizzati nell'impianto, che sono visualizzati dettagliatamente all'interno di una tabella.

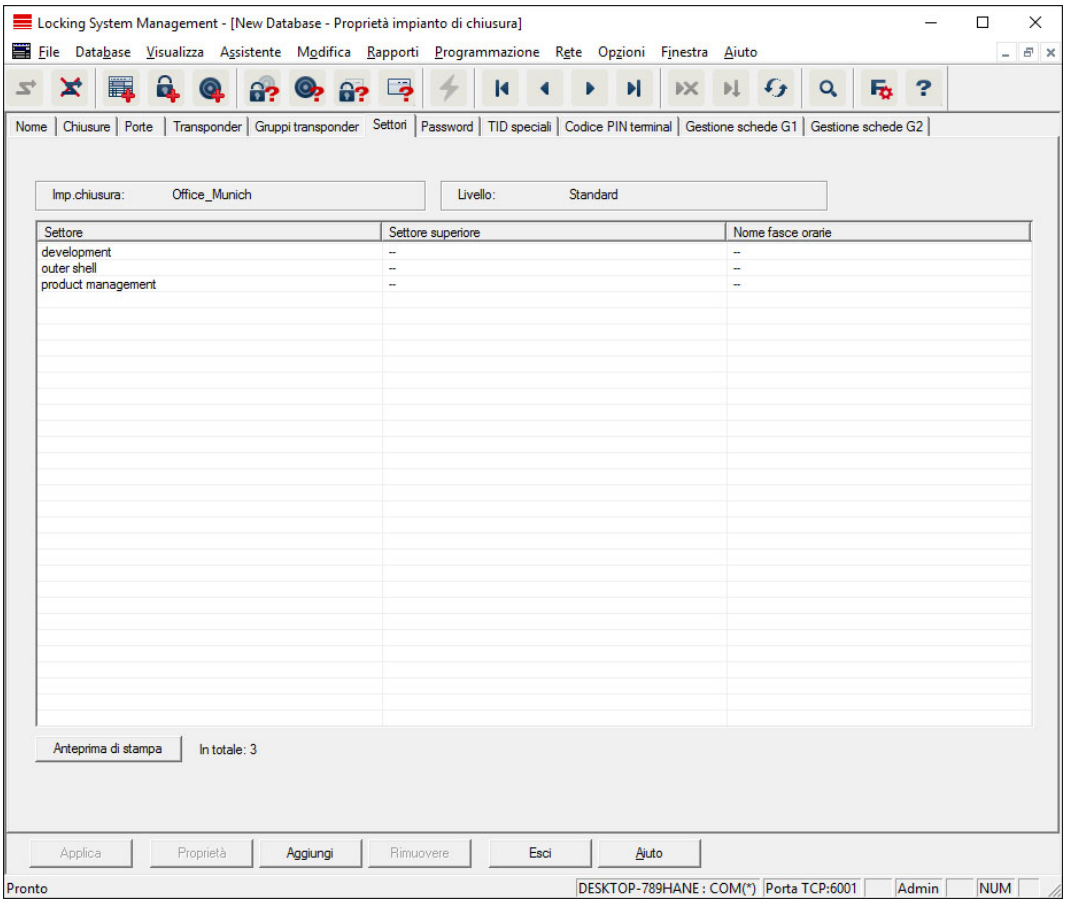
È possibile selezionare uno o più transponder e assegnarli ad un altro gruppo. Tenere presente che i gruppi transponder devono essere già stati creati.

Gruppi di transponder



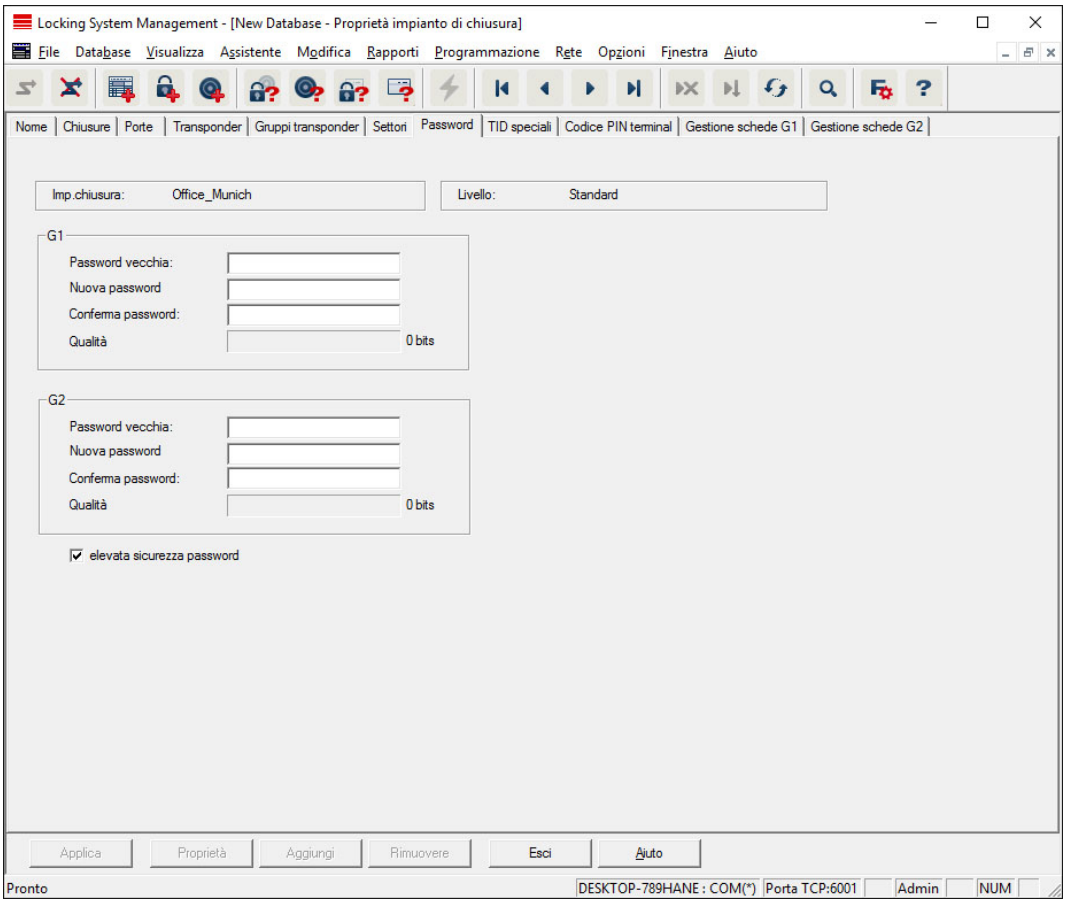
Questa scheda fornisce una panoramica generale dei gruppi di transponder utilizzati nell'impianto, che sono visualizzati dettagliatamente all'interno di una tabella.

Settori



Questa scheda fornisce una panoramica generale dei settori utilizzati nell'impianto, che sono visualizzati dettagliatamente all'interno di una tabella.

Password



Qui è possibile modificare le password dell'impianto di chiusura utilizzate per la programmazione dei componenti.

ATTENZIONE

Perdita della password dell'impianto di chiusura

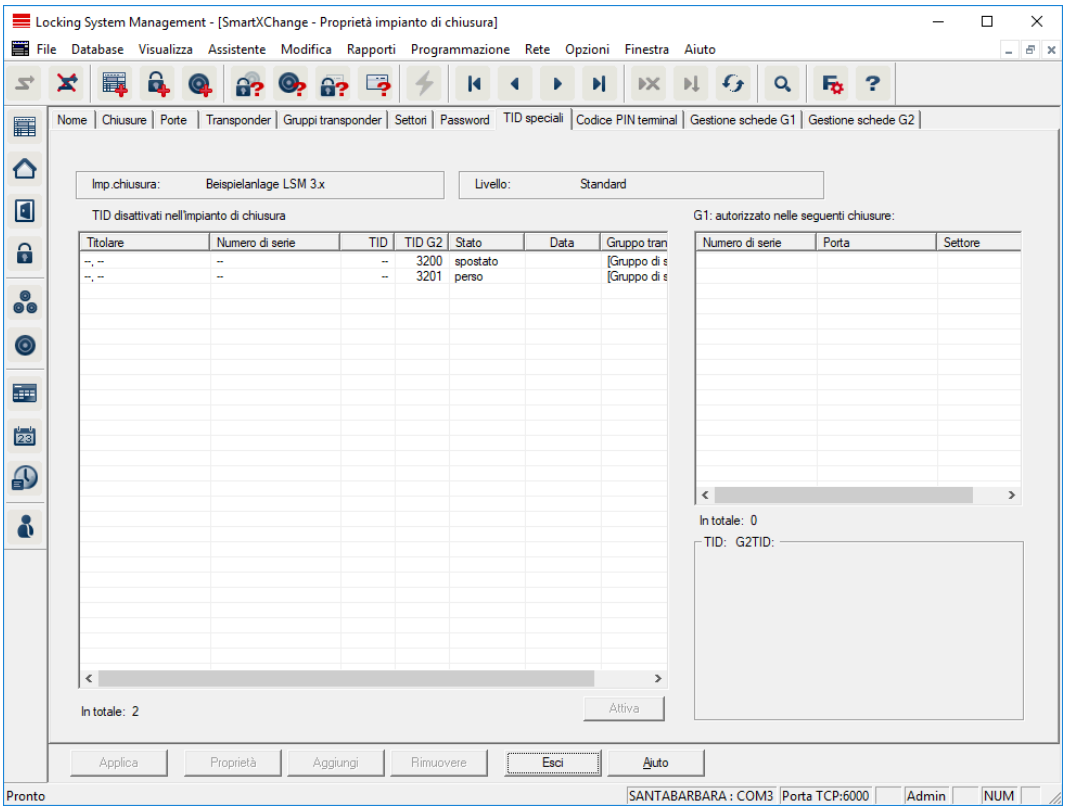
La password dell'impianto di chiusura è la componente centrale del concetto di sicurezza. La perdita della password dell'impianto di chiusura ne limita il funzionamento e costituisce un rischio per la sicurezza.

1. Conservare la password dell'impianto di chiusura in un luogo sicuro (ad es. in una cassaforte)!
2. Rendere sempre visibile la password dell'impianto di chiusura alle persone autorizzate!

NOTA

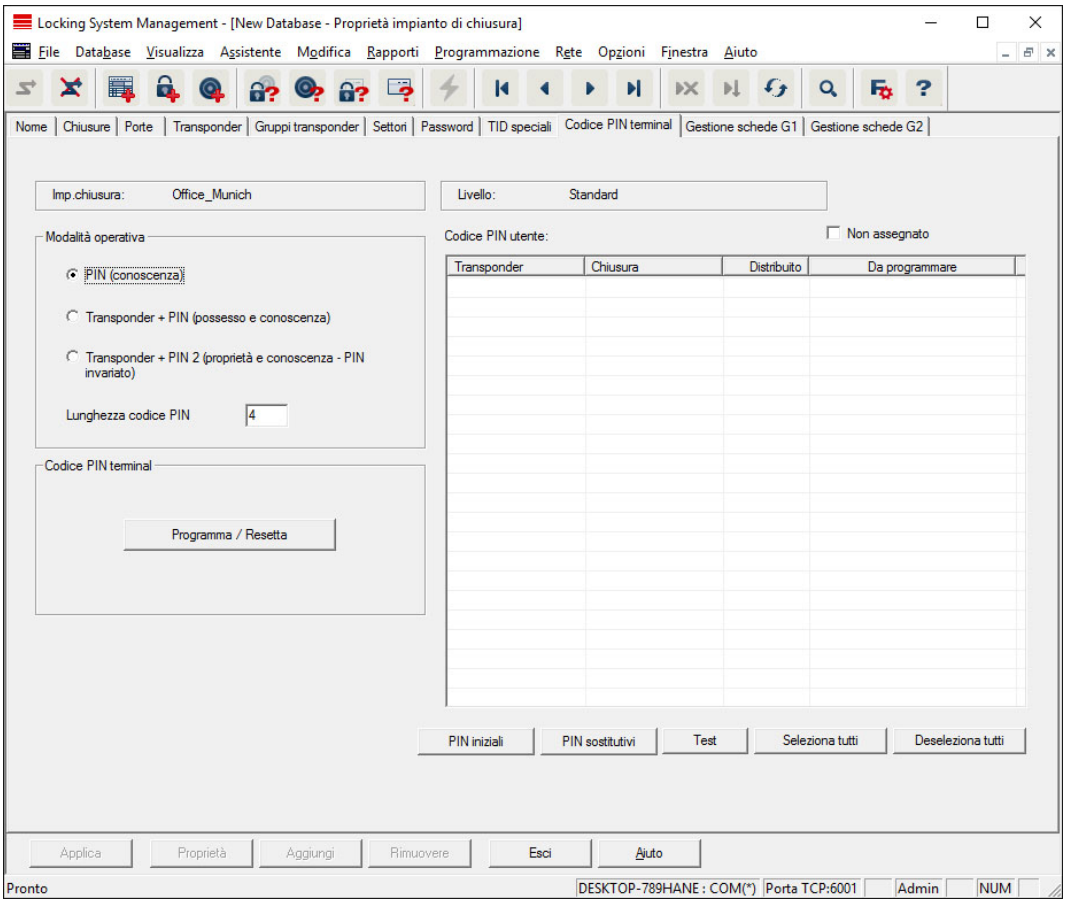
I componenti con password dell'impianto di chiusura diverse non possono comunicare fra di loro!

TID speciali



- La tabella grande a sinistra mostra una panoramica generale di seguenti transponder:
  - Disattivati
  - Rimossi
  - Smarriti
  - Non restituti
  - Temporaneo bloccata
- La tabella piccola a destra mostra tutte le chiusure in cui i transponder selezionati nella tabella di sinistra sono autorizzati.
- Nell'area sotto la tabella piccola di destra sono visualizzate informazioni e osservazioni sul transponder disattivato.
- Con il pulsante "Attiva" è possibile riattivare un transponder selezionato *(a seconda dello stato impostato). In questo caso, nel protocollo G2 al transponder viene assegnato un nuovo TID, che può generare necessità di programmazione per le chiusure autorizzate.*

PIN-Code Terminal



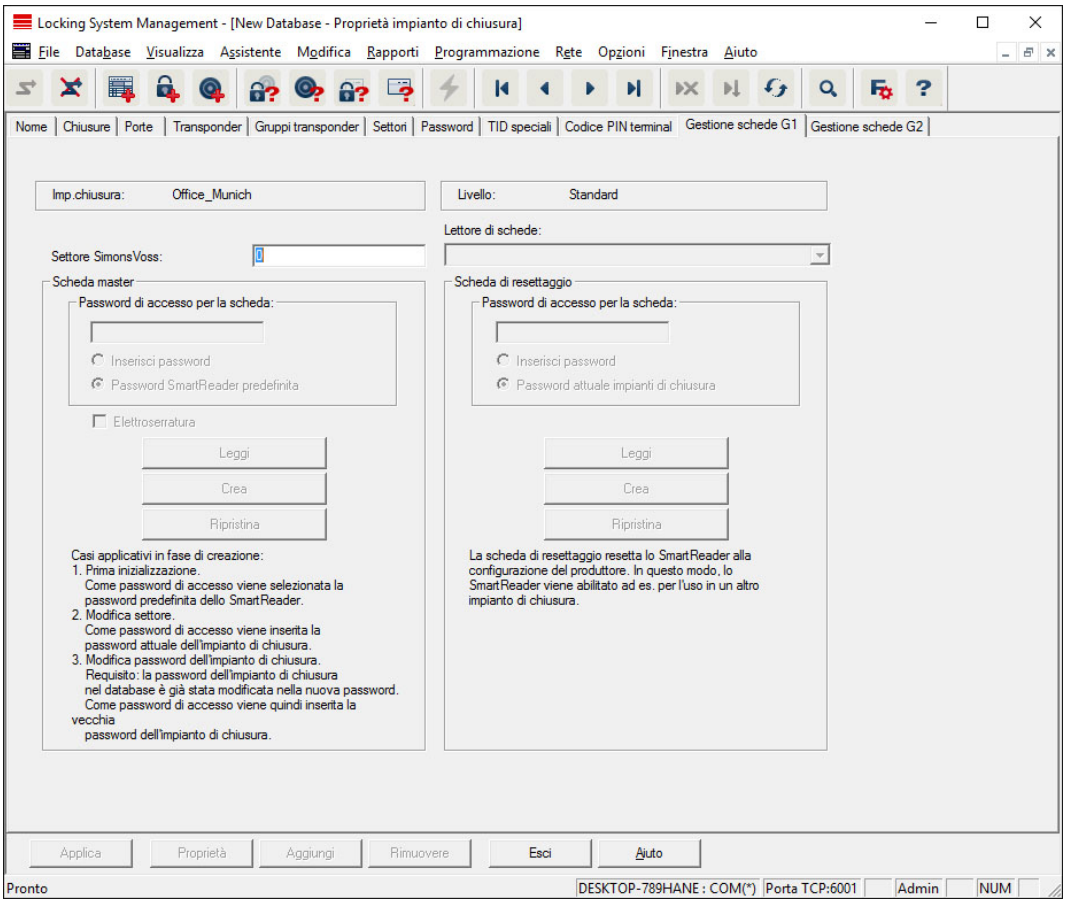
In questa scheda è possibile creare terminali Pin-Code ed eseguire configurazioni avanzate.

Per la configurazione del Pin-Code Terminal osservare il "Manuale Pin-Code Terminal" reperibile alla homepage:

https://www.simons-voss.com/it/documenti.html

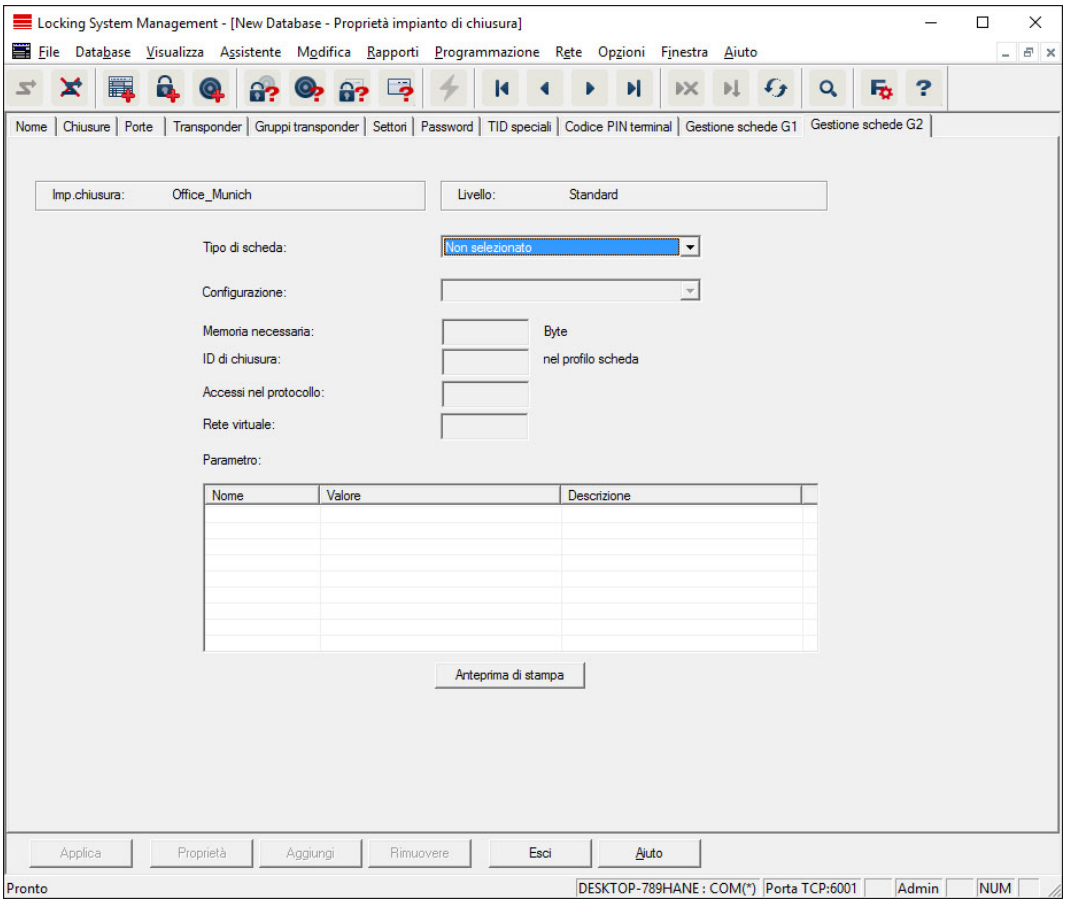
Vedere *Supporto e ulteriori informazioni [▸ 259]*.

Gestione schede G1



Specificare qui le proprietà e le impostazioni avanzate delle schede G1 (Vedi *Gestione schede [▸ 167]*).

Gestione schede G2



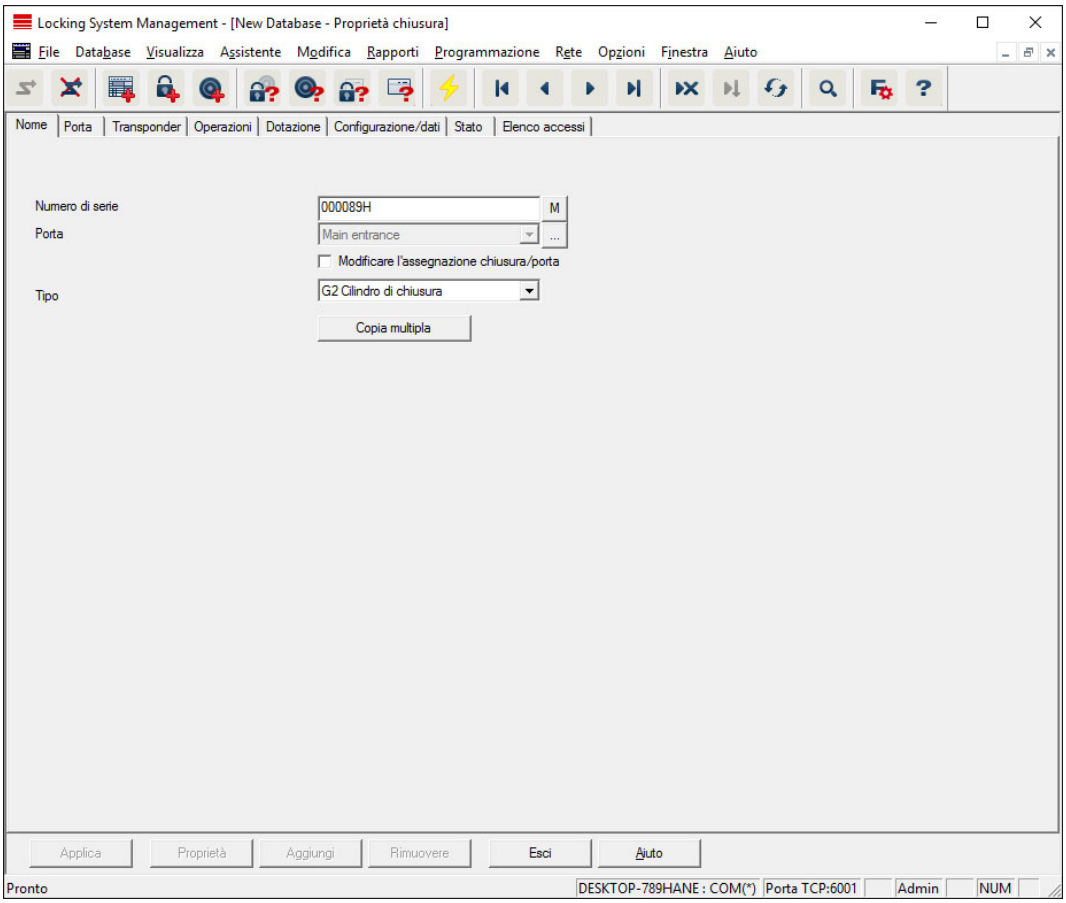
Specificare qui le proprietà e le impostazioni avanzate delle schede G2 (Vedi *Gestione schede [▸ 167]*).

7.1.5.2 Proprietà: Chiusura

Mostra e modifica le proprietà della chiusura al momento selezionata.

Facendo doppio clic su una chiusura si aprono direttamente le proprietà della rispettiva chiusura!

Nome



- **Numero di serie**

  Mostra il numero di serie della chiusura. Il pulsante "..." mostra le proprietà della porta.

- **Porta**

  Con la casella di controllo "Modifica assegnazione della chiusura/porta" è possibile modificare la porta assegnata alla chiusura. Il pulsante "M" mostra la chiusura nella matrice.

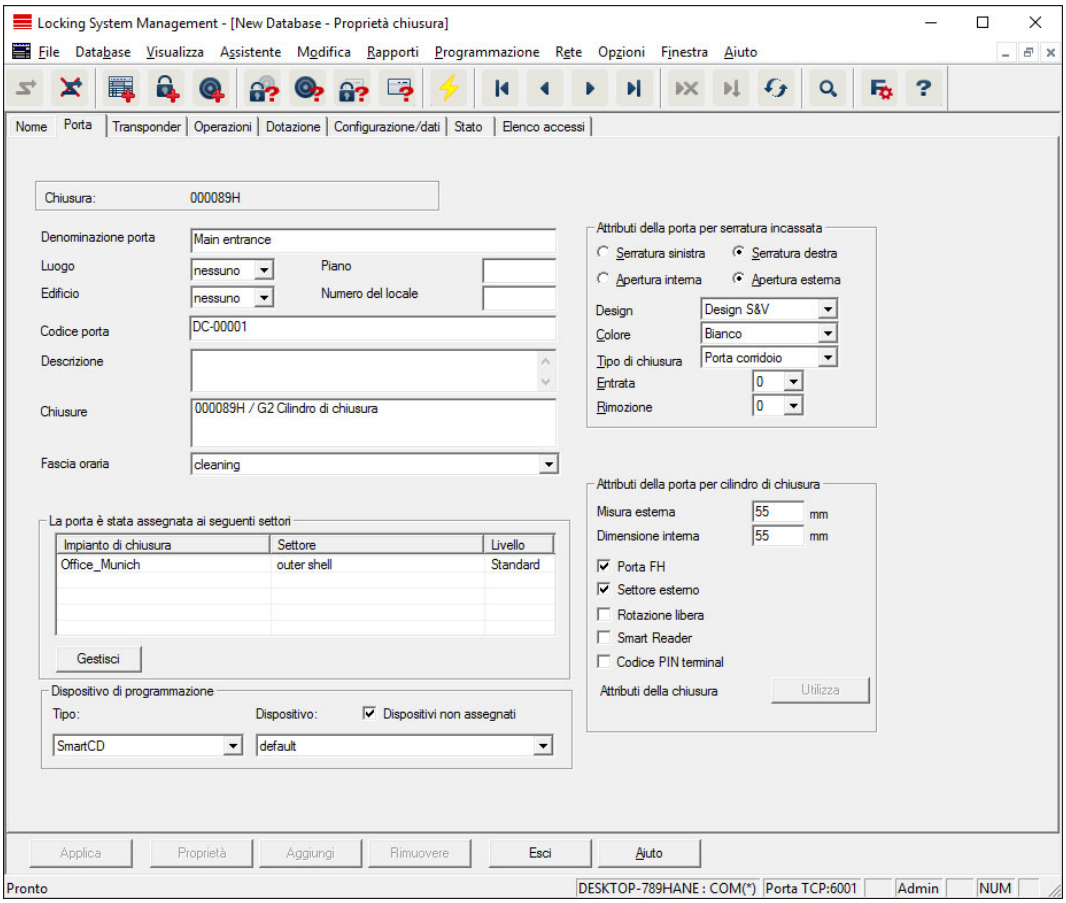
- **Tipo**

  Tipo di chiusura.

- **Copia multipla**

  Crea un numero desiderato di copie della chiusura aventi le medesime proprietà. Oltre al nome della chiusura viene aggiunto un numero progressivo.

Porta



- **Denominazione porta**

  Nome della porta.

- **Luogo**

  Luogo in cui si trova la porta (i luoghi devono essere stati precedentemente creati).

- **Edificio**

  Edificio in cui si trova la porta (gli edifici essere stati precedentemente creati).

- **Piano**

  Piano in cui si trova la porta.

- **Numero di stanza**

  Numero di stanza della porta.

- **Codice porta**

  Denominazione interna della porta.

- **Descrizione**

  Campo libero per la descrizione della porta.

- **Chiusure**

  Chiusure assegnate alla porta.

- **Fascia oraria**

  Fascia oraria della porta.

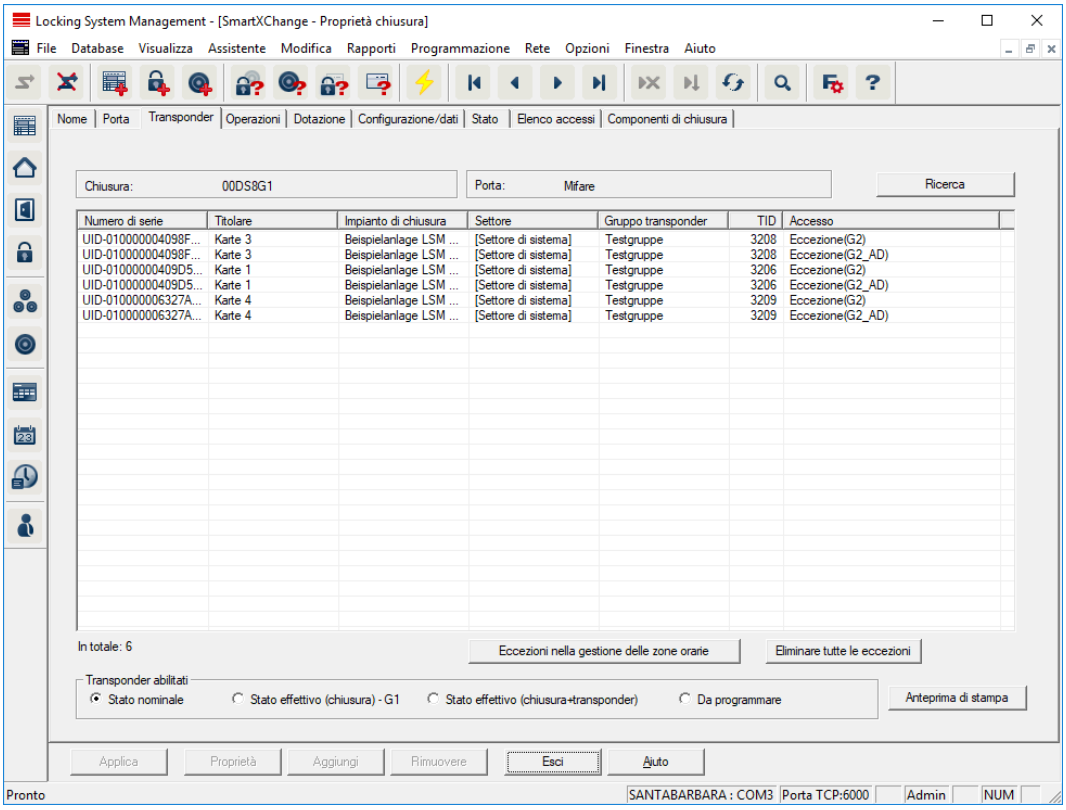
- **Dispositivo di programmazione**

  Scelta di un determinato dispositivo di programmazione (necessario soprattutto con LON e WaveNet. Le chiusure alle quali è assegnato LON o WaveNet possono essere programmate anche via radio "online" senza dispositivo di programmazione).

- **Attributi porta**

  Informazioni sulla serratura ad incasso e la chiusura. All'occorrenza, è immediatamente visibile quali componenti di ricambio servono.

Transponder



- **Tabella**

  Mostra in un elenco dettagliato tutti i transponder autorizzati nella chiusura.

- **Transponder autorizzati**

  La tabella può essere filtrata mediante i singoli pulsanti di opzione.

  - **Stato nominale**

Mostra lo stato desiderato.

- **Stato reale (...)**

  Mostra lo stato al momento programmato.

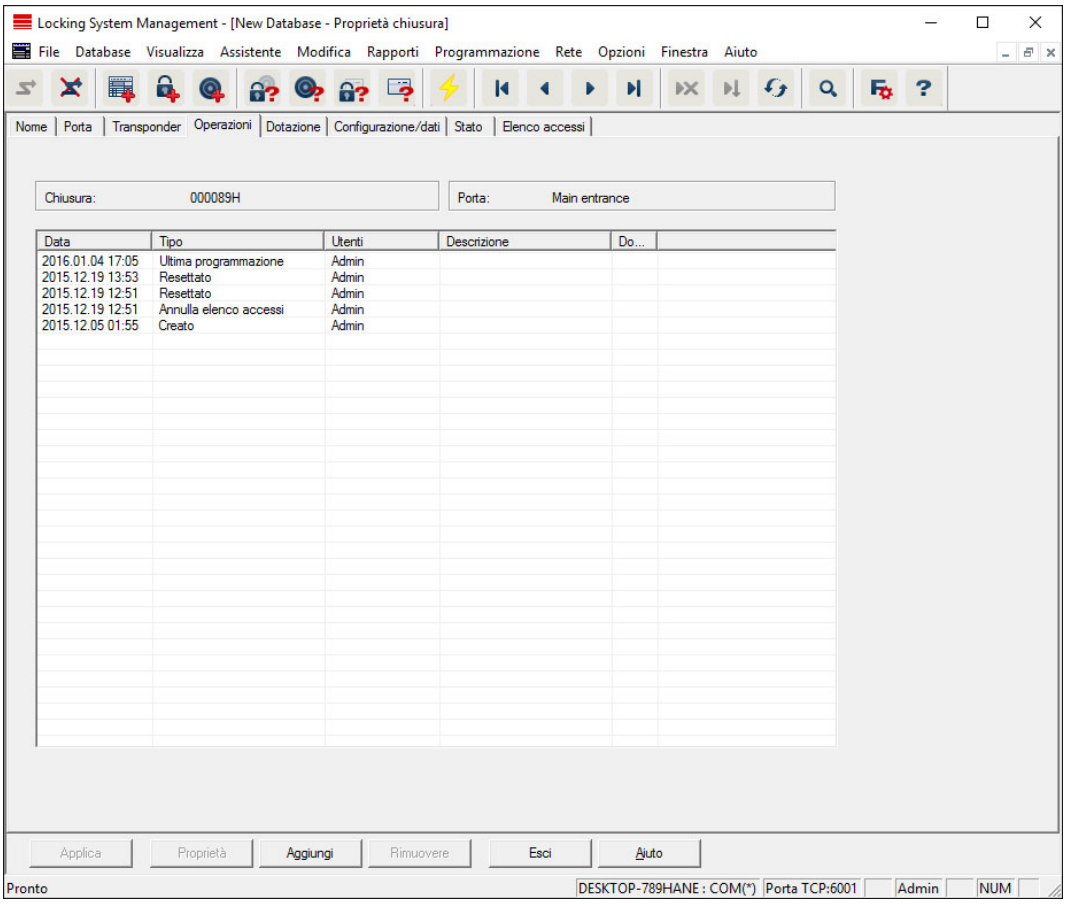
- **Necessità di programmazione**

  Visualizza tutti i transponder con necessità di programmazione.

- Pulsante supplementare "**Eccezioni nella gestione fasce orarie**":

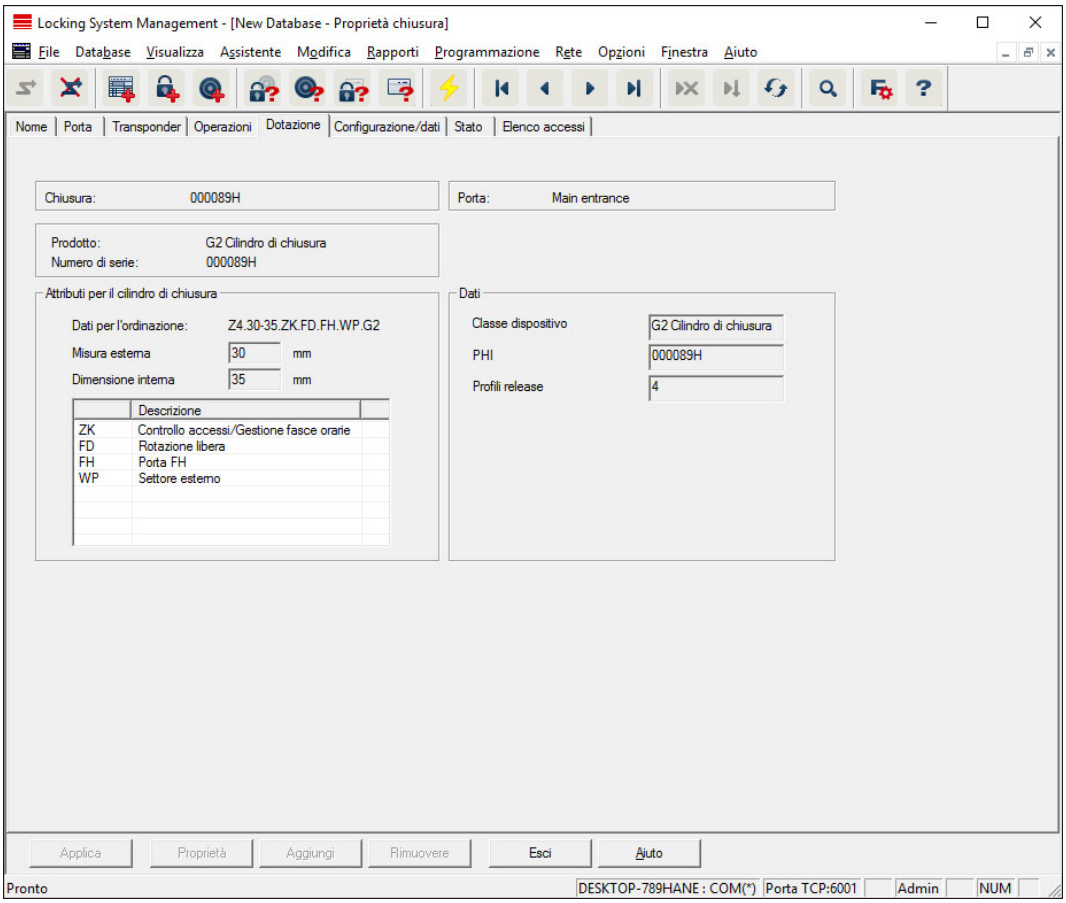
  Qui è possibile visualizzare le eccezioni nella gestione fasce orarie per il transponder.

Azioni



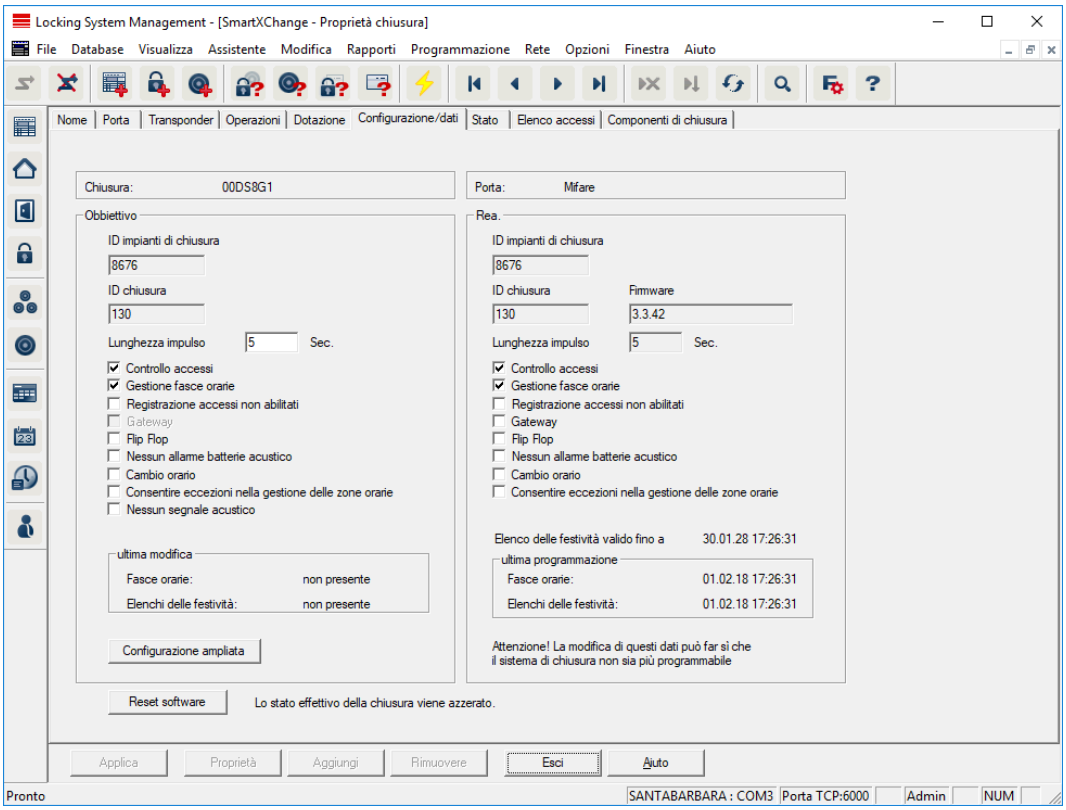
Questa tabella indica le azioni (ad es. programmazione, modifica delle autorizzazioni ecc.) eseguite nella chiusura. Alcune azioni, quali ad es. "Ultimo cambio batteria" possono essere aggiunte anche manualmente con il pulsante "Aggiungi".

Dotazione



Questa scheda mostra le esatte opzioni hardware della chiusura registrate automaticamente nel corso della prima programmazione.

Configurazione/Dati



Questa scheda è suddivisa in due parti:

- La parte a sinistra mostra lo stato nominale della chiusura, ossia lo stato configurato nel software LSM e pertanto desiderato.
- Nella parte destra è visualizzato lo stato reale della chiusura e cioè l'ultimo stato programmato.

A seconda del tipo di chiusura si possono attivare le seguenti funzioni:

- **Controllo accessi**

  Possibilità di registrare gli accessi. *Questa funzione è attiva solo nei componenti dotati della funzione ZK.*

  Chiarire, ad es. con il Consiglio aziendale o il responsabile della protezione dati, se l'uso di questa opzione è consentito nella specifica realtà.

- **Gestione fasce orarie**

  Possibilità di gestione temporizzata degli accessi per i transponder.

- **Registrazione dei tentativi di accesso non autorizzati**

  Le registrazioni transponder rifiutate vengono memorizzate nella chiusura. Ciò vale solo per i supporti di identificazione appartenenti allo stesso impianto di chiusura.

- **Gateway**

Opzione per l'uso di gateway. *Disponibile solo nello SmartRelè.*

- **Flip Flop**

  Dopo un'attivazione del transponder, la chiusura si accoppia e rimane accoppiata fino alla successiva attivazione del transponder.

- **Nessun avviso batteria acustico**

  Attivando questa funzione, non vengono emessi gli avvisi acustici sullo stato della batteria nei componenti.

- **Commutazione temporizzata**

  La chiusura modifica automaticamente il proprio stato al momento stabilito, come impostato alla voce "Configurazione estesa". *Solo nelle versioni ZK.*

- **Eliminazione delle conferme di programmazione acustiche**

  Durante la programmazione, la chiusura non conferma la procedura emettendo segnali acustici.

- **Interfaccia scheda**

  Abbinamento dell'interfaccia scheda alla chiusura.

- **Configurazione estesa**

  Qui si specificano le configurazioni avanzate, come ad es. la commutazione temporizzata della chiusura.

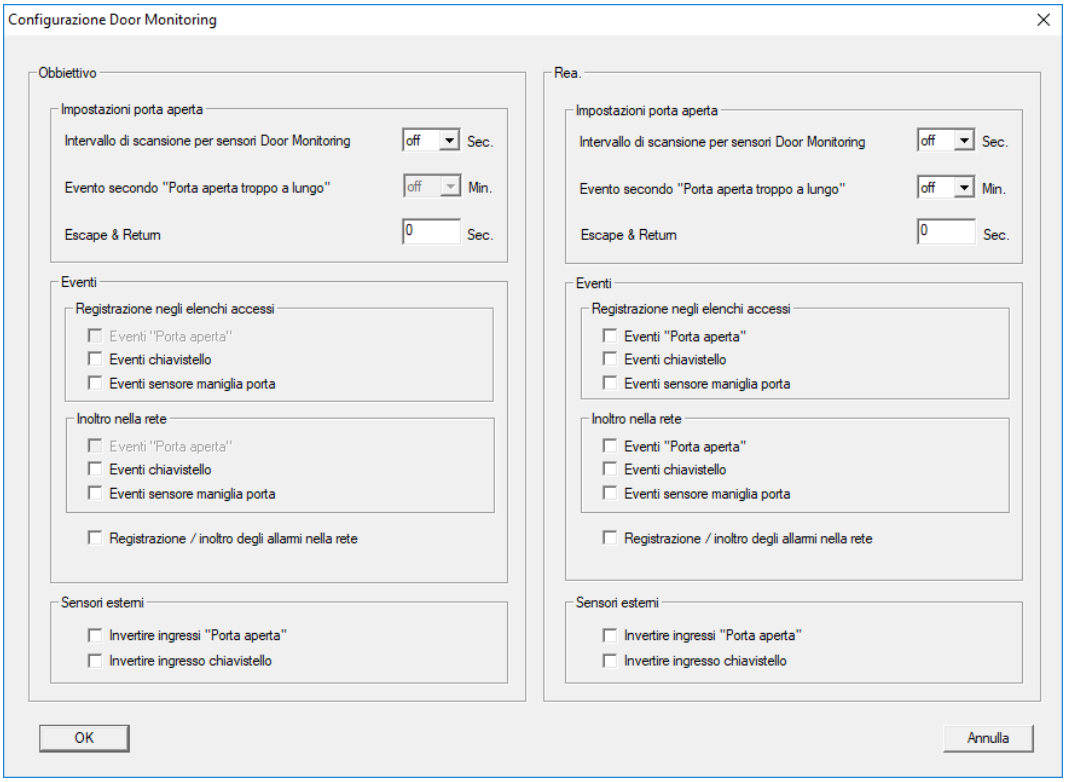
- **Reset software**

  Pulsante per l'azzeramento dello stato reale nel software LSM. Quest'operazione viene contata e il risultato visualizzato accanto a sinistra.

DoorMonitoring SmartHandle

Con il pulsante "Configurazione Monitoring" nella scheda "Configurazione/ Dati" della chiusura è possibile configurare le funzioni DoorMonitoring della SmartHandle (vedi anche *Messa in funzione del chiusure DoorMonitoring [▸ 199]*).

Questa funzione è disponibile solo se la SmartHandle possiede la proprietà DM e se è stata creata nel software LSM direttamente come "SmartHandle G2 DoorMonitoring"!



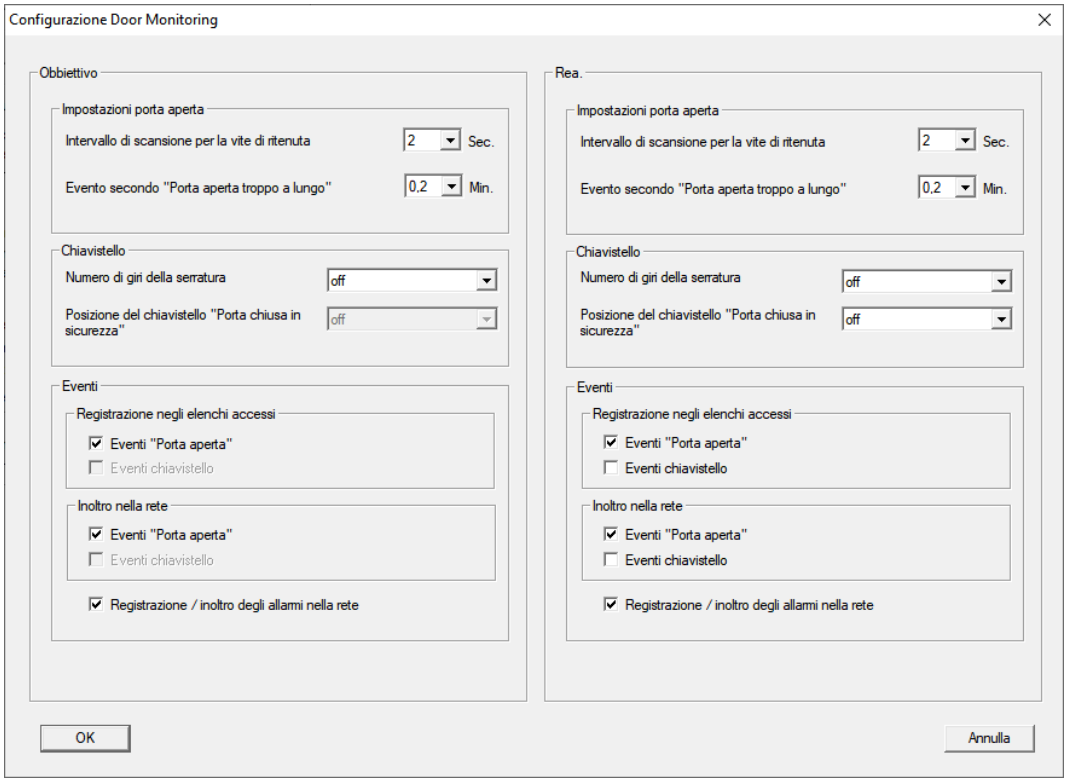
Effettuare le modifiche desiderate nella '"parte nominale" a sinistra.

- **Escape & Return:** Prolunga il tempo di accoppiamento della SmartHandle dopo che la porta è stata rilevata di nuovo come chiusa.

Cilindri di chiusura DoorMonitoring

Con il pulsante "Configurazione Monitoring" nella scheda "Configurazione/ Dati" della chiusura è possibile configurare le funzioni DoorMonitoring del cilindro di chiusura (vedi anche *Messa in funzione del chiusure DoorMonitoring [▸ 199]*).

Questa funzione è disponibile solo se il cilindro di chiusura possiede la proprietà DM e se è stato creato nel software LSM direttamente come "Cilindro G2 Door Monitoring"!

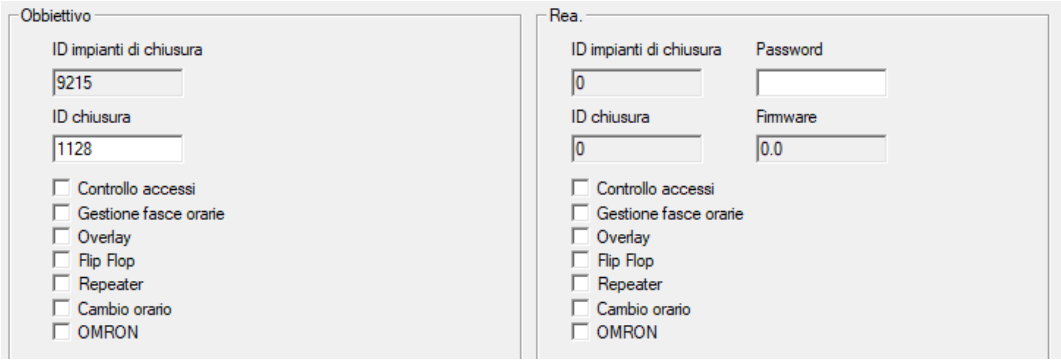


Effettuare le modifiche desiderate nella '"parte nominale" a sinistra.

SmartRelè (G1): SREL, SREL.ADV, SREL.W

Questa scheda ([Configurazione/dati]) è suddivisa in due parti:

- La parte a sinistra mostra lo stato nominale ("Rea.") della chiusura, ossia lo stato configurato nel software LSM e pertanto desiderato.
- Nella parte destra è visualizzato lo stato reale della chiusura ("Obbiettivo") e cioè l'ultimo stato programmato.

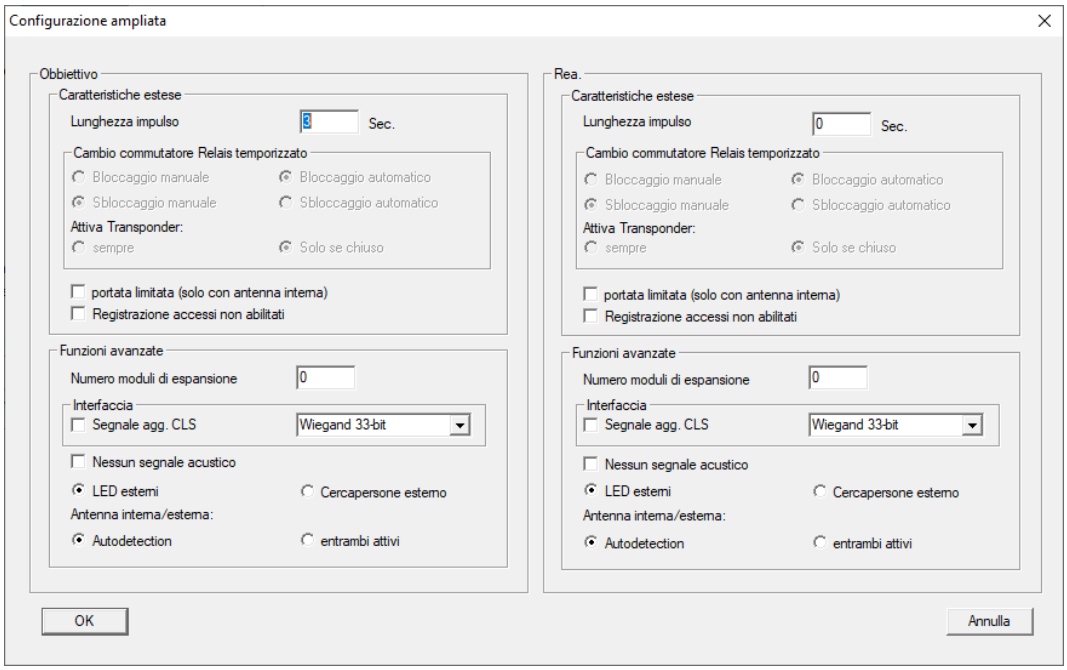


A seconda del tipo di chiusura si possono attivare le seguenti proprietà:

☑ Controllo accessi	Possibile solo in SREL.ZK e SREL.ADV. Le ultime 1.024 attivazioni del transponder vengono salvate con data e ora.

☑ Gestione fasce orarie	Possibile solo in SREL.ZK e SREL.ADV. È possibile caricare un programma delle fasce orarie con il quale i transponder vengono autorizzati o bloccati in base al rispettivo gruppo di fasce orarie.
☑ Overlay	I transponder sostitutivi possono sovrascrivere i transponder originali. Dopo la prima attivazione con un transponder sostitutivo, il transponder originale viene bloccato.
☑ Flip Flop	La modalità ad impulsi (impostazione predefinita) viene disattivata e la durata degli impulsi diventa ininfluente. Con la modalità Flip Flop attivata, lo SmartRelè modifica il suo stato, ad ogni attivazione del transponder, da acceso a spento e viceversa. Questa modalità è consigliata, ad esempio, per l'accensione di luci o macchinari. *In un'installazione di questo tipo, verificare eventualmente che gli alimentatori e i dispositivi apriporta siano adatti al funzionamento con corrente permanente.*
☑ Repeater	Lo SmartRelè riceve un segnale dal transponder e lo inoltra potenziato. Lo SmartRelè può essere utilizzato con questa funzione per coprire tratte radio maggiori. La distanza da un altro SmartRelè può arrivare a 2 m.
☑ Cambio orario	Solo per SREL.ZK e SREL.ADV. Se si attiva la commutazione temporizzata, è necessario caricare un programma delle fasce orarie che consente un'abilitazione generale dello SmartRelè durante gli orari selezionati (nel gruppo 5). Inoltre, una porta può essere liberamente transitabile durante il giorno ed essere apribile di notte solo tramite transponder. *In un'installazione di questo tipo, verificare che gli alimentatori e i dispositivi apriporta siano adatti al funzionamento con corrente permanente.*

☑ OMRON	Solo per SREL.ADV. Numerosi sistemi di controllo accessi e registrazione delle ore possiedono interfacce seriali per il collegamento di lettori schede. Con queste interfacce è possibile collegare anche uno SmartRelè. In questo modo i transponder SimonsVoss possono essere utilizzati anche in sistemi esterni. Se si desidera che lo SmartRelè trasferisca i dati del transponder ad un sistema esterno e che in caso di abilitazione da parte del sistema esterno venga inviato un comando di apertura remoto dallo SmartRelè ad un cilindro, selezionare quest'opzione sia nello SmartRelè che nel cilindro. Il tipo di sistema esterno va impostato sotto "Interfaccia". Fare clic sul pulsante Configurazione ampliata.



Con il pulsante Configurazione ampliata è possibile specificare alcune impostazioni:

Lunghezza impulsi	Qui si immette il valore in secondi per la durata dell'impulso di commutazione. Il valore può essere compreso fra 0,1 e 25,5 secondi. Se si inserisce, ad esempio, 3 secondi, il dispositivo apriporta viene abilitato per 3 secondi e quindi nuovamente bloccato.

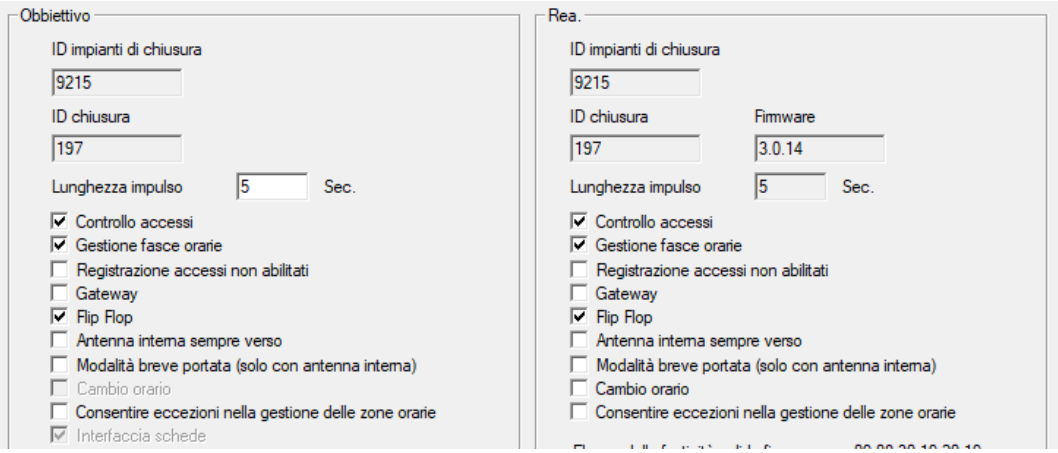
☑ portata limitata	Se si seleziona quest'opzione, la portata di lettura fra transponder e SmartRelè viene ridotta da 1,5 m a 0,4 m circa. Quest'opzione può essere utilizzata, ad esempio, quando nelle immediate vicinanze si trovano più SmartRelè e i singoli transponder sono autorizzati in più SmartRelè.
☑ Registrazione accessi non abilitati	Solo per SREL.ZK e SREL.ADV: Di norma vengono registrate solo le attivazioni dei transponder autorizzati. Se si desidera che vengano acquisiti anche i tentativi di apertura della porta effettuati da transponder non autorizzati, è necessario selezionare quest'opzione.
Numero dei moduli di espansione	Qui si inserisce il numero dei moduli esterni collegati allo SmartRelè. Questi moduli vengono collegati ai morsetti RS-485 C OM, RS-485 A e RS-485 B.
"Interfaccia"	Solo per SREL.ADV: Per il funzionamento come interfaccia seriale è possibile impostare qui il tipo di lettore schede che lo SmartRelè deve simulare. Sono disponibili le seguenti opzioni: ▪ Wiegand 33 bit ▪ Wiegand 26 bit ▪ Primion ▪ Siemens ▪ Kaba Benzing ▪ Gantner Legic ▪ Isgus
☑ Nessun segnale acustico	Solo per SREL.ADV: Se si desidera che durante la programmazione dello SmartRelè non vengano emesse conferme di programmazione acustiche da parte di un cicalino collegato, porre una croce in questo campo.
◉ LED esterni/ ◉ Cercapersone esterno	Solo per SREL.ADV: Qui viene indicato il gruppo costruttivo esterno collegato. Con LED esterno, lo SmartRelè genera, in modalità Flip Flop, un segnale prolungato in condizione commutata, mentre in caso di collegamento di un cicalino viene confermato con un breve segnale acustico solo ogni cambio di stato.

◉ Autodetection/ ◉ entrambi attivi	Solo per SREL.ADV ■ ◉ Autodetection Se è collegata un'antenna esterna, verrà utilizzata solo questa. Lo SmartRelè disattiverà l'antenna interna. Se non è collegata alcuna antenna esterna (situazione standard), lo SmartRelè utilizzerà l'antenna interna. ■ ◉ entrambi attivi Lo SmartRelè può analizzare le registrazioni dei transponder su entrambe le antenne.

SmartRelè (G2): SREL.G2, SREL.W.G2, SREL2.G2.W

Questa scheda ([Configurazione/dati]) è suddivisa in due parti:

- La parte a sinistra mostra lo stato nominale ("Rea.") della chiusura, ossia lo stato configurato nel software LSM e pertanto desiderato.
- Nella parte destra è visualizzato lo stato reale della chiusura ("Obbiettivo") e cioè l'ultimo stato programmato.



A seconda del tipo di chiusura si possono attivare le seguenti funzioni:

- **Lunghezza impulsi**

  Qui si immette il valore in secondi per la durata dell'impulso di commutazione. Il valore può essere compreso fra 0,1 e 25,5 secondi. Se si inserisce, ad esempio, 3 secondi, il dispositivo apriporta viene abilitato per 3 secondi e quindi nuovamente bloccato.

- **Controllo accessi**

  Possibile in ZK e ADV. Le ultime 1.024 attivazioni del transponder vengono salvate con data e ora.

- **Gestione fasce orarie**

Possibile solo in SREL.ZK e SREL.ADV. È possibile caricare un programma delle fasce orarie con il quale i transponder vengono autorizzati o bloccati in base al rispettivo gruppo di fasce orarie.

- **Registrazione dei tentativi di accesso non autorizzati**

  Possibile solo in ZK e ADV: Di norma vengono registrate solo le attivazioni dei transponder autorizzati. Se si desidera che vengano acquisiti anche i tentativi di apertura della porta effettuati da transponder non autorizzati, è necessario selezionare quest'opzione.

- **Gateway**

  Lo SmartRelè può essere utilizzato come gateway.

- **FlipFlop**

  La modalità ad impulsi (impostazione predefinita) viene disattivata e la durata degli impulsi diventa ininfluente. Con la modalità Flip Flop attivata, lo SmartRelè modifica il suo stato, ad ogni attivazione del transponder, da acceso a spento e viceversa. Questa modalità è consigliata, ad esempio, per l'accensione di luci o macchinari.

  In un'installazione di questo tipo, verificare eventualmente che gli alimentatori e i dispositivi apriporta siano adatti al funzionamento con corrente permanente.

- **Antenna interna sempre attivata**

  Anche se è collegata un'antenna esterna, l'antenna interna continuerà ad essere utilizzata in parallelo.

- **Modo prossimità (solo con antenna interna)**

  Si attiva il modo Prossimità.

- **Commutazione temporizzata**

  Solo per SREL.ZK e SREL.ADV. Se si attiva la commutazione temporizzata, è necessario caricare un programma delle fasce orarie che consente un'abilitazione generale dello SmartRelè durante gli orari selezionati (nel gruppo 5). Inoltre, una porta può essere liberamente transitabile durante il giorno ed essere apribile di notte solo tramite transponder.

  In un'installazione di questo tipo, verificare che gli alimentatori e i dispositivi apriporta siano adatti al funzionamento con corrente permanente.

- **Autorizzazione di deroghe nella gestione delle fasce orarie**

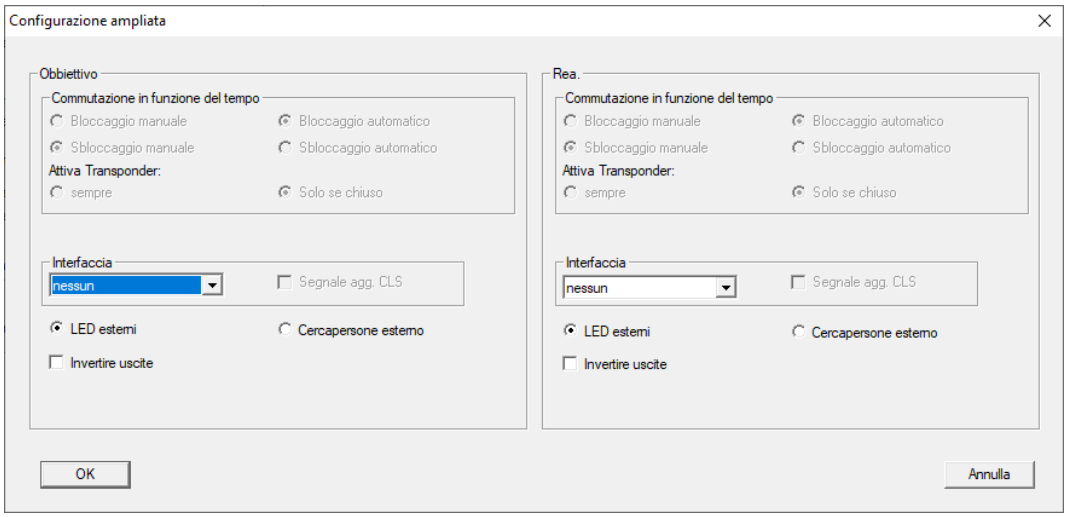
  Se questa casella di controllo è attivata, sono ammesse deroghe nella gestione delle fasce orarie.

- **Interfaccia scheda**

Questa opzione è disponibile di serie per tutti gli SmartRelè G2. L'LSM crea dapprima un record di dati per una chiusura attiva e durante la programmazione controlla se la chiusura dispone di un'interfaccia scheda. Se non viene riconosciuta nessuna interfaccia scheda, la casella di controllo viene disattivata automaticamente dall'LSM. Nell'LSM 3.3 non è più necessario specificare se si possiede uno SmartRelè G2 attivo o ibrido.

NOTA

Se si modifica manualmente l'impostazione Interfaccia scheda, il riconoscimento automatico non sarà più operativo e verranno emessi dei messaggi di avviso.



Con il pulsante "Configurazione avanzata" è possibile specificare alcune impostazioni:

- **Interfaccia**

  Per il funzionamento come interfaccia seriale è possibile impostare qui il tipo di lettore schede che lo SmartRelè deve simulare.

  Sono disponibili le seguenti opzioni:

  - Wiegand 33 bit
  - Wiegand 26 bit
  - Primion
  - Siemens
  - Kaba Benzing
  - Gantner Legic
  - Isgus

- **Cicalino esterno / LED esterno**

Solo per SREL.ADV: Qui viene indicato il gruppo costruttivo esterno collegato. Con LED esterno, lo SmartRelè genera, in modalità Flip Flop, un segnale prolungato in condizione commutata, mentre in caso di collegamento di un cicalino viene confermato con un breve segnale acustico solo ogni cambio di stato.

- **Inversione delle uscite**

  Con queste impostazioni è possibile invertire l'uscita del relè.

SmartRelè 3

Questa scheda è suddivisa in due parti.

- L'area "Rea." mostra lo stato nominale della chiusura. Questo stato è richiesto dall'utente, configurato nell'LSM, ma probabilmente non ancora programmato nel sistema SREL3-3-ADV.
- L'area "Obbiettivo" mostra lo stato reale della chiusura. Questo è l'ultimo stato programmato nel sistema SREL3-ADV.

A seconda del tipo di chiusura possono essere attivate le seguenti funzioni:

- Lunghezza impulsi

  Qui si immette il valore in secondi per la durata dell'impulso di commutazione (da 0 s a 25 s). Se il valore corrisponde, ad esempio, a tre secondi, il dispositivo apriporta viene abilitato per tre secondi e quindi nuovamente bloccato.

- ☑ Controllo accessi

  Il controllo accessi è disponibile solo nella variante ZK. Le ultime 1.024 attivazioni del transponder vengono salvate con data e ora.

- ☑ Gestione fasce orarie

  La gestione delle fasce orarie è disponibile solo nella variante ZK. È possibile caricare un programma delle fasce orarie. I transponder verranno quindi autorizzati o bloccati in base al loro gruppo delle fasce orarie.

- ☑ Registrazione accessi non abilitati

  La registrazione dei tentativi di accesso non autorizzati è disponibile solo nella variante ZK. Attivando questa opzione, oltre agli azionamenti dei transponder autorizzati verranno salvati anche gli azionamenti dei transponder non autorizzati.

- ☑ Gateway

  Lo SmartRelè può essere utilizzato come gateway (vedere Funzione gateway).

- ☑ Flip Flop

Il relè utilizzato nel controller si comporta in genere come un monoflop (apertura ad impulso). Attivando questa opzione, la durata impulsi impostata verrà ignorata e il relè verrà commutato fino al nuovo azionamento di un supporto di identificazione autorizzato. Questa opzione è consigliata ai fini dell'attivazione di impianti di illuminazione, macchinari e dispositivi simili.

AVVISO

Danni causati da corrente continua

I dispositivi dimensionati per l'apertura a impulsi potrebbero non essere idonei al funzionamento con corrente continua. Fare attenzione che gli alimentatori e i dispositivi (ad es. apriporta) utilizzati siano adatti al funzionamento con corrente continua.

- ☑ Modalità zona prossima

  Il modo prossimità riduce la portata di lettura nel campo B dei lettori (vedere Opzione campo vicino).

- ☑ Cambio orario

  La commutazione temporizzata è disponibile solo nella variante ZK. È possibile caricare un programma delle fasce orarie. Attivando la commutazione temporizzata, il sistema SREL3-ADV può essere abilitato o bloccato durante gli orari autorizzati o non autorizzati (nel gruppo 5). A seconda dell'impostazione, il sistema SREL3-ADV commuta anche automaticamente. Ad esempio, una porta può rimanere aperta automaticamente durante il giorno, mentre di notte può essere aperta solo con un transponder (vedere Commutazione temporizzata).

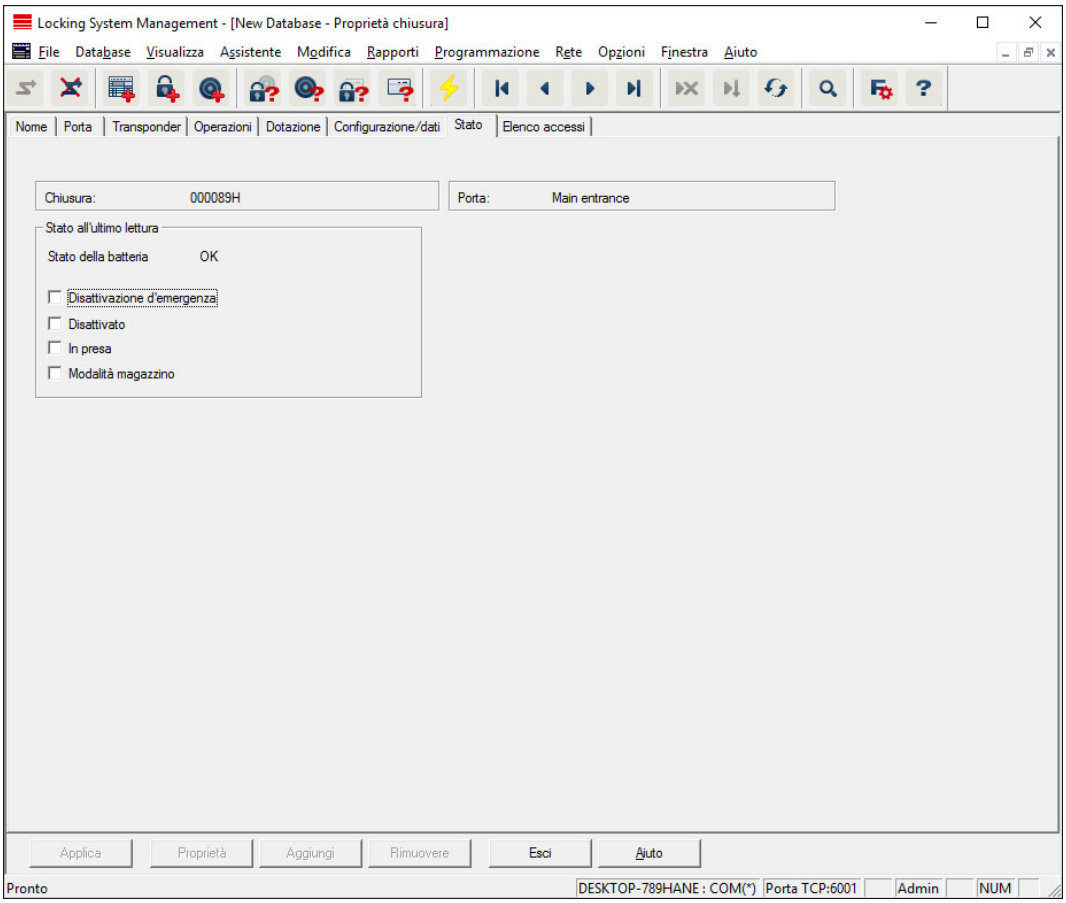
- ☑ Ignora data di attivazione o scandenza

  Ai transponder può essere assegnata una data di validità. Attivare questa opzione se si desidera autorizzare i transponder anche al di fuori di questa data di validità.

- ☑ Interfaccia schede

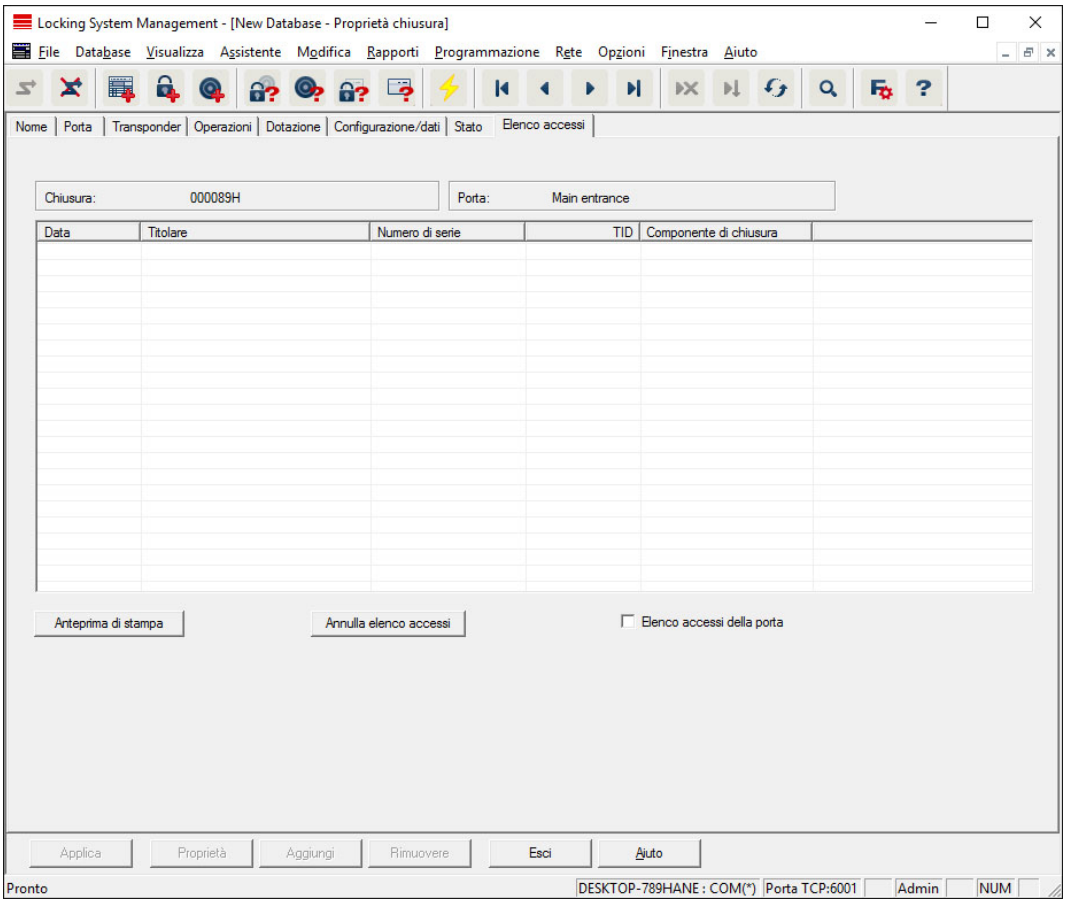
  Questa opzione non deve essere modificata. Con essa, l'LSM riconosce automaticamente, durante la programmazione, se il lettore collegato è ibrido. Se si modifica manualmente l'opzione, il riconoscimento non sarà più operativo.

Stato



L'ultimo stato letto della chiusura viene visualizzato e aggiornato ad ogni lettura della chiusura.

Elenco accessi



In questa scheda è possibile visualizzare l'ultimo stato dell'elenco accessi. *La chiusura deve essere compatibile con la funzione "Controllo accessi" e quest'ultima deve essere attivata nelle proprietà della chiusura.*

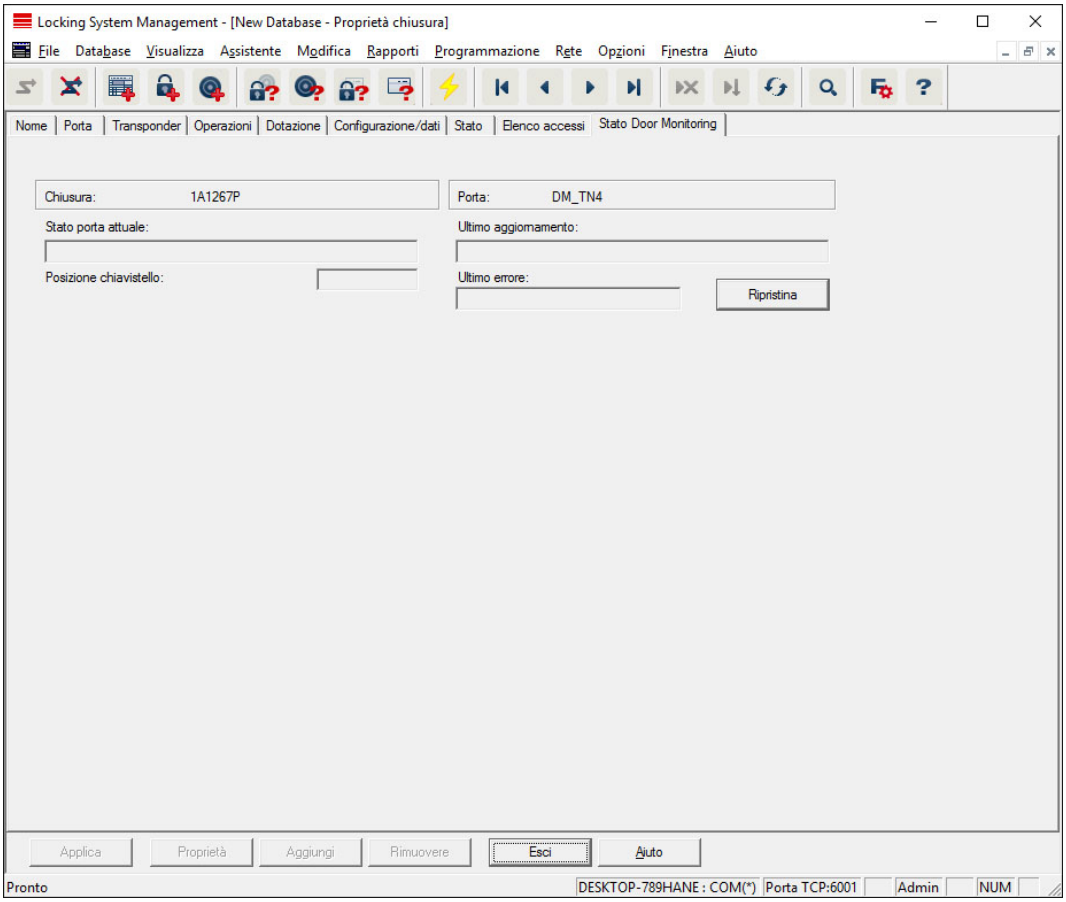
Per leggere l'elenco accessi, procedere come segue:

1. Leggere la chiusura dalla barra menu *Programmazione/Leggi chiusura*.
2. Fare clic sul pulsante "Elenco accessi" per avviare l'operazione di lettura.
   ↳ L'elenco accessi viene rappresentato e salvato automaticamente. Ora è possibile visualizzarlo in qualunque momento tramite la scheda Elenco accessi nelle proprietà della chiusura.

Stato DoorMonitoring

Con la scheda "Stato DoorMonitoring" è possibile visualizzare lo stato attuale della chiusura in tempo reale (vedi anche *Possibili stati (porta) [▸ 199]*). Per questa funzione è necessario una rete WaveNet configurata.

Questa scheda è disponibile solo se la chiusura possiede la proprietà DM e se è stata creata nel software LSM direttamente come "Cilindro/ SmartHandle G2 DoorMonitoring"! L'immagine può variare.



NOTA

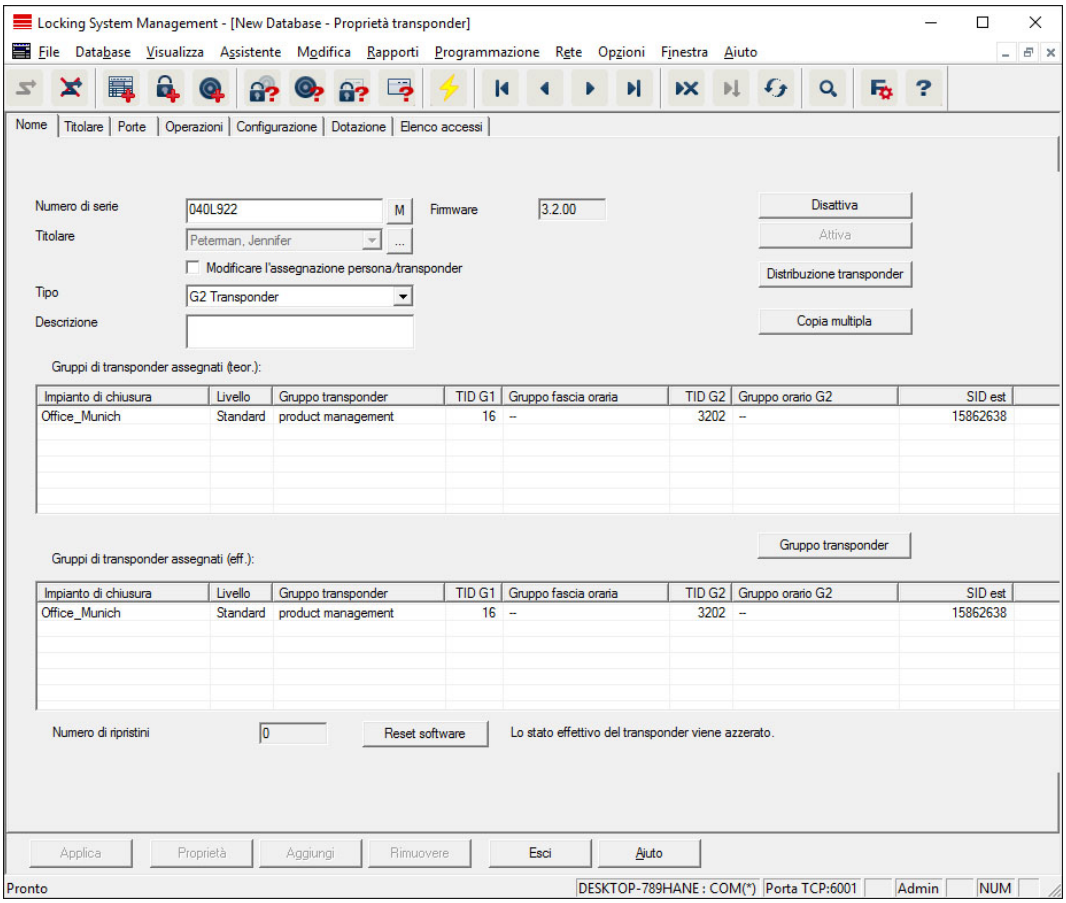
Se si desidera monitorare più chiusure contemporaneamente, con Smart.Surveil è possibile visualizzare in forma tabellare una panoramica delle chiusure e il relativo stato porta.

7.1.5.3 Proprietà: Transponder

Mostra e modifica le proprietà del transponder al momento selezionato.

Facendo clic su un transponder le proprietà del rispettivo transponder si aprono direttamente!

Nome



- **Numero di serie**

  Numero di serie del transponder. Il pulsante "..." mostra le proprietà della persona. Nel corso della programmazione dei transponder G2, il loro "Numero di serie interno" (numero PHI *(Physical Hardware Identifier; stampato sul prodotto)*) viene applicato automaticamente.

- **Proprietario**

  Persona cui è assegnato il transponder. Il pulsante "M" mostra il transponder nella matrice.

- **Tipo**

  Tipo di transponder.

- **Descrizione**

  Campo libero per la descrizione del transponder.

- **Gruppi di transponder assegnati: Stato nominale**

  Stato nominale dei gruppi transponder in cui si trova il transponder.

- **Gruppo transponder**

  Con questo pulsante è possibile assegnare il transponder ad un altro gruppo transponder.

- **Gruppi di transponder assegnati: Stato reale**

  Stato reale (ultima programmazione) dei gruppi transponder in cui si trova il transponder.

- **Reset software**

  Pulsante per l'azzeramento dello stato reale nel software LSM. Quest'operazione viene contata e il risultato visualizzato accanto a sinistra.

NOTA

Utilizzare questa funzione solo se si è certi di mantenere i componenti programmati! Quest'azione può essere eseguita, ad es., su un transponder fisicamente difettoso. In talune circostanze, un transponder programmato correttamente e funzionante, nel quale è stato eseguito solo un reset software, può essere ancora autorizzato nelle chiusure. Ciò rappresenta un elevato rischio per la sicurezza!

- **Disattiva**

  Pulsante per la disattivazione di un transponder.

- **Attiva**

  Pulsante per l'attivazione di un transponder.

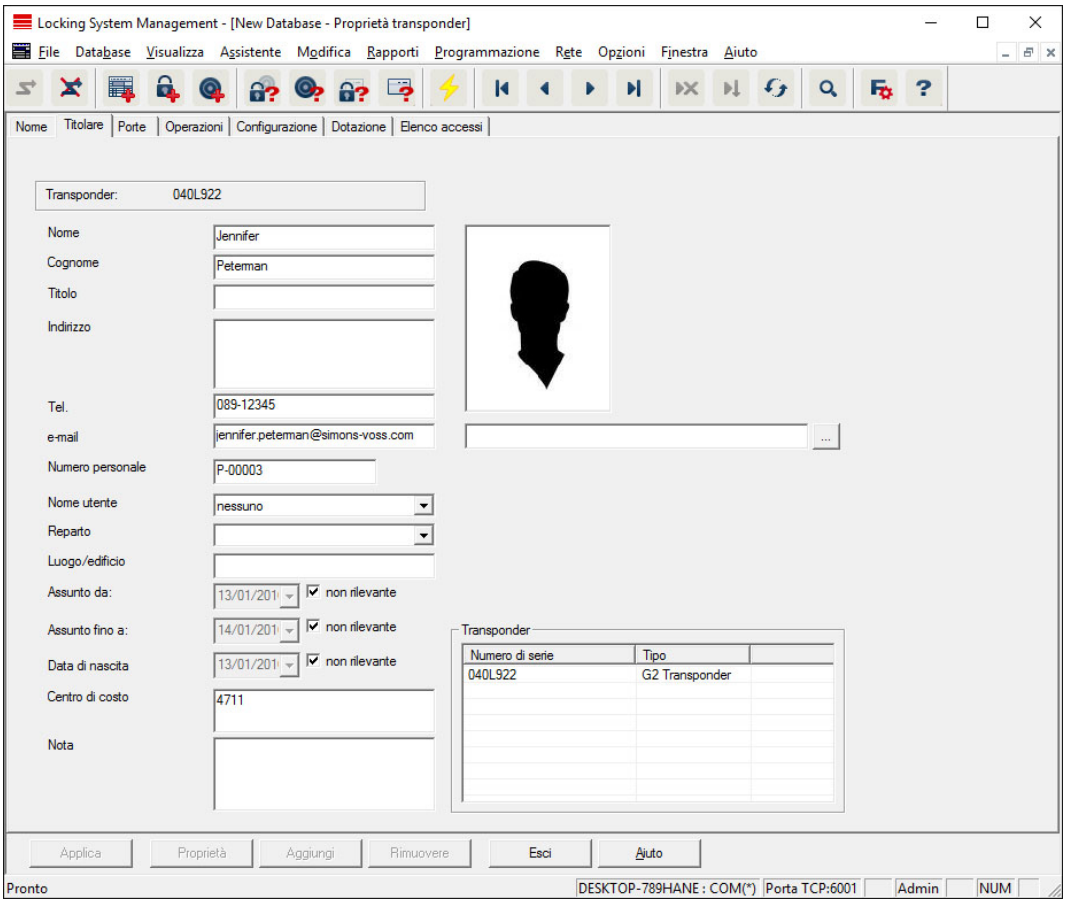
- **Consegna transponder**

  Generazione di un modulo con firma per la consegna. Il modulo contiene anche un elenco di tutte le porte autorizzate.

- **Copia multipla**

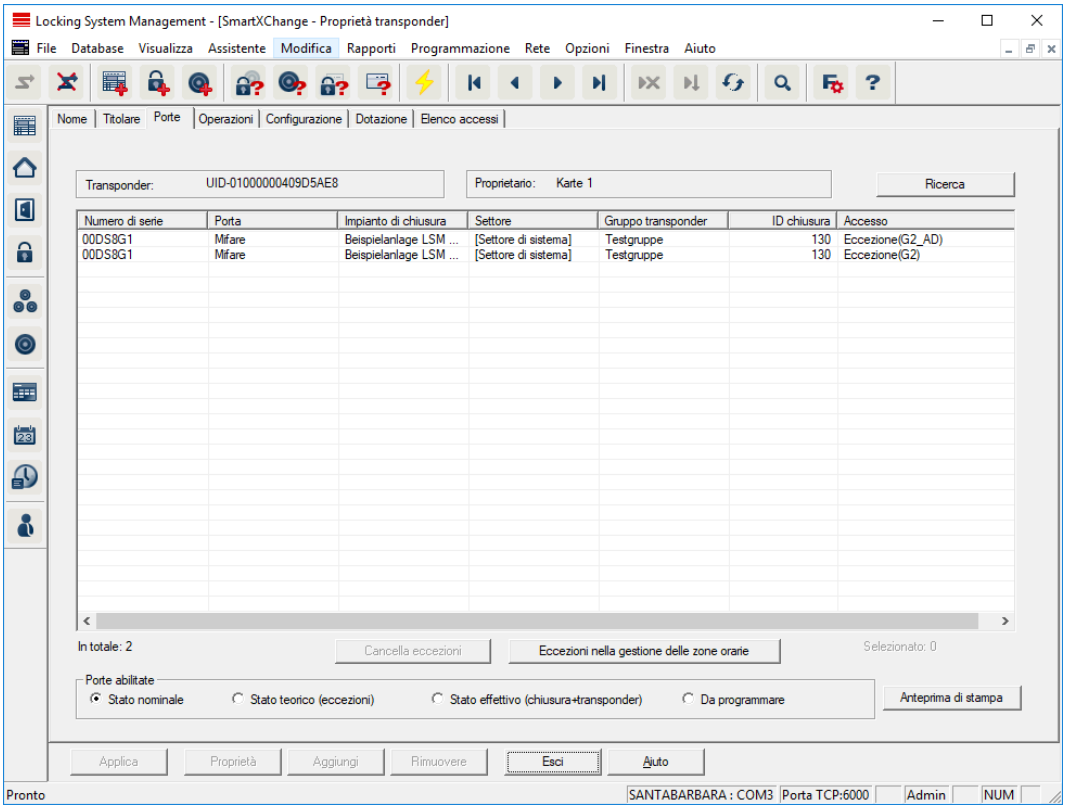
  Crea un numero desiderato di copie del transponder aventi le medesime proprietà.

Proprietario



Nella scheda "Proprietario" è possibile inserire tutte le informazioni sul proprietario del transponder. La tabella "Transponder" mostra quanti e quali transponder sono assegnati all'utente. Con il pulsante "..." è possibile inserire una foto dell'utente. *Si consiglia di utilizzare immagini in formato JPEG con dimensioni superiori a 500 kB.*

Porte



Questa scheda fornisce una panoramica generale delle autorizzazioni porta per il transponder selezionato. che sono visualizzati dettagliatamente all'interno di una tabella.

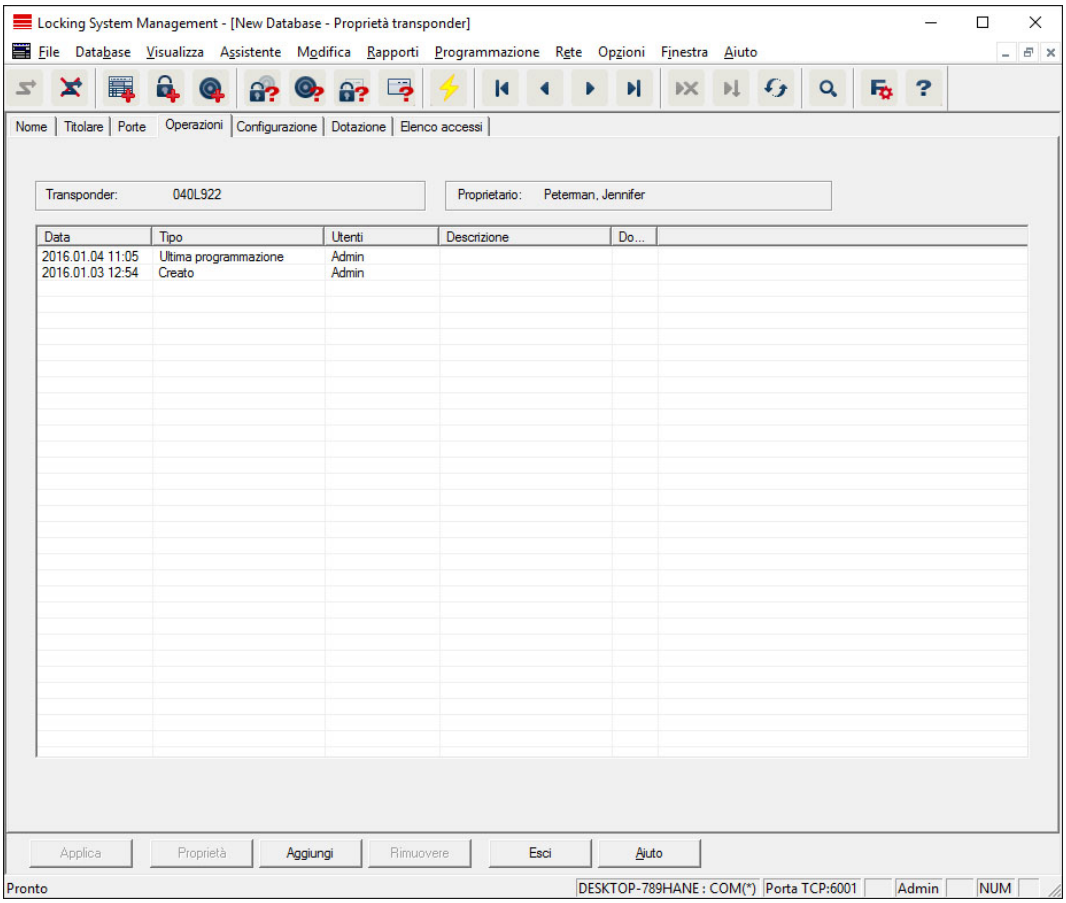
- **Tabella**

  Mostra in un elenco dettagliato tutte le porte autorizzate per il transponder.

- **Porte autorizzate**

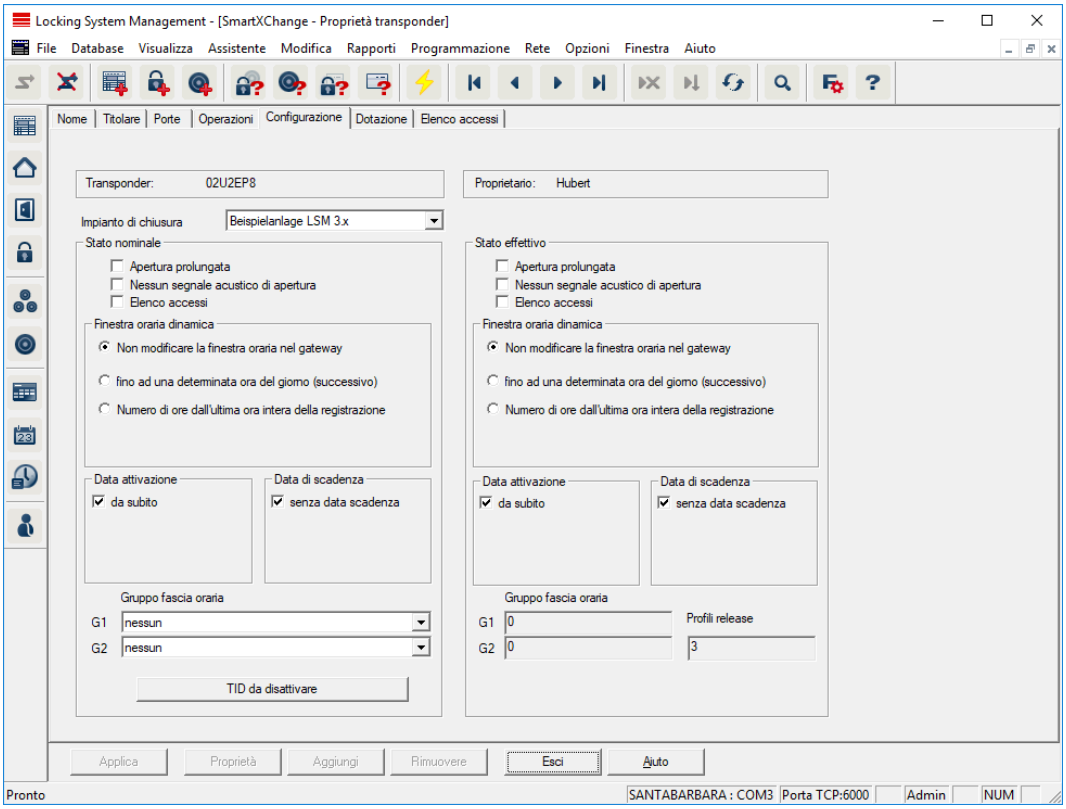
  La tabella può essere ordinata e filtrata mediante i singoli pulsanti di opzione.

Azioni



Questa tabella indica le azioni (ad es. programmazione, modifica delle autorizzazioni ecc.) eseguite nel transponder selezionato. Certe azioni, quali ad es. "Restituzione programmata" possono essere aggiunte anche manualmente con il pulsante "Aggiungi".

Configurazione



Questa scheda è suddivisa in due parti:

- La parte a sinistra mostra lo stato nominale del transponder, ossia lo stato configurato nel software LSM e pertanto desiderato.
- Nella parte destra è visualizzato lo stato reale del transponder e cioè l'ultimo stato programmato.
- **Impianto di chiusura**

  Mostra l'impianto di chiusura attualmente assegnato per il transponder.
- **Apertura prolungata**

  La chiusura rimane accoppiata più a lungo. La lunghezza degli impulsi della chiusura viene raddoppiata. *Esempio di applicazione: Persone disabili, che possono aver bisogno di più tempo per l'apertura della porta.*
- **Nessun segnale acustico di apertura**

  La chiusura risponde al transponder senza segnale acustico di conferma. *Esempio di applicazione: residenze assistite. L'infermiera del turno di notte può entrare nella stanza senza fare rumore.*
- **Elenco azionamenti**

  Salva tutti gli azionamenti nel transponder.
- **Non modificare fascia oraria nel gateway**

La validità di questo transponder G2 che si registra nel gateway non viene limitata temporalmente.

- **Fino ad una determinata ora del giorno successivo**

  La validità di questo transponder G2 che si registra nel gateway viene limitata temporalmente fino ad una determinata ora. Immettere un'ora.

- **Numero ore dall'ultima ora piena di registrazione**

  La validità di questo transponder G2 che si registra nel gateway viene prolungata della durata in ore stabilita. Immettere un numero di ore.

- **Data di attivazione**

  Data e ora a partire dalle quali il transponder deve essere valido.

- **Data di scadenza**

  Data e ora a partire dalle quali il transponder non deve essere più valido.

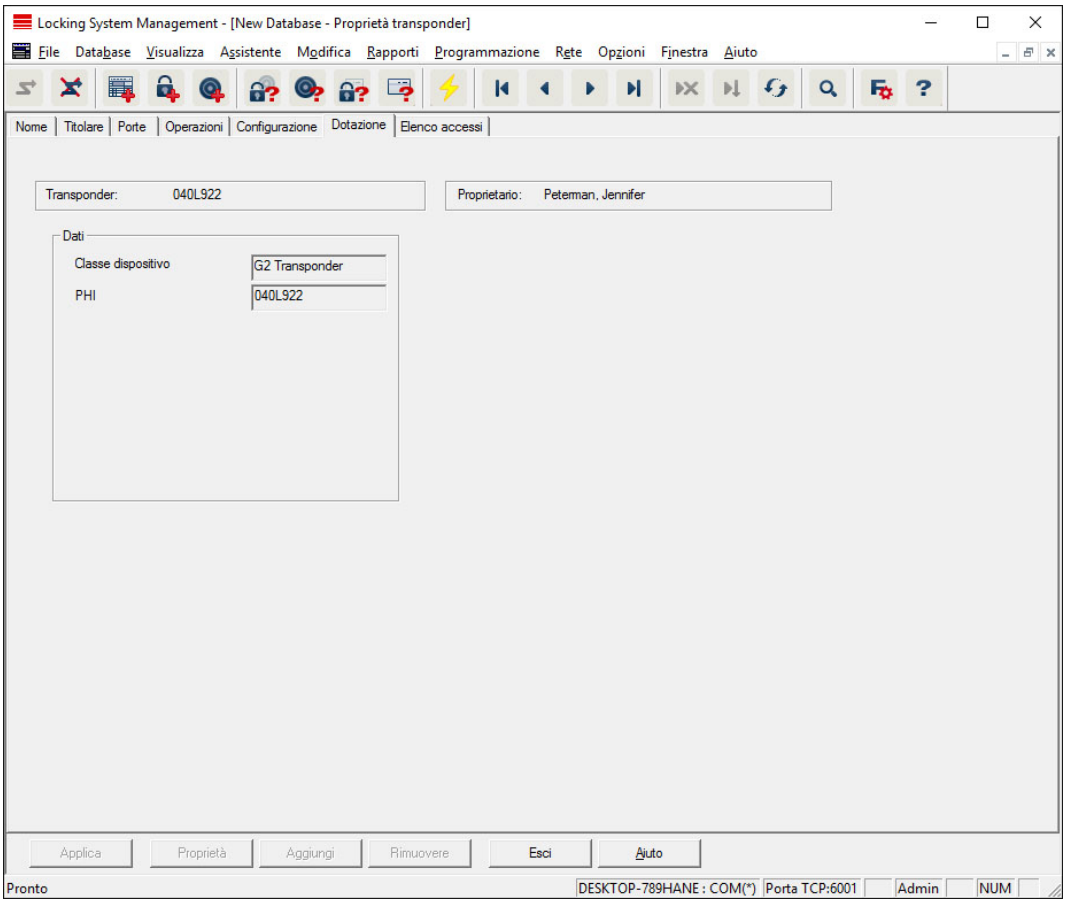
- **Gruppo di fasce orarie**

  È possibile assegnare al transponder un gruppo di fasce orarie predefinito.

- **TID da disattivare**

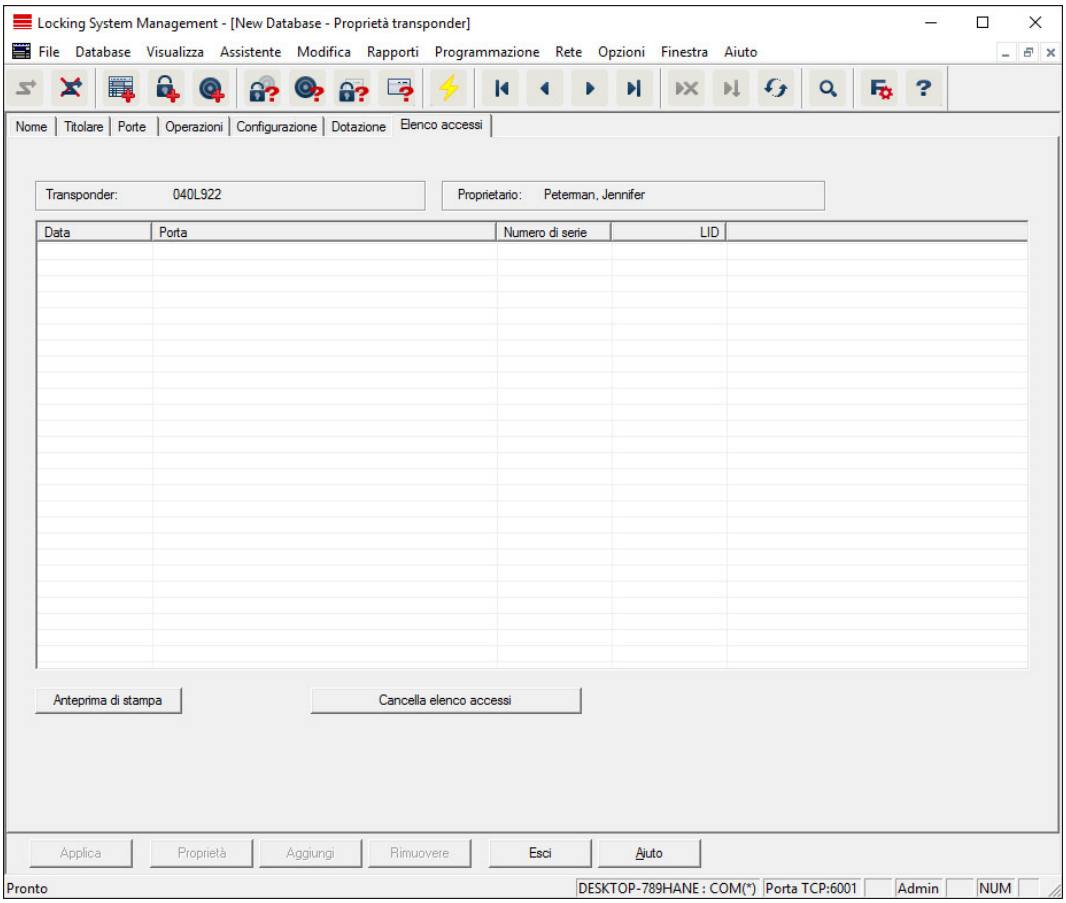
  È possibile salvare sul transponder gli ID di altri transponder bloccati. Non appena il transponder si registra in una chiusura, i blocchi diventano attivi nella chiusura.

Dotazione



Consultazione delle specifiche esatte del transponder.

Elenco azionamenti



In questa scheda è possibile visualizzare l'ultimo stato dell'elenco azionamenti. *Deve essere attiva la funzione "Elenco azionamenti".*

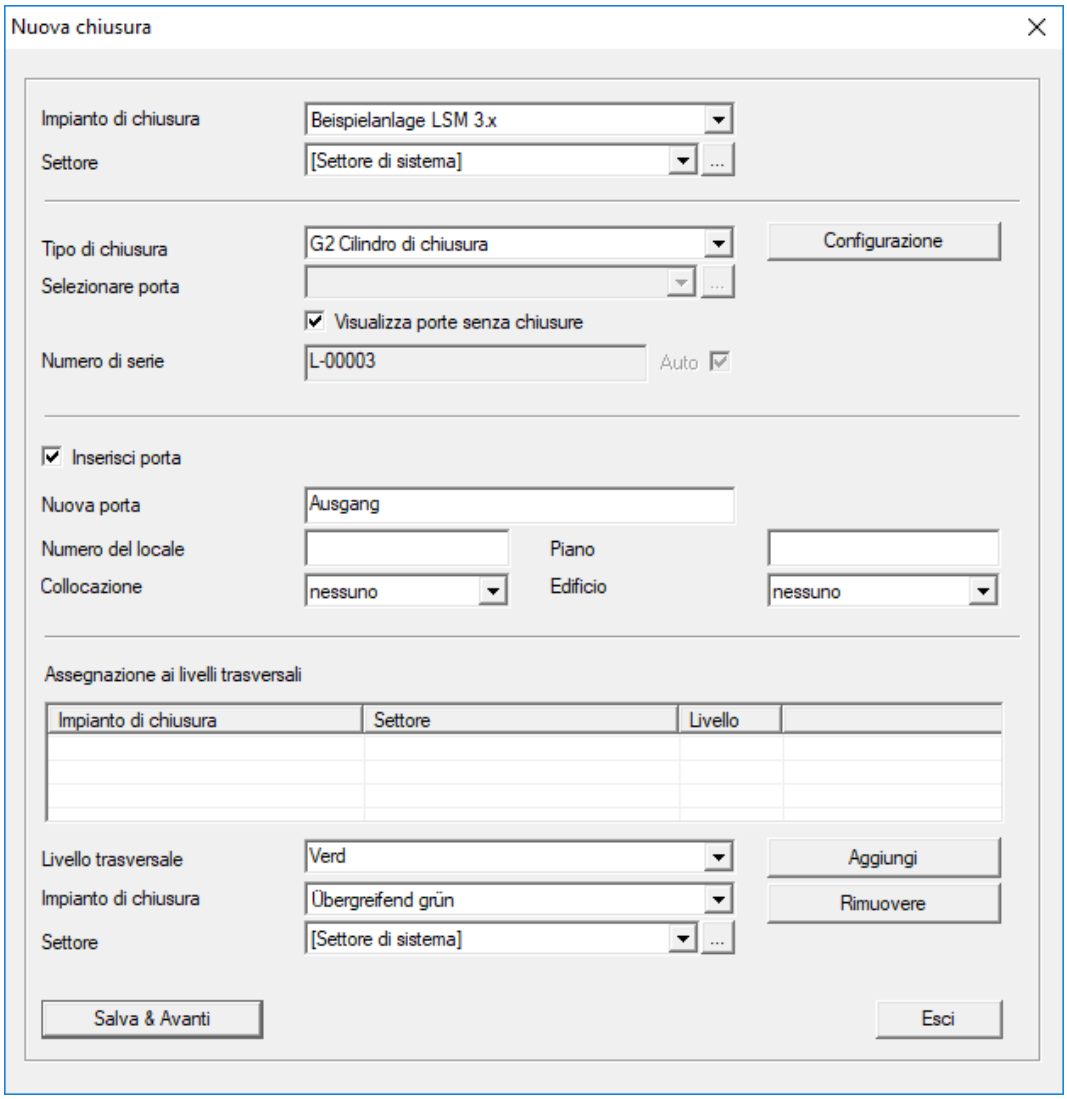
Per leggere l'elenco azionamenti, procedere come segue:

1. Leggere il transponder dalla barra menu *Programmazione/Leggi transponder*.
2. Fare clic sul pulsante "Elenco azionamenti" per avviare l'operazione di lettura.
   ↳ L'elenco azionamenti viene rappresentato e salvato automaticamente. Ora è possibile visualizzarlo in qualunque momento tramite la scheda Elenco accessi nelle proprietà del transponder.

7.1.5.4 Nuovo impianto di chiusura

Qui è possibile creare un nuovo impianto di chiusura all'interno del progetto.

7.1.5.5 Nuova chiusura



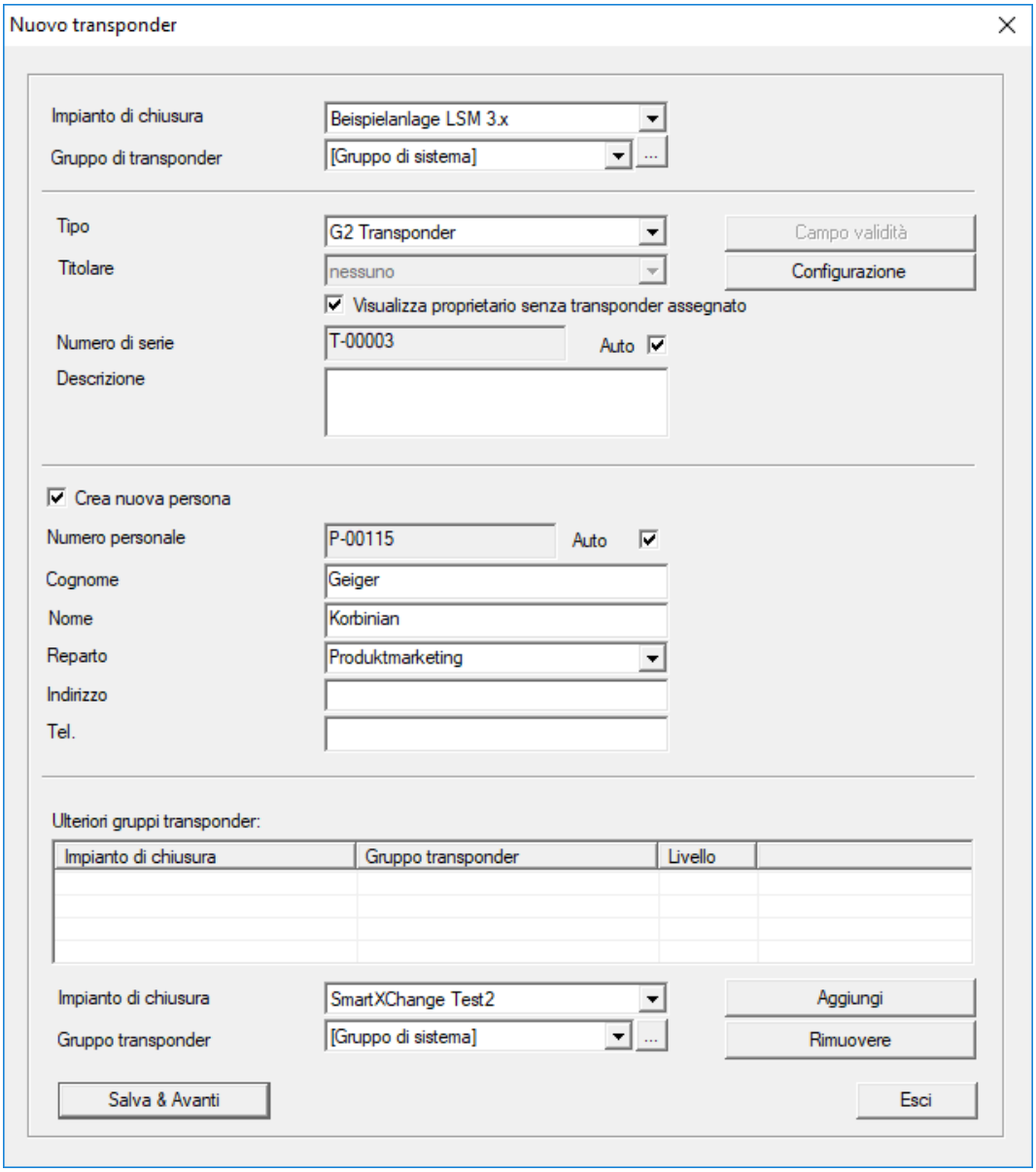
Utilizzare quest'opzione per aggiungere manualmente una nuova chiusura.

Se sono già stati creati più impianti di chiusura e più livelli di chiusura trasversali, è possibile assegnarvi la nuova chiusura direttamente. A tale scopo, le varie opzioni sono disponibili sotto forma di elenchi a discesa.

- Per assegnare subito la chiusura in modo corretto, selezionare facoltativamente un impianto di chiusura e il settore. Gli impianti di chiusura e i settori devono essere stati precedentemente definiti. È possibile modificare queste impostazioni successivamente in qualunque momento.
- Con il pulsante "Aggiungi porta" è possibile creare una nuova porta. Una porta può contenere più chiusure.
- Con il pulsante "Salva & Avanti" la nuova chiusura viene creata nel piano di chiusura. Scegliere "Termina" per ritornare alla matrice o creare subito un'altra porta.

A seconda dell'hardware utilizzato, nel software LSM è possibile gestire diverse chiusure. Selezionare, nel rispettivo elenco a discesa, il tipo di chiusura che si desidera creare.

7.1.5.6 Nuovo transponder



Quest'opzione consente di creare manualmente un nuovo transponder.

Se sono già stati creati più impianti di chiusura e più gruppi transponder, è possibile assegnarvi il nuovo transponder direttamente. A tale scopo, le varie opzioni sono disponibili sotto forma di elenchi a discesa.

- Per assegnare subito il transponder in modo corretto, selezionare facoltativamente un impianto di chiusura e il gruppo transponder. Gli impianti di chiusura e i gruppi transponder devono essere stati precedentemente definiti. È possibile modificare queste impostazioni in qualunque momento.

- Con il pulsante "Configurazione" è possibile effettuare impostazioni avanzate, quali la validità del transponder.
- Con il pulsante "Salva & Avanti" il transponder viene creato nel piano di chiusura. Scegliere "Termina" per ritornare alla matrice o creare subito un altro transponder.

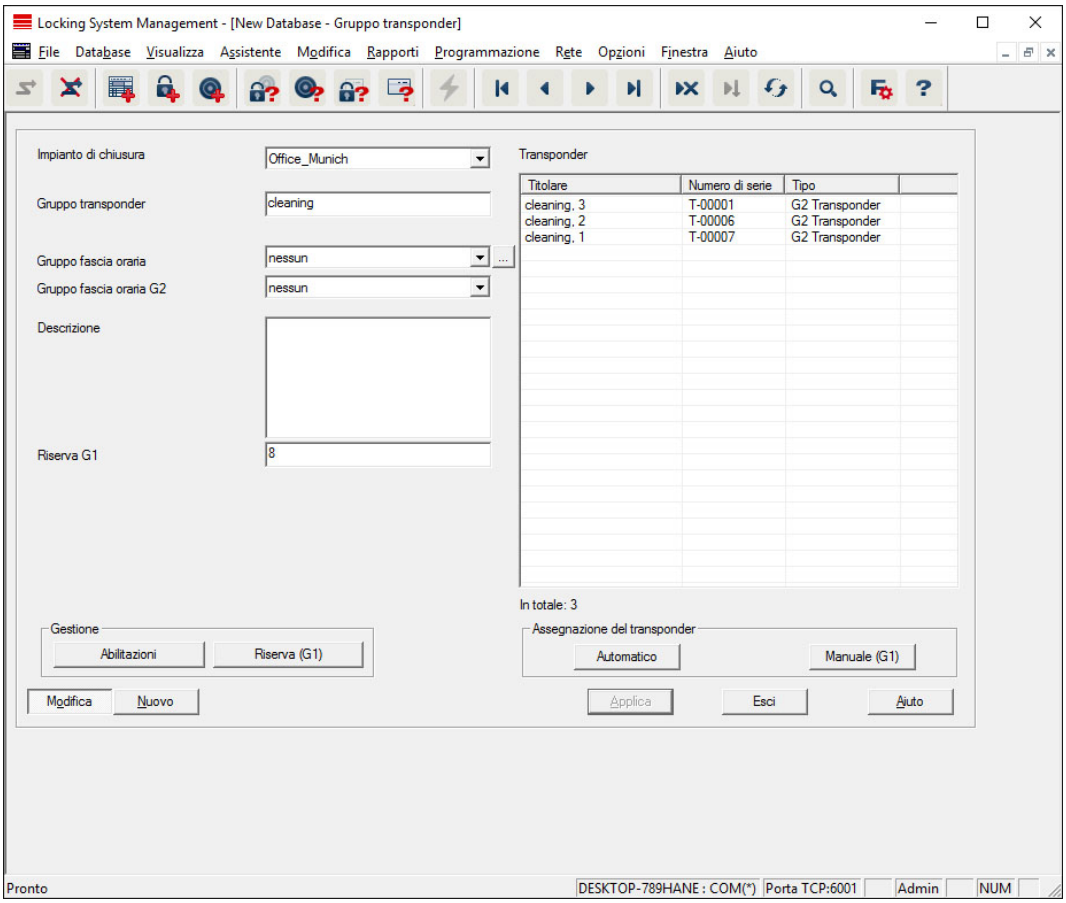
Tenere presente che nel software LSM ogni supporto di identificazione è definito transponder. A seconda dell'hardware utilizzato, nel software LSM è possibile gestire diversi supporti di identificazione:

Biometria G1	Transponder biometrico
Utente lettore biometrico G1	Utente lettore biometrico con standard G1
Scheda G1	Scheda con standard G1
SmartClip G1	SmartClip con standard G1
Transponder G1	Transponder con standard G1
Scheda G2	Scheda con standard G2
Utente PIN-Code G2	Utente di un Pin-Code Terminal
Transponder G2	Transponder con standard G2
Non definito	Transponder G1 non ancora definito

NOTA

I transponder non devono essere assegnati mai contemporaneamente ad un impianto di chiusura e ad un livello trasversale!

7.1.5.7 Gruppo transponder



Questo menu mostra i gruppi transponder già creati. Con i pulsanti "Record dati successivo" e "Record dati precedente" della barra multifunzione è possibile passare da un gruppo transponder all'altro. Il pulsante "Nuovo" permette di creare altri transponder.

- **Impianto di chiusura**

  Selezione dell'impianto di chiusura creato.

- **Gruppo transponder**

  Nome del gruppo transponder.

- **Gruppo superiore**

  Gruppo transponder posto in una posizione più in alto all'interno della gerarchia.

- **Gruppo di fasce orarie G1**

  Specifica la fascia oraria G1 per il gruppo transponder.

- **Gruppo fasce orarie G2**

  Specifica la fascia oraria G2 per il gruppo transponder.

- **Descrizione**

  Campo libero per la descrizione del gruppo transponder.

- **Riserva G1**

  Numero di ID transponder totali disponibili nel gruppo transponder.

- **Autorizzazioni**

  Possibilità di assegnare autorizzazioni di gruppo.

- **Riserva (G1)**

  Possibilità di amministrare gli ID transponder G1.

- **Automatico**

  Possibilità di assegnare automaticamente un transponder libero al gruppo transponder.

- **Manuale (G1)**

  Possibilità di assegnare manualmente un determinato transponder ad un determinato ID transponder.

7.1.5.8 Persona

Questo menu mostra le persone già create. Con i pulsanti "Record dati successivo" e "Record dati precedente" della barra multifunzione è possibile passare da una persona all'altra.

Il menu corrisponde alla scheda "Proprietario" in *Modifica/Proprietà: Transponder*.

Con il pulsante "Nuovo" è possibile creare nuove persone.

7.1.5.9 Settore

Questo menu si utilizza per visualizzare i singoli settori transponder. Con i pulsanti "Record dati successivo" e "Record dati precedente" della barra multifunzione è possibile passare da un gruppo transponder all'altro.

Con il pulsante "Nuovo" è possibile creare nuovi settori.

7.1.5.10 Porta

Questo menu mostra le porte già create. Con i pulsanti "Record dati successivo" e "Record dati precedente" della barra multifunzione è possibile passare da una porta all'altra.

Il menu corrisponde alla scheda "Porte" in *Modifica/Proprietà: Chiusura*.

Con il pulsante "Nuovo" è possibile creare nuove porte.

7.1.5.11 Edificio

Con questo menu è possibile aggiungere un nuovo edificio all'impianto di chiusura o modificarne uno esistente. Gli edifici possono essere creati solo se è già stato creato un luogo.

7.1.5.12 Luogo

Con questo menu è possibile aggiungere un nuovo luogo all'impianto di chiusura o modificarne uno esistente.

7.1.5.13 Elenco giorni festivi

L'elenco si applica a tutto il progetto. Qui si possono selezionare i giorni festivi a seconda della Regione e crearne di nuovi.

7.1.5.14 Giorno festivo

Qui si possono creare singoli giorni festivi e c'è la possibilità di definire un nuovo "Giorno festivo" o periodo di vacanza. *I nuovi giorni festivi creati devono essere assegnati ad un elenco di giorni festivi nella gestione dei giorni festivi.*

7.1.5.15 Programma delle fasce orarie

In quest'area si possono creare programmi delle fasce orarie.

- **Nome**

  Nome adatto e univoco per il programma delle fasce orarie.

- **Descrizione**

  Descrizione appropriata del programma delle fasce orarie.

- **Elenco giorni festivi**

  Selezionare una Regione.

- **Visualizzare nome dei gruppi per l'impianto di chiusura**

  Selezione dell'impianto di chiusura del quale devono essere visualizzati i nomi dei gruppi temporali modificati manualmente.

- **Tabella dei gruppi temporali**

  Per ogni programma delle fasce orarie si possono definire fino a 100 gruppi temporali. Selezionare prima un gruppo e quindi modificare il programma settimanale.

NOTA

Il quinto gruppo è riservato alla commutazione temporizzata (vedere Commutazione temporizzata).

- **Tabelle piccole in alto a destra**

  Se il programma delle fasce orarie è già stato assegnato ad un settore, ciò verrà visualizzato nelle due tabelle piccole.

NOTA

Creare prima sempre un programma delle fasce orarie e assegnarlo quindi ad un settore *o ad una singola chiusura*. Ciò avviene ad es. con *Modifica/ Settore*.

- **Programma settimanale**
  - I campi di colore blu corrispondono ad un'autorizzazione per il rispettivo orario.
  - Per modificarli, è possibile fare clic sui singoli campi oppure selezionarli tenendo premuto il tasto del mouse.
- **Modifica**

  Per modificare il programma delle fasce orarie, questo pulsante deve essere attivato. Le modifiche possono essere salvate con il pulsante "Applica".

- **Nuovo**

  Il pulsante "Nuovo" crea un programma delle fasce orarie nuovo.

7.1.5.16 Gruppo temporale

Nel gruppo temporale si possono visualizzare tutti i gruppi temporali assegnati nel programma delle fasce orarie. Questa vista risulta particolarmente adatta per ottenere una panoramica generale dell'impianto di chiusura, del gruppo temporale, del gruppo transponder e dei transponder.

Con il pulsante "Transponder assegnati" è possibile stampare una panoramica.

7.1.5.17 Fuso orario locale

In questa finestra si inserisce il fuso orario locale in caso di gestione di luoghi in fusi orari diversi. Il pulsante "Leggi da registrazione" offre una selezione dei principali fusi orari mondiali.

Se una chiusura è programmata con un fuso orario locale, il passaggio fra l'orario estivo e invernale avverrà automaticamente.

7.1.5.18 Utenti

Nell'LSM, il primo login avviene automaticamente con il ruolo di amministratore ("Admin"). Questo ruolo possiede tutte le autorizzazioni.

Nell'LSM BUSINESS si possono creare diversi utenti. In questo modo più utenti possono gestire un database o un impianto di chiusura.

In *Modifica/Utenti* si possono creare nuovi utenti e visualizzarne le autorizzazioni (vedi anche *Gestione utenti [▸ 167]*). Con i pulsanti "Record dati precedente" e "Record dati successivo" è possibile alternare fra gli utenti.

- "Account utente bloccato"

  Se la casella di controllo è attivata, l'utente è al momento bloccato.

- "Richiesta di modifica della password utente al successivo login"

  Se questa casella di controllo è attivata, l'utente deve definire una nuova password al momento del successivo login (tale operazione può essere eseguita in ogni momento alla voce *File/Modifica password utente*).

- Pulsante "Gruppi utente"

  Qui è possibile assegnare l'utente ad uno o più gruppi utenti già esistenti. Il gruppo utente definisce i diritti assegnati all'utente.

- Pulsante "Modifica"

  Con questo pulsante si possono modificare i dati utente.

- Pulsante "Nuovo"

  Con questo pulsante è possibile creare un nuovo utente.

7.1.5.19 Gruppo utenti

Gli utenti vengono aggiunti a gruppi utenti. In questo modo si distribuiscono i diritti degli utenti. Il primo login in LSM BUSINESS avviene come "Admin", assegnato al gruppo utenti "Administrator" con tutti i diritti.

In *Modifica/Gruppo utenti* si possono creare nuovi gruppi utenti e limitarne le autorizzazioni. Con i pulsanti "Record dati precedente" e "Record dati successivo" è possibile alternare fra i gruppi utenti.

- Nome gruppo

  Nome del gruppo.

- Descrizione

  Descrizione del gruppo.

- Utenti

  Utenti già assegnati al gruppo utenti. Con il pulsante "Modifica" si possono aggiungere utenti esistenti al gruppo utenti. Ciò è possibile anche tramite *Modifica/Utenti.*

- Accesso in scrittura

  Se la casella di controllo è attivata, si possono modificare i dati ed eseguire le programmazioni. Se la casella di controllo è disattivata, i dati possono essere soltanto letti o visualizzati.

- Ruolo

  Qui si possono assegnare i diritti ad un gruppo utenti. *Le assegnazioni dei ruoli sono descritte più dettagliatamente nel seguente capitolo* *Ruoli e diritti [▸ 104].*

- Pulsante "Modifica"

  Consente di modificare impostazioni quali "Diritti" o "Nome gruppo".

- Pulsante "Nuovo"

  Crea un nuovo gruppo utenti.

Ruoli e diritti

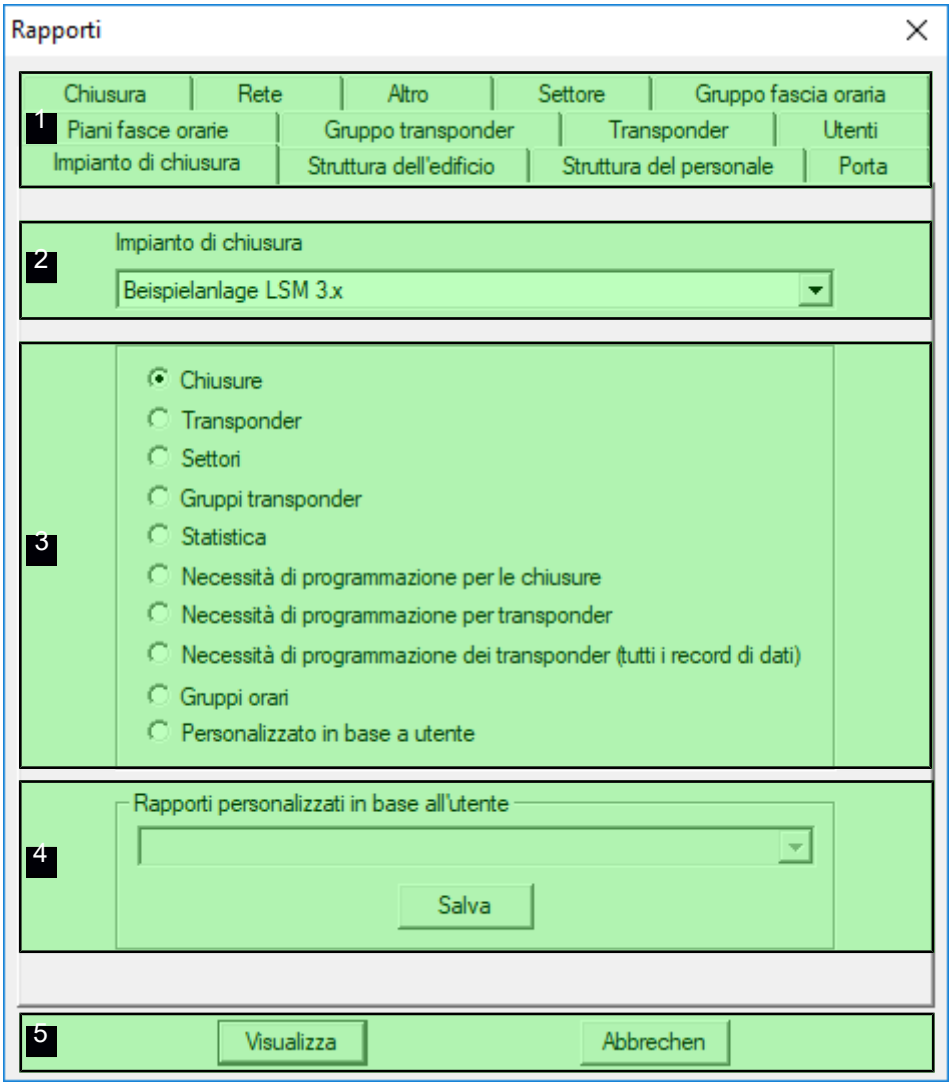
Ruolo	Descrizione
Gestione dell'impianto di chiusura	Gestire le autorizzazioni nella matrice.
Programmazione/lettura di transponder	Consentire la comunicazione fra i transponder e l'LSM mediante un dispositivo di programmazione.
Programmazione/lettura delle chiusure	Consentire la comunicazione fra la chiusura e l'LSM mediante un dispositivo di programmazione.

Modifica di transponder e gruppi	Modificare i transponder e i gruppi transponder.
Modifica di chiusure e settori	Modificare le chiusure e i settori.
Configurazione della rete	Creare e modificare le reti.
Gestione rete	Eseguire compiti, quali ad es. operazioni cumulative o manager eventi tramite le reti configurate.
Amministrazione elenchi accessi	Diritto generale di assegnare a un gruppo utenti l'autorizzazione alla lettura degli elenchi accessi e azionamenti.
Gestione elenchi accessi	Consentire la lettura di elenchi accessi e azionamenti.
Gestione del personale	Modificare le persone.
Utilizzo di LSM Mobile	Consentire l'esportazione o l'importazione da LSM Mobile.
Gestione temporale	Creare e modificare elenchi di giorni festivi, zone temporali e gruppi temporali.
Stampa di report	Consentire la stampa di report ed etichette.
Lettura del protocollo	Accesso al menu "Vista/Protocollo".
Apertura di emergenza	Consentire l'esecuzione di aperture di emergenza.

7.1.6 Report

Per poter utilizzare il sistema di reporting completo, è necessario almeno LSM Basic Online o superiore.

Ogni tipo di report fornisce le seguenti opzioni di scelta:



1. Tipo di report, ad es. un componente SimonsVoss, un edificio, un gruppo transponder ecc.
2. Prima delimitazione all'oggetto del report.
3. Seconda delimitazione all'oggetto esatto del report.
4. Possibilità di selezionare un report definito dall'utente e di memorizzarlo. *SimonsVoss Technologies GmbH offre la possibilità di ordinare report personalizzati definiti dall'utente.*
5. Il pulsante "Visualizza" mostra il report in base ai criteri precedentemente impostati.

L'intestazione e il piè di pagina dei report possono essere adattati in Opzioni/Report.

I report visualizzati possono essere stampati direttamente o esportati in altri formati.

7.1.6.1 Impianto di chiusura

7.1.6.2 Settore

7.1.6.3 Gruppo transponder

7.1.6.4 Porta

7.1.6.5 Chiusura

7.1.6.6 Transponder

7.1.6.7 Gruppo temporale

7.1.6.8 Programma delle fasce orarie

7.1.6.9 Rete

7.1.6.10 Struttura personale

7.1.6.11 Struttura edificio

7.1.6.12 Utenti

7.1.6.13 Varie

Elenco permanenze

Da LSM 3.4 SP2 in poi, è possibile vedere in un report chi si trova attualmente in una zona.

AVVERTENZA

Mancata evacuazione in caso di pericolo

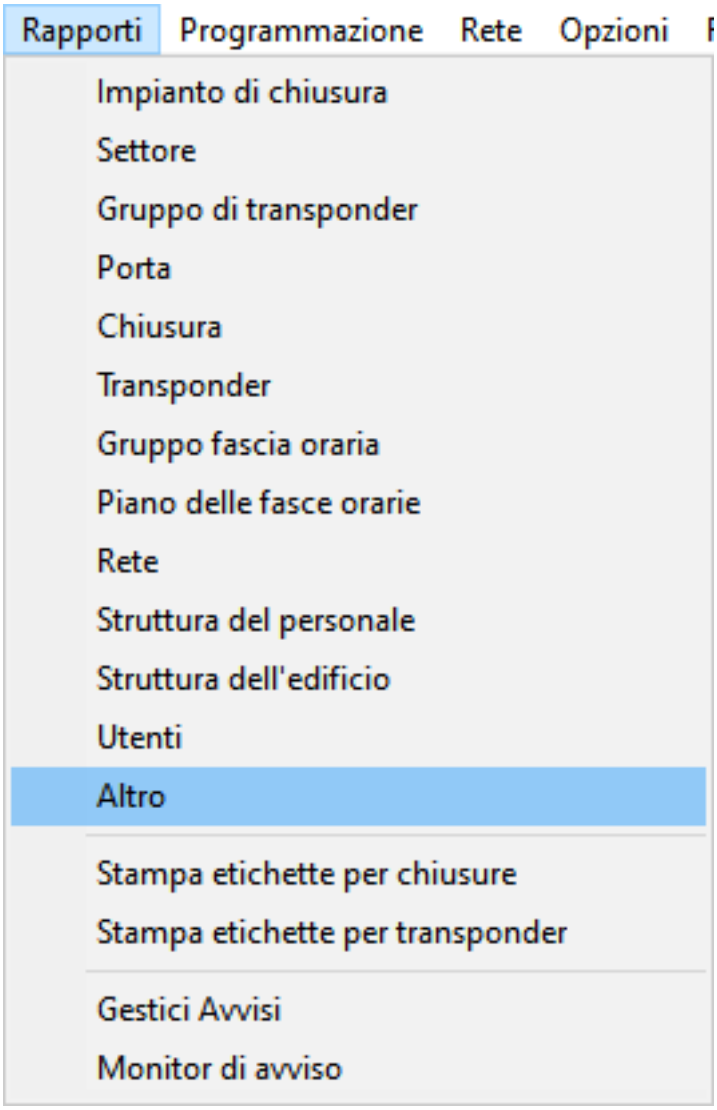
Il report si basa sui dati memorizzati nella banca dati LSM. Queste non devono necessariamente corrispondere allo stato reale, in quanto, ad esempio, le persone che passano attraverso una porta già aperta non possono essere rilevate. Un tornello a tutte le entrate e le uscite aumenta la qualità del report, ma non garantisce che tutte le persone nell'edificio o nell'area siano coperte da esso.

Se viene effettuata un'evacuazione sulla base di questo report, è possibile che le persone non registrate non vengano evacuate.

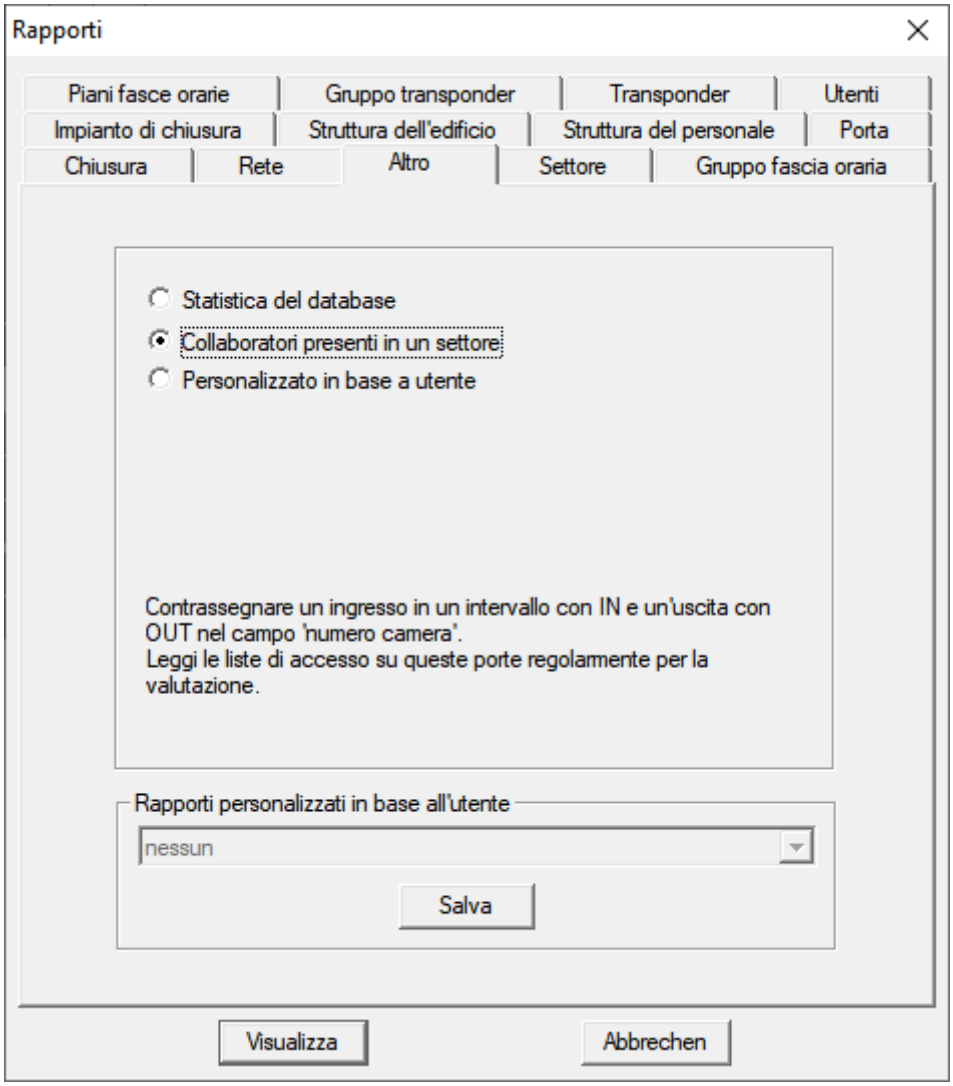
- Non utilizzare il report come sostituto di una lista di evacuazione.

✓ LSM aperto.
✓ Porte e chiusure raggruppate per zone.
✓ I nomi delle aree possono essere identificati senza specificare il sistema di chiusura.
✓ Ingressi e uscite dei campi contrassegnati (vedere *Contrassegnare gli ingressi e le uscite delle aree [▸ 110]*).
✓ Ingressi e uscite nella stessa area.

1. Selezionare da | Rapporti | la voce Altro.



↳ La finestra "Rapporti" si apre con la scheda [Altro].



2. Selezionare l'opzione ◉ Collaboratori presenti in un settore.
3. Fare clic sul tasto Visualizza.

↳ La finestra "Anteprima di stampa" si apre.

Il report contiene le seguenti informazioni:

- Area a cui si riferisce la sezione del report
  - Possessore del mezzo di identificazione
  - Codice dipendente del possessore
  - Ora in cui è stata effettuato l'accesso all'area (data e ora)
  - Porta da cui è stato effettuato l'accesso
  - Luogo
  - Edificio
- Numero di dipendenti nell'area
- Numero totale dei dipendenti

Contrassegnare gli ingressi e le uscite delle aree

È possibile definire le aree. A partire da LSM 3.4 SP2, è possibile creare un elenco di presenza per le rispettive aree. A tal fine è necessario definire le porte attraverso le quali si entra e si esce da un'area.

Definizione degli ingressi

Si definisce un ingresso utilizzando uno dei seguenti metodi:

- Inserire l'espressione *IN* al posto del numero di stanza nelle proprietà della chiusura, nella scheda [Porta].
- Inserire l'espressione *IN* al posto di un nome nelle proprietà della chiusura, nella scheda [Componenti di chiusura].

Definizione delle uscite

Si definisce un'uscita utilizzando uno dei seguenti metodi:

- Inserire l'espressione *OUT* al posto del numero di stanza nelle proprietà della chiusura, nella scheda [Porta].
- Inserire l'espressione *OUT* al posto di un nome nelle proprietà della chiusura, nella scheda [Componenti di chiusura].

NOTA

Priorità nella valutazione delle definizioni

Si possono inserire espressioni a piacere. In primo luogo, LSM valuta l'espressione nel campo del nome della chiusura (scheda [Componenti di chiusura]). Se non viene utilizzata nessuna delle suddette espressioni (IN o OUT), LSM valuta l'espressione nel numero di stanza della porta (scheda [Porta]).

7.1.6.14 Stampa etichette chiusura

Dapprima viene visualizzato un elenco di tutte le chiusure. Si possono selezionare tutte le chiusure o solo alcune.

Con il pulsante "OK" si possono selezionare vari tipi di etichette da stampare.

7.1.6.15 Stampa etichette transponder

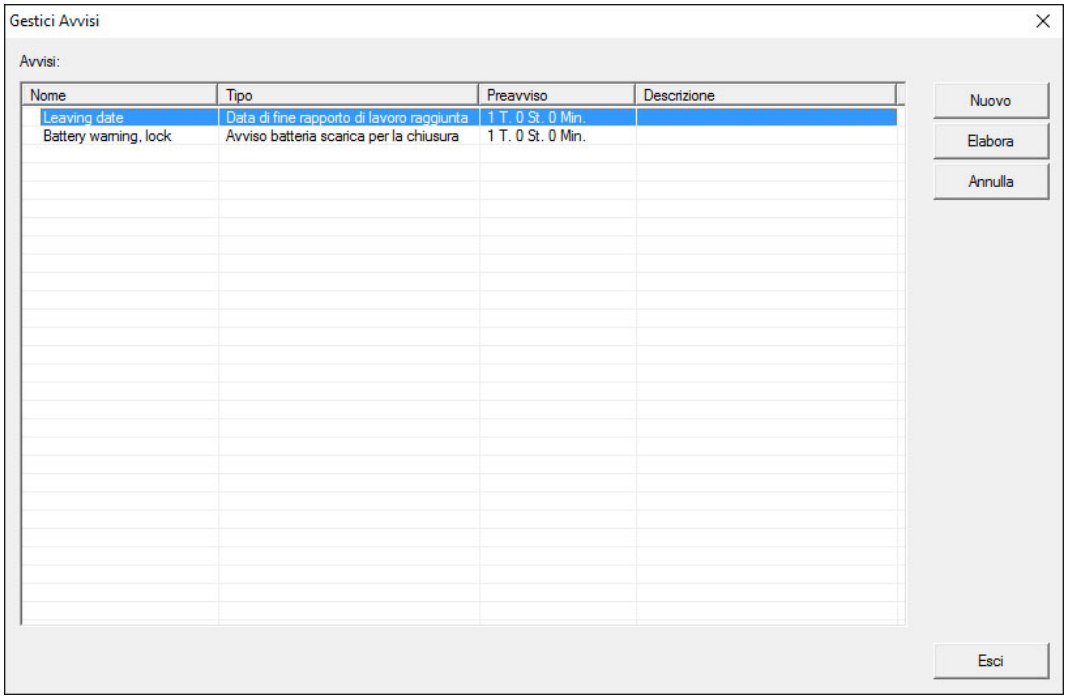
Dapprima viene visualizzato un elenco di tutti i transponder. Si possono selezionare tutti i transponder o solo alcuni.

Con il pulsante "OK" si possono selezionare vari tipi di etichette da stampare.

7.1.6.16 Gestione avvisi

Solo disponibile in LSM Business con modulo Online attivato.

La funzione di avviso offre supporto nell'uso quotidiano di LSM BUSINESS. Si può scegliere di essere avvisati dal sistema in alcune situazioni (ad es. approssimarsi della restituzione del transponder) o altri eventi (avviso batteria chiusura). Gli avvisi vengono visualizzati nel monitor avvisi al momento dell'avvio di LSM. Il monitor avvisi si riapre ogni 15 minuti.



- **Tabella**

  Panoramica degli avvisi creati.

- **Nuovo**

  Creazione di un nuovo avviso.

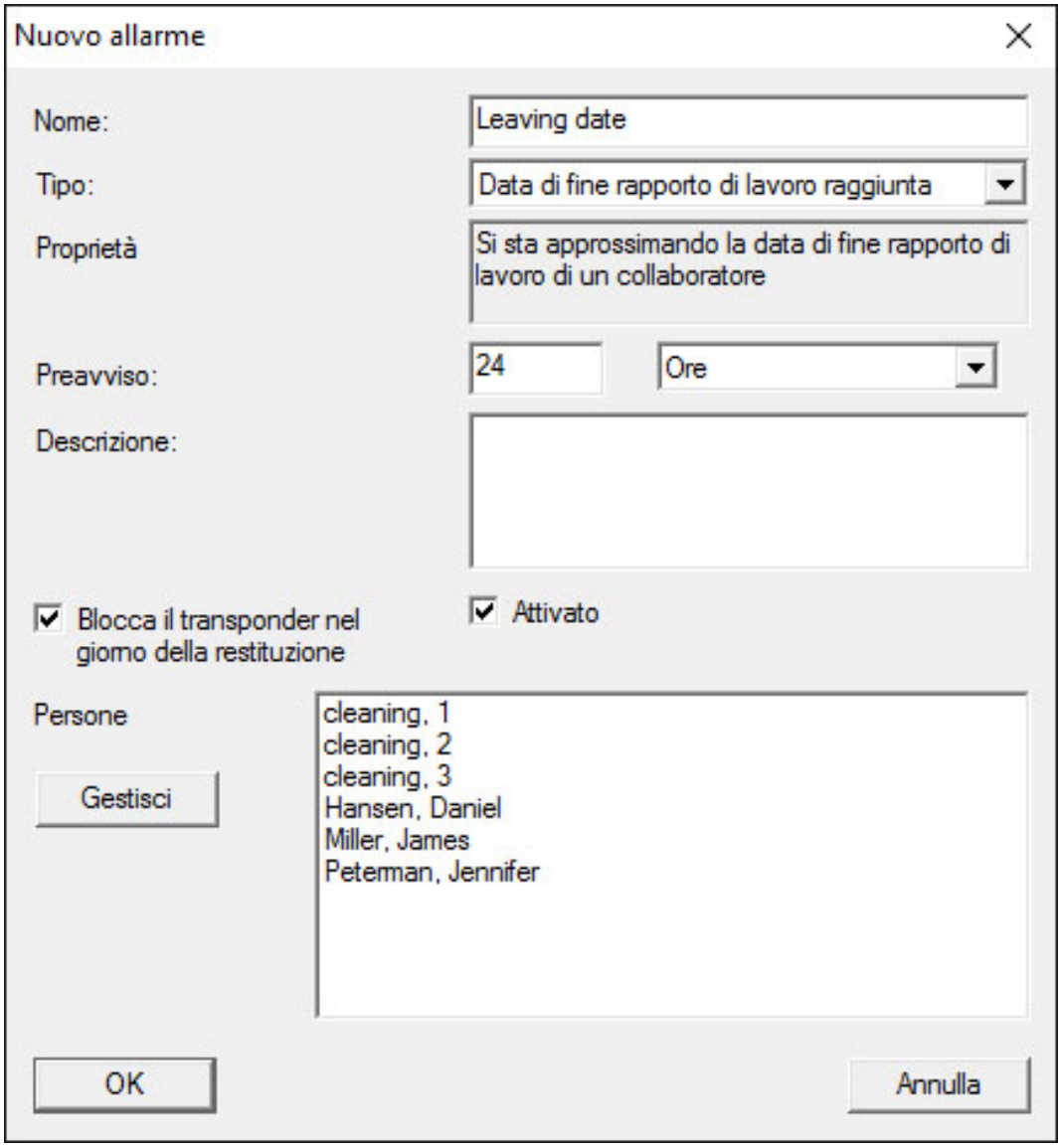
- **Modifica**

  Dopo la selezione dell'avviso si possono modificare le impostazioni.

- **Elimina**

  Dopo averlo selezionato, è possibile cancellare l'avviso.

Con il pulsante "Nuovo" è possibile aggiungere un nuovo avviso:



- **Nome**

  Nome dell'avviso

- **Tipo**

  Tipo di avviso, ad es. avviso batteria chiusura.

- **Proprietà**

  Dipendono dal tipo di avviso.

- **Scadenza**

  Intervallo fra l'avviso e il verificarsi del motivo dell'avviso.

- **Descrizione**

  Campo libero per la descrizione dell'avviso.

- **Blocco transponder il giorno della restituzione**

Il giorno della restituzione, nel piano di chiusura vengono tolte ai transponder le autorizzazioni per le chiusure -> necessità di programmazione.

- **Attivato**

  Se impostato, l'avviso viene applicato.

- **Gestisci**

  Selezione degli oggetti da monitorare.

- **Tabella**

  Visualizzazione dei componenti selezionati.

Si possono selezionare i seguenti tipi di avviso:

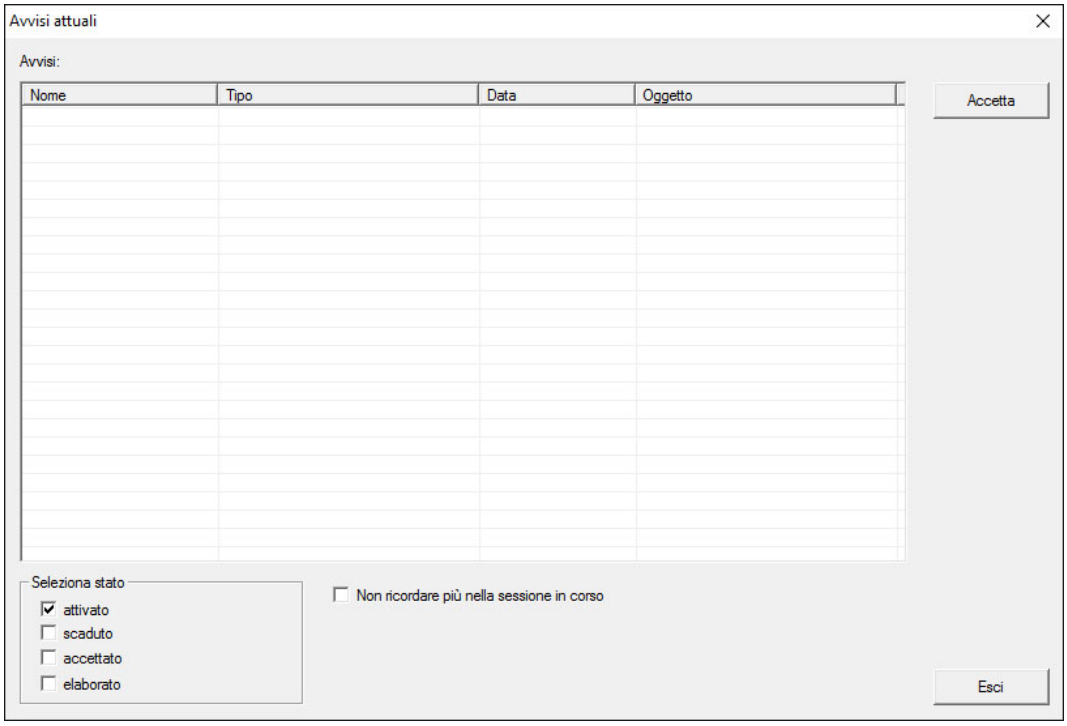
- Data di licenziamento raggiunta
- Avviso batteria chiusura
- Avviso batteria transponder
- Esportazione su handheld PDA
- Cambio batteria programmato
- Restituzione transponder prossima
- Data di scadenza transponder

7.1.6.17 Videata allarmi

Disponibile soltanto nell'LSM Business con modulo online attivato.

Nella videata allarmi vengono visualizzati gli allarmi intervenuti e attivi. La videata degli allarmi si apre automaticamente dopo il login e presenta tutti gli allarmi cumulati. Selezionando la visualizzazione di stato si possono vedere anche allarmi già confermati o cessati. Facendo doppio click sulla voce, aprite le proprietà del relativo oggetto.

Tramite *Report/Videata allarmi* si può aprire la videata degli allarmi:



- **Tabella**

  Prospetto degli allarmi cumulati

- **Accetta**

  Si possono accettare singoli allarmi , che con l'accettazione vengono nascosti.

- **Attivo**

  Vengono visualizzati solo gli allarmi in corso.

- **Cessato**

  Gli allarmi già cessati sono allarmi, il cui tempo di impostazione è già trascorso.

- **Accettato**

  Vengono visualizzati gli allarmi già accettati.

- **Processato**

  Gli allarmi già processati sono allarmi per i quali si è già espletato un task sequenziale (es.: “Blocco dei transponder”).

7.1.7 Programmazione

7.1.7.1 Transponder

Questa funzione è attivabile solo se è stato selezionato un transponder nella matrice. Nell'elenco a discesa è selezionato direttamente il transponder scelto nella matrice. Fare clic sul pulsante "Programma" per avviare l'operazione di programmazione per il transponder selezionato nell'elenco a discesa.

Se si desiderano programmare più transponder in successione, si può iniziare con il primo transponder e selezionare l'opzione "Salta al transponder successivo dopo la programmazione".

7.1.7.2 Chiusura

Questa funzione è attivabile solo se è stata selezionata una chiusura nella matrice. Nell'elenco a discesa è selezionata direttamente la chiusura scelta nella matrice. Fare clic sul pulsante "Programma" per avviare l'operazione di programmazione per la chiusura selezionata nell'elenco a discesa.

Nel campo "Dispositivo di programmazione", selezionare il dispositivo da utilizzare per la programmazione.

7.1.7.3 Imposta ora

Per impostare l'ora o leggere l'elenco accessi, leggere la chiusura selezionata nella matrice.

7.1.7.4 Leggi chiusura

Con questo comando, una chiusura viene letta direttamente con il dispositivo di programmazione standard (SmartCD.G2).

NOTA

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

7.1.7.5 Leggi chiusura Mifare

Con questo comando, una chiusura Mifare passiva viene letta direttamente con il dispositivo di programmazione passivo (SmartCD.MP).

NOTA

Tenere la parte elettronica della chiusura (riconoscibile, ad es., nel cilindro dall'anello nero fra l'alloggiamento PZ e il pomolo) direttamente sul simbolo dell'antenna del dispositivo di programmazione!

7.1.7.6 Leggi transponder

Con questo comando, un transponder viene letto direttamente con il dispositivo di programmazione standard (SmartCD.G2). Osservare le istruzioni del software LSM.

7.1.7.7 Leggi scheda G1

Con questo comando, una scheda G1 viene letta direttamente con il dispositivo di programmazione CD.MIFARE *(non più disponibile)*. Osservare le istruzioni del software LSM.

7.1.7.8 Leggi scheda G2

Con questo comando, una scheda G2 viene letta direttamente con il dispositivo di programmazione SmartCD.HF. Osservare le istruzioni del software LSM.

Nei componenti ibridi, oltre allo SmartCD.HF deve essere collegato al computer anche lo SmartCD.G2.

7.1.7.9 Funzioni speciali

Leggi Compact Reader

Legge un Compact Reader.

Transponder di attivazione

Questa funzione consente di creare un transponder di attivazione. Con un transponder di attivazione si possono riattivare le chiusure disattivate. Per aprire la chiusura è necessario anche un transponder autorizzato!

Scheda di attivazione G2

Questa funzione consente di creare una scheda di attivazione G2. Con una scheda di attivazione G2 si possono riattivare le chiusure disattivate. Per aprire la chiusura è necessaria anche una scheda G2 autorizzata.

Transponder per sostituzione batteria G2

Dopo che la chiusura è passata in modalità Freeze in seguito ad uno stato batteria critico, può essere riattivata solo con l'ausilio di un transponder per sostituzione batteria. Per aprire la chiusura è necessario anche un transponder autorizzato!

Scheda per sostituzione batteria G2

Dopo che la chiusura è passata in modalità Freeze in seguito ad uno stato batteria critico, può essere riattivata solo con l'ausilio di una scheda per sostituzione batteria G2. Per aprire la chiusura è necessaria anche una scheda G2 autorizzata.

7.1.7.10 Esegui apertura di emergenza

È possibile aprire una chiusura con il software LSM e il rispettivo dispositivo di programmazione. Tenere presente che a tale scopo va immessa la password dell'impianto di chiusura.

7.1.7.11 Test SmartCD attivo

Questa funzione consente di testare la funzionalità di un dispositivo di programmazione SmartCD.G2 collegato.

7.1.7.12 Test SmartCD Mifare

Questa funzione consente di testare la funzionalità di un dispositivo di programmazione SmartCD.MP o SmartCD.HF collegato. Fare attenzione che al momento del test sia collegato solo uno dei dispositivo di programmazione passivi.

7.1.7.13 LSM Mobile

Con un laptop, netbook o PDA con sistema operativo Microsoft Windows è possibile esportare i task di programmazione dal software LSM. In questo modo è possibile, ad esempio, programmare in parallelo più componenti SimonsVoss con dispositivi mobili.

Esportazione in LSM Mobile

Esporta i comandi di programmazione di un impianto di chiusura.

Importazione da LSM Mobile

Reimporta nel software LSM i task di programmazione eseguiti.

Task esportati

Mostra le attuali esportazioni dei task di programmazione a LSM Mobile.

7.1.7.14 Rete virtuale

Per ulteriori informazioni consultare anche qui: *Gestione della rete virtuale (VN) [▸ 225]*

Esportazione su rete VN

Importazione - sincronizzazione

Reset task VN

Task VN esportati

7.1.8 Opzioni

7.1.8.1 Metodi di lavoro conformi alla protezione dei dati secondo il RGPD

Vedi *Metodi di lavoro conformi alla protezione dei dati secondo il RGPD [▸ 145]*.

7.1.8.2 Stampa matrice

La matrice può essere stampata solo se al momento è visualizzata la vista matrice.

7.1.8.3 Registrazione

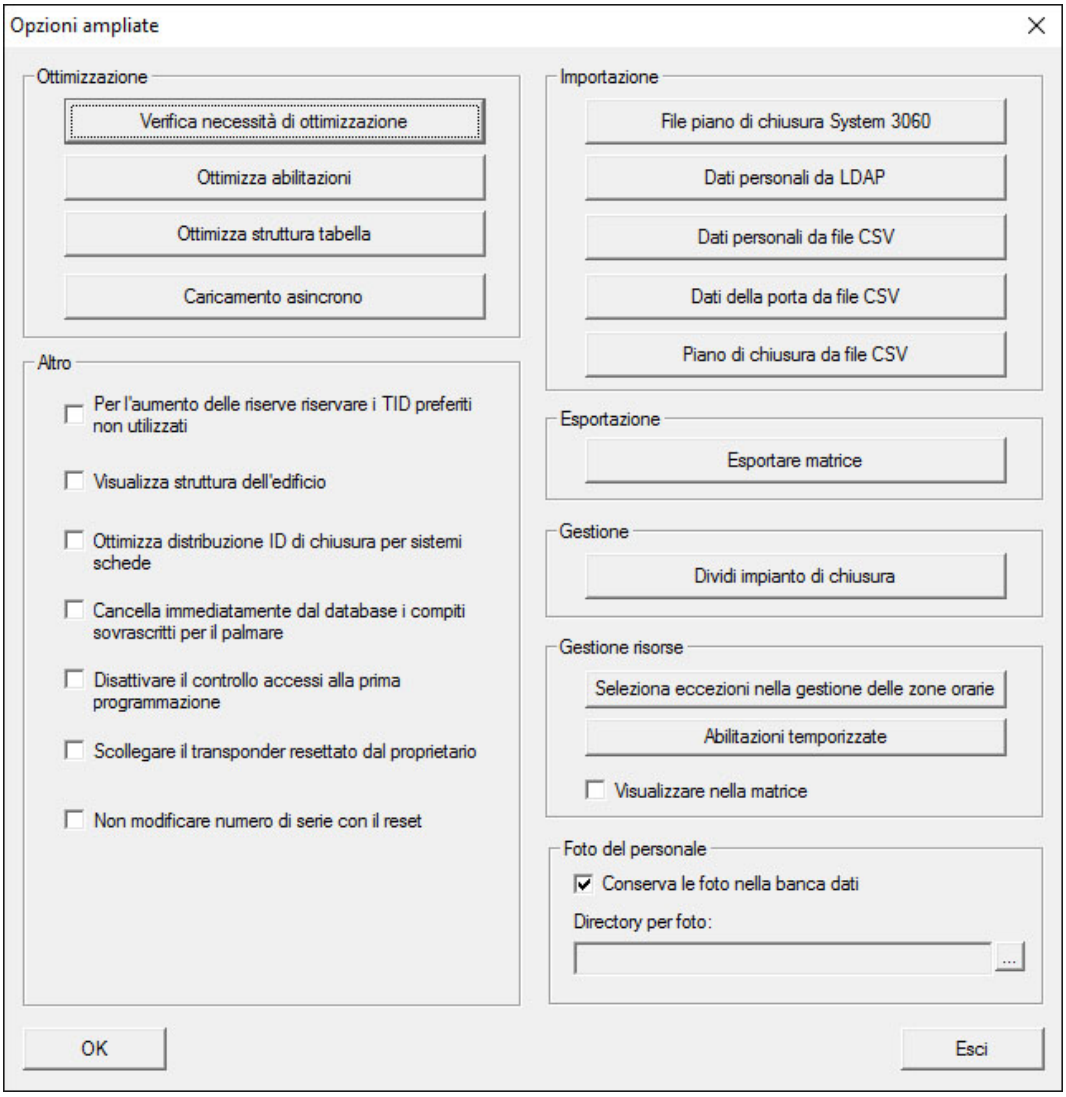
In questo punto è possibile indicare quali voci del protocollo debbano essere salvate e per quanto tempo. Di norma tutte le registrazioni vengono salvate per 180 giorni. È possibile impostare intervalli compresi fra 7 e 670 giorni.

7.1.8.4 Numerazione automatica

I nuovi componenti presentano di serie una numerazione progressiva. In questo campo opzionale è possibile definire la sintassi dei diversi componenti.

7.1.8.5 Ampliate

Assicurarsi che prima di eseguire l'ottimizzazione del database sia stato effettuato sempre un backup dati aggiornato e funzionante.



Verifica necessità di ottimizzazione

Per gli utenti che utilizzano il software LSM già da tempo si pone occasionalmente il problema della corretta performance dell'applicazione database. In seguito alle ristrutturazioni, può avvenire che più dati (crocette delle autorizzazioni) sovraccarichino il database. Può così avvenire che ad un gruppo transponder venga assegnata un'autorizzazione e ad una persona di questo gruppo venga assegnata un'apposita autorizzazione singola. Ciò significa che una persona può avere due distinte autorizzazioni per la stessa porta. Oltre a generare confusione, ciò risulta anche superfluo.

Fare clic sul pulsante "Verifica necessità di ottimizzazione" per controllare se sia necessario ottimizzare l'impianto di chiusura. Osservare altresì le istruzioni del software LSM.

Ottimizza autorizzazioni

Eseguire questo comando se consigliato dalla verifica della necessità di ottimizzazione.

Fare clic sul pulsante "Ottimizza autorizzazioni" per controllare se sia necessario ottimizzare le autorizzazioni. Osservare altresì le istruzioni del software LSM.

Ottimizza struttura tabelle

In caso di prolungato utilizzo di un database, si possono verificare irregolarità in alcune tabelle. Grazie all'ottimizzazione della struttura, gli indici delle tabelle vengono reimpostati, eliminando le eventuali incoerenze dei dati.

Caricamento asincrono

Funzione al momento non supportata.

Varie

- **Usa preferibilmente TID inutilizzati in caso di aumento della riserva**

  In caso di aumento della riserva di un gruppo transponder, vengono utilizzati TID non ancora impiegati all'interno dell'impianto di chiusura (purché vi siano TID disponibili). In caso di casella di controllo non attivata, si utilizzano anche TID già programmati in precedenza in una chiusura ma che al momento non sono utilizzati.

- **Mostra struttura edificio**

  Con casella di controllo attivata, all'interno della maschera "Gestisci WaveNet" nella colonna "Porta" viene visualizzata, prima del nome porta, la sigla dell'edificio e del piano della porta selezionata (se disponibile).

- **Ottimizza distribuzione degli ID chiusura per i sistemi a schede**

  Con casella di controllo attivata e configurazione impostata nella gestione schede G2 con "L" o "L_AV", in caso di creazione di nuove chiusure G2 i LID devono essere assegnati come segue:

  - in caso di chiusure ibride e Mifare si utilizza il successivo LID libero.
  - In caso di chiusure con tecnologia attiva, si assegna un LID superiore all'intervallo LID indicato nella gestione schede G2 alla voce "ID chiusura".

- **Elimina immediatamente dal database i task sovrascritti per LSM Mobile**

  Con casella di controllo attivata, nella maschera "Attività esportate" viene eliminata l'attività di esportazione precedente per lo stesso utente GUI (in caso di nuova esportazione).

NOTA

Le attività di esportazione per lo stesso utente eseguite prima dell'impostazione del segno di spunta non vengono eliminate automaticamente!

- **Disattiva il controllo accessi alla prima programmazione**

  Attivare questa casella di controllo se non si desidera, in generale, un controllo accessi nell'impianto di chiusura, ma si desidera utilizzare la gestione delle fasce orarie. Al momento della creazione di nuove chiusure questa funzione viene automaticamente disattivata.

- **Scollega il transponder resettato dal proprietario**

  Attivare questa casella di controllo se il transponder dopo il reset deve essere scollegato dal proprietario e il numero di serie del transponder deve essere sostituito dalla data attuale + ora.

- **Non modificare numero di serie con il reset**

  Attivare questa casella di controllo se il numero di serie di un transponder (per motivi di revisione) non deve essere modificato con il reset.

File piano di chiusura sistema 3060

Importazione di un qualsiasi piano di chiusura da un database LDB *(software precedente a LSM: Locking Database Software)*.

Dati personali da LDAP

Se in un server vengono forniti dati personali tramite LDAP, quest'ultimi possono essere importati con il pulsante "Dati personali da LDAP" nel software LSM.

Dati personali da file CSV

Questo pulsante permette di importare dati personali (cognome, nome, ufficio, numero personale ecc.) da un file CSV nel software LSM.

Dati porta da file CSV

Questo pulsante permette di importare dati porta (porta, numero di stanza, dimensioni interne ecc.) da un file CSV nel software LSM.

Piano di chiusura da file CSV

Questo pulsante permette di importare piani di chiusura da un file CSV nel software LSM.

Esporta matrice

Questo pulsante consente di esportare la matrice o il piano di chiusura in un file CSV. Fare attenzione che siano esportati solo i contenuti dei settori e gruppi transponder aperti nella matrice.

Suddividi impianto di chiusura

Qui è possibile suddividere un impianto di chiusura esistente in due impianti. Ciò risulta utile, ad es. quando nell'immobile arriva un nuovo inquilino che desidera gestire autonomamente una parte dell'impianto di chiusura già presente.

Seleziona eccezioni nella gestione fasce orarie

Se ad un gruppo transponder è stato assegnato un gruppo temporale, questa funzione consente di ritirare ai singoli transponder di tale gruppo l'assegnazione al gruppo temporale in determinate chiusure G2.

Autorizzazioni temporizzate

Con questa funzione si possono consentire o bloccare (in stato nominale!) singole crocette di autorizzazione in un determinato momento. Ciò ha senso solo in caso di chiusure collegate in rete, poiché dopo la modifica delle autorizzazioni le chiusure vanno programmate tempestivamente affinché la modifica sia applicata.

Foto personali

Di norma le foto personali vengono salvate direttamente nel database. Esiste tuttavia la possibilità di salvare le foto personali in una qualsiasi directory di propria scelta.

7.1.8.6 Report

Qui si inseriscono centralmente tutti i dati che devono essere emessi nel report.

In LSM BUSINESS, i dati possono essere impostati singolarmente o contemporaneamente per tutti i report.

7.1.8.7 Elenchi accessi

È possibile delimitare gli elenchi accessi. Si possono registrare, ad es., gli accessi avvenuti solo in un determinato momento del giorno o un numero massimo di accessi alla chiusura.

Attenersi al numero massimo di accessi memorizzabili nelle rispettive chiusure.

7.1.8.8 Sicurezza password utente

Quest'opzione consente di garantire una protezione ancora superiore all'intero impianto di chiusura.

- **Cambio password periodico**

  Attivare l'opzione per obbligare gli utenti a modificare la password dopo un determinato periodo di tempo.

- **Utilizza storico password delle ultime 10 password**

  Attivare l'opzione per impedire l'uso delle ultime 10 password.

- **Password errata per tre volte**

  Attivare l'opzione per bloccare un utente dopo tre tentativi errati di immissione della password.

- **Sicurezza password elevata**

  Consente solo l'uso di password con elevato livello di sicurezza.

7.1.9 Rete

L'uso delle reti (ad es. WaveNet o VN) può risultare molto complesso. Per l'uso delle reti, consultare il manuale WaveNet.

7.1.9.1 Attivazione della chiusura

Qui è possibile

- attivare
- disattivare
- aprire in remoto le chiusure della rete

7.1.9.2 Task cumulativi

Con la voce Task cumulativi è possibile avviare contemporaneamente un'operazione quale la programmazione di più chiusure.

7.1.9.3 Manager eventi

- *Configurazione dell'Event management (eventi) [▸ 215]*
- *Creazione di una reazione [▸ 218]*

7.1.9.4 Manager dei compiti

Solo disponibile in LSM Business con modulo Online attivato.

- *Configurazione dell'Event management (eventi) [▸ 215]*
- *Lettura della chiusura [▸ 251]*

7.1.9.5 Notifiche e-mail

Solo disponibile in LSM Business con modulo Online attivato.

7.1.9.6 Servizio VN

Impostazioni avanzate per la rete virtuale.

7.1.9.7 Nodi di comunicazione

Questa selezione permette di definire i nodi di comunicazione e i rispettivi dispositivi di connessione (ad es. RouterNode o CentralNode).

7.1.9.8 Collegamenti locali

Qui si gestiscono i collegamenti locali del PC/server.

7.1.9.9 Gestione WaveNet

Con "Gestione WaveNet" è possibile creare la topologia della rete WaveNet ed eseguire ulteriori impostazioni.

7.1.9.10 WaveNet Manager

Quest'azione avvia il WaveNet Manager. Il WaveNet Manager deve essere installato separatamente.

7.1.9.11 Importa topologia WaveNet

Quest'azione apre una finestra per l'importazione di topologie WaveNet.

7.1.9.12 Gestione rete LON

Qui si possono gestire centralmente le reti LON obsolete.

7.1.9.13 Impostazioni Terminalserver-Client

7.1.10 Finestre

Alterna la visualizzazione delle finestre aperte.

7.1.11 Guida

7.1.11.1 Argomenti della guida

Argomenti della guida sull'uso del software LSM.

7.1.11.2 Supporto online SimonsVoss

SimonsVoss offre un servizio di supporto online per la rapida risoluzione dei problemi. Questa funzione consente di avviare una conversazione gratuita con TeamViewer via Internet. Per poterla utilizzare, il computer deve

disporre di una connessione a Internet. Un addetto all'assistenza si collegherà per breve tempo al PC del cliente, su sua autorizzazione, per aiutarlo a risolvere il problema.

NOTA

Prima di lanciare il supporto online, mettersi in contatto prima con SimonsVoss Technologies GmbH (Vedi *Supporto e ulteriori informazioni [▸ 259]*)!

7.1.11.3 SimonsVoss nel web

Mostra la homepage di SimonsVoss (Vedi anche *Supporto e ulteriori informazioni [▸ 259]*). Per poter utilizzare questa funzione, il computer deve disporre di una connessione a Internet.

7.1.11.4 Info su LockSysMgr...

Mostra la versione software e driver del software LSM utilizzato.

7.1.11.5 Registrazione

Mostra i moduli registrati (Vedi anche Registrazione LSM). Qui è anche possibile disattivare i client attivati.

7.1.11.6 Panoramica versioni

Mostra la versione di tutti i software LSM installati.

7.1.11.7 FAQ

Mostra il database delle FAQ SimonsVoss nel browser (Vedi anche *Supporto e ulteriori informazioni [▸ 259]*). Per poter utilizzare questa funzione, il computer deve disporre di una connessione a Internet.

7.1.11.8 Controlla aggiornamenti

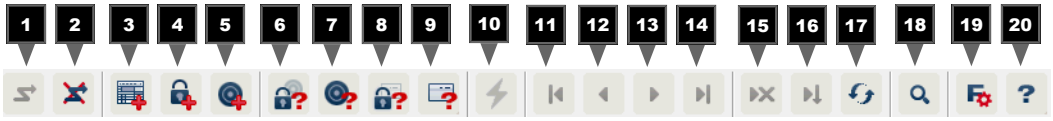
Verifica gli eventuali aggiornamenti disponibili per il software LSM installato. Per poter utilizzare questa funzione, il computer deve disporre di una connessione a Internet.

7.1.11.9 Report database

Esporta un report in formato CSV.

7.2 Barra multifunzione

Nella barra multifunzione si possono richiamare direttamente le funzioni più importanti e utilizzate.



1. Login
2. Logout
3. Nuovo impianto di chiusura
4. Nuova chiusura
5. Nuovo supporto di identificazione *(ad es. transponder o scheda)*
6. Leggi chiusura
7. Leggi transponder
8. Leggi chiusura MIFARE
9. Leggi scheda/tag G2
10. Programmazione
11. Primo record dati
12. Record dati precedente
13. Record dati successivo
14. Ultimo record dati
15. Rimuovi
16. Applica
17. Aggiorna
18. Cerca
19. Filtri
20. Guida

7.3 Impianto di chiusura

In questa sezione si può scegliere fra i diversi impianti di chiusura all'interno di un progetto. È inoltre possibile visualizzare le proprietà del rispettivo impianto di chiusura e modificarle a posteriori.

7.4 Gruppi e settori

Queste sezioni contengono una guida alla navigazione in cui i due raggruppamenti (gruppi transponder e settori) sono raffigurati tramite una rappresentazione ad albero.

Le dimensioni della finestra possono essere modificate trascinando il mouse sulla barra di separazione fra i settori e i gruppi transponder e fra la matrice e l'area di navigazione.

Per muoversi in modo efficace e sicuro all'interno della struttura ad albero, nella vista ad albero sono rappresentati vari simboli a seconda dello stato di visualizzazione:

	Gruppi transponder impianto di chiusura
	Gruppo transponder senza transponder
	Gruppo transponder nascosto
	Gruppo transponder visualizzato

	Settore impianto di chiusura
	Settore senza porte
	Settore nascosto
	Settore visualizzato

Procedura:

I settori e i gruppi transponder suddivisi in un massimo di 6 livelli sono ammessi solo in LSM BUSINESS.

- Per visualizzare il successivo livello inferiore del raggruppamento suddiviso, fare clic sul segno Più a sinistra accanto al simbolo rosso.
- Facendo nuovamente clic sugli altri segni Più si può accedere ad altri livelli più bassi. La massima profondità della gerarchia prevede 6 livelli.
- Facendo clic sul segno Meno a sinistra accanto al simbolo blu i livelli inferiori vengono chiusi.
- Facendo doppio clic sul segno Meno accanto all'impianto di chiusura, tutti i raggruppamenti aperti vengono chiusi.
- Facendo doppio clic su un settore o un gruppo, la visualizzazione cambia in modo corrispondente (visualizzazione attiva o non attiva dei contenuti nella matrice).
- È anche possibile ottenere rapidamente una panoramica generale aprendo l'intera struttura ad albero:
  - Vista/Tutti i settori inferiori/Apri gruppi
- Per richiudere tutti i settori o gruppi aperti è necessario chiudere il gruppo più in alto nella struttura ad albero.

Tenere presente che in caso di aumento delle dimensioni della struttura ad albero, anche il tempo necessario alla preparazione dei dati da visualizzare e alla rappresentazione sullo schermo sarà maggiore. Tale fenomeno si può osservare sia in caso di nuova struttura che di aggiornamento della vista.

7.5 Matrice

Questa vista crea una matrice che visualizza le strutture gerarchiche del personale e dei locali ed è in grado di autorizzare gruppi completi di transponder per settori completi. In questo modo, nella vista Settori/Gruppi transponder si possono creare autorizzazioni di base in modo semplice e rapido. Qualora sia necessario assegnare autorizzazioni diverse sotto forma di estensioni o limitazioni specifiche, è possibile farlo nella vista Porte/Persone.

Vista Porte/persone

✕	Autorizzazione impostata, ma non ancora programmata nella chiusura.
✕	Autorizzazione programmata nella chiusura.
✕	Autorizzazione eliminata e non ancora trasferita alla chiusura.
✕	Le autorizzazioni non ancora programmate, conformi alla struttura di gruppo dell'impianto di chiusura e provenienti quindi dalla vista gruppo, sono contrassegnate da un piccolo triangolo nero.
✕	Le autorizzazioni programmate, conformi alla struttura di gruppo dell'impianto di chiusura e provenienti quindi dalla vista gruppo, sono contrassegnate da un piccolo triangolo nero.
✕	Autorizzazioni rimosse, conformi alla struttura di gruppo dell'impianto di chiusura e non ancora programmate.
✕	Le autorizzazioni non conformi alla struttura di gruppo dell'impianto di chiusura, presentano solo la crocetta, ma non il triangolo nero (autorizzazione singola).
	Le autorizzazioni che, rispetto alla struttura di gruppo dell'impianto di chiusura, sono state successivamente ritirate presentano il triangolo nero, ma non più la crocetta dell'autorizzazione.
	Casella a righe (disattivata): Non è possibile impostare autorizzazioni. Non si possiede alcun diritto di scrittura o il piano di chiusura blocca la casella (ad es. in caso di transponder disattivato o scheda G2 su cilindro attivo).

Vista Settori/Gruppo transponder

✕	La crocetta nera con cerchio interno rappresenta un'autorizzazione di gruppo.
✕	La crocetta grigia con cerchio interno simboleggia un'autorizzazione "ereditata".

Vista ad albero autorizzazione di gruppo

✔	impostata manualmente (nera)
✔	eredita direttamente (verde)
✔	Ereditata indirettamente – tramite gruppo inferiore (blu)
✔	Ereditata sia direttamente che indirettamente (blu/verde)

Necessità di programmazione

Può essere necessario eseguire la programmazione di un transponder o di una chiusura per varie ragioni. Per distinguere i vari motivi della necessità di programmazione, il simbolo del lampo viene rappresentato con colori diversi.

⚡	Necessità di programmazione di un componente (giallo)
⚡	▪ Necessità di programmazione del transponder (rosso): ▪▪ Validità scaduta ▪▪ Disattivato ▪ Chiusura (rossa): ▪▪ Solo livello di chiusura trasversale assegnato ▪▪ Non assegnata ad alcuna porta ▪▪ Non assegnata ad alcun impianto di chiusura ▪▪ Porta senza chiusura
⚡	Necessità di programmazione di una chiusura dopo la creazione di un transponder sostitutivo in modalità Overlay di un impianto G1

▪ Facendo doppio clic su un componente della matrice è possibile passare direttamente alle proprietà dell'oggetto.

8. Conoscenze generali sull'LSM

Nel presente capitolo sono descritte alcune procedure teoriche mirate ad agevolare l'uso del software LSM.

8.1 Autorizzazioni di gruppo

Con un'autorizzazione di gruppo è possibile autorizzare un gruppo completo di transponder per un'intera area. In questo modo è possibile creare le autorizzazioni di base nel piano di chiusura in modo molto rapido e chiaro. Qui è utile essere chiari in anticipo sull'uso previsto dell'edificio e sulla struttura organizzativa dell'azienda al momento dell'assegnazione delle autorizzazioni. Un sistema chiaramente strutturato contribuisce in modo significativo a rilasciare dichiarazioni rapide e precise sui possibili accessi in un secondo momento della giornata e consente la routine quotidiana nell'azienda o nell'organizzazione. Le eccezioni alle autorizzazioni di gruppo possono, in *Vista/Porte/Persone* essere modificate in qualsiasi momento, anche in un secondo tempo, rimuovendo o aggiungendo una singola croce di autorizzazione

Aree e gruppi di transponder

Un caso applicativo tipico è il seguente: Un'azienda è composta da diversi reparti con dipendenti che hanno bisogno di accedere a uno, più o tutti i reparti. Sarebbe possibile autorizzare ogni singolo transponder di un dipendente presso i singoli sistemi di chiusura, ovvero quelli a cui è richiesto l'accesso. Tuttavia, l'onere amministrativo aumenta con il numero di transponder.

È molto più comodo lavorare con aree e gruppi di transponder. Ciò significa che un'autorizzazione, l'autorizzazione di gruppo, deve essere assegnata una sola volta. Ogni transponder assegnato a questo gruppo ha automaticamente gli stessi diritti del gruppo. Lo stesso vale per le chiusure. Se un sistema di chiusura è assegnato ad un'area, tutti i transponder autorizzati per quest'area sono autorizzati anche per questo sistema di chiusura.

Esempio: il personale addetto alle pulizie dovrebbe essere autorizzato ad entrare anche nelle stanze del Servizio di assistenza. L'azienda è logicamente divisa in reparti:

- Sviluppo
- Marketing
- Vendita
- Servizio di assistenza
- Area ad alta sicurezza
- Produzione

Tutti i transponder del personale addetto alle pulizie sono riuniti in un gruppo di transponder Personale di pulizia. Allo stesso modo, tutte le chiusure che appartengono ai rispettivi reparti vengono assegnate ad un'area al momento della loro creazione, ad esempio il Servizio di assistenza. Supponiamo che il reparto del Servizio di assistenza abbia dieci chiusure e che ci siano dieci addetti alle pulizie che lavorano in azienda. Se queste dovessero essere autorizzate individualmente, dovrebbero essere assegnate e gestite un centinaio di autorizzazioni. Se invece il personale addetto alle pulizie del gruppo di transponder viene semplicemente assegnato all'area del servizio di assistenza, è necessario rilasciare una sola autorizzazione affinché il personale addetto alle pulizie abbia accesso all'area del servizio di assistenza.

8.1.1 Riserve gruppo (solo G1)

Assegnando un transponder ad un gruppo, il transponder ottiene immediatamente tutte le autorizzazioni assegnate al gruppo stesso. Se un nuovo transponder viene assegnato ad un gruppo, nelle chiusure interessate si verificherà una necessità di programmazione. Per evitare che ciò accada, ai gruppi è possibile assegnare i cosiddetti "ID transponder di riserva" durante la creazione (e anche successivamente). Tali ID transponder non sono ancora assegnati ad una persona. Le riserve vengono specificate nelle chiusure durante la programmazione, risultando così disponibili.

Se a questo punto un ID transponder di riserva viene assegnato ad una persona e il transponder viene programmato, nelle chiusure non vi sarà alcuna necessità di programmazione. I transponder possono così essere autorizzati ed attivati nelle chiusure automaticamente, senza che l'utente debba compiere altre operazioni, quali la programmazione della chiusura.

8.1.2 Eredità

L'eredità è la possibilità di rappresentare la gerarchia di un'azienda nell'impianto di chiusura. Se applicata correttamente, l'eredità semplifica notevolmente il lavoro dell'utente. Essa consente infatti di automatizzare determinati processi tramite l'assegnazione di un transponder ad un certo gruppo transponder. L'eredità si può applicare in caso di utilizzo di una gerarchia nei gruppi transponder e nei settori. L'eredità si basa sulle autorizzazioni di gruppo; le autorizzazioni singole non vengono ereditate.

8.2 Autorizzazioni nel protocollo G2

Nel protocollo G2 le autorizzazioni vengono salvate in tutti i componenti. Ciò consente di azionare un nuovo transponder in una chiusura autorizzata senza dover riprogrammare la chiusura. I blocchi (i cosiddetti ID di blocco)

vengono trasferiti analogamente. Dopo che un nuovo transponder è stato azionato per la prima volta nella chiusura, l'autorizzazione originaria viene eliminata nella chiusura.

8.3 Programmi delle fasce orarie

Il software LSM offre la possibilità di autorizzare i transponder nelle chiusure solo in determinati orari.

Esempio: Un addetto alle pulizie possiede un transponder autorizzato solo nei locali da pulire. Le stanze devono essere pulite solo di lunedì, mercoledì e venerdì fra le 16:00 e le 20:00.

È a questo punto che entrano in gioco i programmi delle fasce orarie. Di seguito si descrive in modo esemplificativo l'uso dei programmi delle fasce orarie. Si illustrerà inoltre il diverso comportamento dei programmi delle fasce orarie nei vari componenti SimonsVoss:

I programmi delle fasce orarie dovrebbero essere possibilmente semplici. In genere, i programmi delle fasce orarie vengono creati per le chiusure. Nel programma delle fasce orarie della chiusura vengono a loro volta creati singoli gruppi temporali. In questi gruppi si descrivono gli orari in cui il transponder può essere autorizzato.

Per mantenere il programma delle fasce orarie il più possibile semplice e generico si utilizzano interi settori anziché singole chiusure. Parallelamente, a determinati gruppi temporali non vengono assegnati singoli transponder, ma interi gruppi transponder. Nell'esempio, la situazione si presenterebbe così:

Creazione di un programma delle fasce orarie

- Creazione di un nuovo programma delle fasce orarie per il settore *Facciata esterna*. Questo settore comprende tutte le porte che consentono l'accesso all'edificio.
- Nel nuovo programma delle fasce orarie *Facciata esterna* si seleziona un gruppo temporale (ad es. Gruppo 1). Questo gruppo viene denominato, ad es., *Orari di pulizia*.
- Per il gruppo *Orari di pulizia* si definisce ora una fascia oraria all'interno del programma delle fasce orarie. I rispettivi orari possono essere scelti a piacimento in base ad un calendario settimanale.

Assegnazione del programma delle fasce orarie al settore

- Il programma delle fasce orarie *Facciata esterna* creato viene ora assegnato, insieme al gruppo temporale *Orari di pulizia* definito, al settore *Involucro esterno*.

- Il settore *Involucro esterno* viene quindi associato al programma delle fasce orarie. Tuttavia non sono ancora stati definiti i gruppi transponder assegnati al gruppo temporale *Orari di pulizia*.

Assegnazione di un gruppo temporale ad un gruppo transponder

- Il gruppo transponder *Addetti alle pulizie* deve essere quindi associato al gruppo delle fasce orarie.
- Ora è stato creato un programma delle fasce orarie *Involucro esterno* il cui gruppo temporale *Orari di pulizia* è associato al gruppo transponder *Addetti alle pulizie*.

Dopo questa procedura teorica, è possibile definire il numero e la complessità dei programmi delle fasce orarie desiderati. Infine, si descriverà ora ciò che avviene sullo sfondo fra i dispositivi:

- Il programma delle fasce orarie viene programmato in ogni chiusura del settore *Involucro esterno* purché supporti la funzione ZK.
- Nei transponder del gruppo transponder *Addetti alle pulizie* viene salvato il gruppo di fasce orarie *Orari di pulizia*.
- Se ora il transponder *Addetto alle pulizie 1* viene azionato nella chiusura *Ingresso principale*, il transponder invierà il proprio ID transponder e il gruppo temporale alla chiusura.
- La chiusura *Ingresso principale* controlla in primo luogo se il transponder è autorizzato nella chiusura. In secondo luogo, si verifica se il gruppo temporale è autorizzato nella chiusura in quel momento (giorno e ora correnti).
- Se entrambi i controlli vanno a buon fine, la chiusura può essere azionata. Se uno dei due controlli è negativo, l'accesso viene negato.
- Nelle chiusure con opzione ZK si possono memorizzare sia gli accessi che i transponder rifiutati.

8.4 Livello di chiusura trasversale

In un progetto si possono gestire più impianti di chiusura. Si possono verificare, ad es., i seguenti scenari tipici:

- **Azienda con più sedi/edifici**

  Un'azienda ha sedi in più luoghi diversi. Di norma un collaboratore lavora sempre presso la stessa filiale. Alcuni gruppi speciali di persone devono tuttavia avere accesso a più sedi/edifici.

In questo caso, le sedi/gli edifici singoli vengono suddivisi in impianti di chiusura separati. Un dipendente della filiale principale deve essere autorizzato anche nelle porte di altre sedi. Il dipendente della sede principale verrà quindi associato all'impianto di chiusura dell'altra filiale. Qui potranno essere impostate autorizzazioni singole.

- **Edificio con più parti**

  In un edificio sono alloggiati più inquilini. I singoli inquilini necessitano di impianti di chiusura autonomi. Gli inquilini devono tuttavia condividere alcune chiusure (ad es. sbarra, tornello, ingresso principale ecc.).

  In questo caso, i singoli inquilini vengono suddivisi in impianti di chiusura separati. Quindi viene creato un livello di chiusura trasversale. In questo livello di chiusura trasversale si possono aggiungere, ad es., tutte le chiusure utilizzate in comune. Contemporaneamente, si aggiungono le persone e/o i settori all'impianto di chiusura trasversale e si impostano le rispettive autorizzazioni.

- **Transponder per Vigili del fuoco per alcune chiusure di tutti gli impianti di chiusura**

  Gli speciali transponder per Vigili del fuoco, ad es. per tubi per chiavi, contengono autorizzazioni per tutte le porte di un edificio. I Vigili del fuoco possono così aprire tutte le chiusure con un unico transponder.

  In questo caso, viene creato un nuovo livello di chiusura trasversale avente il colore "rosso". Qui tramite le proprietà del settore vengono aggiunte tutte le porte desiderate del progetto. In aggiunta viene creato un gruppo transponder "Vigili del fuoco" che viene autorizzato in tutte le porte del livello di chiusura trasversale tramite un clic del mouse.

Indicazioni generali sui livelli di chiusura trasversali:

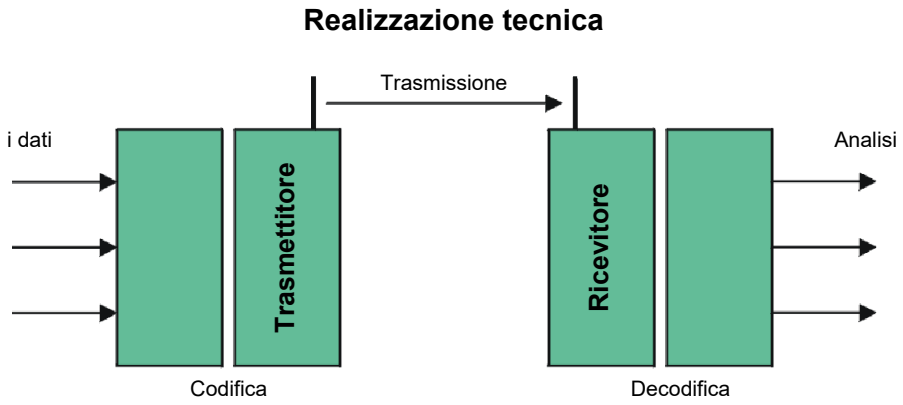
- Se una chiusura o un transponder viene associato ad un altro piano di chiusura, tale associazione si comporta come l'originale creato inizialmente. Se il transponder o la chiusura originali vengono modificati o cancellati, ciò si ripercuote direttamente anche sull'associazione all'altro impianto di chiusura.
- Il livello rosso presenta altresì speciali caratteristiche (ad es. anche l'apertura di chiusure disattivate) concepite espressamente per i Vigili del fuoco. Utilizzare questo livello possibilmente solo per l'accesso in condizioni di emergenza.

NOTA

Se si crea un livello di chiusura trasversale con chiusure già programmate, dopo andranno riprogrammate tutte le chiusure. Fare attenzione alla conseguente necessità di programmazione, visualizzata dai simboli dei lampi di programmazione.

8.5 Crittografia (WaveNet)

La crittografia avanzata protegge i dati che vengono trasportati nella tua WaveNet.



Crittografia end-to-end

In questo contesto, "end-to-end" significa: tra il software centrale e le chiusure. I dati vengono criptati e lasciano il software centrale. Saranno decifrati solo nella chiusura.

Comunicazione	Crittografia
End-to-end (generale)	3DES (112 bit)
Elenchi degli accessi (contro la lettura non autorizzata)	DES semplice (56 bit)
Segnali Broadcast	AES (128 bit)

Pacchetti di dati con firma digitale

La firma a 128 bit dei pacchetti di dati protegge dalle manipolazioni sul collegamento radio. Se la firma di un pacchetto di dati non è corretta, il pacchetto di dati viene ignorato.

Protezione contro gli attacchi di replay

Ogni pacchetto di dati rilevanti per la sicurezza contiene un contatore. Questo contatore viene incrementato per ogni nuovo pacchetto di dati. Se arriva di nuovo un pacchetto dati con lo stesso valore contatore, il pacchetto di dati viene ignorato. Se un pacchetto dati viene intercettato e reinviato (attacco di replay), il suo numero progressivo è lo stesso del pacchetto originale e la copia viene riconosciuta e ignorata.

9. 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.

9.1 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 [▸ 133].*
3. Fare clic sul pulsante "Applica".
4. Fare clic sul pulsante "Termina".

9.2 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".

9.3 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".

9.4 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.

9.5 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".

9.6 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".

9.7 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.

9.7.1 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.

9.7.2 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*

9.7.3 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.

9.8 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.

9.9 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.

9.10 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.

9.11 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!

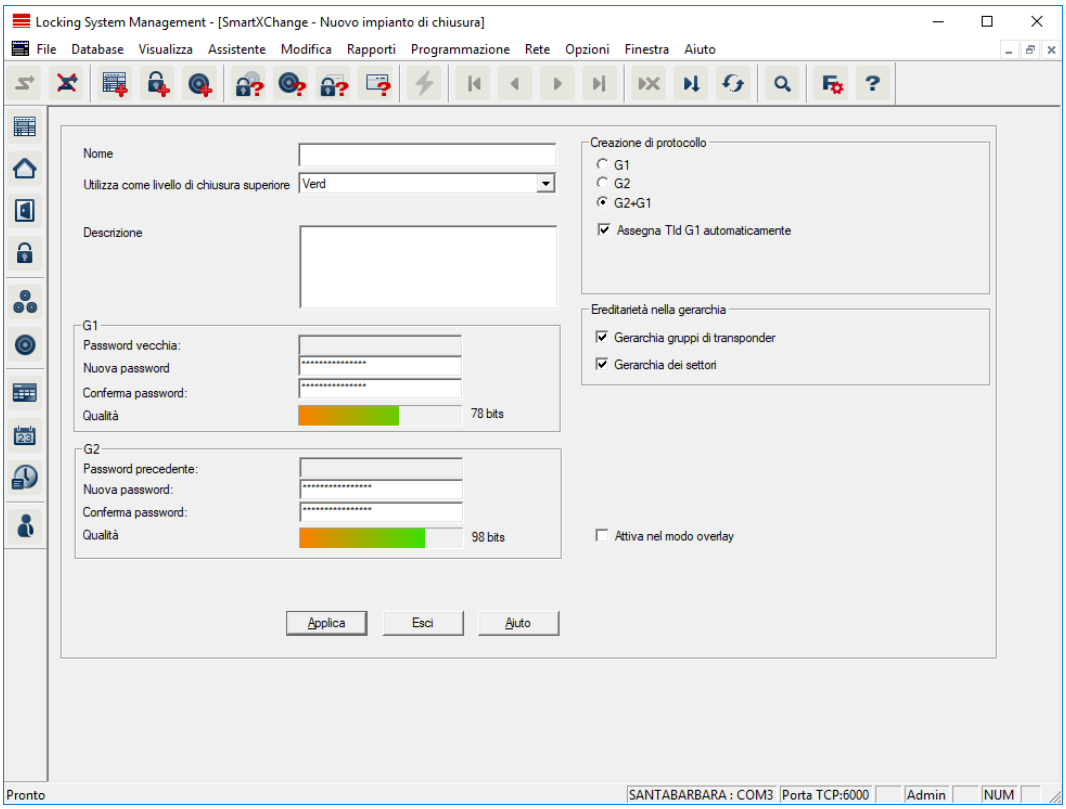
9.11.1 Creazione di un livello di chiusura trasversale

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.

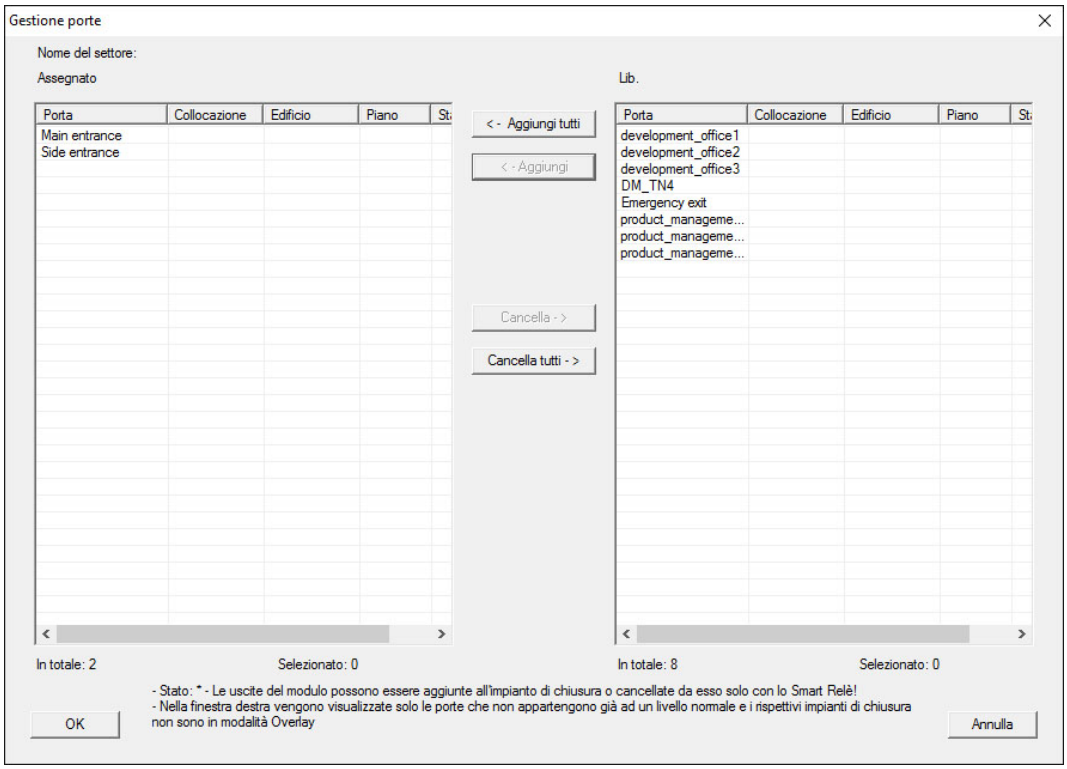


9.11.2 Associazione delle chiusure

✓ 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".

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



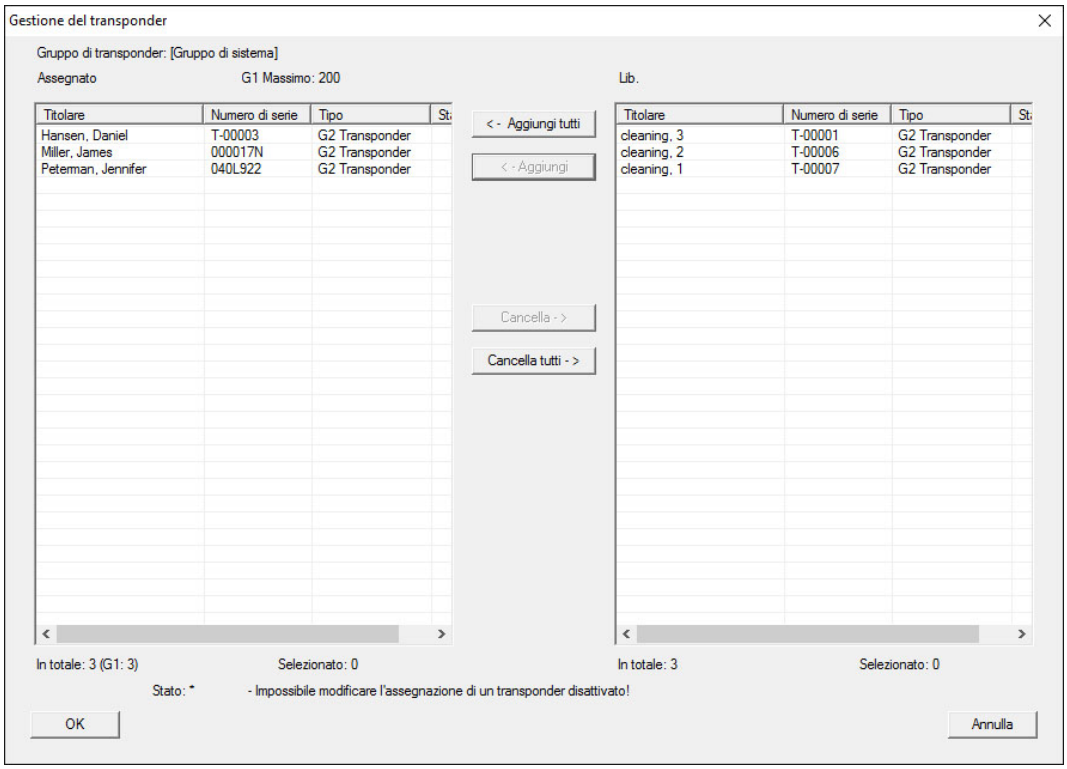
9.11.3 Associazione dei transponder

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

✓ Sono già stati creati i transponder o i gruppi di transponder.

1. Fare clic con il tasto destro su un gruppo di transponder e selezionare "Proprietà".
2. 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".



9.11.4 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.

9.12 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*.

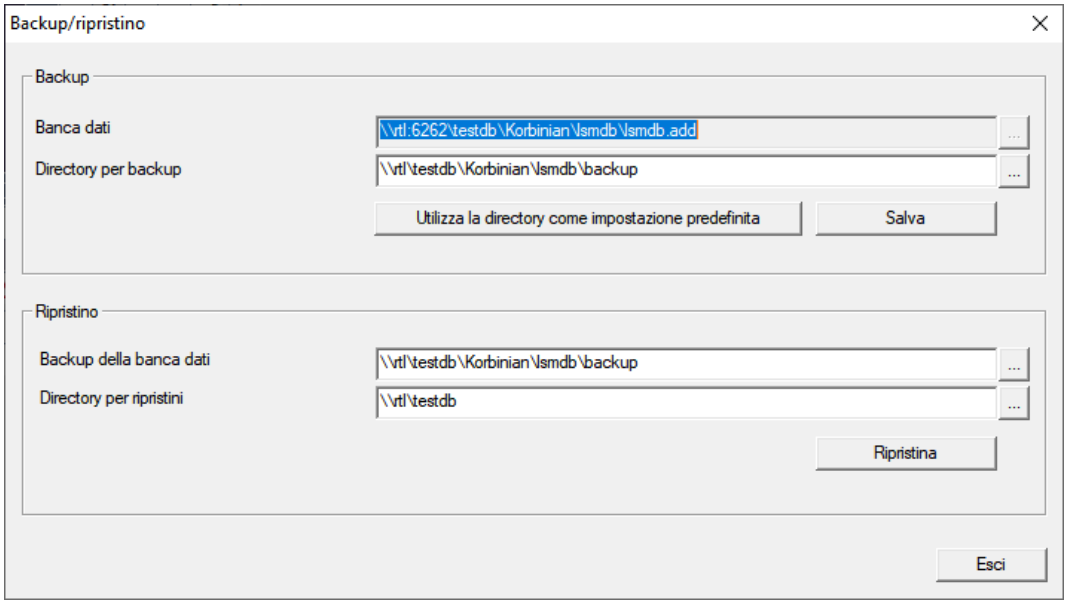
2. Aggiungere un nuovo settore, ad es. "Tutte le chiusure" e assegnarvi tutte le chiusure desiderate tramite "Gestione porta".
3. Nel livello di chiusura trasversale, creare un nuovo gruppo transponder "Vigili del fuoco".
4. Nelle proprietà del gruppo transponder "Vigili del fuoco" fare clic sul pulsante "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 insorta.*

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".

9.13 Backup manuale della banca dati

✓ LSM aperto.

1. Selezionare da | Banca dati | la voce Backup.
   ↳ La finestra "Back-up/ripristino" si apre.



2. Nell'area "Backup" specificare su quale banca dati deve essere eseguito il backup.
3. Fare clic sul tasto Salva.
   ↳ Backup creato.

4. Fare clic sul pulsante Esci.
   ↳ La finestra "Back-up/ripristino" si chiude.

9.14 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 *Registrazione [▸ 118]*).

9.14.1 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:

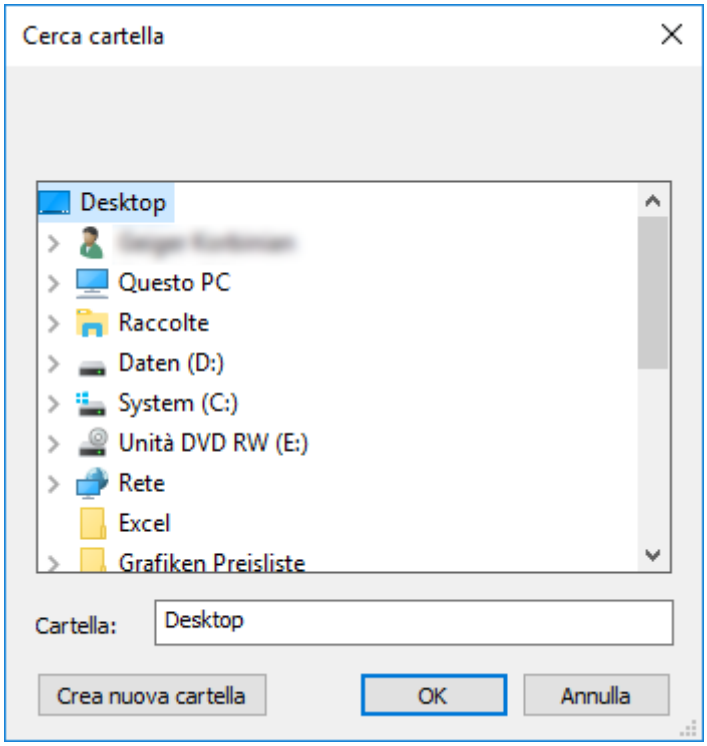
Persona	Il file contiene i dati personali con cui è possibile identificare la persona (ad es. cognome, indirizzo o foto).
PersonHistory	Questo file contiene la data di creazione e cancellazione del record di dati.
PersonLog	Questo file contiene l'andamento delle modifiche apportate al record di dati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

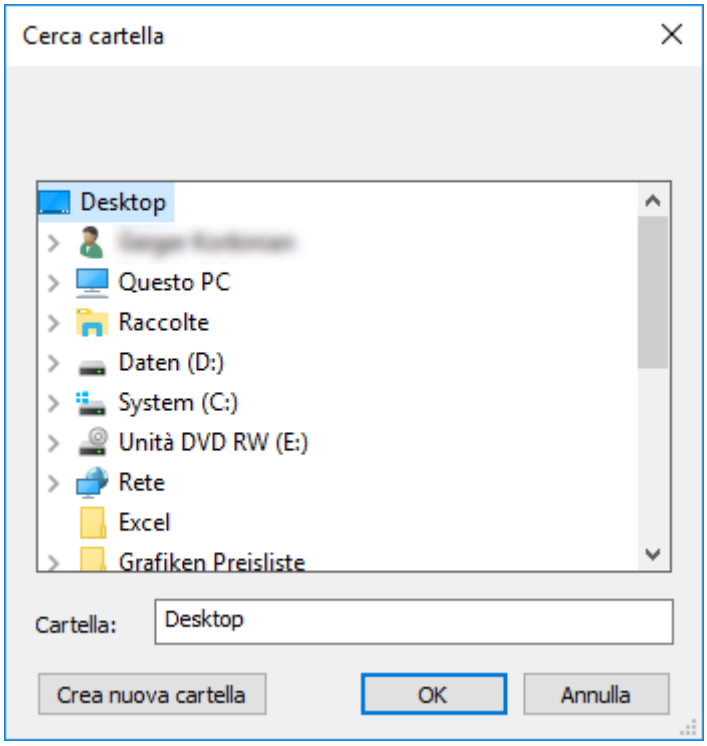
User	Questo file contiene i dati riguardanti l'utente (ad es. nome utente e gruppo utenti).

UserLog	Questo file contiene l'andamento delle modifiche apportate da questo utente (ad es. creazione di una nuova chiusura).

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.

9.14.2 Cancellazione dei dati

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

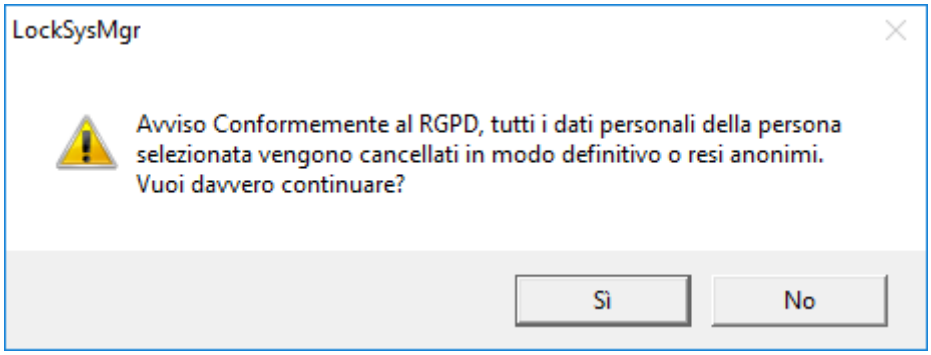
Persone

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 Sì.

↳ Dati personali della persona selezionata cancellati o resi anonimi.

NOTA

Cancellazione dei dati residui dopo le precedenti cancellazioni

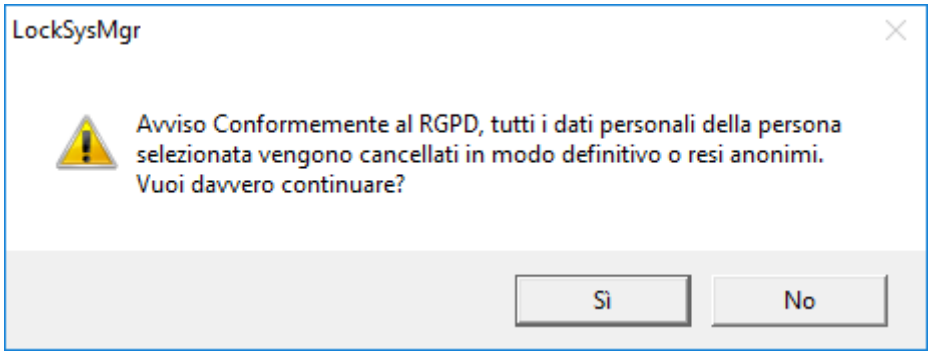
È possibile cancellare i dati delle persone anche con il pulsante nella scheda [Nome] dei supporti di identificazione assegnati. A differenza della cancellazione tramite modulo RGPD, in questo caso i protocolli non vengono cancellati e permangono all'interno del sistema. In questo modo solo una parte 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

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 Sì.

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

9.14.3 Quali dati personali vengono memorizzati nel software?

Vi è la possibilità di memorizzare i seguenti dati personali nel software:

- Nome
- Cognome*
- Qualifica
- Indirizzo
- Telefono
- Indirizzo email
- Numero personale*
- Nome utente
- Reparto
- Luogo/edificio
- Impostato da/a
- Data di nascita
- Centro di costo
- Foto

Di questi dati solo il cognome e il numero personale sono *campi obbligatori e sono necessari per l'utilizzo del software.

Ai sensi dell'art. 9 del RGPD non vengono memorizzate categorie particolarmente sensibili di dati personali.

9.14.4 Per quale finalità i dati personali vengono memorizzati nel software?

Per poter utilizzare nella loro completezza le funzioni di un impianto di chiusura elettronico è necessario poter assegnare a un determinato utente (ad es. un collaboratore) i supporti di identificazione utilizzati (ad es. transponder).

9.14.5 Per quanto tempo i dati personali sono memorizzati nel software?

I dati vengono memorizzati almeno per la durata di utilizzo di un supporto di identificazione all'interno dell'impianto di chiusura (ad es. appartenenza a una società).

La durata di conservazione dei dati (ad es. nelle registrazioni e gli elenchi di accesso) può essere modificata dal gestore dell'impianto di chiusura e adattata alle indicazioni aziendali.

9.14.6 I dati personali memorizzati nel software sono protetti dall'accesso di terzi?

Fondamentalmente l'utente (il cliente finale) dell'impianto di chiusura e del software è responsabile della gestione e della messa in sicurezza dei diritti di accesso.

Nel sistema di chiusura stesso tutti i dati sono protetti da metodi crittografici articolati in vari livelli. Non è possibile aprire l'interfaccia grafica utente, per poter accedere ai dati, senza una password e i relativi diritti utente.

Nell'ambito della gestione delle attività non avvengono la trasmissione automatica a terzi, l'utilizzo o l'elaborazione da parte di SimonsVoss.

9.14.7 Può essere messa a disposizione una copia dei dati memorizzati?

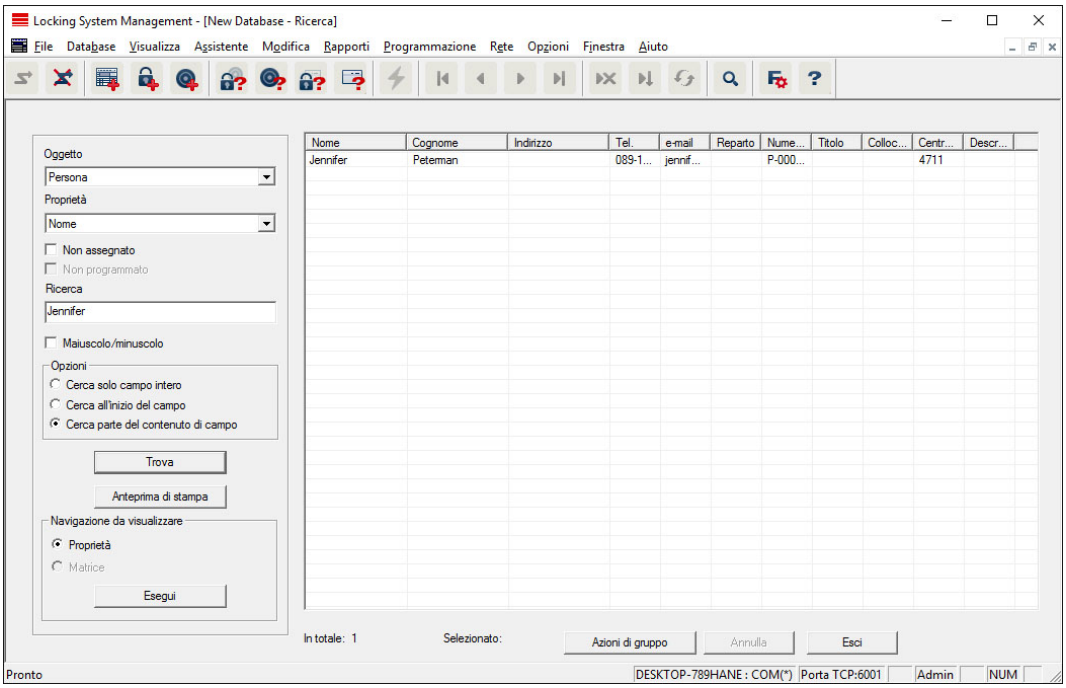
Tutti i dati raccolti relativi a una persona interessata (a partire dalla versione 3.4), presupposti i relativi diritti di utilizzo, possono essere messi a disposizione come copia da parte del cliente (ad es. nell'ambito di un audit) tramite la funzione Esporta. Ciò permette al cliente di osservare il diritto di accesso ai sensi dell'art. 15, comma 3 del RGPD.

9.14.8 I dati personali possono essere cancellati dal software?

I dati personali possono essere cancellati definitivamente dal software (a partire dalla versione 3.4 SP) e dalla relativa banca dati da parte del cliente su richiesta di una persona interessata ai sensi dell'art. 17 del RGPD.

9.15 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.

9.16 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.

9.17 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 *Blocca permanente il transponder e crea un transponder sostitutivo [▸ 158]*).

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.

9.18 Programmazione della chiusura

✓ Una chiusura è stata creata nell'impianto di chiusura ed è visibile nella matrice.

1. Fate clic con il tasto destro sulla chiusura desiderata.

2. Fate clic su Programmazione.
3. Seguite le istruzioni del software LSM.

Assicuratevi di selezionare il dispositivo di programmazione appropriato.

NOTA

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

Rifiuto del primo azionamento del transponder dopo la programmazione iniziale dei prodotti AX

Se il primo mezzo di identificazione azionato dopo la programmazione iniziale è un transponder, allora il transponder viene respinto una volta e sincronizzato con la chiusura in background. Dopo di che, i transponder funzionano come di consueto.

9.19 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.

9.19.1 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.

9.20 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 ± 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/Zeitzonenplan (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 “Zeitzonengruppe” (“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.

9.21 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.

9.22 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!

9.23 Blocca transponder

Può capitare che i transponder vadano smarriti, rimangano danneggiati o siano rubati.

- *Blocca permanente il transponder e crea un transponder sostitutivo [▸ 158]*
- *Blocca temporaneamente il transponder [▸ 161]*

NOTA

Trasferimento degli ID di blocco con le carte ai blocchi a doppia faccia

Le carte possono trasferire solo singoli ID di blocco, non un protocollo di programmazione completo.

- Tenere sempre la scheda che trasmette gli ID di blocco a entrambi i lettori.

9.23.1 Blocca permanente il transponder e crea 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.

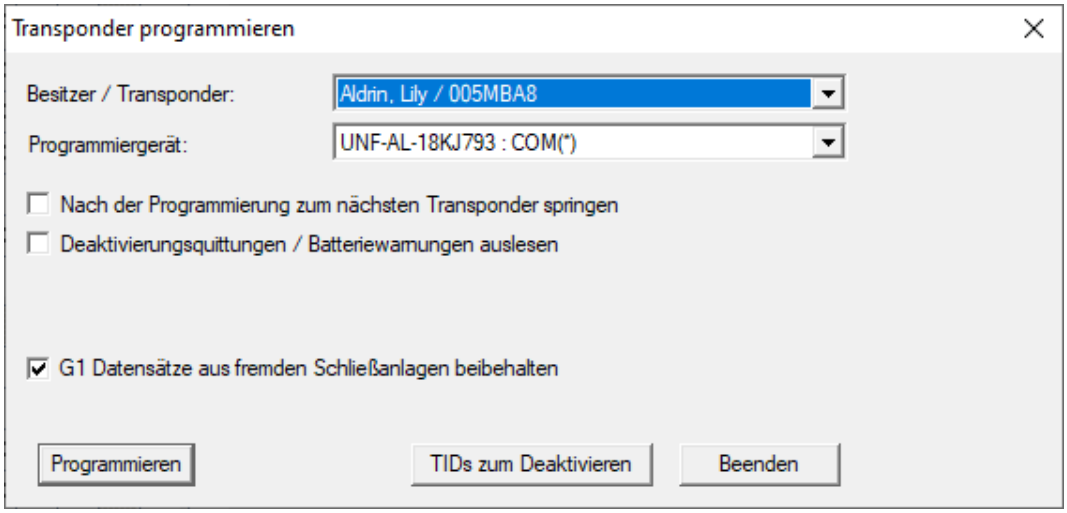
A partire dalla versione LSM 3.5 SP3 è possibile aggiungere ai transponder desiderati fino a due altri ID transponder da bloccare.

Programmazione diretta dei TID da bloccare

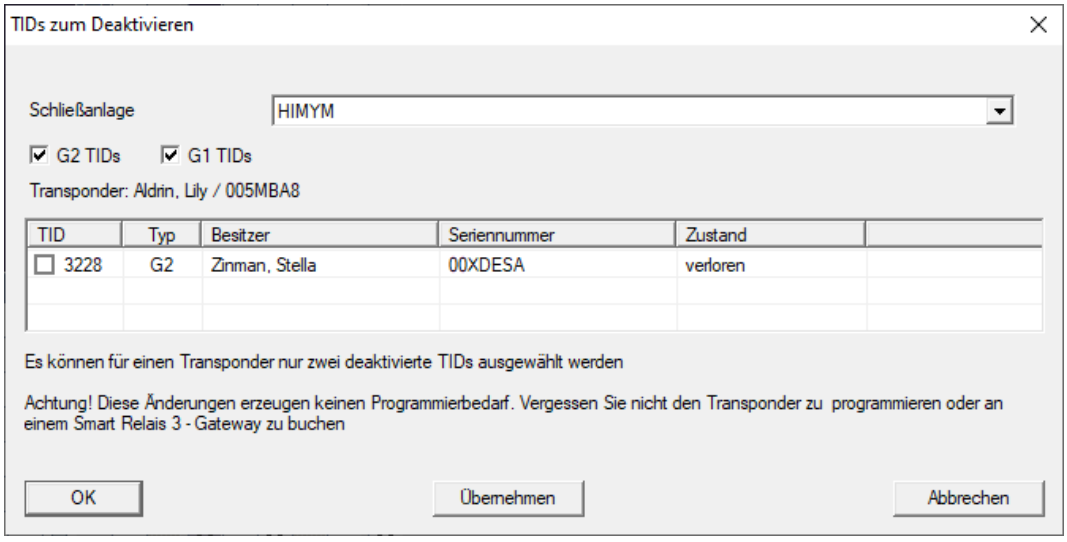
Gli ID da bloccare vengono memorizzati sul transponder durante il processo di programmazione.

✓ Il transponder è fisicamente disponibile.
✓ La finestra di programmazione del transponder è aperta.

1. Cliccate sul pulsante TID da disattivare.



↳ L'elenco si apre.



2. Apponete un massimo di due segni di spunta nella colonna TID per memorizzare i TID da cancellare sul transponder.
3. Confermare l'inserimento con il pulsante "OK".
4. Continuate con la programmazione.

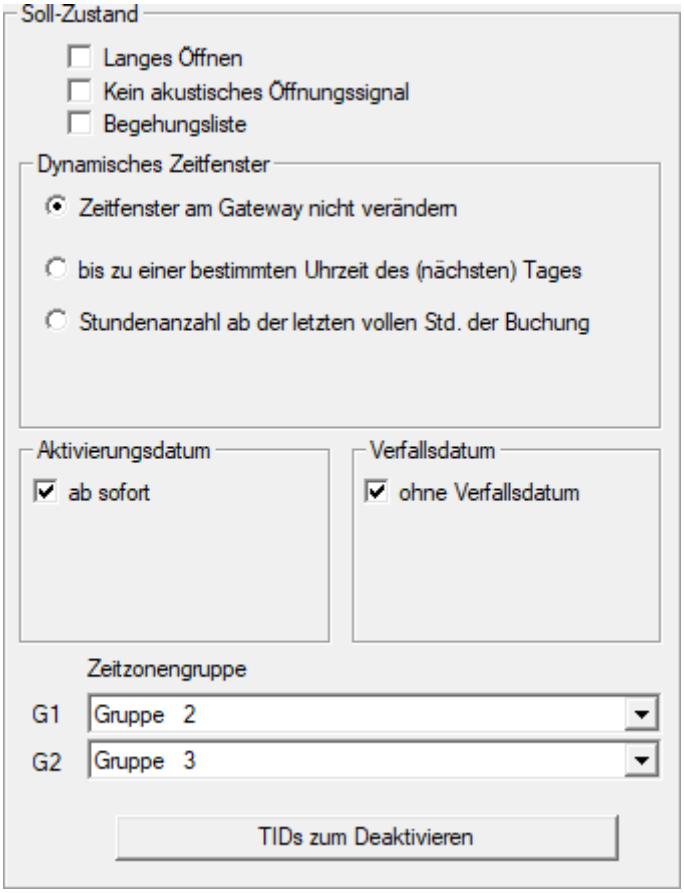
↳ I TID contrassegnati sono memorizzati sul transponder come da cancellare. Quando il transponder si autentica nella chiusura interessata, i TID da cancellare vengono bloccati nella chiusura.

Memorizzazione dei TID da bloccare nelle Proprietà

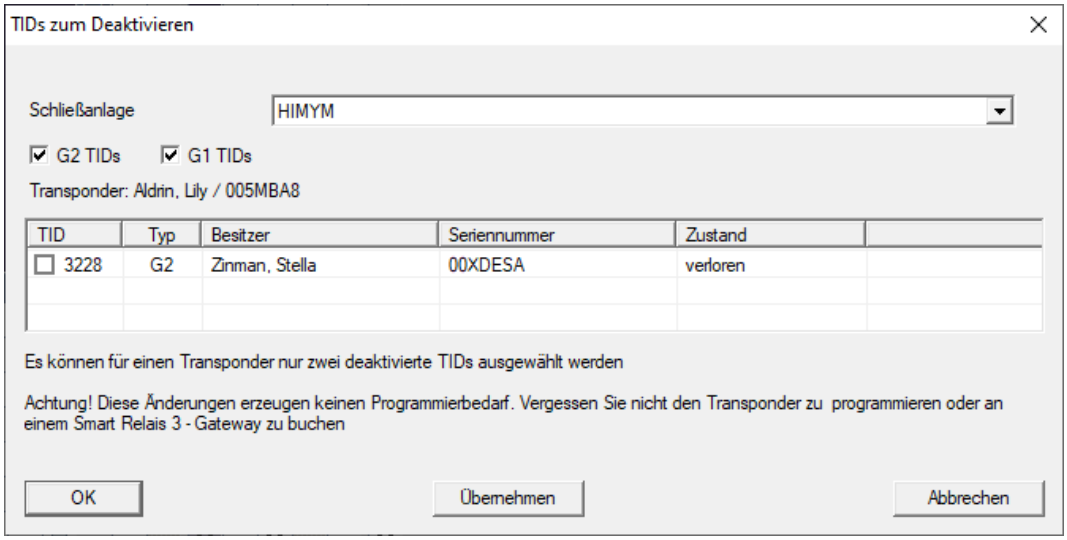
Gli ID da bloccare vengono memorizzati sul transponder durante il successivo processo di programmazione o durante la successiva prenotazione su un gateway.

✓ La finestra Proprietà del transponder è aperta.

1. Passate alla scheda di registro [Configurazione].



2. Cliccate sul pulsante TID da disattivare.
   ↳ L'elenco si apre.

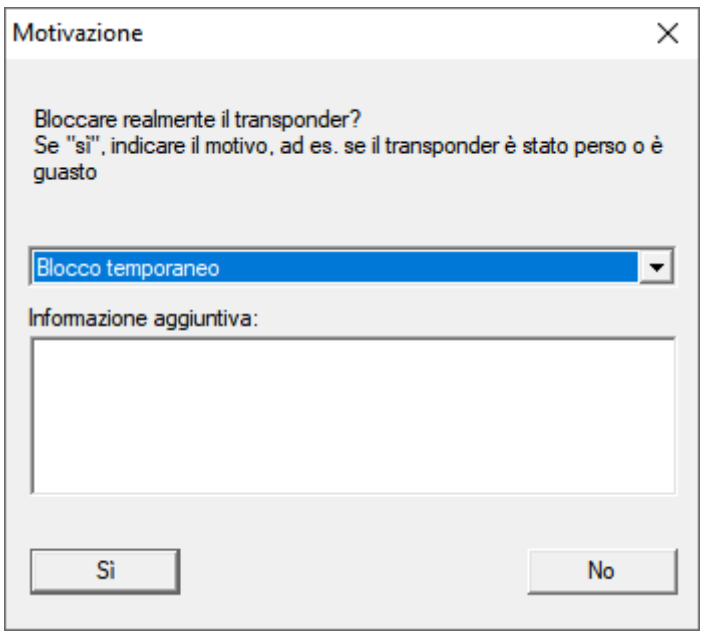


3. Apponete un massimo di due segni di spunta nella colonna TID per memorizzare i TID da cancellare sul transponder.
4. Confermare l'inserimento con il pulsante "OK".

↳ I TID contrassegnati vengono memorizzati sul transponder durante la successiva programmazione o la successiva prenotazione su un gateway.

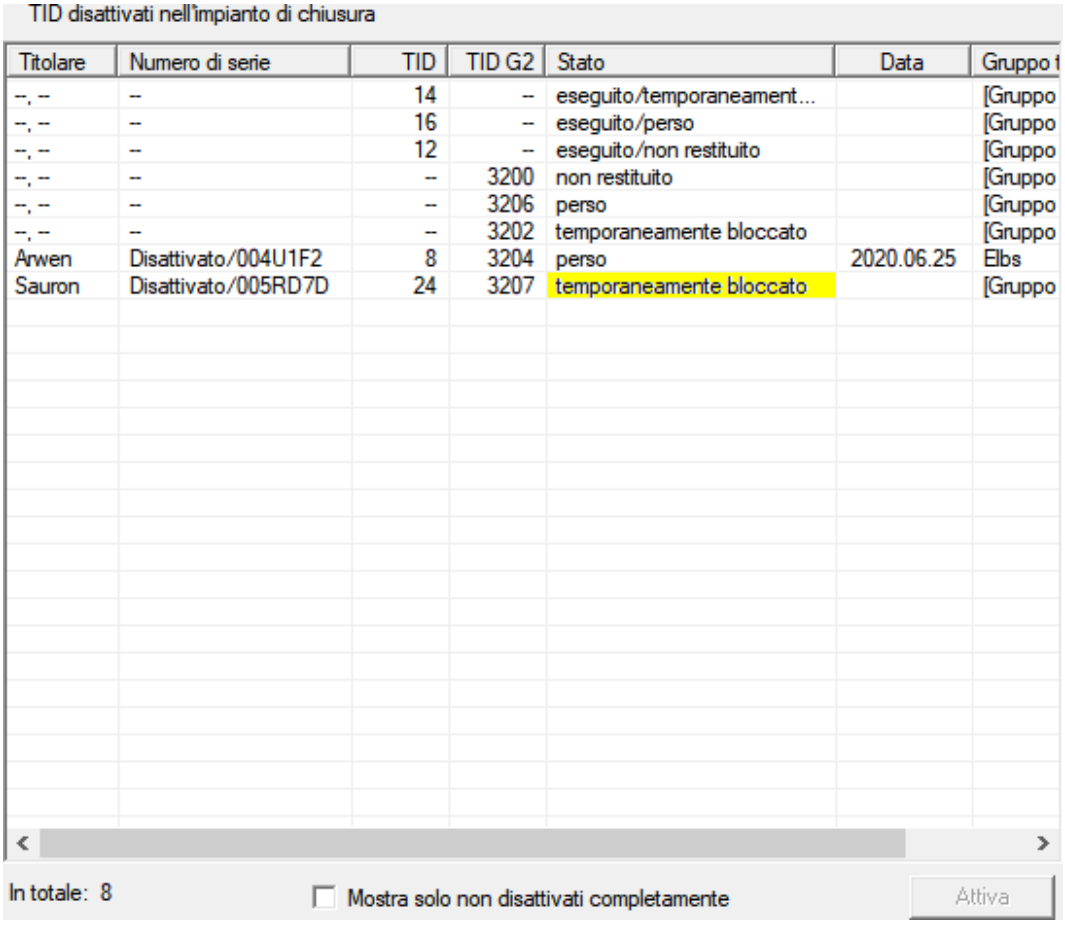
9.23.2 Blocca temporaneamente il transponder

Il blocco permanente di un mezzo di identificazione porta alla perdita di un TID. Per questo motivo, con LSM 3.5 è stata introdotta una funzione che consente di bloccare un transponder o una scheda solo temporaneamente: "Blocco temporaneo".



Il TID non viene effettivamente bloccato. Invece, si ritirano tutte le autorizzazioni alla persona con la semplice pressione di un pulsante. Le porte interessate richiedono naturalmente una programmazione e devono essere programmate. Se il transponder ricompare o viene ceduto a una nuova persona, è possibile ripristinare semplicemente le autorizzazioni prima del blocco.

I transponder temporaneamente bloccati sono visibili nelle proprietà del sistema di chiusura alla scheda [TID speciali].



9.24 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*), 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".

9.25 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.

9.26 Reset della modalità Freeze nelle chiusure G2

Rispetto alla generazione G1, nella G2 l'apertura di emergenza della chiusura e l'eliminazione della modalità di emergenza (modalità Freeze) risulta più semplice.

✓ Supporto di identificazione per cambio batteria creato (vedere *Transponder per sostituzione batteria G2 [▸ 116]*).

✓ Supporto di identificazione per cambio batteria programmato.

1. Azionare il supporto di identificazione per cambio batteria nella chiusura.
   ↳ La modalità Freeze è disattivata.
2. Azionare un qualunque supporto di identificazione autorizzato.
   ↳ La chiusura si apre.
3. Sostituire la batteria.
4. Azionare il supporto di identificazione per cambio batteria nella chiusura.
   ↳ La modalità Freeze è disattivata.
5. Testare il funzionamento della chiusura con un qualunque supporto di identificazione autorizzato.

↳ Modalità Freeze resettata.

AVVISO

Guasto della chiusura a causa di un uso improprio

Il mezzo di identificazione del cambio batteria è destinato esclusivamente ad annullare la modalità Freeze prima di un cambio batteria. In caso di uso improprio, le batterie possono scaricarsi completamente. Il risultato è un guasto totale della chiusura.

9.27 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 [▸ 167]*.

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".

9.27.1 Elenchi degli accessi

Le chiusure con funzione ZK registrano gli accessi in una lista degli accessi:

- Data
- Ora
- ID del supporto di identificazione
- Nome dell'utente

È possibile leggere e visualizzare l'elenco degli accessi con il software LSM. Il numero di voci nell'elenco degli accessi dipende dalla chiusura e dalla configurazione.

	Standard	Gateway
Cilindro	Fino a 3000	
SmartHandle	Fino a 3000	
Smart Relè	Fino a 3600	Fino a 200

In un sistema di chiusura in rete, è possibile anche automatizzare il processo di lettura (vedere *Lettura della chiusura [▸ 251]*).

9.28 Gestione utenti

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".

9.29 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.

9.29.1 Modifica della configurazione

Avete due possibilità per l'impiego di schede.

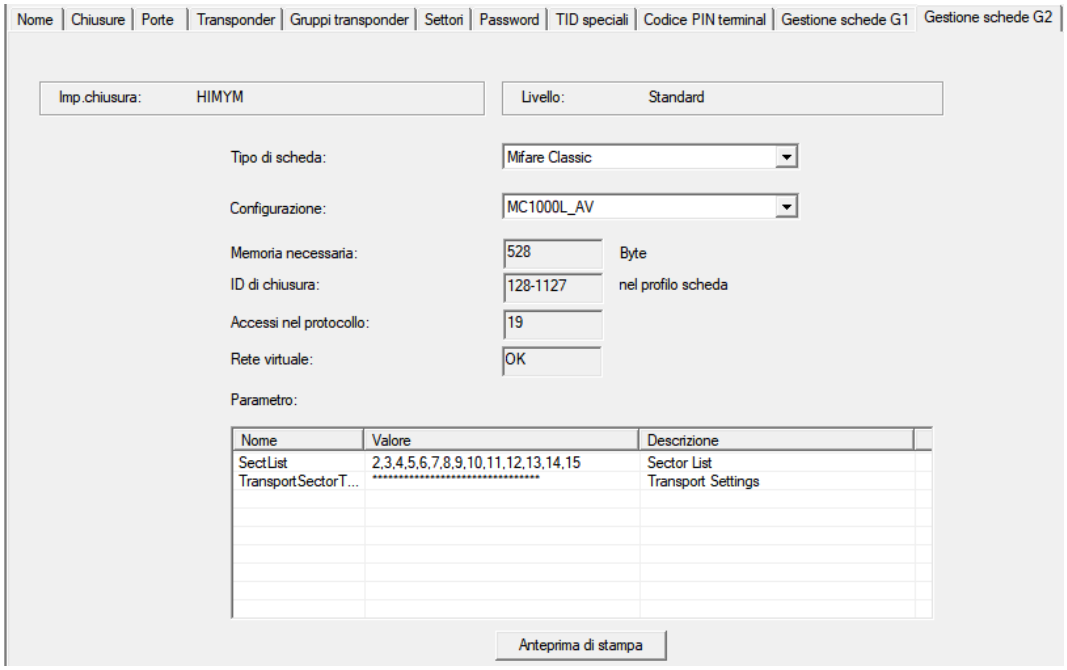
- Potete utilizzare schede già impiegate.
- Potete utilizzare schede nuove.

In entrambi i casi inserite il tipo di scheda, la configurazione ed eventualmente i settori da illustrare (vedi *Tabella [▸ 169]*).

Predisposizione della scheda

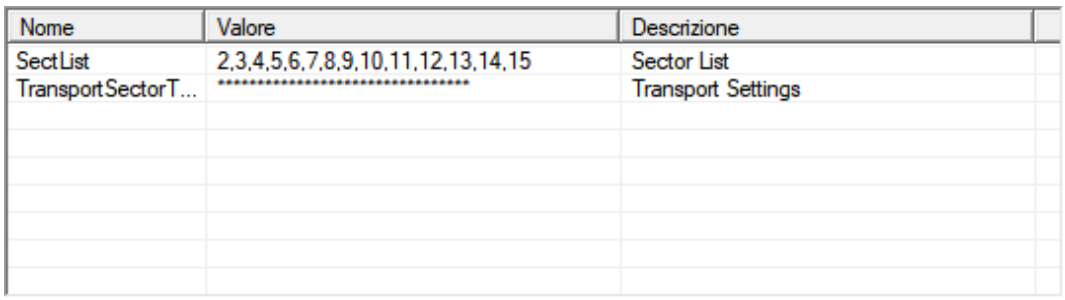
✓ LSM aperto.

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).



7. Fare clic sul pulsante Applica.

↳ Avete modificato la configurazione

9.29.2 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 + DESFire	MIFARE Plus S/X
MCBasic	✓	✓	✓	✕	✓
MC1200L	✓	✓	✓	✕	✓
MC3800L	✓	✓	✓	✕	✓
MC1000L_AV	✕	✓	✓	✕	✓
MC2400L_AV	✕	✓	✓	✕	✓

	MIFARE Classic	MIFARE Classic Pre-defined A	MIFARE Classic Pre-defined B	MIFARE Classic + DESFire	MIFARE Plus S/X
MC8000L_AV	✗	✓	✓	✗	✓
MBasic	✗	✗	✗	✓	✗
M1200L	✗	✗	✗	✓	✗
M3800L	✗	✗	✗	✓	✗
M1000L_AV	✗	✗	✗	✓	✗
M4000L_AV	✗	✗	✗	✓	✗
M8000L_AV	✗	✗	✗	✓	✗
M10000L_AV	✗	✗	✗	✓	✗

	G1/G2	Lock-IDs	Anzahl der Schließungen	Begehungsliste	Sektoren	Benötigter Speicherplatz	Virtuelles Netzwerk
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗
MC3800L	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	✓
MC8000L_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	✓

	G1/G2	Lock-IDs	Anzahl der Schließungen	Begehungsliste	Sektoren	Benötigter Speicherplatz	Virtuelles Netzwerk
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	✗
MD3800L	G2	128-3927	3800	✗	n.a. (DESFire)	528	✗
MD2500L_AV	G2	128-2627	2500	58	n.a. (DESFire)	1024	✓
MD4000L_AV	G2	128-4127	4000	100	n.a. (DESFire)	1600	✓
MD1000L_AV	G2	128-10127	10000	225	n.a. (DESFire)	3048	✓
MD3200L_AV	G2	128-32127	32000	470	n.a. (DESFire)	7000	✓
MD2400L_AV	G2	128-2527	2400	34	n.a. (DESFire)	830	✓
MD3650L_AV	G2	128-3777	3650	2	n.a. (DESFire)	830	✓

9.30 Inoltro dei dispositivi di programmazione USB ai terminal server (LSM Professional)

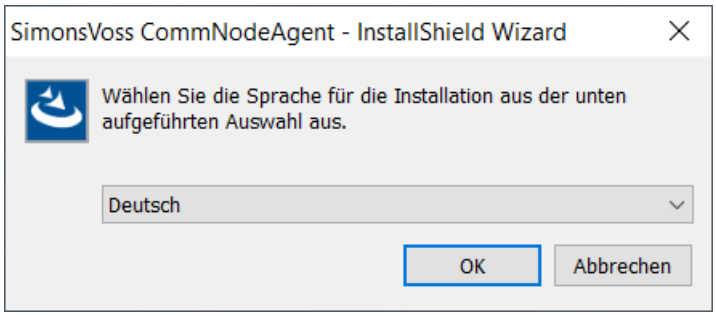
9.30.1 SmartCD.G2 / SmartCD2.G2

9.30.1.1 CommNodeAgent

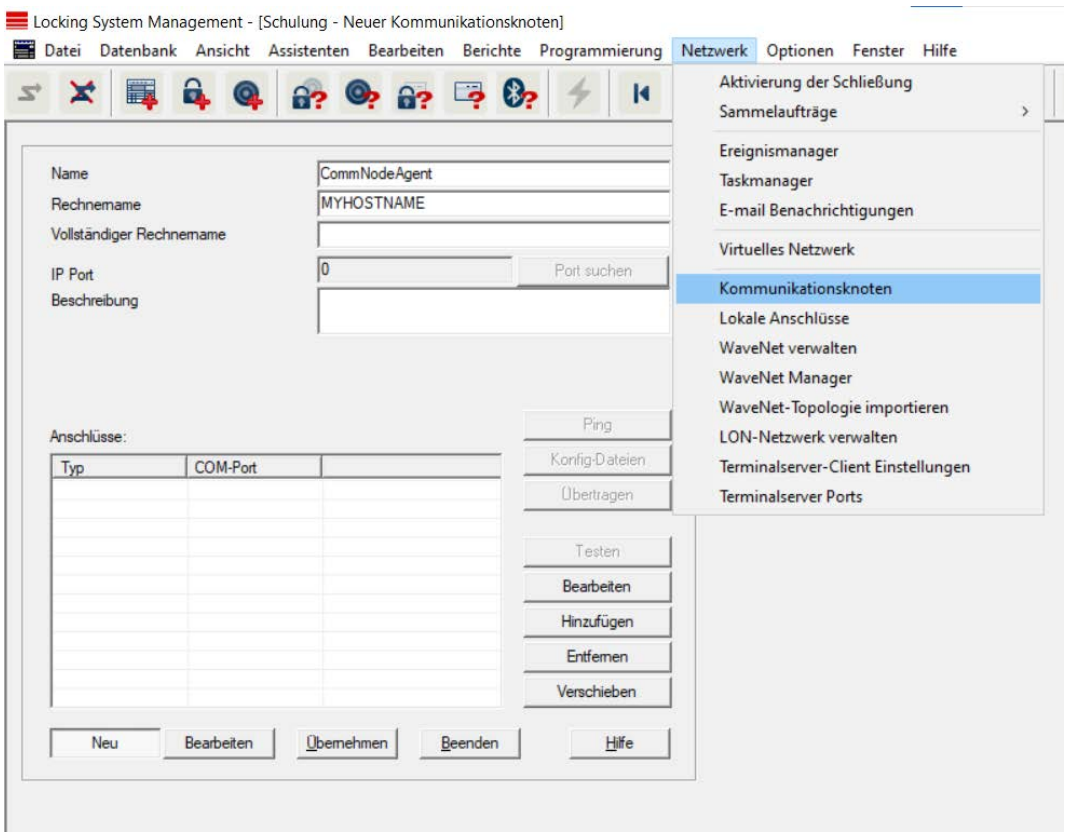
Il CommNodeAgent è un'applicazione di SimonsVoss (solo per sistemi Windows completi, non Windows RT) per l'utilizzo dello SmartCD attivo (SmartCD.G2 / SmartCD2.G2) in una sessione di desktop remoto. Il CommNodeAgent esegue la trasmissione dello SmartCD USB alla sessione di desktop remoto desiderata. Il CommNodeAgent deve essere installato nel Terminal Client ed essere rispettivamente configurato nel LSM.

- ✓ Porta USB libera nel Terminal Client
- ✓ Consensi porte nel firewall (vedere matrice di comunicazione di SimonsVoss)
- ✓ Risoluzione DNS bidirezionale Client ↔ Server
- ✓ Versione CommNodeAgent identica o compatibile con la versione LSM

1. Installare il CommNodeAgent e il driver per SmartCD nel Terminal Client

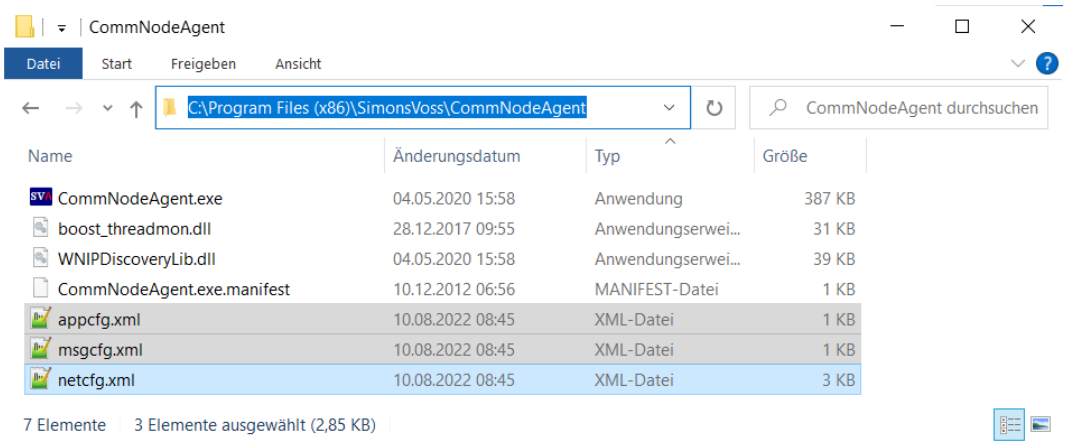


2. Selezionare nella barra superiore del programma da | Rete | la voce Nodi di comunicazione.

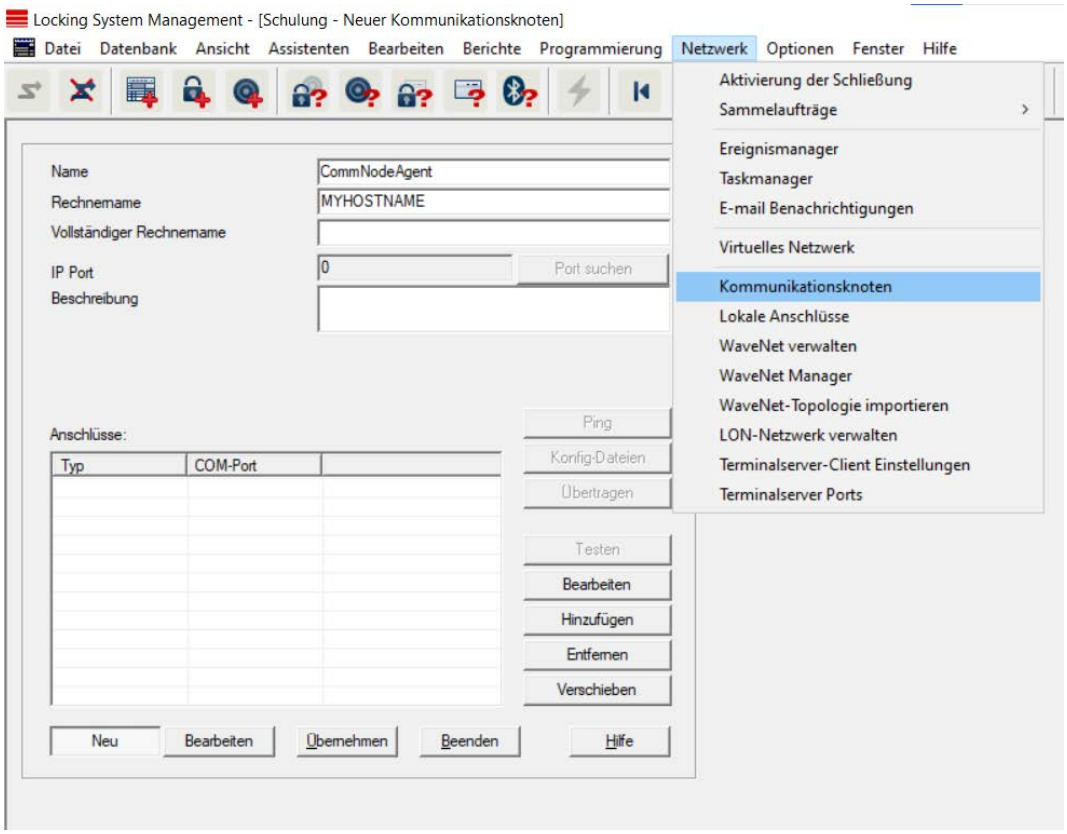


3. Fare clic sul tasto Nuovo.
4. Nel campo di immissione Name [offen] inserire un nome liberamente selezionabile per il nodo di comunicazione, ad esempio CommNodeAgent.

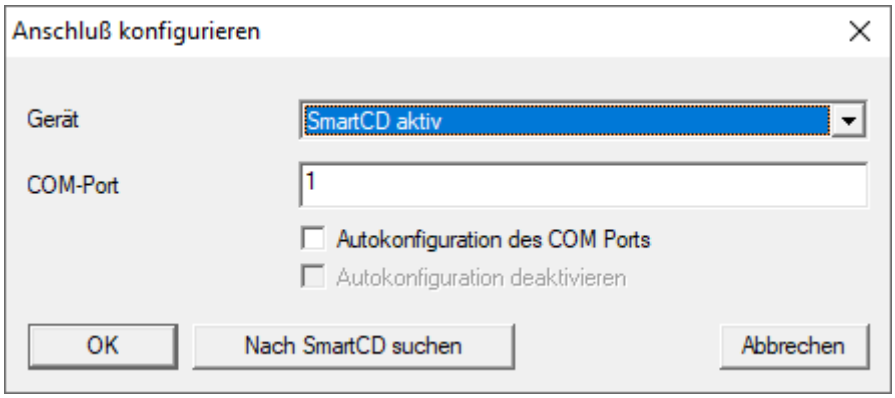
5. Inserire il nome host del Terminal Client nel campo di immissione Rechnername [offen].
6. Fare clic sul tasto Applica.
7. Fare clic sul tasto File di configurazione per memorizzare i file a scelta.
8. Per trasferire i file di configurazione, copiare i tre file di configurazione XML creati durante i passaggi precedenti nella cartella d'installazione del CommNodeAgent.



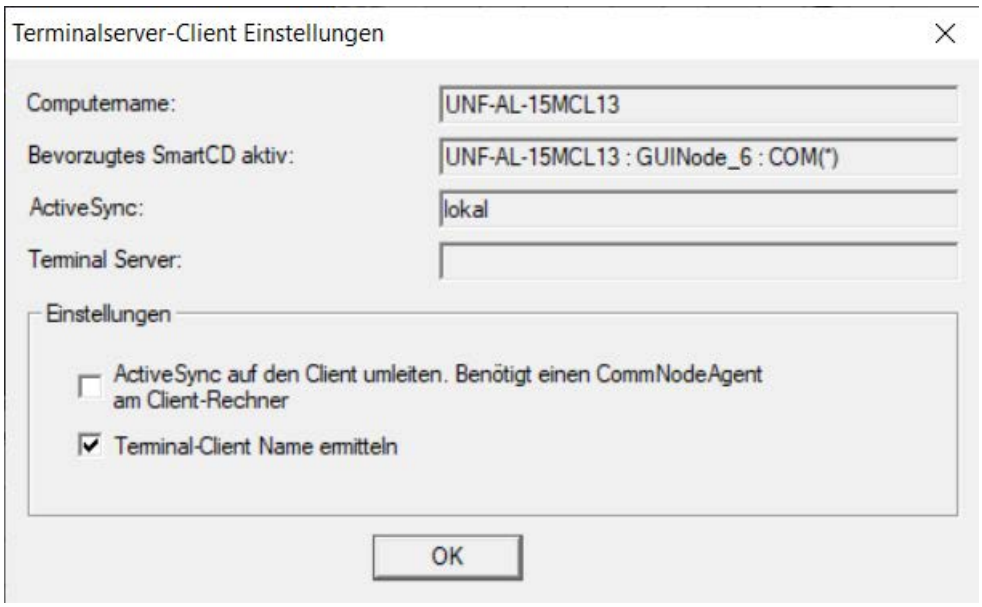
9. Eseguire CommNodeAgent.exe come amministratore.
10. Per aggiungere lo SmartCD al CommNodeAgent, selezionare nella barra superiore del programma da | Rete | la voce Nodi di comunicazione.



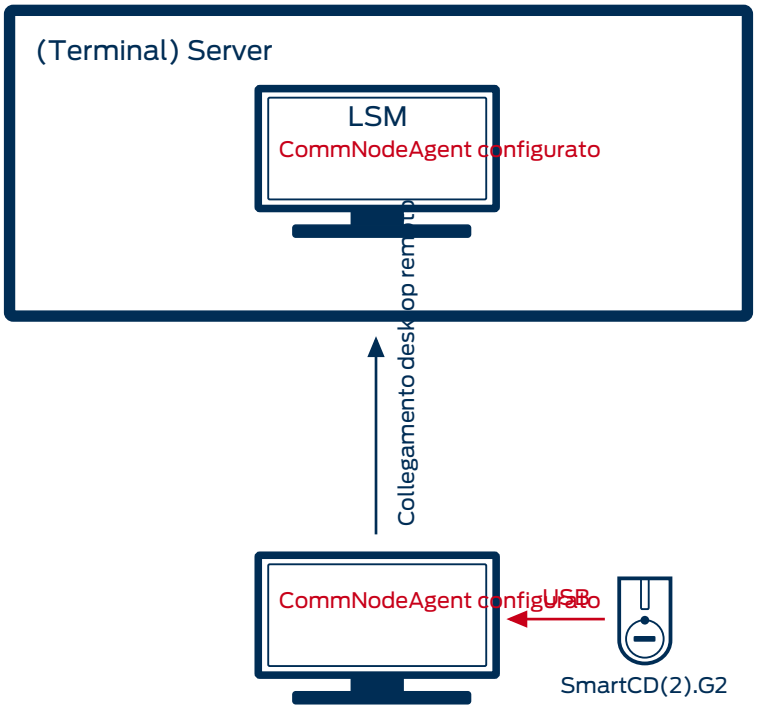
11. Fare clic sul tasto Aggiungi .
    ↳ La finestra "LSM Hinzufügen Kommunikationsknoten: Anschluß konfigurieren [offen]" si apre.



12. Selezionare nella seguente finestra di dialogo nel menu a discesa ▼ **Dispositivo** la voce "SmartCD".
13. Attivare la casella di controllo ☑ LSM Kommunikationsknoten hinzufügen: Autokonfiguration des COM Ports [offen].
14. Fare clic sul pulsante OK .
15. Fare clic sul tasto Trasferisci .
16. Selezionare nella barra superiore del programma da | Rete | la voce Terminalserver-Client Einstellungen .
17. Attivare la casella di controllo ☑ Netzwerk: Terminal-Client Name ermitteln [offen].



    ↳ Le impostazioni del Client del Terminal Server vengono verificate.



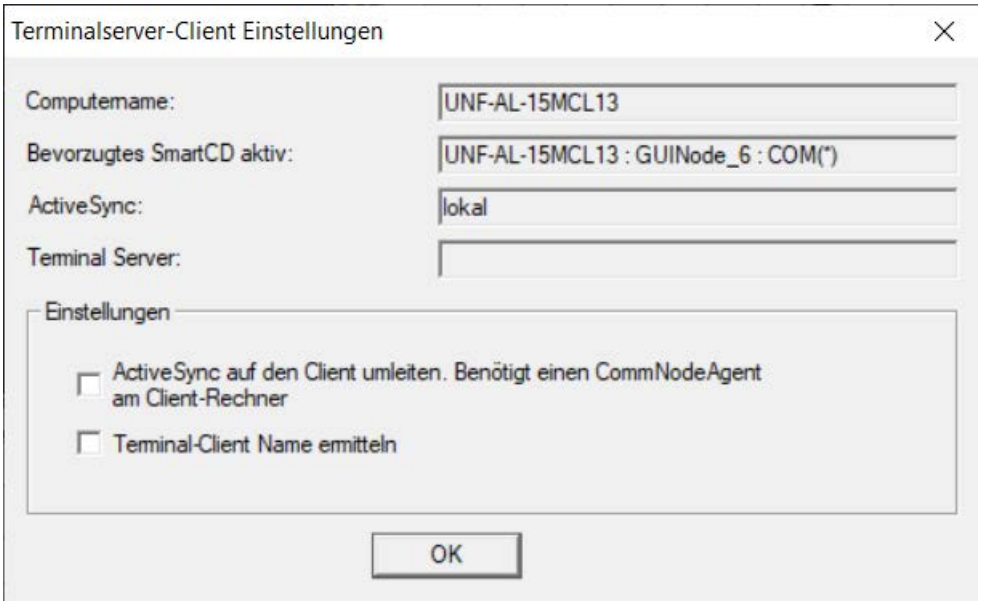
9.30.1.2 Server USB / Ethernet

I dispositivi USB possono essere trasmessi mediante server USB/Ethernet tramite la rete cliente a un (Terminal) server.

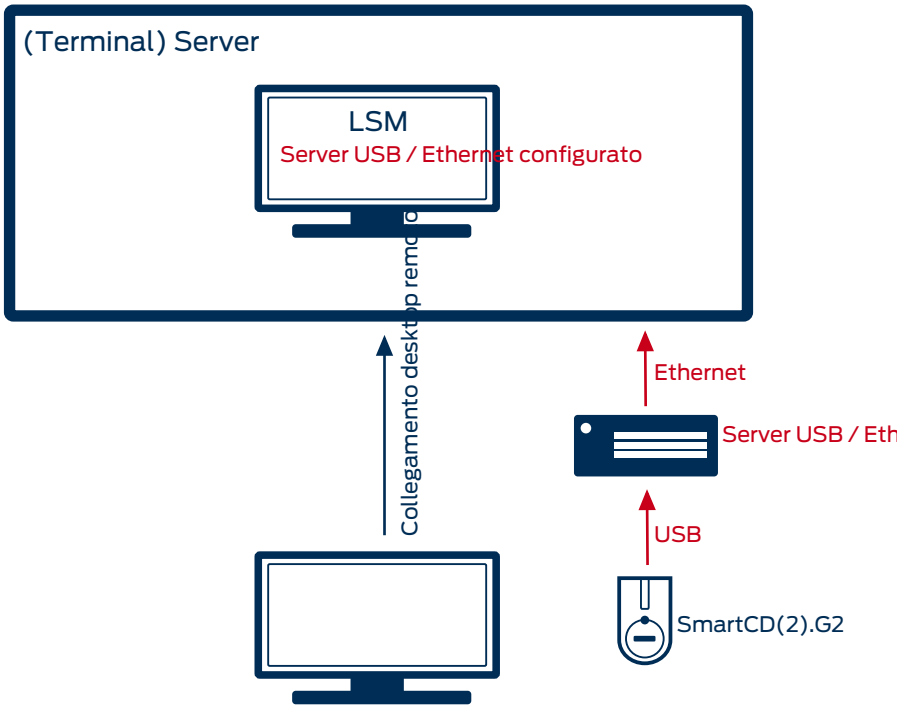
Nel Terminal Client non deve essere eseguita nessuna installazione.

- ✓ Il software server USB deve essere installato centralmente sul server.
- ✓ Anche il server USB necessita della relativa configurazione di rete.

1. Selezionare nella barra superiore del programma da | Rete | la voce Terminalserver-Client Einstellungen.
2. Disattivare la casella di controllo ☐ Netzwerk: Terminal-Client Name ermitteln [offen].



In questo caso, non si tratta dell'hardware di SimonsVoss, pertanto non può essere eseguita nessuna installazione/assistenza da parte di SimonsVoss. Noti produttori di tali dispositivi sono, ad esempio, le aziende Silex e W&T.



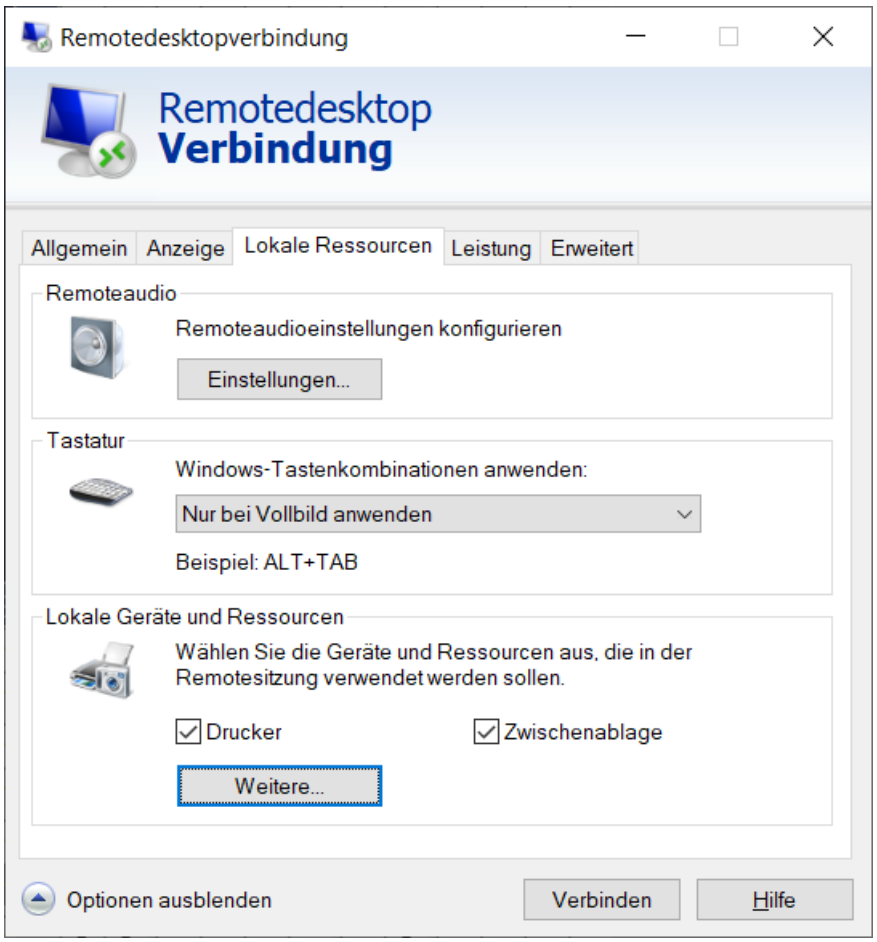
9.30.2 SmartCD MP / HF

9.30.2.1 Collegamento desktop remoto (fino a LSM 3.5 SP1)

✓ Lo SmartCD.MP e lo SmartCD.HF non possono essere collegati tramite il CommNodeAgent. La trasmissione avviene direttamente tramite il collegamento desktop remoto.

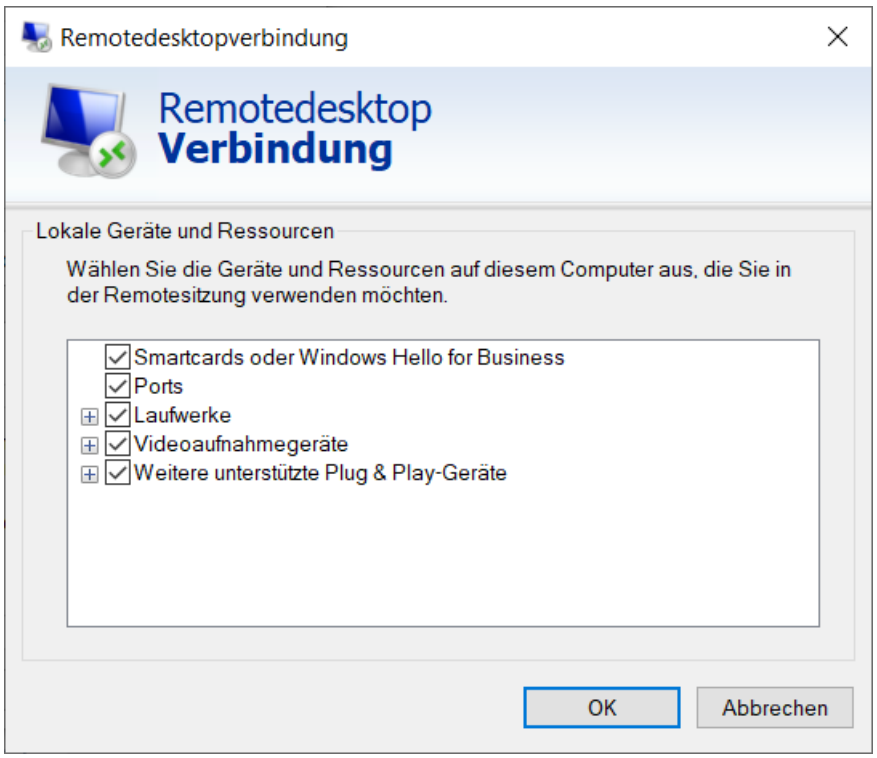
1. Aprire le impostazioni di collegamento della sessione di desktop remoto.
2. Fare clic sul tasto remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen], per visualizzare le opzioni.

3. Passare alla scheda [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

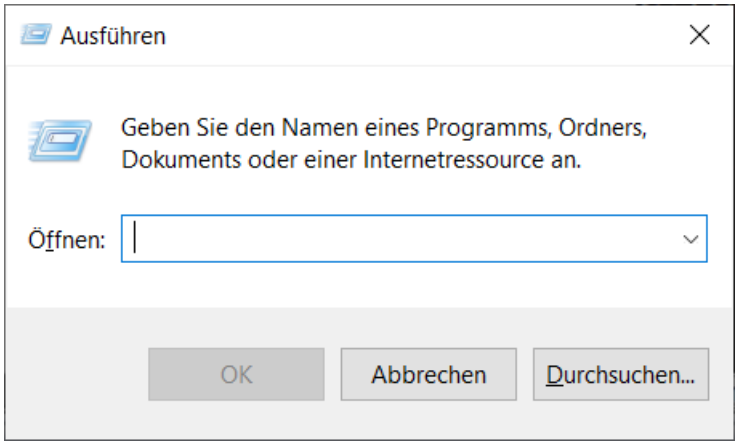


4. Fare clic sul tasto Remotedesktop Einstellungen lokale: Weitere [offen] .

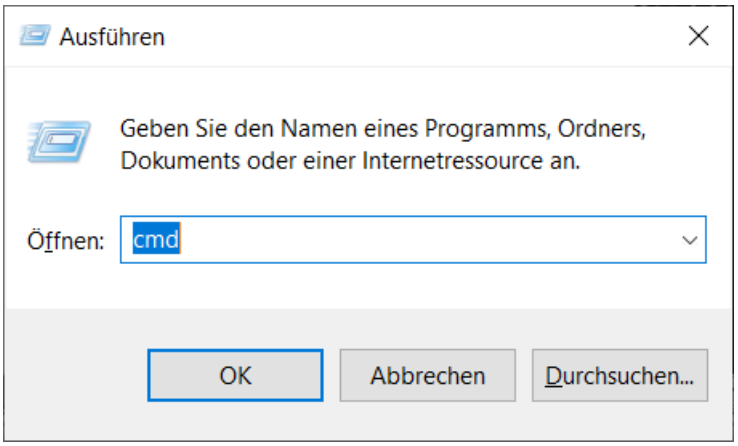
5. Assicurarsi che la casella di controllo ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] sia attivata.



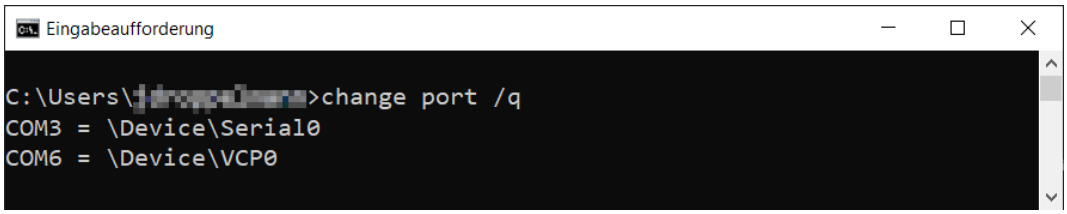
6. Fare clic sul pulsante OK.
7. Collegarsi al desktop remoto.
8. Toccare il tasto Windows e R contemporaneamente.
   ↳ La finestra "Esegui" si apre.



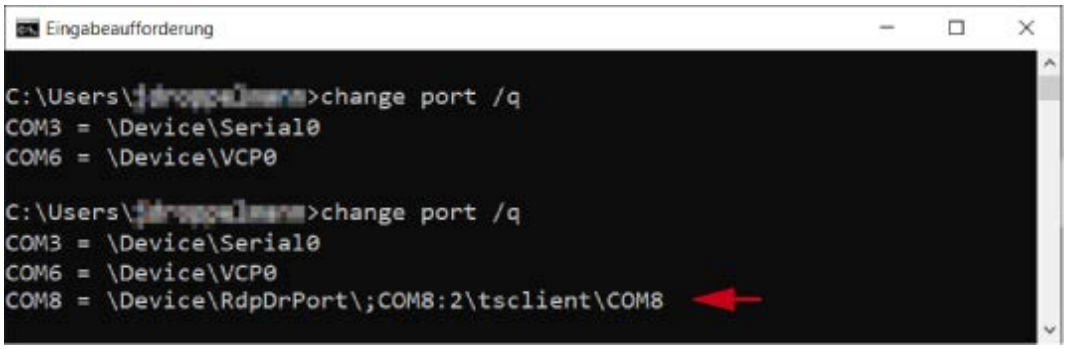
9. Nel campo di immissione inserire **CMD**.



10. Fare clic sul pulsante OK.
    ↳ La finestra "Terminalserver: Eingabeaufforderung [offen]" si apre.
11. Disinserire lo SmartCD.MP/SmartCD.HF nel Terminal Client.
12. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

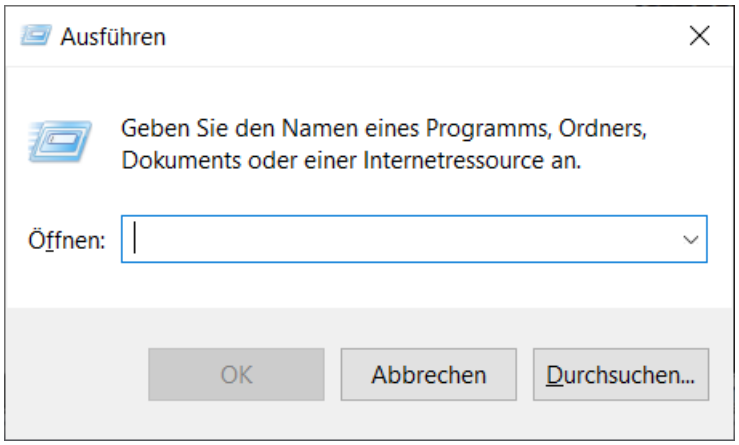


    ↳ Il comando mostra l'uscita senza lo SmartCD.MP/SmartCD.HF collegato.
13. Reinserire lo SmartCD.MP/SmartCD.HF nel Terminal Client.
14. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

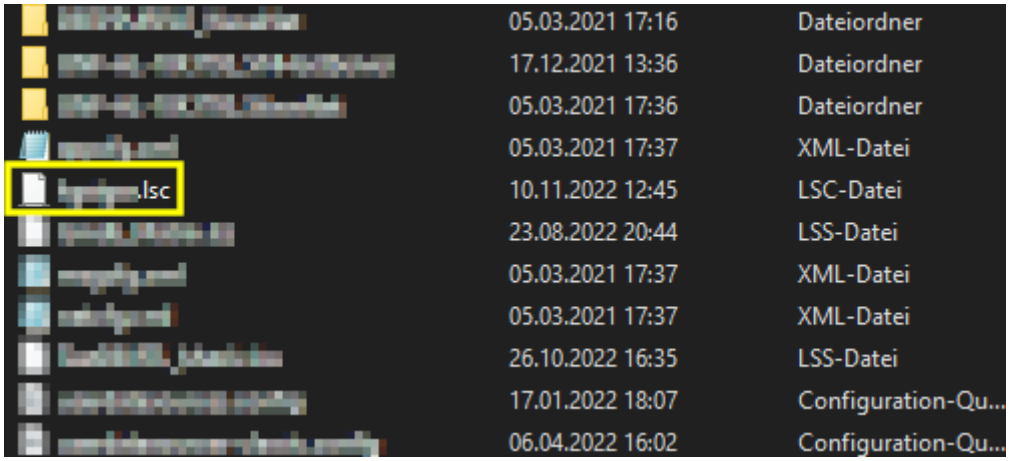


    ↳ Il secondo comando mostra l'uscita con lo SmartCD.MP/SmartCD.HF collegato. È stata aggiunta una nuova porta.
    → In questo caso la porta COM 8 è lo SmartCD.MP/SmartCD.HF trasmesso.

15. Toccare il tasto Windows e R contemporaneamente.
    ↳ La finestra "Esegui" si apre.



16. Inserire il percorso nella directory dell'utente LSM: %localappdata%\SimonsVoss\LockSysMgr\config\.
17. Fare clic sul pulsante OK.
    ↳ Explorer mostra la directory dell'utente LSM.



NOTA

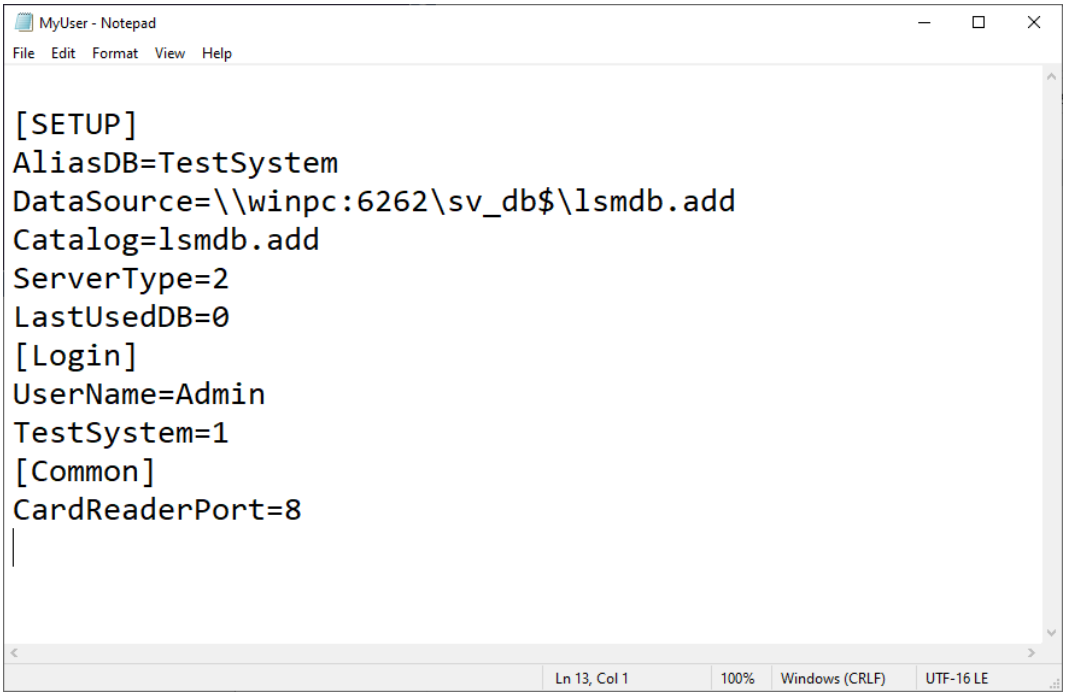
File LSC per gli utenti LSM

In questa posizione, LSM crea un file di configurazione (.lsc) per ogni utente che abbia effettuato il login almeno una volta.

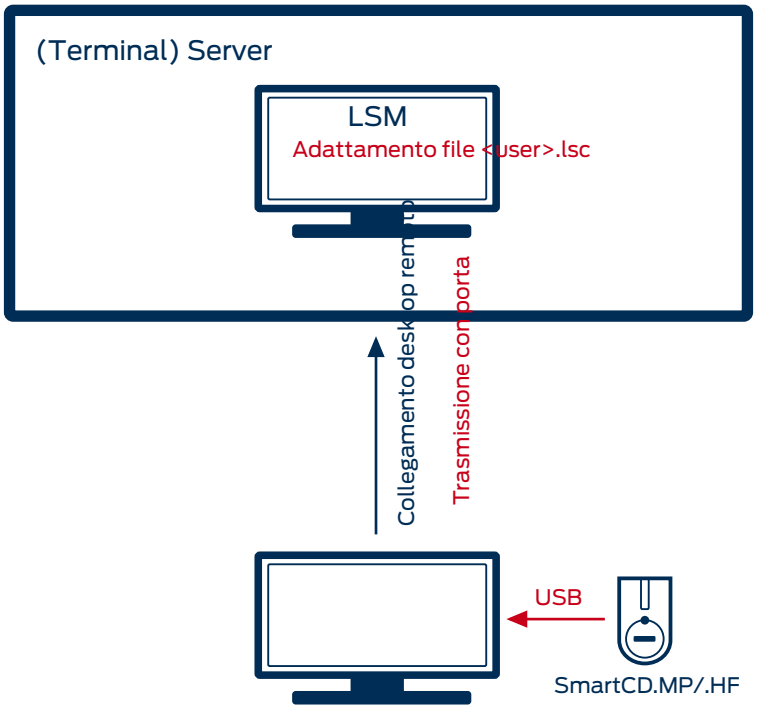
- Se per un utente non è ancora disponibile un file di configurazione, chiedere all'utente di effettuare il login a LSM.

18. Aprire il file di configurazione facendo doppio clic.
19. In questo file, sotto la riga [Common] aggiungere la riga: **CardReaderPort=<PORT>**

20. Sostituire **<PORT>** con il valore precedentemente determinato con il "Terminalserver: Eingabeaufforderung [offen]".



21. Salvare il file di configurazione modificato.
22. Se necessario, aggiungere le righe anche per tutti gli altri utenti nei relativi file di configurazione.
23. Se necessario, terminare la sessione LSM.
24. Riavviare la sessione di desktop remoto.

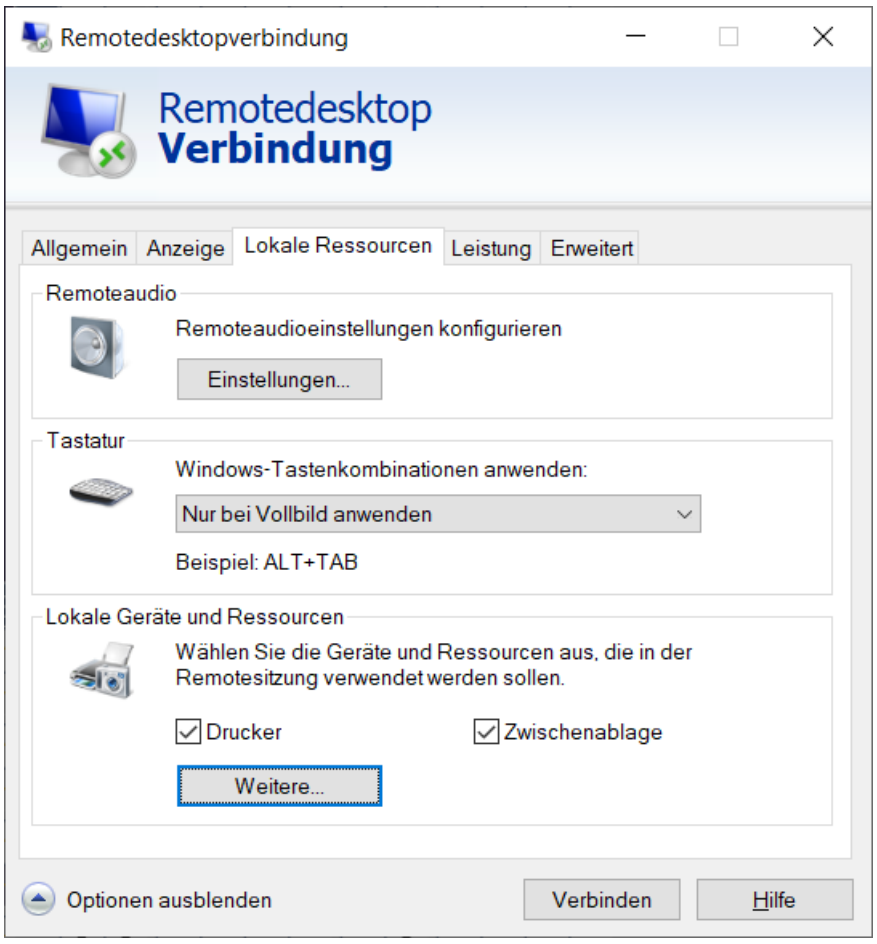


9.30.2.2 Collegamento desktop remoto (a partire da LSM 3.5 SP2)

A partire da LSM 3.5 SP2 è possibile gestire direttamente in LSM le porte di desktop remoto trasmesse per ogni nome host.

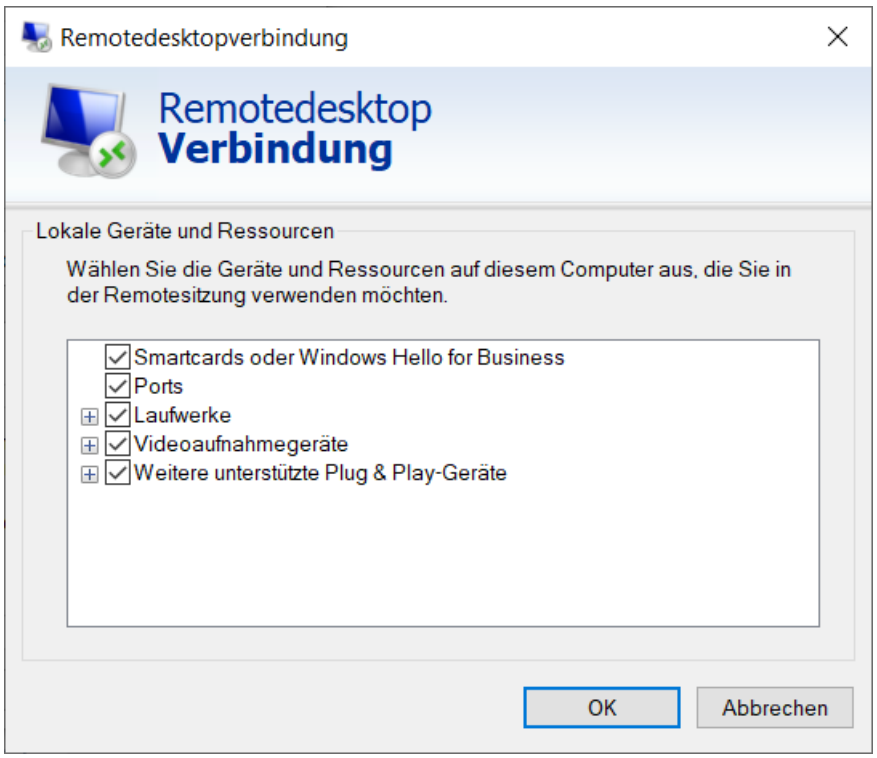
✓ Lo SmartCD.MP e lo SmartCD.HF non possono essere collegati tramite il CommNodeAgent. La trasmissione avviene direttamente tramite il collegamento desktop remoto.

1. Aprire le impostazioni di collegamento della sessione di desktop remoto.
2. Fare clic sul tasto remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen] , per visualizzare le opzioni.
3. Passare alla scheda [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

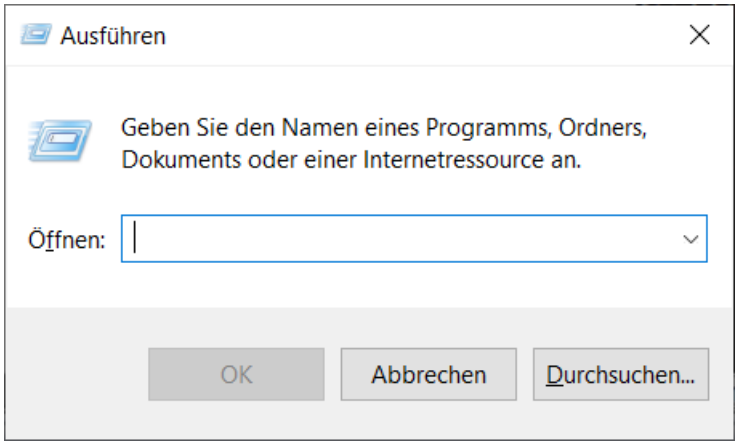


4. Fare clic sul tasto Remotedesktop Einstellungen lokale: Weitere [offen] .

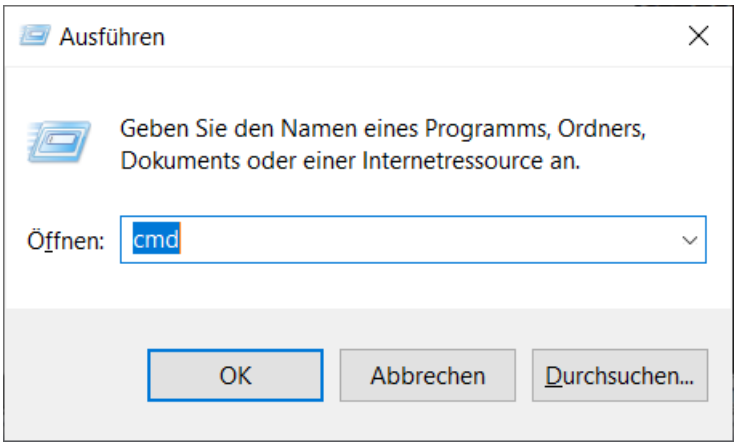
5. Assicurarsi che la casella di controllo ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] sia attivata.



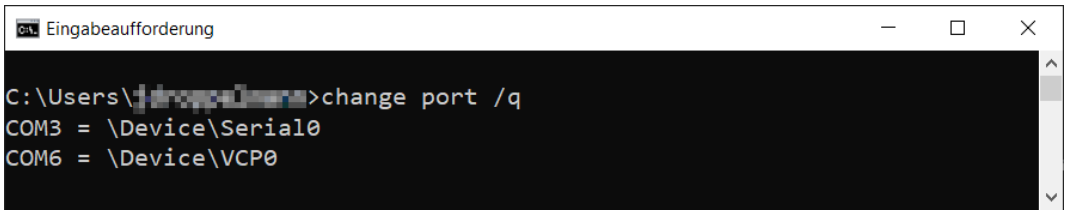
6. Fare clic sul pulsante OK.
7. Collegarsi al desktop remoto.
8. Toccare il tasto Windows e R contemporaneamente.
   ↳ La finestra "Esegui" si apre.



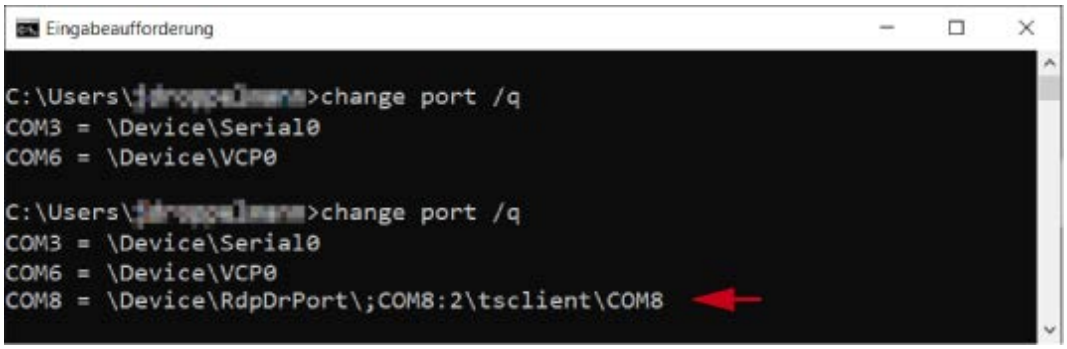
9. Nel campo di immissione inserire **CMD**.



10. Fare clic sul pulsante OK.
    ↳ La finestra "Terminalserver: Eingabeaufforderung [offen]" si apre.
11. Disinserire lo SmartCD.MP/SmartCD.HF nel Terminal Client.
12. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

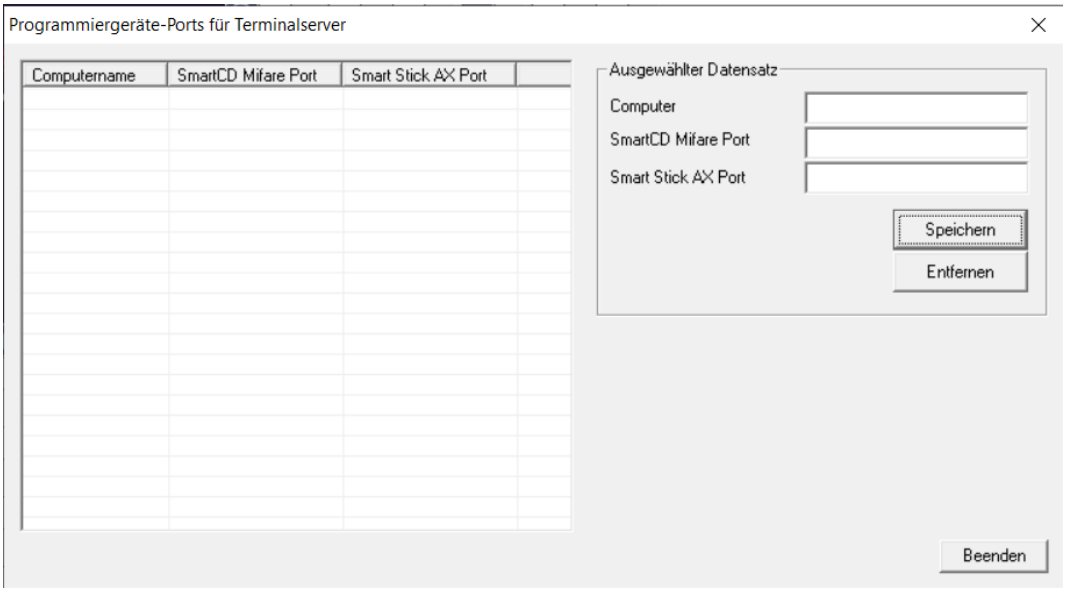


    ↳ Il comando mostra l'uscita senza lo SmartCD.MP/SmartCD.HF collegato.
13. Reinserire lo SmartCD.MP/SmartCD.HF nel Terminal Client.
14. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

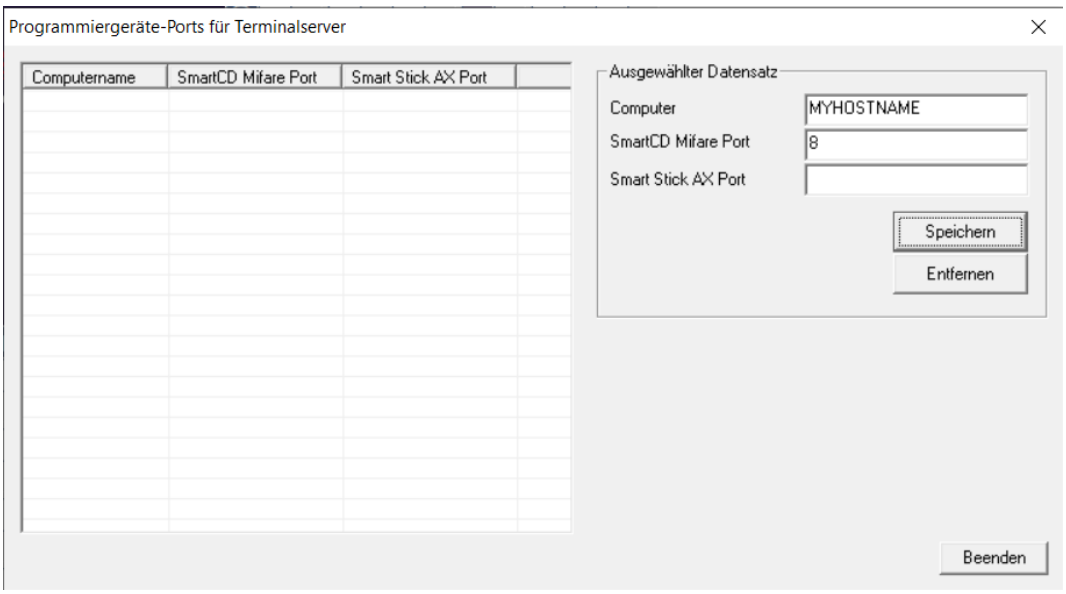


    ↳ Il secondo comando mostra l'uscita con lo SmartCD.MP/SmartCD.HF collegato. È stata aggiunta una nuova porta.
    → In questo caso la porta COM 8 è lo SmartCD.MP/SmartCD.HF trasmesso.

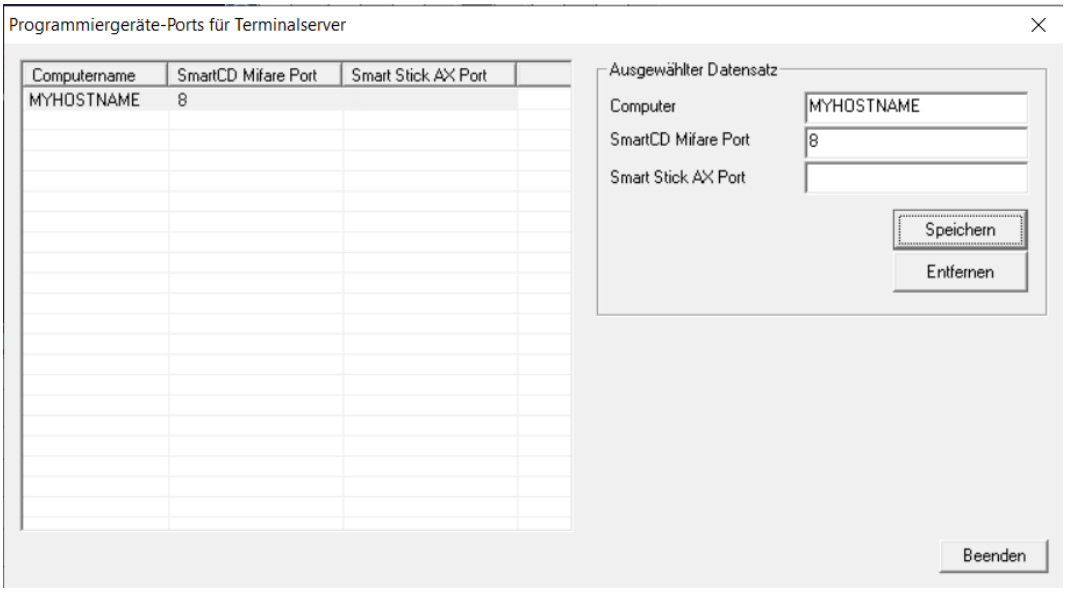
15. In LSM selezionare nella barra superiore del programma da | Rete | la voce Terminalserver Ports.
    ↳ La finestra "LSM: Netzwerk - Programmiergeräte-Ports für Terminalserver [offen]" si apre.



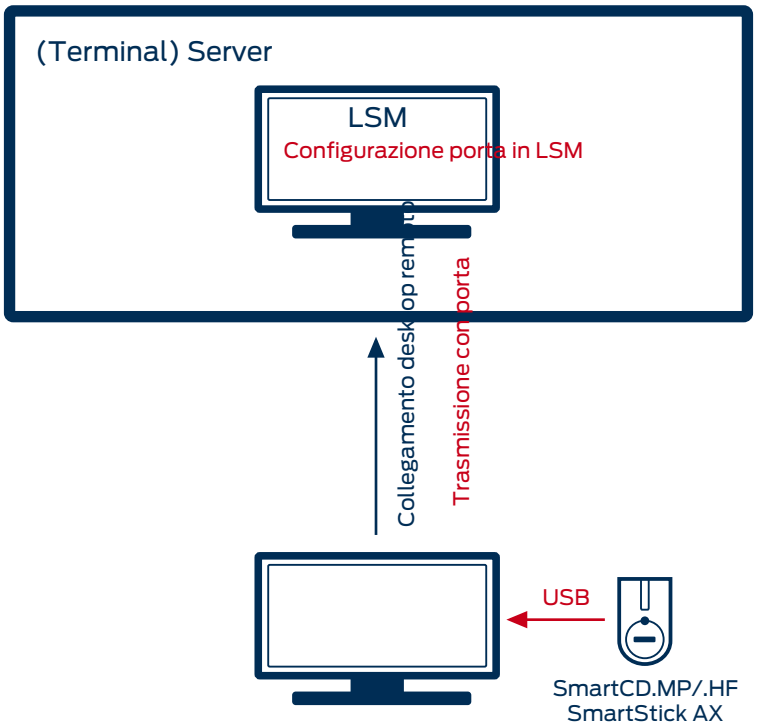
16. Nel campo di immissione Computer [offen] inserire il nome host.
17. Nel campo di immissione LSM Terminalserver Port+Hostname: SmartCD Mifare Port [offen] inserire la porta individuata mediante la finestra "Terminalserver: Eingabeaufforderung [offen]".



18. Fare clic sul tasto LSM Netzwerk Port für Terminalserver und Hostnamen eingeben: Speichern [offen].
    ↳ Viene creata la riga per il nome host e la porta.



19. Se necessario, terminare la sessione LSM.
20. Riavviare la sessione di desktop remoto.



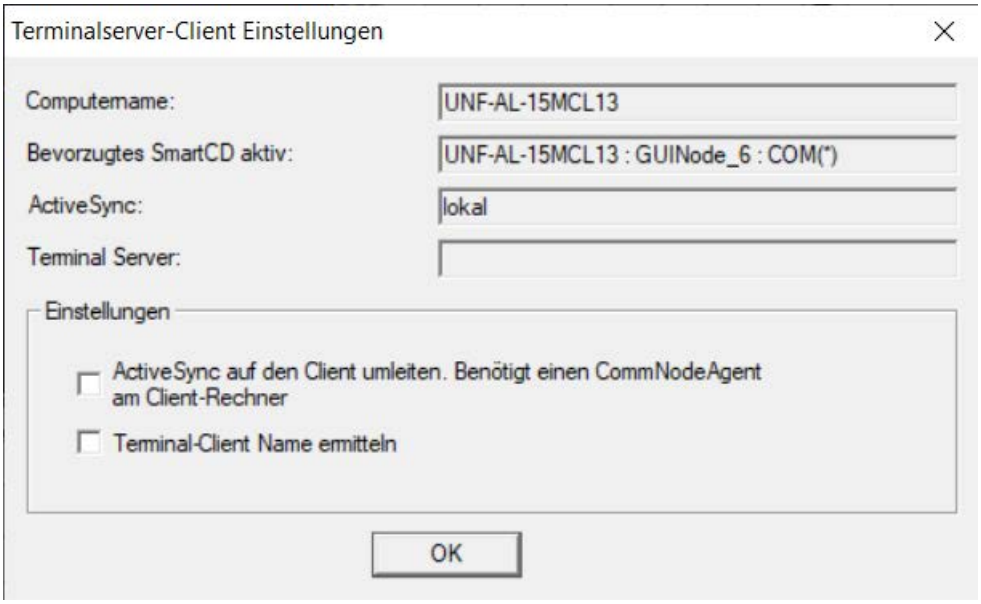
9.30.2.3 Server USB / Ethernet

I dispositivi USB possono essere trasmessi mediante server USB/Ethernet tramite la rete cliente a un (Terminal) server.

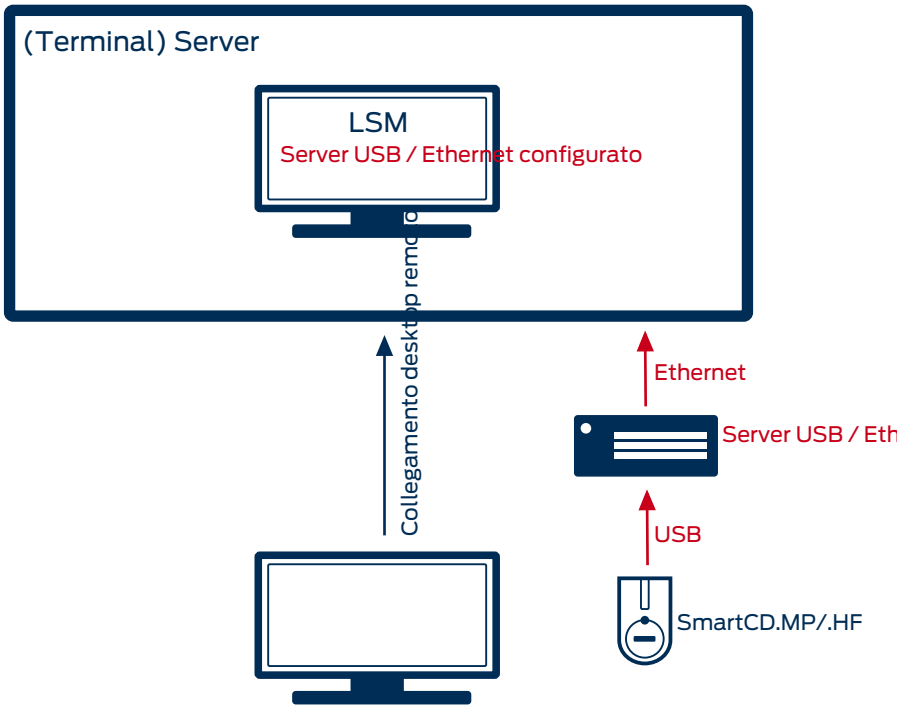
Nel Terminal Client non deve essere eseguita nessuna installazione.

✓ Il software server USB deve essere installato centralmente sul server.
✓ Anche il server USB necessita della relativa configurazione di rete.

1. Selezionare nella barra superiore del programma da | Rete | la voce Terminalserver-Client Einstellungen.
2. Disattivare la casella di controllo ☐ Netzwerk: Terminal-Client Name ermitteln [offen].
   ↳ Un file di configurazione personalizzato (*.lsc, vedere *Collegamento desktop remoto (fino a LSM 3.5 SP1) [▸ 176]*) può determinare malfunzionamenti; se necessario, rimuovere le voci.



In questo caso, non si tratta dell'hardware di SimonsVoss, pertanto non può essere eseguita nessuna installazione/assistenza da parte di SimonsVoss. Noti produttori di tali dispositivi sono, ad esempio, le aziende Silex e W&T.



9.30.3 SmartStick AX

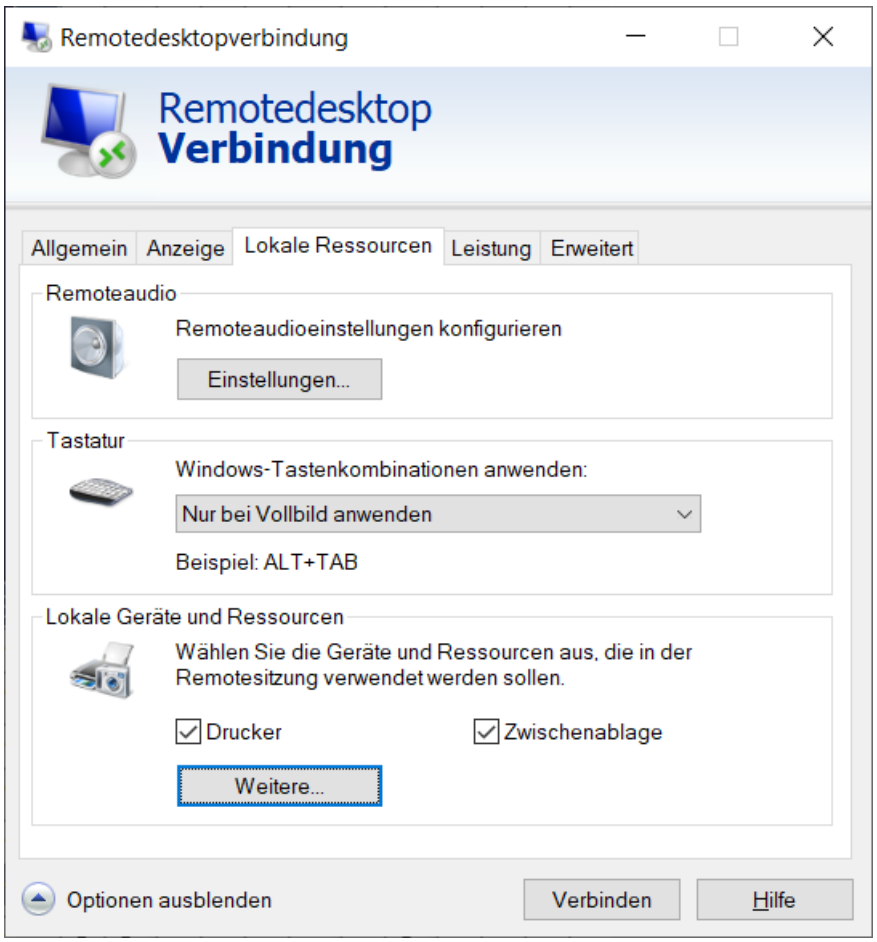
9.30.3.1 Collegamento desktop remoto (a partire da LSM 3.5 SP2)

A partire da LSM 3.5 SP2 è possibile gestire direttamente in LSM le porte di desktop remoto trasmesse per ogni nome host.

✓ Lo SmartStick AX non può essere collegato tramite il CommNodeAgent. La trasmissione avviene direttamente tramite il collegamento desktop remoto.

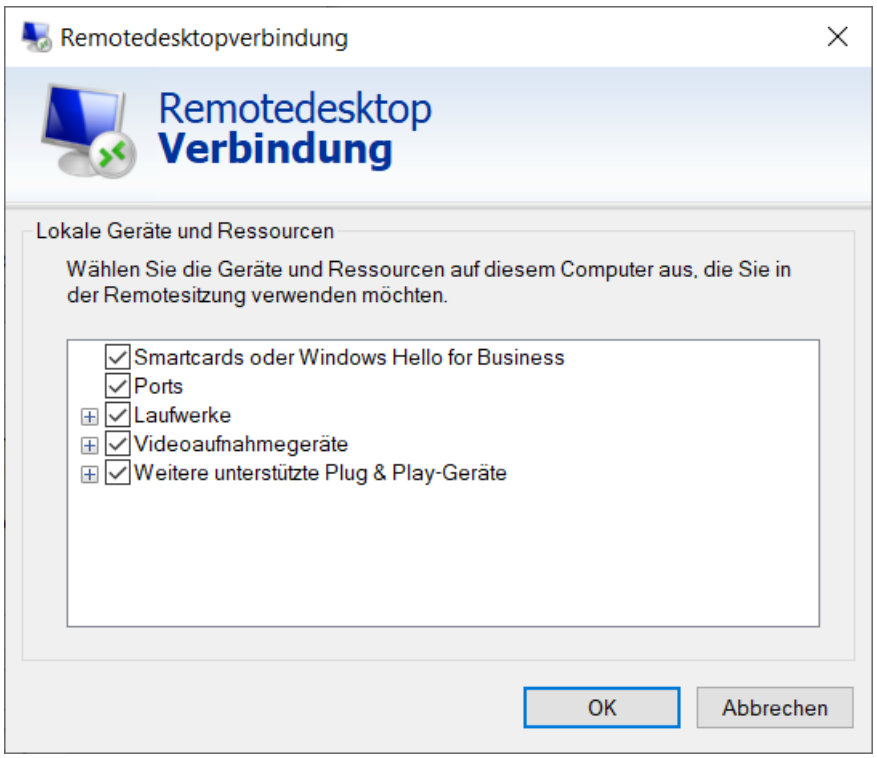
1. Aprire le impostazioni di collegamento della sessione di desktop remoto.
2. Fare clic sul tasto remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen], per visualizzare le opzioni.

3. Passare alla scheda [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

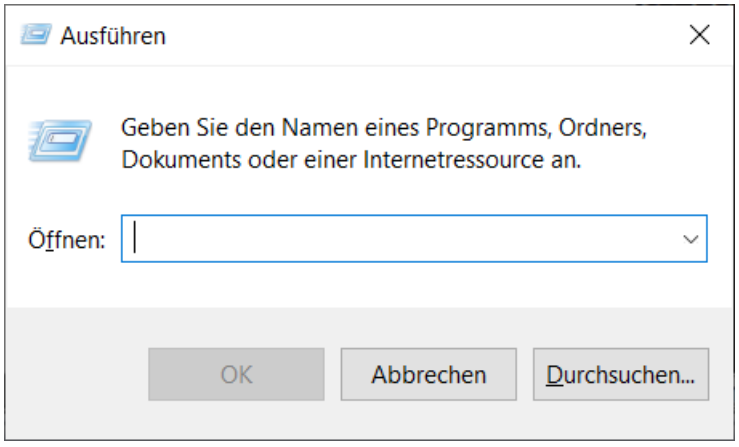


4. Fare clic sul tasto Remotedesktop Einstellungen lokale: Weitere [offen] .

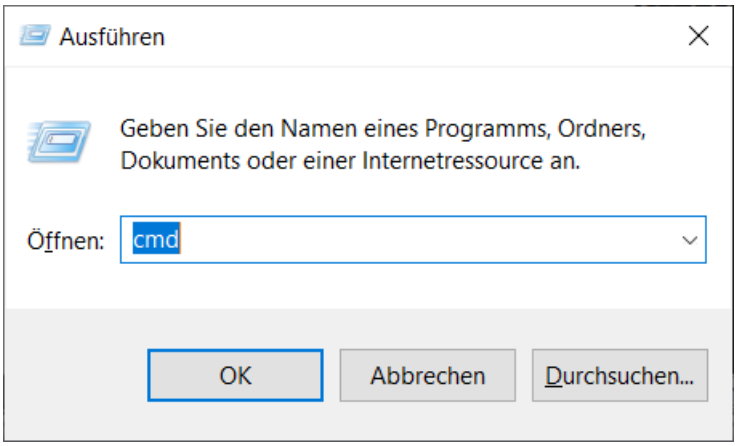
5. Assicurarsi che la casella di controllo ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] sia attivata.



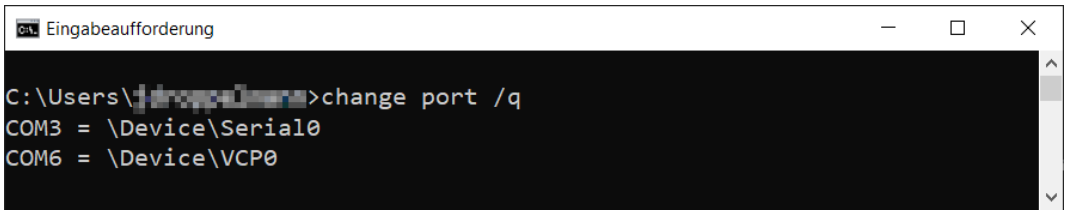
6. Fare clic sul pulsante OK.
7. Collegarsi al desktop remoto.
8. Toccare il tasto Windows e R contemporaneamente.
   ↳ La finestra "Esegui" si apre.



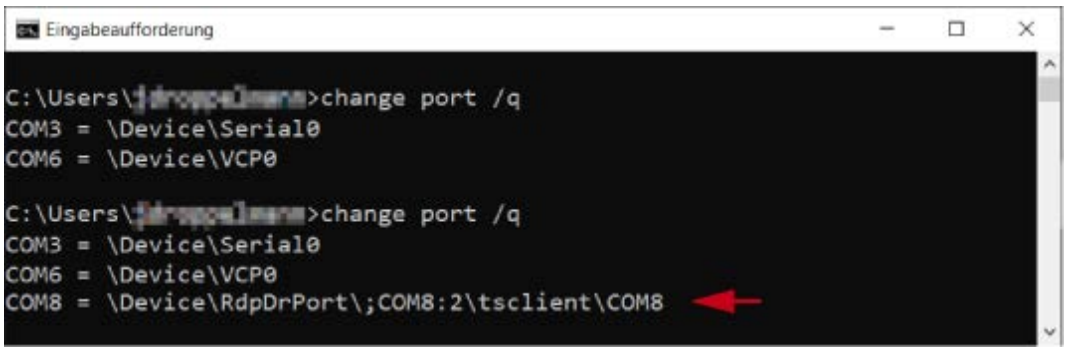
9. Nel campo di immissione inserire **CMD**.



10. Fare clic sul pulsante OK.
    ↳ La finestra "Terminalserver: Eingabeaufforderung [offen]" si apre.
11. Disinserire lo SmartStick AX nel Terminal Client.
12. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

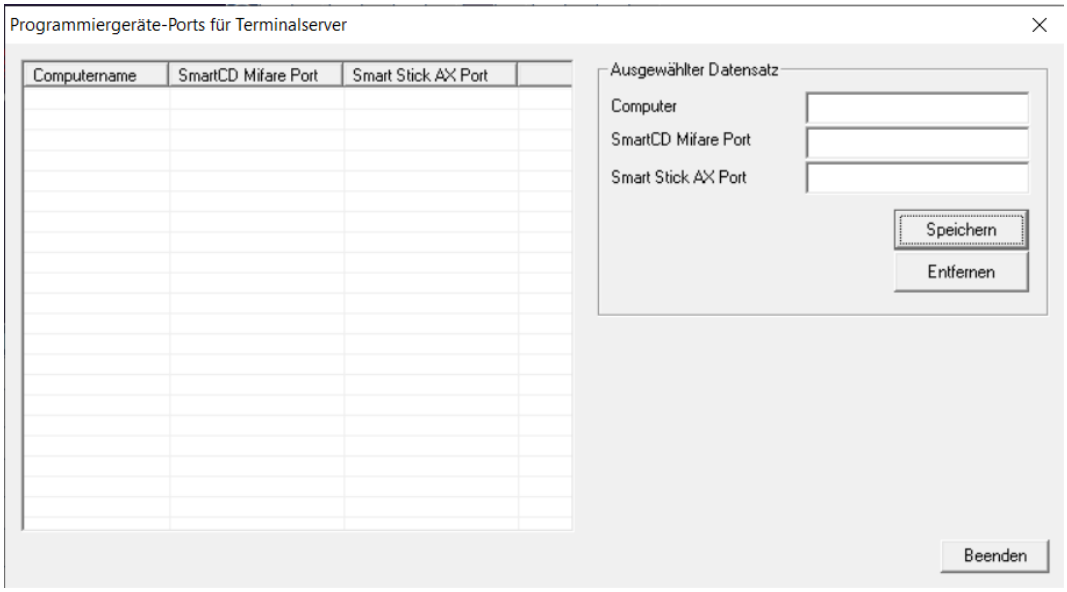


    ↳ Il comando mostra l'uscita senza lo SmartStick AX collegato.
13. Ricollegare lo SmartStick AX nel Terminal Client.
14. Inserire *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

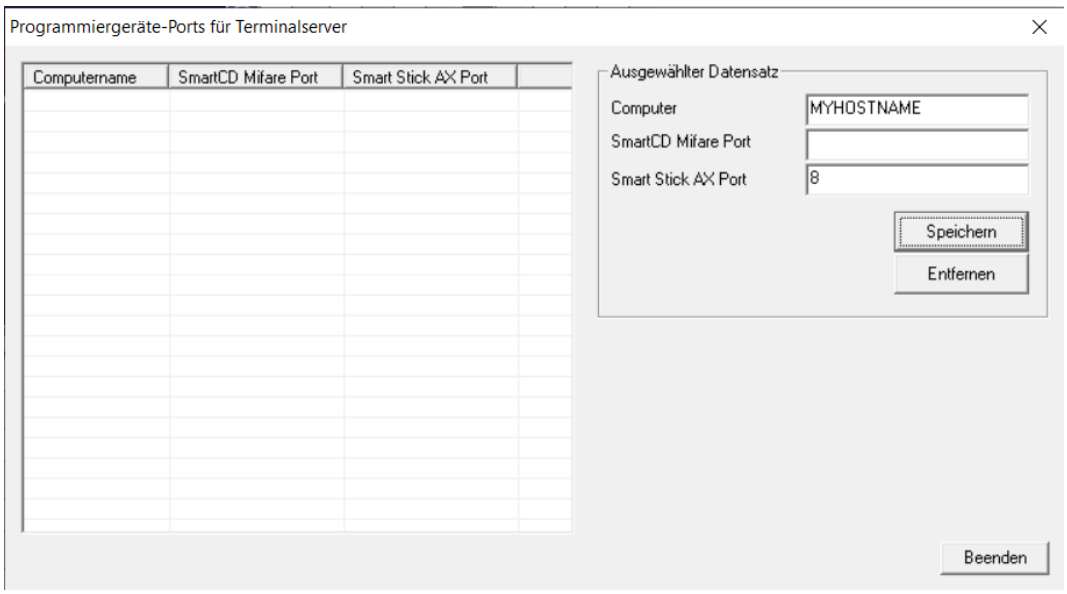


    ↳ Il secondo comando mostra l'uscita con lo SmartStick AX collegato. È stata aggiunta una nuova porta.
    → In questo caso la porta COM 8 è lo SmartStick AX trasmesso.

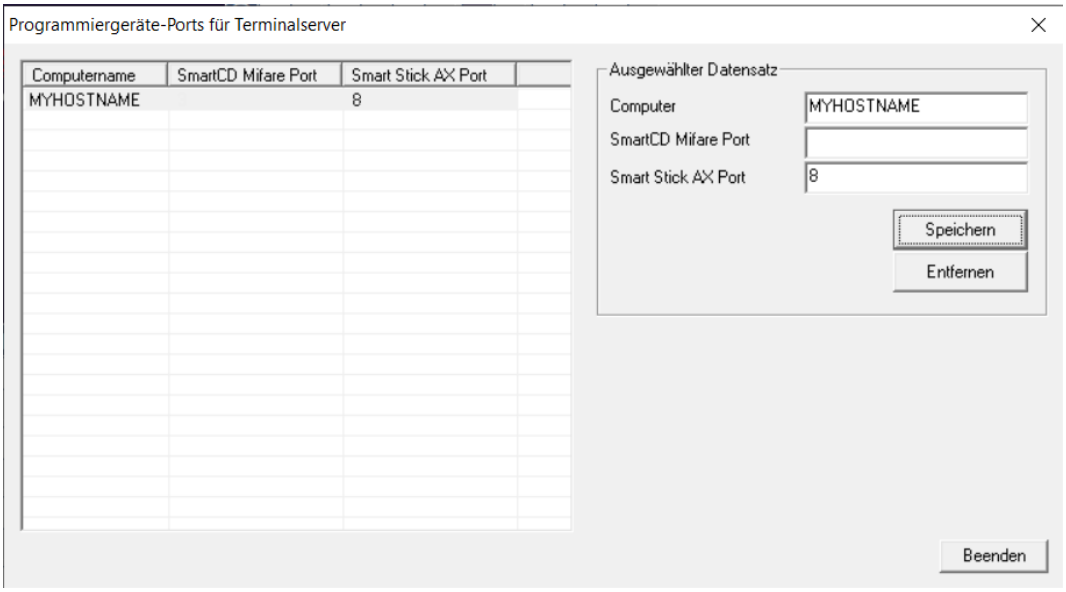
15. In LSM selezionare nella barra superiore del programma da | Rete | la voce Terminalserver Ports.
    ↳ La finestra "LSM: Netzwerk - Programmiergeräte-Ports für Terminalserver [offen]" si apre.



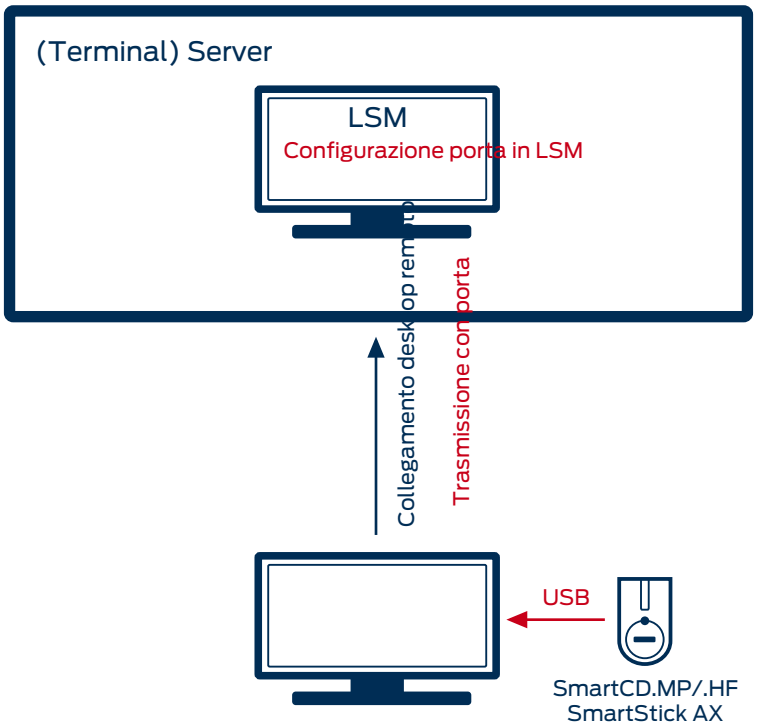
16. Nel campo di immissione Computer [offen] inserire il nome host.
17. Nel campo di immissione LSM Terminalserver Port+Hostname: Smart Stick AX Port [offen] inserire la porta individuata mediante la finestra "Terminalserver: Eingabeaufforderung [offen]".



18. Fare clic sul tasto LSM Netzwerk Port für Terminalserver und Hostnamen eingeben: Speichern [offen].
    ↳ Viene creata la riga per il nome host e la porta.



19. Se necessario, terminare la sessione LSM.
20. Riavviare la sessione di desktop remoto.



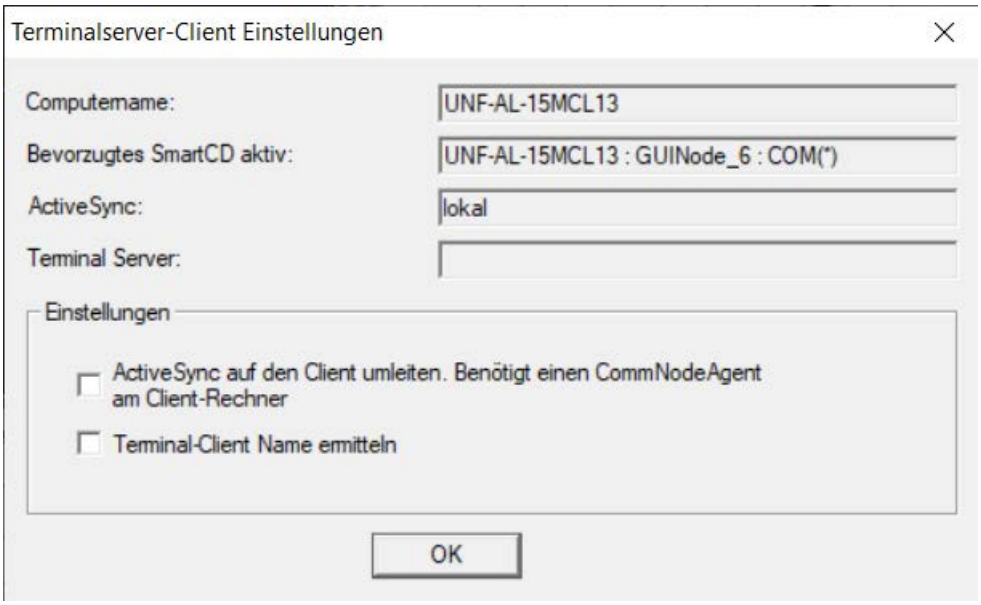
9.30.3.2 Server USB / Ethernet

I dispositivi USB possono essere trasmessi mediante server USB/Ethernet tramite la rete cliente a un (Terminal) server.

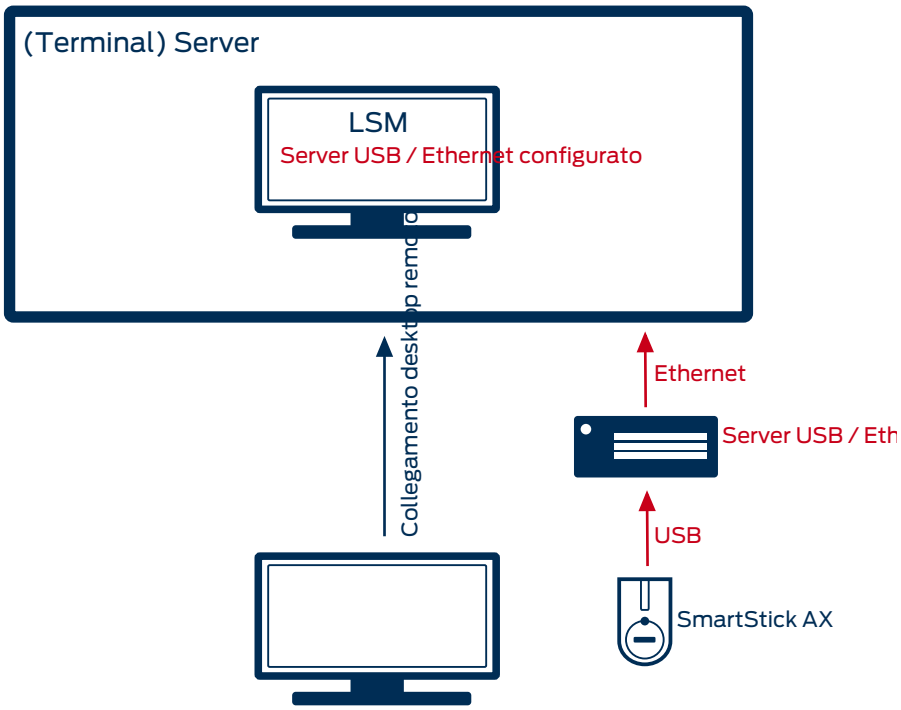
Nel Terminal Client non deve essere eseguita nessuna installazione.

✓ Il software server USB deve essere installato centralmente sul server.
✓ Anche il server USB necessita della relativa configurazione di rete.

1. Selezionare nella barra superiore del programma da | Rete | la voce Terminalserver-Client Einstellungen.
2. Disattivare la casella di controllo ☐ Netzwerk: Terminal-Client Name ermitteln [offen].



In questo caso, non si tratta dell'hardware di SimonsVoss, pertanto non può essere eseguita nessuna installazione/assistenza da parte di SimonsVoss. Noti produttori di tali dispositivi sono, ad esempio, le aziende Silex e W&T.



10. Esecuzione di attività correnti basate su WaveNet in LSM

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.

10.1 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.

10.1.1 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 Decompressione)
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.

10.1.2 Prima programmazione dei componenti di chiusura

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

10.1.2.1 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".

10.1.2.2 Programmazione della chiusura

✓ Una chiusura è stata creata nell'impianto di chiusura ed è visibile nella matrice.

1. Fate clic con il tasto destro sulla chiusura desiderata.
2. Fate clic su Programmazione.
3. Seguite le istruzioni del software LSM.

Assicuratevi di selezionare il dispositivo di programmazione appropriato.

NOTA

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

Rifiuto del primo azionamento del transponder dopo la programmazione iniziale dei prodotti AX

Se il primo mezzo di identificazione azionato dopo la programmazione iniziale è un transponder, allora il transponder viene respinto una volta e sincronizzato con la chiusura in background. Dopo di che, i transponder funzionano come di consueto.

10.1.3 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.

10.1.4 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.

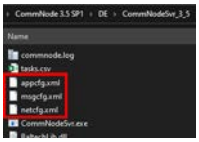
1. Aprire il software LSM.
2. Selezionare | Rete |/ Nodi di comunicazione .
3. Compilare le informazioni "Nome", "Nome PC" e "Descrizione".

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

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

   ↳ *Ad es. UNF-AL-18KJ793; UNF-AL-18KJ793.ALLEGION.COM; Nodo di comunicazione per la rete radio WaveNet 123.*

4. Fare clic sul pulsante File di configurazione .
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 Esci .

10.1.5 Configurazione della rete e importazione nell'LSM

10.1.5.1 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 RounterNode2 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.

10.1.5.2 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".

10.1.5.3 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 *(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".

10.1.5.4 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.

10.2 Messa in funzione del chiusure DoorMonitoring

Questo esempio mostra le impostazioni da effettuare per la configurazione delle chiusure DoorMonitoring. I requisiti sono indicati al capitolo "*Creazione di una rete radio WaveNet e integrazione di una chiusura [▸ 195]*".

10.2.1 Possibili stati (porta)

Gli stati visualizzati dipendono dai componenti.

10.2.1.1 Possibili stati DoorMonitoring della SmartHandle

- Porta aperta/chiusa
- Porta aperta troppo a lungo
- Bloccata (solo per chiusure autobloccanti)
- Maniglia premuta/non premuta

10.2.1.2 Possibili stati DoorMonitoring del cilindro di chiusura

- Porta aperta/chiusa
- Porta bloccata
- Porta bloccata con sicurezza
- Porta aperta troppo a lungo
- Vite di fissaggio manipolata

10.2.1.3 Possibili stati DoorMonitoring dello SmartRelè 3

- Input 1 attivo/non attivo
- Input 2 attivo/non attivo
- Input 3 attivo/non attivo
- *Riconoscimento sabotaggi [▸ 202]*

10.2.1.4 Possibili stati RouterNode 2 / GatewayNode 2

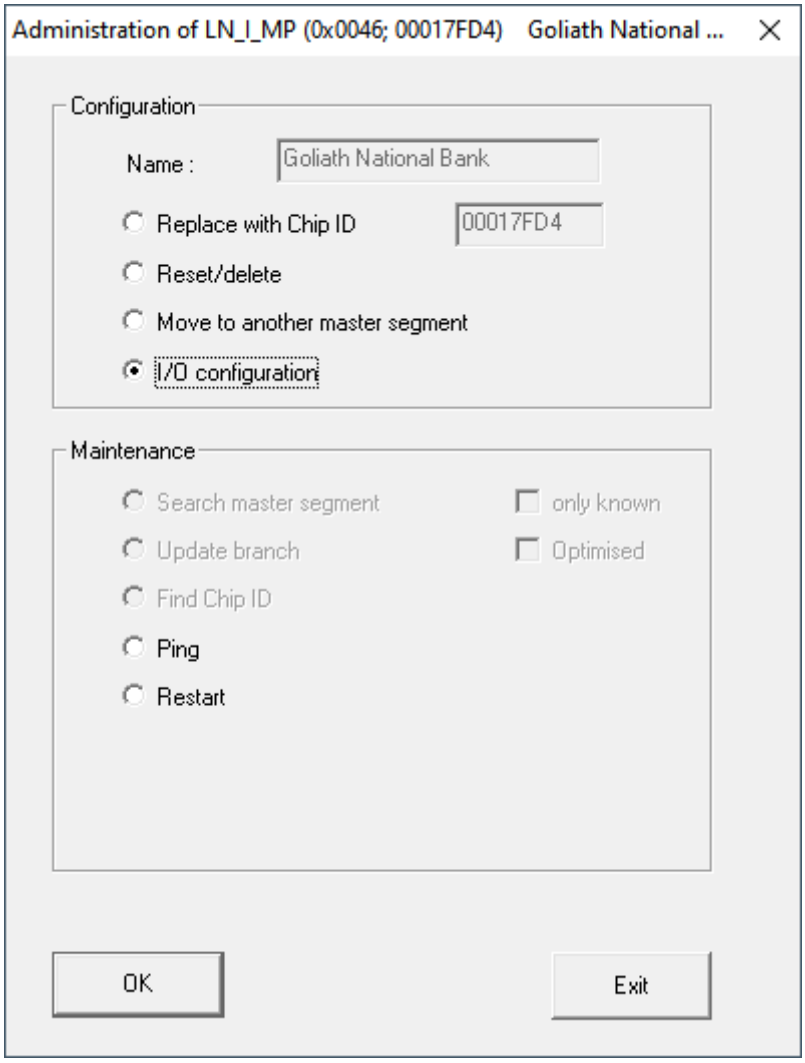
- Input attivo/non attivo/non attivo
- Tensione analogica sopra/sotto il valore di soglia

10.2.2 Integrazione di chiusure DoorMonitoring nella rete

Come integrare le chiusure DM nella rete WaveNet:

- ✓ WaveNet Manager è già configurato.
- ✓ Il RouterNode, al quale deve essere assegnata la nuova chiusura, è già configurato e "online".
- ✓ Il LockNode è montato correttamente sulla chiusura DM.
- ✓ ID Chip noto.

1. Avviare il WaveNet Manager da | Rete | - WaveNet Manager.
2. Fare clic con il tasto destro del mouse sul RouterNode.
   ↳ La finestra "Administration" si apre.
3. Selezionare l'opzione ◉ Find Chip ID.
4. Fare clic sul pulsante OK.
   ↳ La finestra "Administration" si chiude.
5. Seguire la finestra di dialogo e assegnare la chiusura o il corrispondente LockNode al RouterNode2 tramite il suo ID chip.
6. Fare clic con il tasto destro del mouse sul LockNode DM appena aggiunto.
7. Selezionare l'opzione ◉ I/O configuration.
8. Fare clic sul pulsante OK.
   ↳ La finestra "Administration" si apre.



9. Attivare la casella di controllo ☑ Send all events to I/O router.
10. Fare clic sul pulsante OK.
    ↳ La finestra "Administration" si chiude.
11. Fate click sul pulsante SALVA.
12. Fare clic sul pulsante Esci.
13. Fare clic sul pulsante Sì.
    ↳ WaveNet Manager si chiude.
14. Importare le nuove impostazioni e assegnarle al corrispondente nodo di comunicazione.

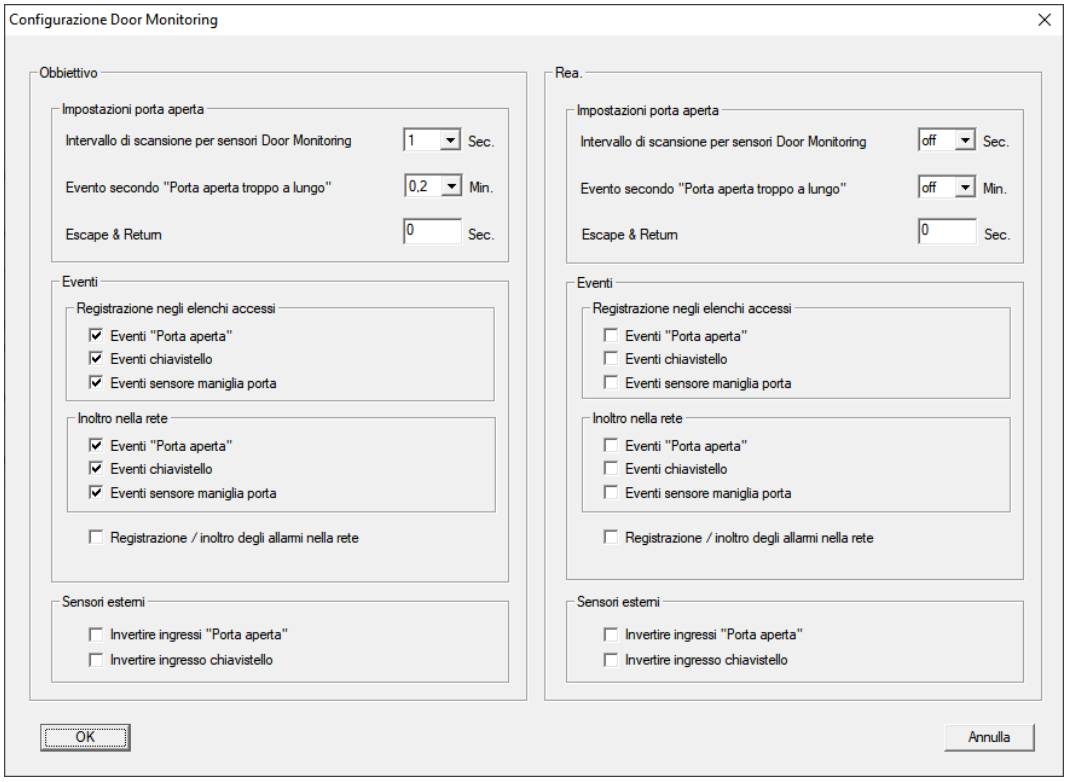
10.2.3 SmartHandle DoorMonitoring

Nella LSM o Smart.Surveil è possibile monitorare le SmartHandle DoorMonitoring. Per fare ciò, tuttavia, è necessario prima configurare le SmartHandle DoorMonitoring in LSM:

✓ LSM aperto.
✓ Vista matrice aperta

1. Aprire le impostazioni facendo doppio clic su SmartHandle DM.

2. Passare alla scheda di registro [Configurazione/dati].
3. Fare clic sul tasto Configurazione Monitoring.
   ↳ La finestra "Configurazione Door Monitoring" si apre.



4. Attivare nell'area "Obbiettivo"-"Eventi" nelle aree "Registrazione negli elenchi accessi" e "Inoltro nella rete" gli eventi DoorMonitoring, che si desidera monitorare (ad es. ☑ Eventi "Porta aperta", ☑ Eventi chiavistello e ☑ Eventi sensore maniglia porta).
5. Se necessario effettuare ulteriori impostazioni DoorMonitoring, ad es. nell'area "Impostazioni porta aperta".
6. Fare clic sul pulsante OK.
   ↳ La finestra "Configurazione Door Monitoring" si chiude.
7. Fare clic sul pulsante Applica.
8. Programmazione della SmartHandle.

↳ Gli eventi DoorMonitoring vengono memorizzati nel database LSM e possono essere analizzati da LSM e da SmartSurveil.

10.2.3.1 Riconoscimento sabotaggi

A partire dall'LSM 3.4 SP2 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) [▸ 215]*).

10.2.3.2 DoorMonitoring (SmartHandle) - Eventi Maniglie

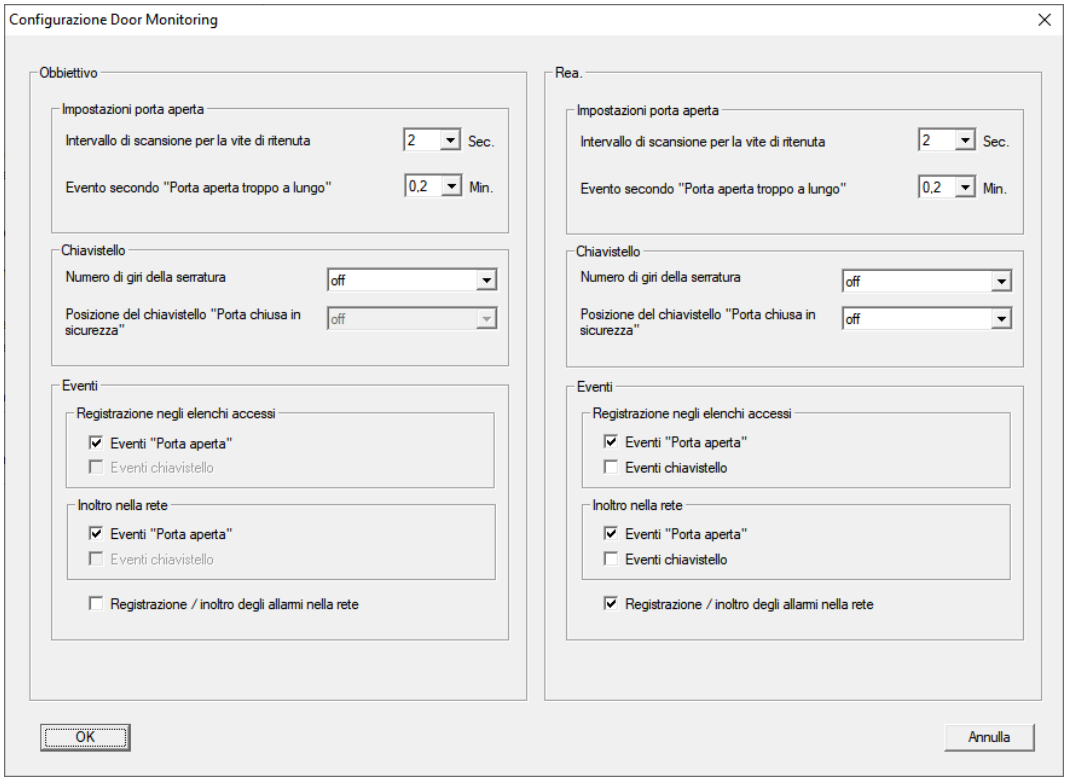
Dall'LSM 3.5 SP3 potete riconoscere lo stato della maniglia sull' SmartHandle AX . Quando la maniglia viene spinta in basso, l'elettronica lo rileva e invia l'informazione all'LSM. Se volete analizzare l'informazione, potete allora impostare un evento al riguardo e reagire (vedi (*Configurazione dell'Event management (eventi) [▸ 215]*).

10.2.4 Cilindri DoorMonitoring

Nella LSM o Smart.Surveil è possibile monitorare i cilindri DoorMonitoring. Per fare ciò, tuttavia, è necessario prima configurare i cilindri DoorMonitoring in LSM:

✓ LSM aperto.
✓ Vista matrice aperta

1. Aprire le impostazioni facendo doppio clic sul cilindro DM.
2. Passare alla scheda di registro [Configurazione/dati].
3. Fare clic sul tasto Configurazione Monitoring .
   ↳ La finestra "Configurazione Door Monitoring" si apre.



4. Attivare nell'area "Obbiettivo"-"Eventi" nelle aree "Registrazione negli elenchi accessi" e "Inoltro nella rete" gli eventi DoorMonitoring, che si desidera monitorare (ad es. ☑ Eventi "Porta aperta").
5. Se necessario effettuare ulteriori impostazioni DoorMonitoring, ad es. nell'area "Impostazioni porta aperta".

6. Fare clic sul pulsante OK.
   ↳ La finestra "Configurazione Door Monitoring" si chiude.
7. Fare clic sul pulsante Applica.
8. Programmare il cilindro.

↳ Gli eventi DoorMonitoring vengono memorizzati nel database LSM e possono essere analizzati da LSM e da SmartSurveil.

10.2.5 Valutazione degli input del controller

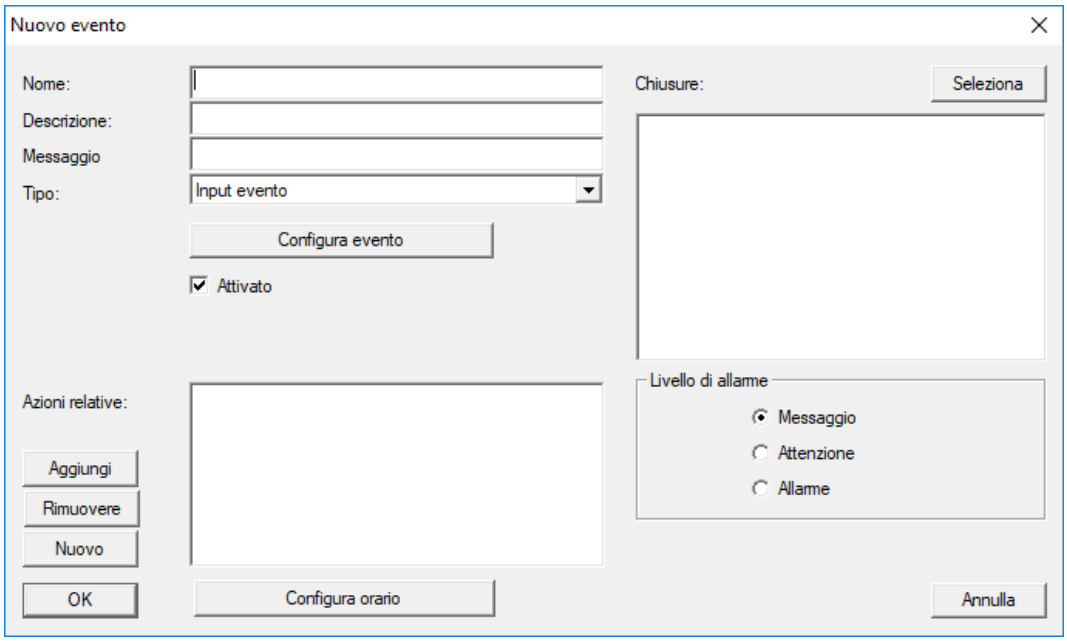
Gli ingressi digitali sul controller del sistema SREL3 ADV possono essere trasferiti all'LSM e qui avviare azioni.

Creazione evento

Se si desidera valutare un imput 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.

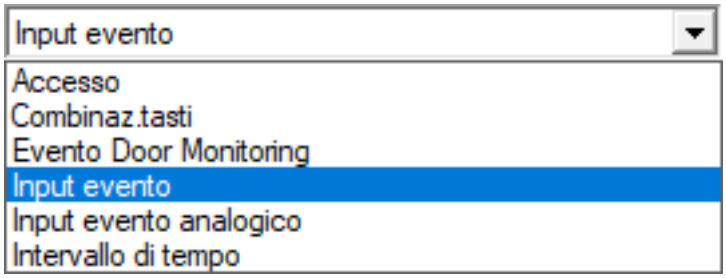
✓ LSM aperto.
✓ Sistema SREL3 ADV creato nella matrice.

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".

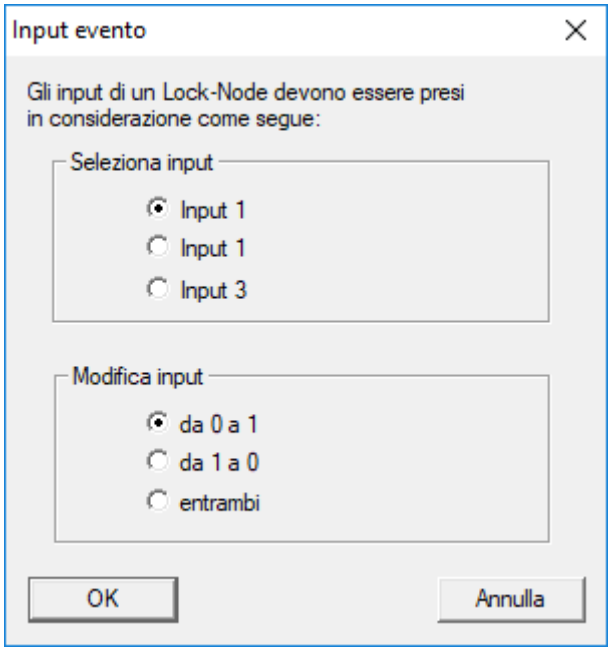


3. Inserire un nome per l'evento.
4. Opzionalmente, inserire una descrizione per l'evento.
5. Opzionalmente, inserire un messaggio.

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.

10.2.6 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".

10.2.7 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".

10.2.8 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 desideri 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.

10.3 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).

10.3.1 Preparare RouterNode per RingCast

NOTA

Disponibilità di RingCast per RouterNode in funzione del firmware

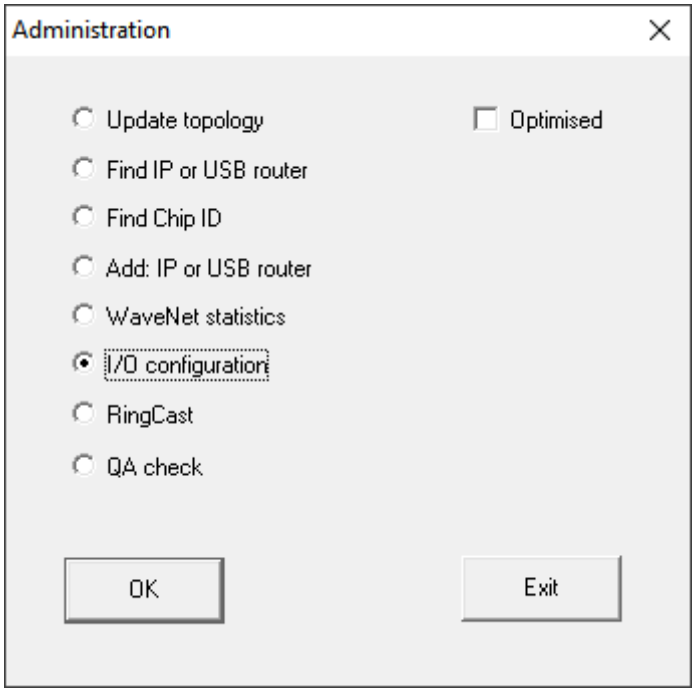
Il supporto RingCast dipende dal firmware (vedere Informazioni firmware).

- Se necessario, aggiornare il firmware (vedere Aggiornamento del firmware).

Preparare i RouterNode per il RingCast:

- ✓ Nella rete radio Wavenet sono configurati e "online" almeno due diversi RouterNode Ringcast compatibili (vedere Informazioni firmware).
- ✓ 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 RouterNode: ingresso digitale).
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.

10.3.2 Creazione del RingCast

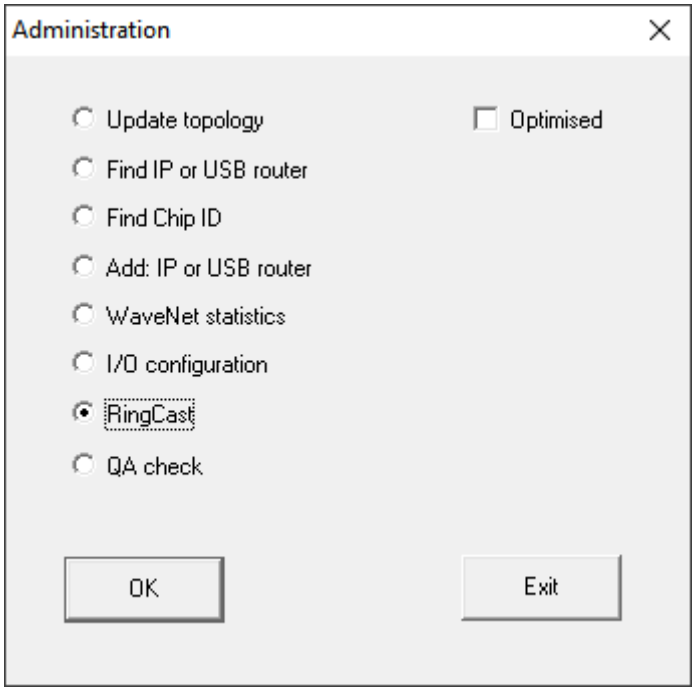
NOTA

Ricalcolo del RingCast

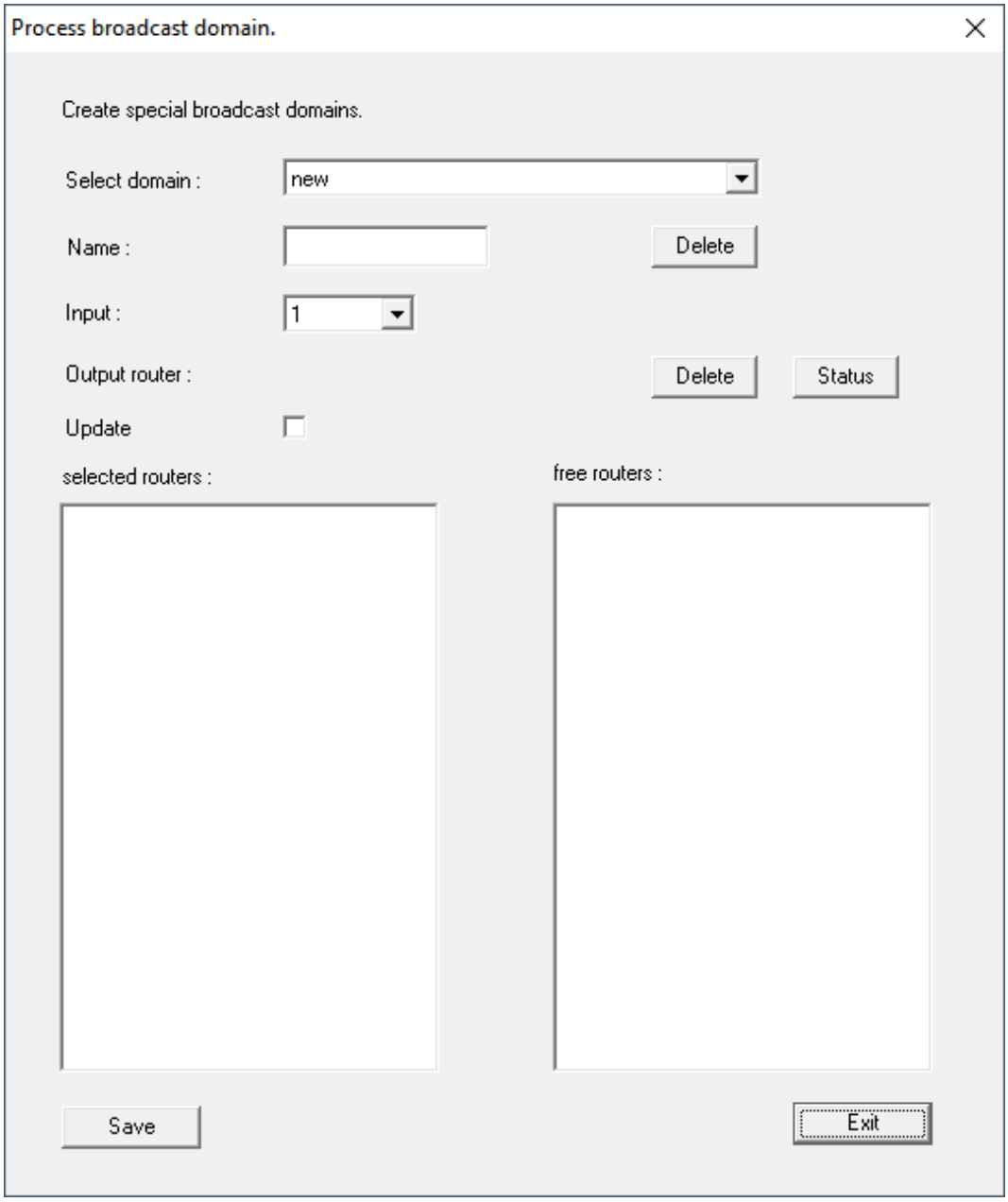
Se si sostituisce o elimina un RouterNode nel RingCast oppure se si modifica la sua configurazione IO rilevante per il RingCast, il RingCast viene ricalcolato automaticamente dopo aver salvato le modifiche e confermato la richiesta.

- ✓ WaveNet Manager aperto tramite LSM (vedere Best Practice: Dal software LSM).
- ✓ RouterNode e LockNode collegati all'alimentazione elettrica.
- ✓ RouterNode e LockNode importati nella topologia WaveNet (vedere Trovare e aggiungere dispositivi).
- ✓ RouterNode per RingCast preparati (vedere *Preparare RouterNode per RingCast [▸ 207]*).

1. Fare clic con il tasto destro del mouse sulla voce WaveNet XX_X.
   ↳ La finestra "Administration" si apre.

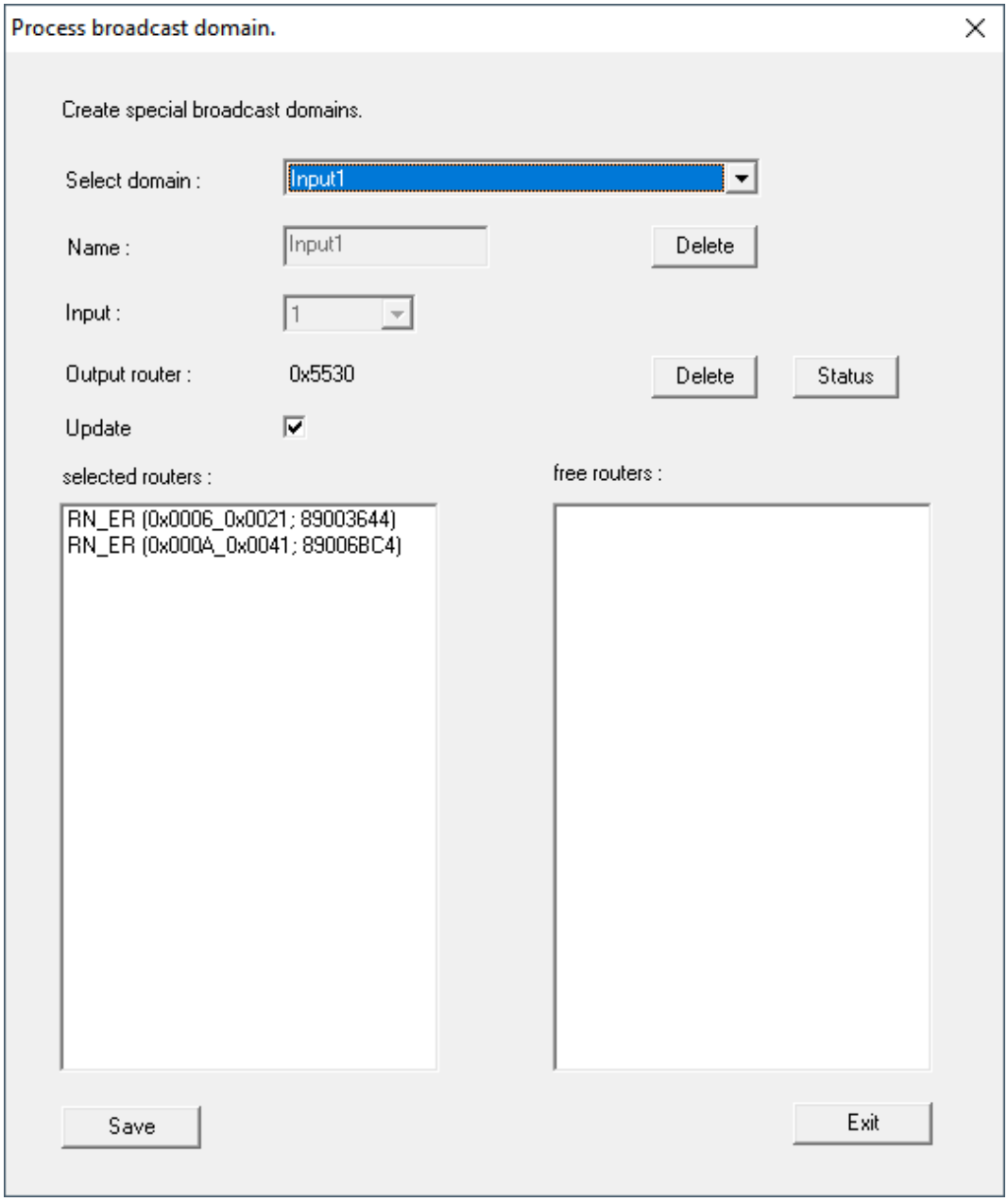


2. Selezionare l'opzione ◉ RingCast.
3. Fare clic sul tasto OK.
   ↳ La finestra "Administration" si chiude.
   ↳ La finestra "Edit radio domains" si apre.

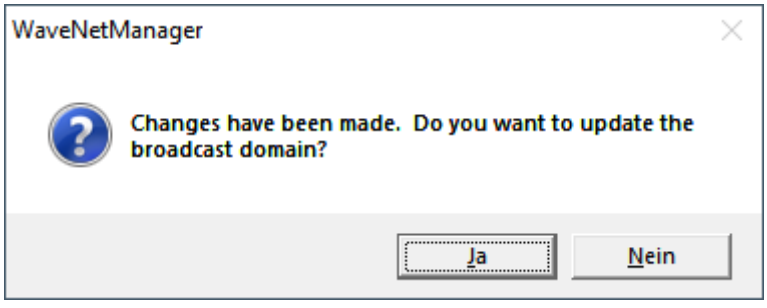


4. Scegliere nel menu a discesa ▼ **Select domain** un ingresso, per il quale con ▼ **Delay [s]** il "RingCast" è stato selezionato.

↳ Nel campo "selected routers" vengono visualizzati tutti i RouterNode2, per cui sull'ingresso con ▼ **Delay [s]** la voce "RingCast" è stata selezionata (=domini).

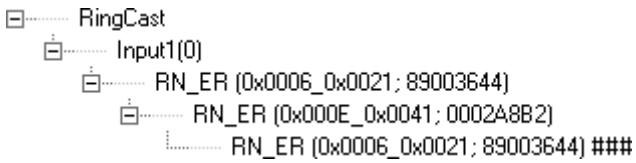


5. Fare clic sul tasto Save.
6. Fare clic sul tasto Esci.
   ↳ La finestra "Edit radio domains" si chiude.
   ↳ La finestra "WaveNetManager" si apre.



7. Fare clic sul tasto Sì.
   ↳ La finestra "WaveNetManager" si chiude.
   ↳ Le modifiche vengono aggiornate.

↳ Il RingCast viene creato ed è visibile nel WaveNet Manager dopo poco.



Salvare le nuove impostazioni e terminare il WaveNet Manager.

10.3.3 Test di funzionamento RingCast

Il RingCast non ha alcuna funzione di autotest.

AVVERTENZA

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 Rete radio e Sfide nelle reti radio). 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 [▸ 212]*).
2. Se necessario, osservare anche altre direttive o ordinanze rilevanti per il vostro impianto di chiusura (soprattutto per le vie di fuga e di emergenza e per la protezione antincendio. Assicuratevi sotto la vostra responsabilità che queste direttive e regolamenti siano rispettati).

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 Test di funzionamento dei dispositivi. In base ad altre normative riguardanti il vostro sistema complessivo, possono essere richieste distanze più brevi).
2. Verificare le funzioni di protezione almeno una volta al mese (vedere *Test di funzionamento RingCast [▸ 212]*).

Attivare l'ingresso corrispondente sull'attuatore e controllare:

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

Test con router di uscita centrale

NOTA

Router di uscita centrale nel RingCast con RouterNode R/CR

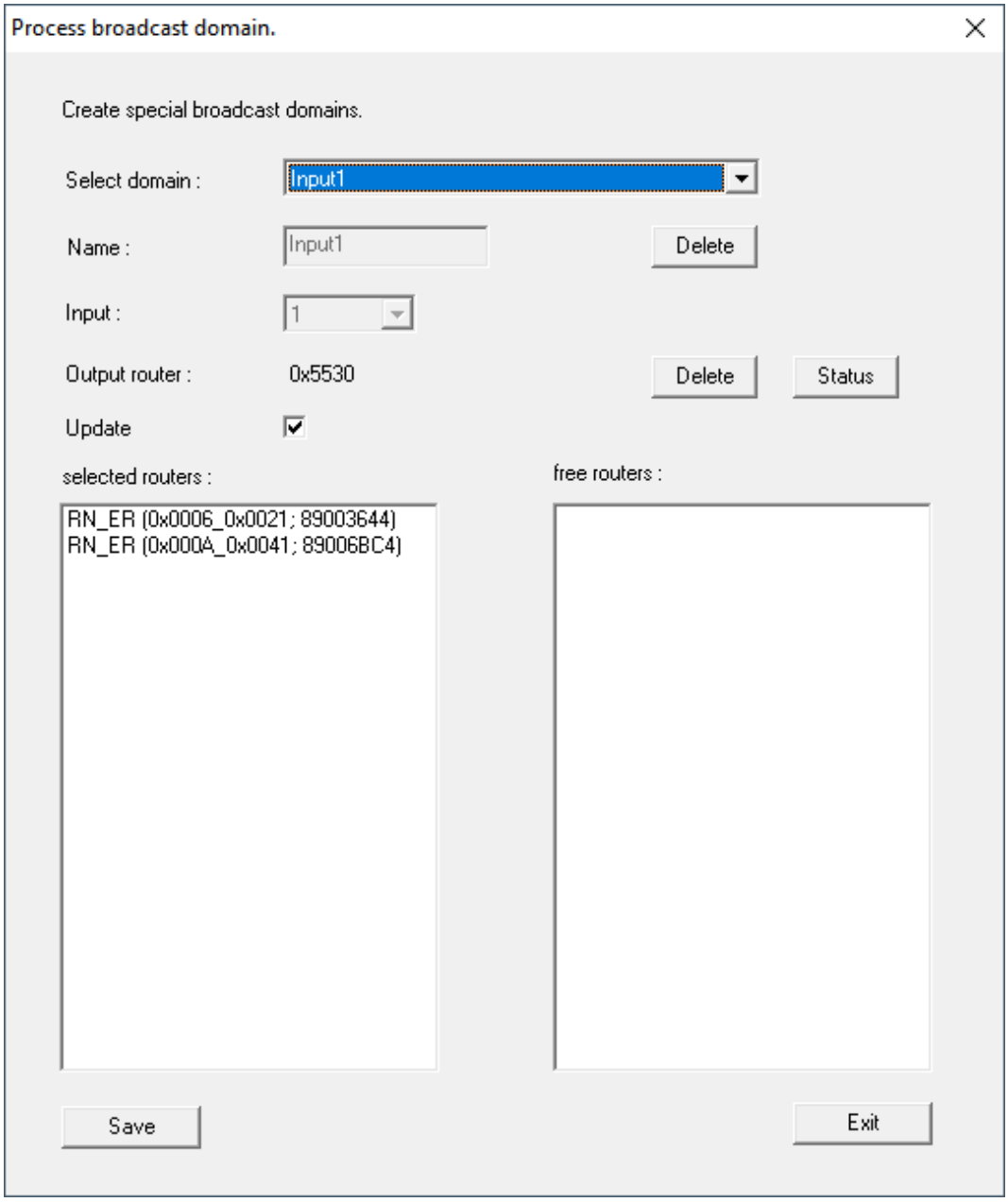
Il router di uscita centrale riceve la conferma di ingresso dei RouterNode partecipanti esclusivamente tramite una connessione Ethernet. Il router di uscita centrale ignora quindi lo stato dei RouterNode che non sono RouterNode Ethernet (.ER). Se si utilizza il router di uscita centrale e il RingCast 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 Verifica dell'accessibilità (LSM) e RouterNode o Stato IO e capacità di reazione LockNode).

L'utilizzo di un router di uscita centrale (vedere Router di uscita centrale) 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 non commuta, controllare quali RouterNode hanno causato problemi:

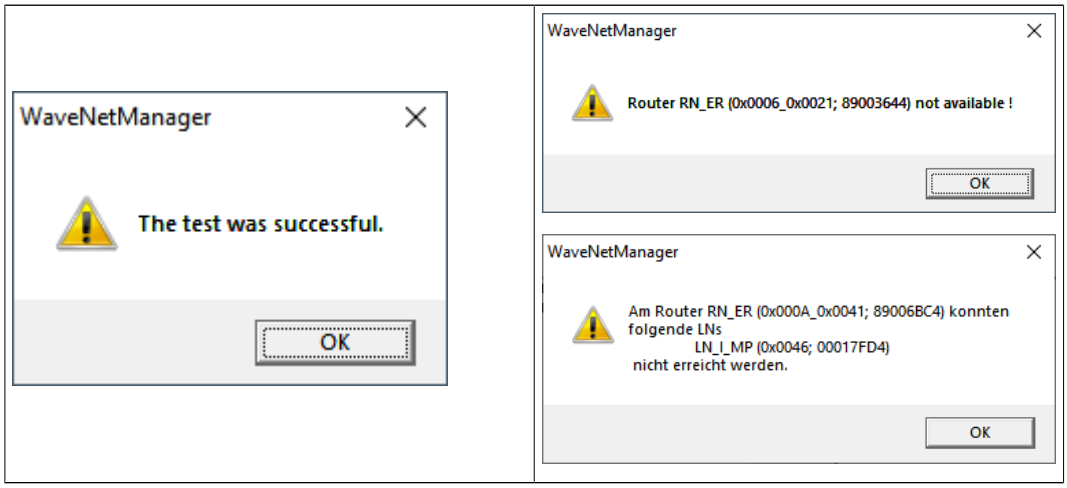
✓ WaveNet Manager aperto tramite LSM (vedere Best Practice: Dal software LSM).

1. Fare clic con il tasto destro del mouse sulla voce del RingCast che si desidera testare.
2. Scegliere nel menu a discesa ▼ **Select domain** l'ingresso di cui si desidera testare il RingCast.
   ↳ La finestra "Edit radio domains" si apre.



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 Router di uscita centrale): ■ 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 RouterNode e Verifica dell'accessibilità (LSM)). 2. Verificare l'accessibilità dei LockNode (vedere LockNode e Verifica dell'accessibilità (LSM)). 3. Controllare le ultime reazioni dei LockNode (vedere Stato IO e capacità di reazione LockNode).

10.4 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 [▸ 195]*.
- È stato attivato l'inoltro degli eventi della chiusura come descritto al passo *Attivazione degli eventi di input della chiusura [▸ 206]*.

10.4.1 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".

10.4.2 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".

10.4.3 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.

10.4.4 Inoltro degli eventi di input tramite il sistema SREL3-ADV

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

10.4.4.1 Valutazione degli input del controller

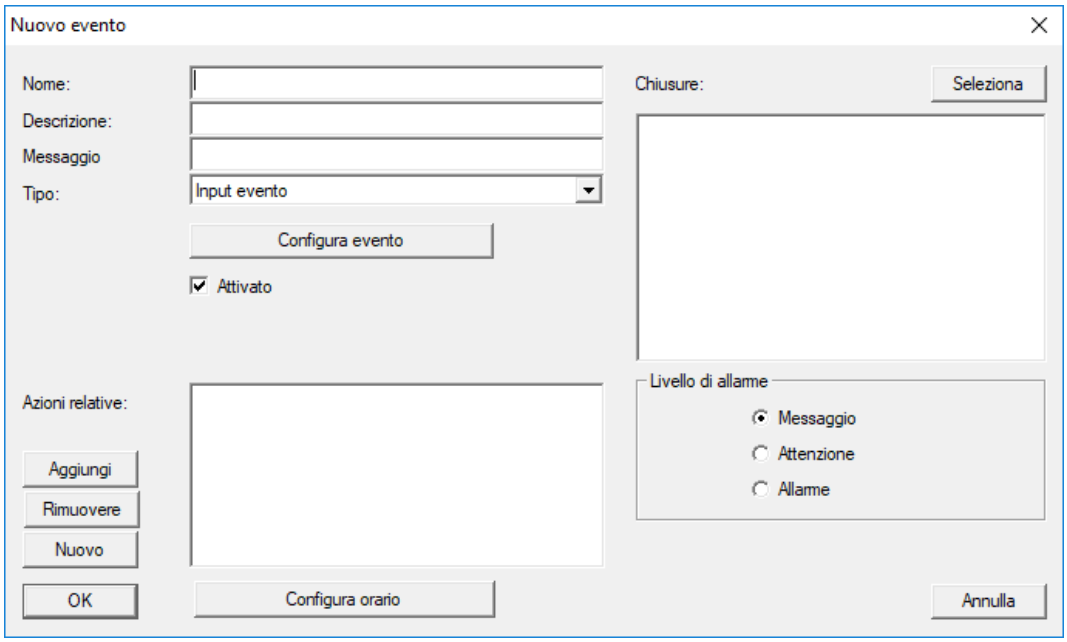
Gli ingressi digitali sul controller del sistema SREL3 ADV possono essere trasferiti all'LSM e qui avviare azioni.

Creazione evento

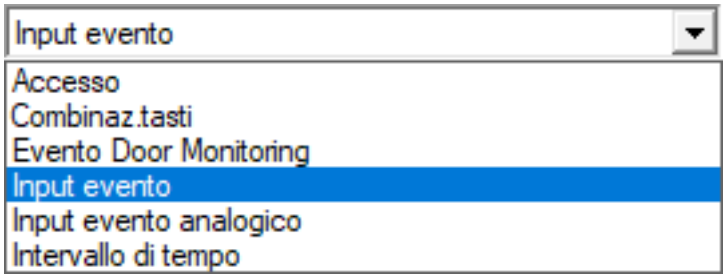
Se si desidera valutare un imput attraverso l'LSM o SmartSurveil (vedi SmartSurveil), è necessario prima creare l'input corrispondente nell'LSM come evento. Solo allora le modifiche all'input sono depositate anche nella banca dati LSM.

✓ LSM aperto.
✓ Sistema SREL3 ADV creato nella matrice.

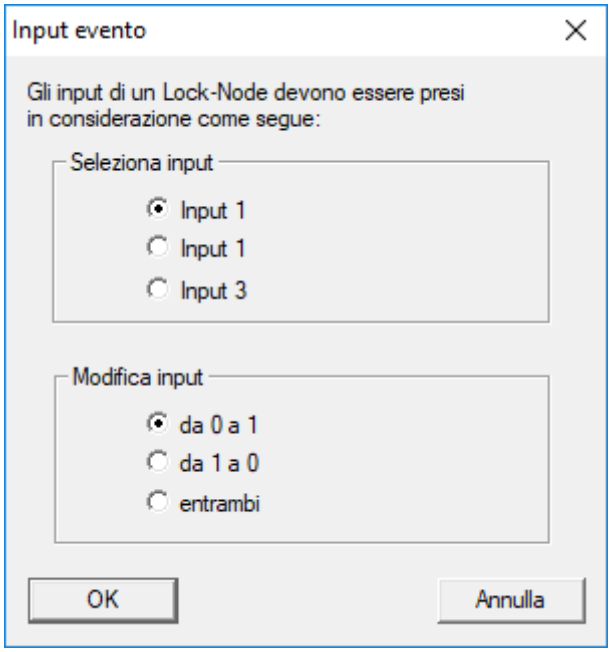
1. Tramite | Rete | selezionare la voce Gestione eventi.
   ↳ Si apre la finestra "Manager eventi rete".
2. Fare clic sul pulsante Nuovo.
   ↳ Si apre la finestra "Nuovo evento".



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.

10.4.5 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".

10.4.6 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".

10.4.6.1 Possibili eventi

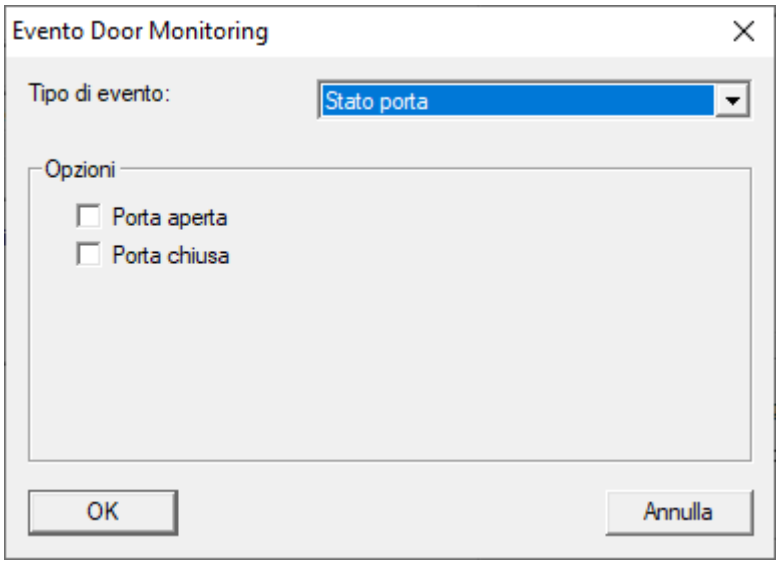
Nella finestra "Nuovo evento" vari eventi sono disponibili nel menu a discesa ▼ **Tipo**.

Per gli eventi di DoorMonitoring è necessaria una chiusura compatibile con il DoorMonitoring (DM).

Eventi di DoorMonitoring

Sono disponibili i seguenti eventi di DoorMonitoring:

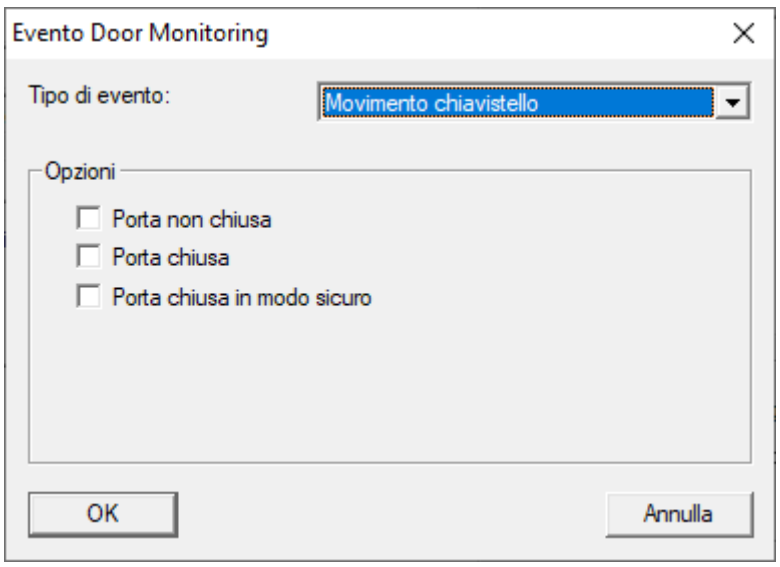
Stato porta



Possono essere rilevati i seguenti stati. Un segno di spunta fa scattare l'evento non appena la condizione si verifica:

- ☑ Porta aperta
- ☑ Porta chiusa

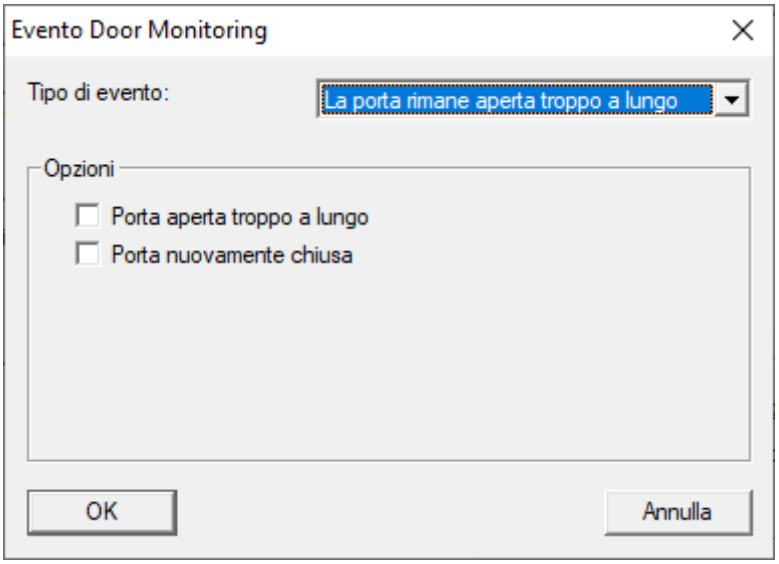
Movimento chiastello



Possono essere rilevati i seguenti stati. Un segno di spunta fa scattare l'evento non appena la condizione si verifica:

- ☑ Porta non chiusa
- ☑ Porta chiusa
- ☑ Porta bloccata con sicurezza

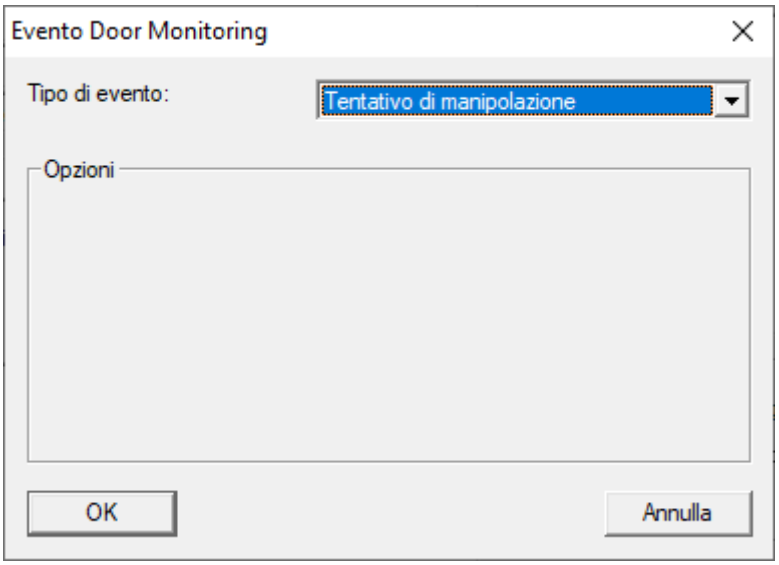
La porta rimane aperta troppo a lungo



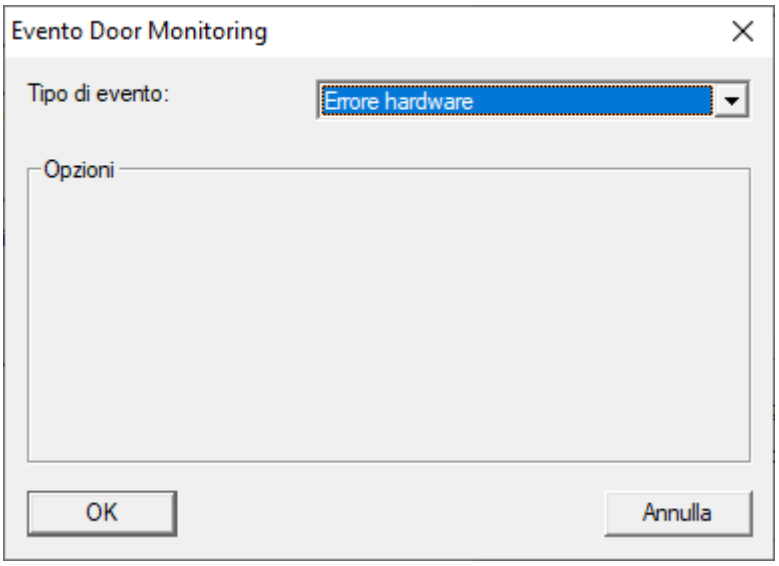
Possono essere rilevati i seguenti stati. Un segno di spunta fa scattare l'evento non appena la condizione si verifica:

- ☑ Porta aperta troppo a lungo
- ☑ Porta richiusa

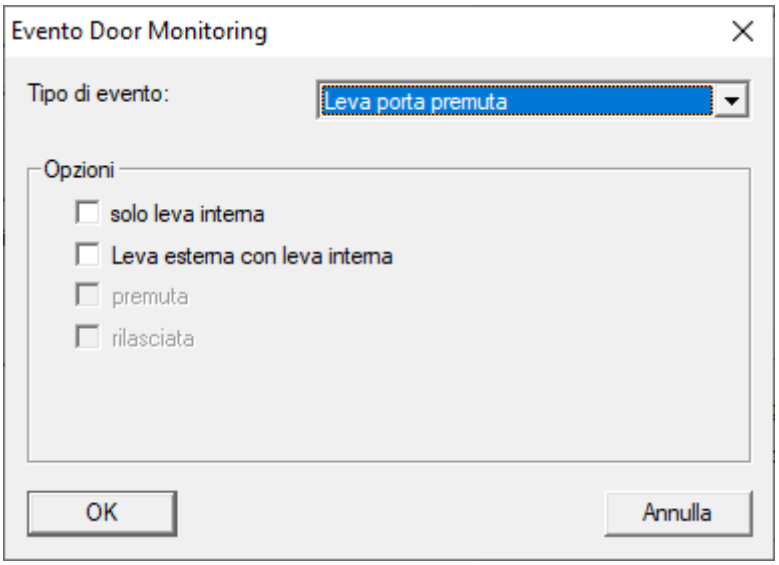
Tentativo di manipulazione



Errore hardware



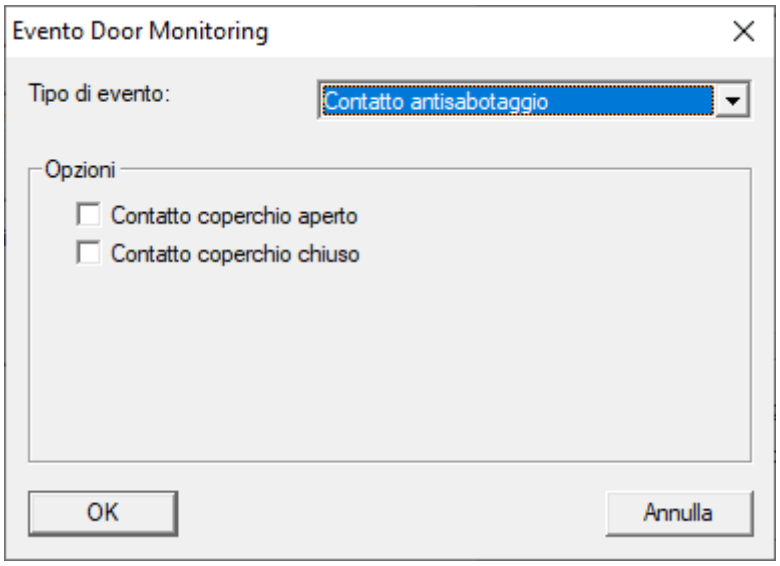
Leva porta premuta



Possono essere rilevati i seguenti stati. Un segno di spunta fa scattare l'evento non appena la condizione si verifica:

- ☑ solo maniglia interna
- ☑ Maniglia esterna con maniglia interna
- ☑ premuta
- ☑ rilasciata

Contatto antisabotaggio



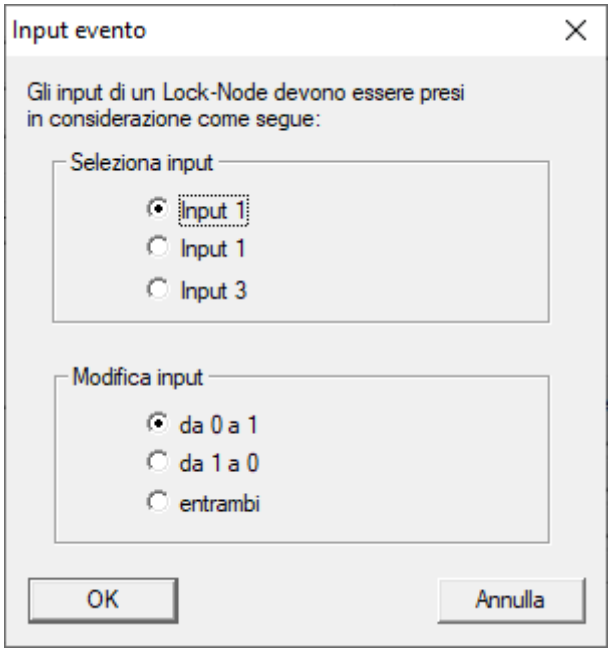
Possono essere rilevati i seguenti stati. Un segno di spunta fa scattare l'evento non appena la condizione si verifica:

- Contatto copertura aperto
- Contatto copertura chiuso

Eventi standard

Sono disponibili i seguenti eventi standard:

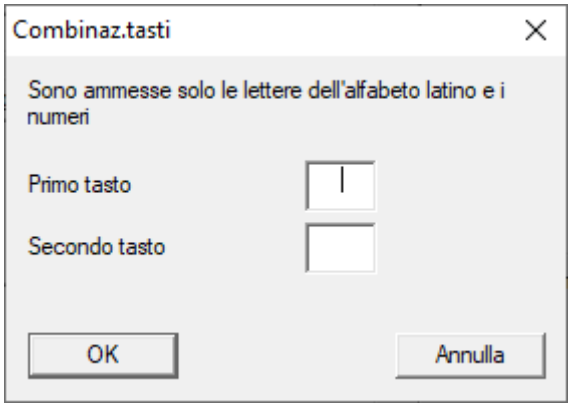
Input evento



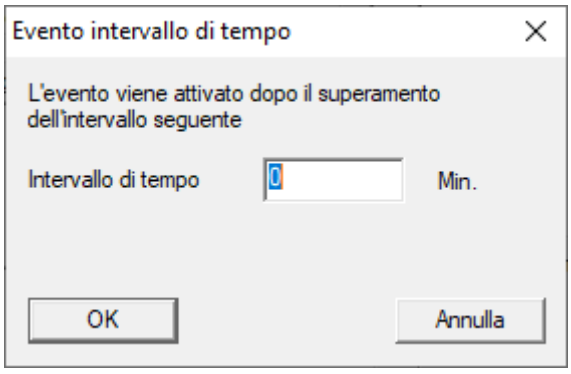
Evento di input analogico

Le impostazioni per gli eventi dell'ingresso analogico sono effettuate direttamente sul rispettivo dispositivo (per esempio RouterNode 2).

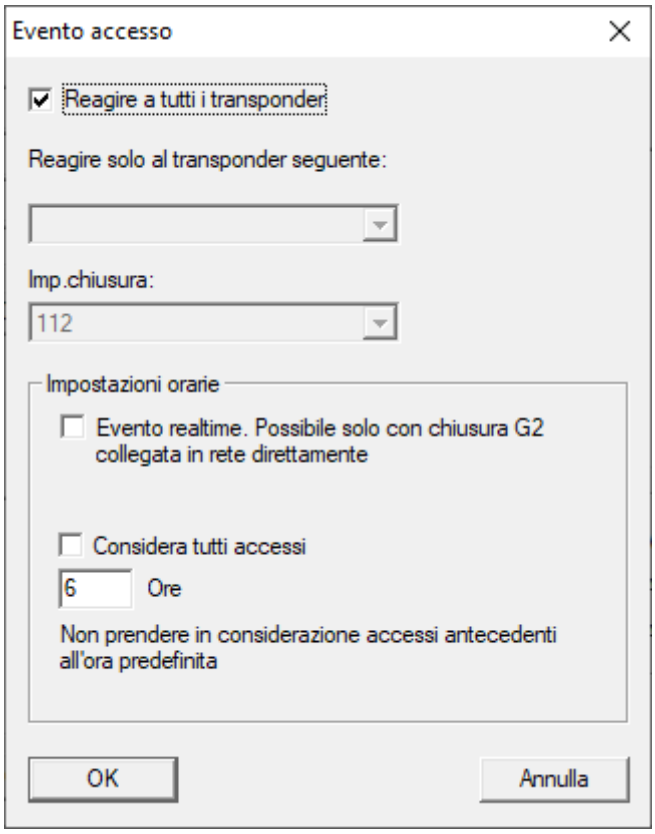
Combinazione di tasti



Intervallo di tempo



Accesso



10.5 Gestione della rete virtuale (VN)

Tramite una rete virtuale (rete VN), le autorizzazioni possono essere modificate e regolate comodamente e rapidamente anche senza una rete completa. L'autorizzazione per le chiusure (e gli ID di chiusura dei mezzi di identificazione bloccati) è memorizzata direttamente nel mezzo di identificazione e trasmessa ogni volta che si aziona una chiusura. Pertanto, nelle reti virtuali è importante registrare tutti i mezzi di identificazione su un gateway a intervalli regolari.

Questo esempio mostra la configurazione di base di una rete virtuale.

Per tutti i tipi di rete virtuale, è necessario un modello di scheda AV quando si usano schede (AV = **A**udit trail / **V**irtual network).

10.5.1 Rete virtuale con SmartRelè 3 Advanced

NOTA

Requisiti di sistema superiori per le reti virtuali con SmartRelè 3 Advanced

La rete virtuale con server VNHost e lo SmartRelè 3 Advanced è molto performante e pone maggiori requisiti in termini di potenza messa a disposizione.

- Prestare attenzione ai maggiori requisiti di sistema (vedere *Requisiti di sistema [▸ 8]*).

10.5.1.1 Principio di funzionamento

L'uso come gateway nella rete virtuale è possibile. A tal fine, il controller stabilisce una connessione con il server VNHost. Il server VNHost trasferisce le autorizzazioni modificate (necessità di programmazione) e i dati dal database LSM al controller. Ciò significa che non è più necessario il caricamento completo e dispendioso del database, ma che il controller recupera i dati a disposizione quando viene riconosciuto un mezzo di identificazione (principio Pull). L'intero sistema viene programmato attraverso una sola interfaccia: il controller.

Il server VNHost controlla a intervalli regolari se ci sono modifiche nel database LSM che devono essere distribuite tramite il gateway. Viceversa, controlla anche se le informazioni che devono essere scritte nel database sono disponibili nel gateway (vedere *Controllo dello stato della rete virtuale [▸ 231]*).

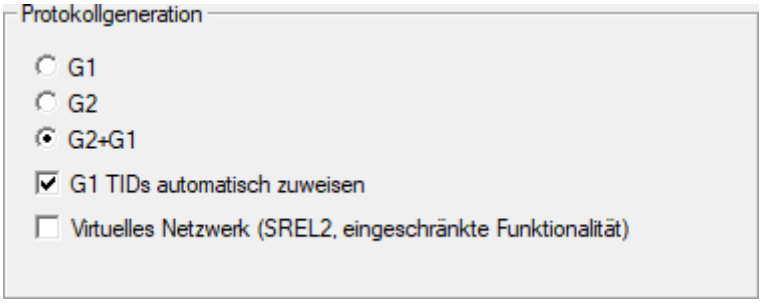
10.5.1.2 Configurazione dell'impianto di chiusura

Non è necessaria alcuna preparazione speciale per una rete virtuale con SmartRelè 3 Advanced.

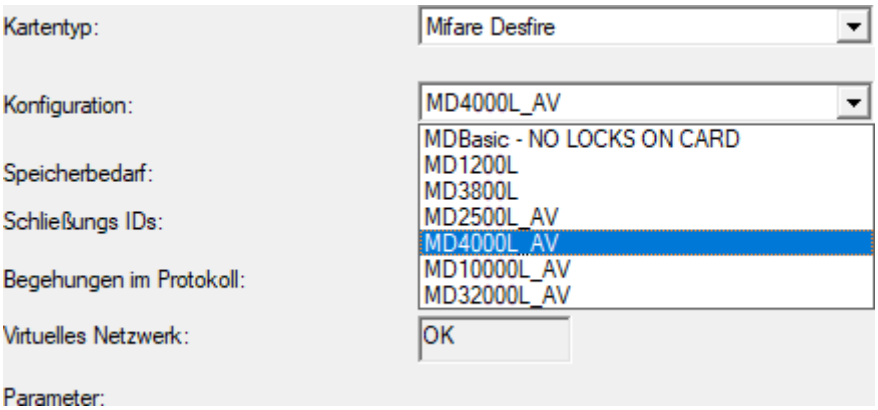
Nelle proprietà dell'impianto di chiusura la casella di controllo ☐ Rete virtuale (SREL2, funzionalità limitata) non deve essere attivata.

1. Aprire da | Elabora | - Proprietà impianto di chiusura le proprietà del proprio sistema di chiusura.
2. Passare alla scheda di registro [Nome].

3. Assicurarsi che la casella di controllo ☐ Rete virtuale (SREL2, funzionalità limitata) non sia attivata.



4. Fare clic sul pulsante Applica.
5. Se state usando delle schede: selezionate nella scheda di registro [Gestione schede G2] un modello di scheda AV.



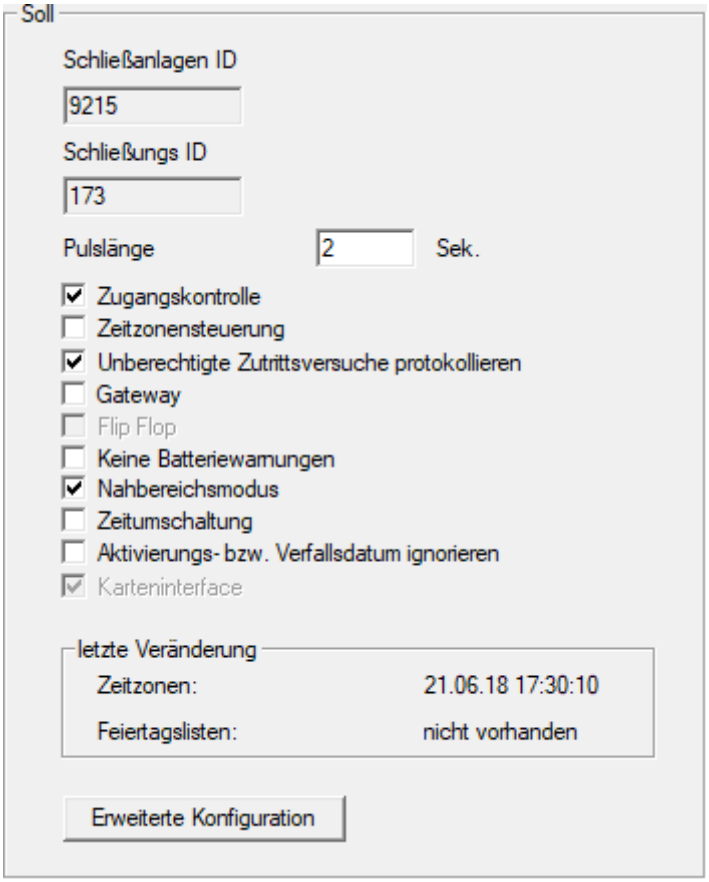
6. Fare clic sul pulsante Applica.

10.5.1.3 Configurazione di gateway e server VNHost

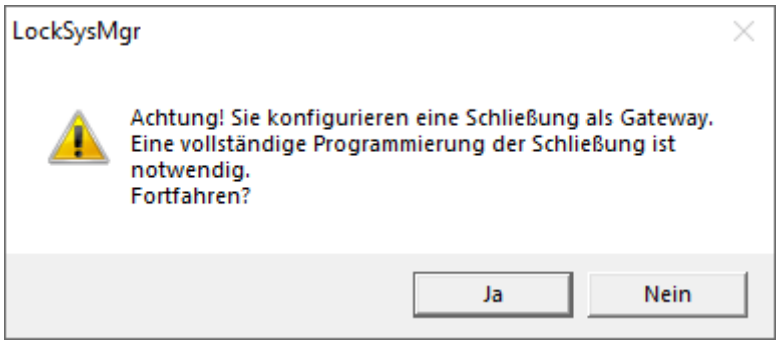
✓ Impianto di chiusura creato (vedere *Configurazione dell'impianto di chiusura [▸ 226]*).
✓ SmartRelè 3 Advanced configurato e collegato in rete (vedere il manuale di sistema di SmartRelè 3 Advanced).
✓ VNHost installato (vedere *VNHost [▸ 22]*).

1. Aprite tramite | Elabora | - Proprietà di chiusura le proprietà dello SmartRelè 3 Advanced (alterativa: fate doppio clic).

2. Passate alla scheda di registro [Configurazione/dati].

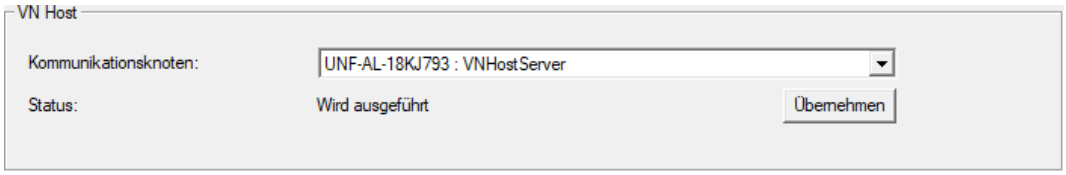


3. Attivate le caselle di testo ☑ Gestione fasce orarie e ☑ Controllo accessi.
4. Attivate la casella di controllo ☑ Gateway.
   ↳ Si apre l'avviso relativo all'imminente programmazione.



5. Fare clic sul pulsante OK.
   ↳ L'avviso si chiude.
6. Fare clic sul pulsante Sì.
   ↳ Viene visualizzata la necessità di programmazione (lampo).
7. Autorizzate tutti i mezzi di identificazione che successivamente devono ricevere nuove autorizzazioni sul gateway.

8. Programmate lo SmartRelè 3 Advanced.
   ↳ La necessità di programmazione scompare.
9. Selezionate tramite | Rete | la voce Rete virtuale .
   ↳ Si apre la finestra "VN Host Server".



10. Assicuratevi che nell'area "VNHost" nel menu a discesa ▼ **Nodi di comunicazione** sia selezionata la voce "VNHostServer".

NOTA

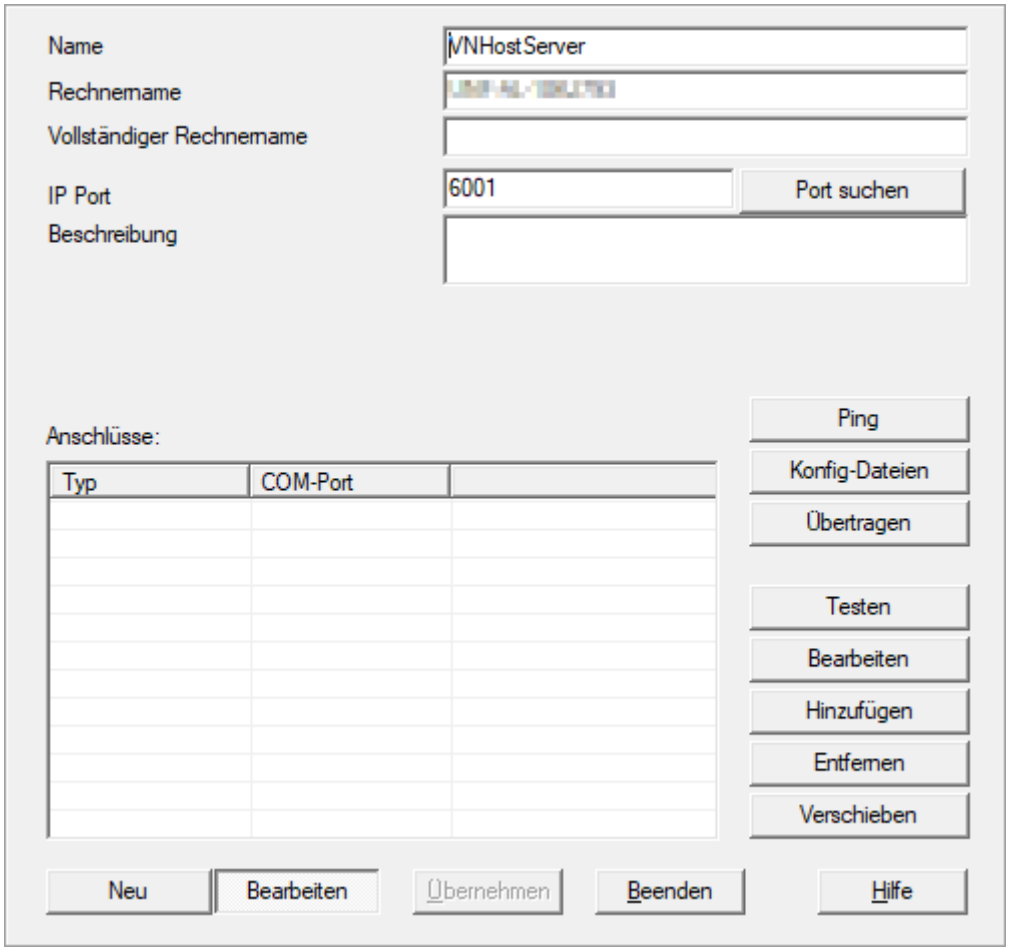
Diversi nodi di comunicazione sullo SmartRelè 3 Advanced

Per la rete virtuale su SmartRelè 3 Advanced viene sempre utilizzato il VNHostServer. Per la programmazione, l'apertura a distanza ecc., invece, si può usare anche un altro nodo di comunicazione.

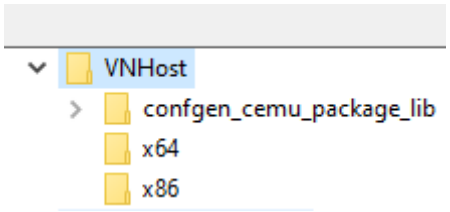
- Per la rete virtuale selezionate anche la voce "VNHostServer", se il vostro SmartRelè 3 Advanced utilizza un altro nodo di comunicazione ancora.

11. Se necessario, fate clic sul pulsante Applica .
12. Fare clic sul pulsante OK .
    ↳ Si chiude la finestra "VN Host Server" .
13. Selezionate tramite | Rete | la voce Nodi di comunicazione .

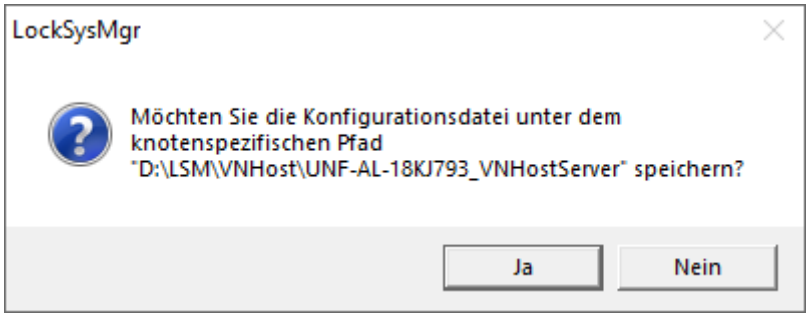
14. Passate con i tasti ◂ e ▸ al nodo di comunicazione VNHostServer.



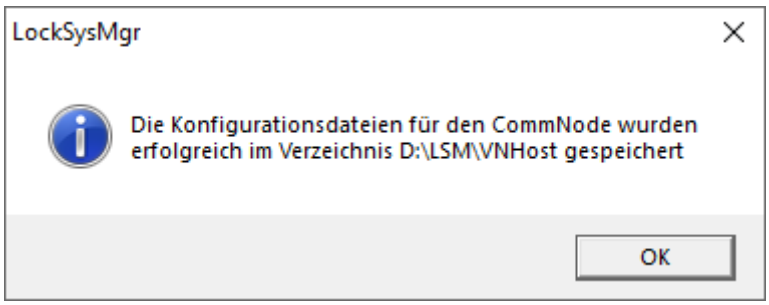
15. Cliccate sul pulsante File di configurazione.
    ↳ Si aprirà la finestra Esplora risorse.
16. Evidenziate la cartella di installazione del server VNHost.



17. Fare clic sul pulsante OK.
    ↳ La finestra Esplora risorse si chiude.
    ↳ Si apre la finestra "LockSysMgr".



18. Cliccate sul pulsante No.
    ↳ I file di configurazione vengono salvati.



19. Cliccate sul pulsante Trasferisci.
    ↳ I file di configurazione sono trasferiti al nodo di comunicazione VNHostServer.
20. Se il vostro SmartRelè 3 Advanced è collegato tramite un altro nodo di comunicazione: salvate e trasferite anche i file di configurazione per questo nodo di comunicazione.

↳ Rete virtuale pronta per l'uso.

Ora potete monitorare lo stato della vostra rete virtuale (vedere *Controllo dello stato della rete virtuale [▸ 231]*).

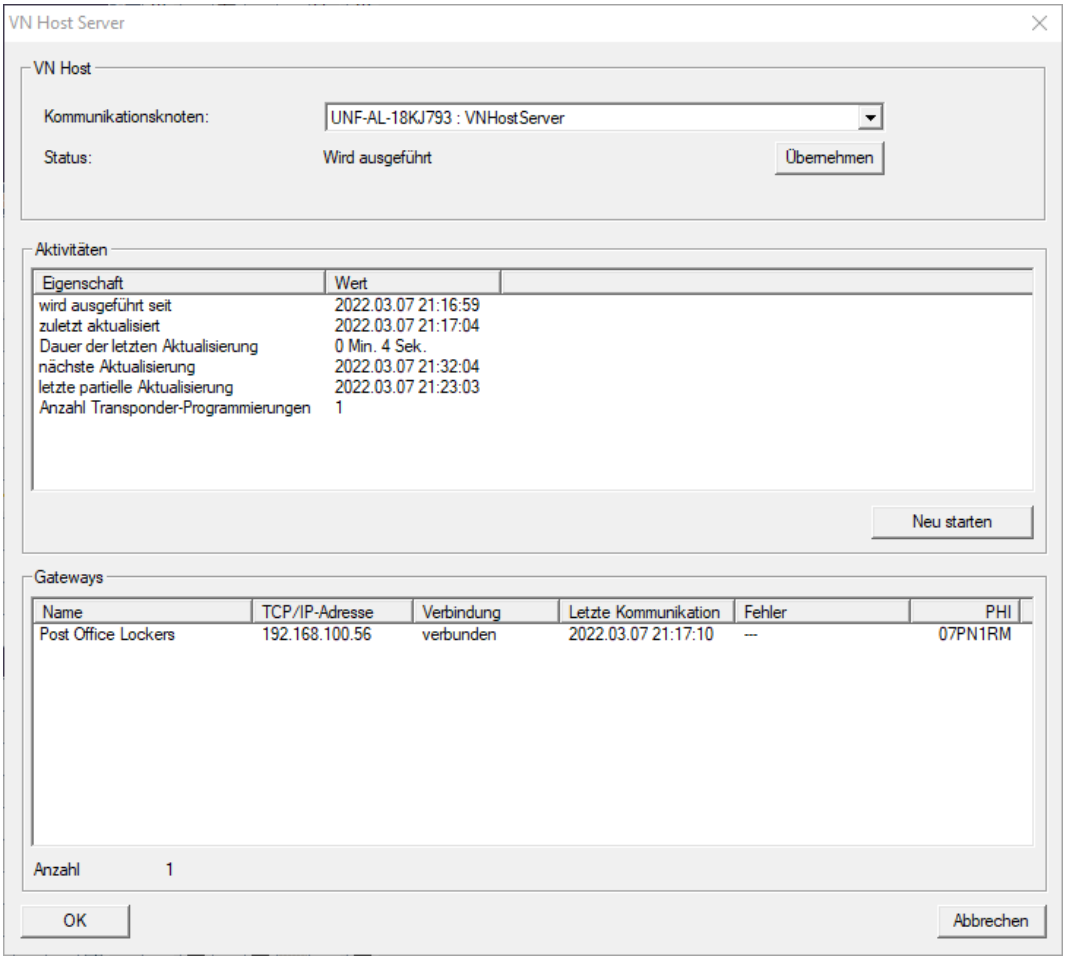
10.5.1.4 Controllo dello stato della rete virtuale

Dopo aver impostato la rete virtuale, potete monitorarne lo stato.

✓ Rete virtuale configurata (vedere *Configurazione dell'impianto di chiusura [▸ 226]* e *Configurazione di gateway e server VNHost [▸ 227]*).

- Selezionate tramite | Rete | la voce Rete virtuale.

↳ La finestra "VN Host Server" mostra lo stato attuale.



Nell'area "VNHost" si vede il nodo di comunicazione attualmente utilizzato (per la rete virtuale: "VNHostServer").

Nell'area "Attività" potete vedere:

- Avvio del server VNHost
- Data dell'ultimo aggiornamento
- Data del prossimo aggiornamento previsto
- Numero di programmazioni in sospeso

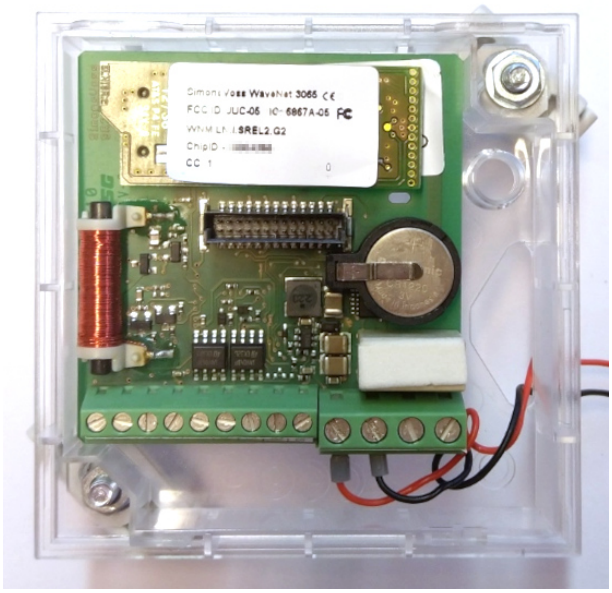
Nell'area potete trovare un elenco di tutti gli "SmartRelè 3 Advanced" configurati come ☑ Gateway e il loro stato.

10.5.2 Rete virtuale con SmartRelè 2 G2

10.5.2.1 Principio di funzionamento

A differenza dello SmartRelè 3, lo SmartRelè 2 G2 (SREL2.G2) non è collegato tramite un cavo di rete, ma tramite la WaveNet. Pertanto, per il funzionamento di una rete virtuale con SmartRelè 2 G2, sono necessari un LockNode e un RouterNode integrati, idealmente un RouterNode 2 (vedere *Creazione di componenti e configurazione dell'LSM [▸ 238]*).

L'LSM invia quindi i dati da distribuire nella rete virtuale tramite un cavo di rete al RouterNode 2 e poi tramite WaveNet allo SmartRelè 2 G2. Questo funge quindi da gateway.



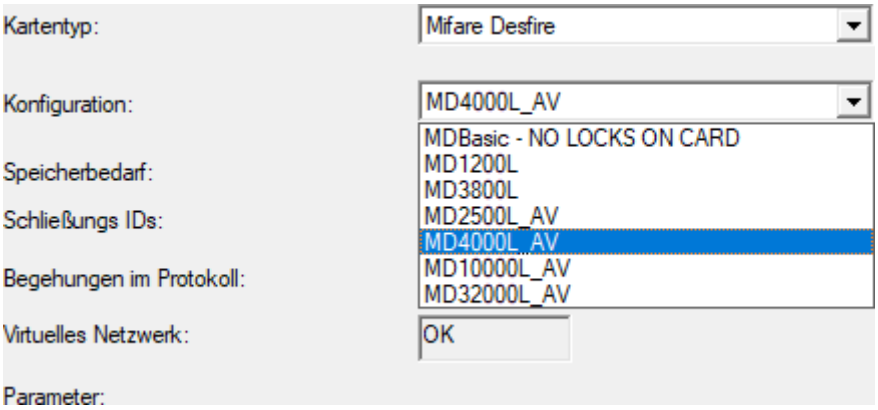
I mezzi di identificazione azionati sul gateway distribuiscono i dati alle chiusure.

10.5.2.2 Configurazione dell'impianto di chiusura

Nel (puro) impianto di chiusura G2, la casella di controllo ☑ Rete virtuale (SREL2, funzionalità limitata) deve essere attivata.

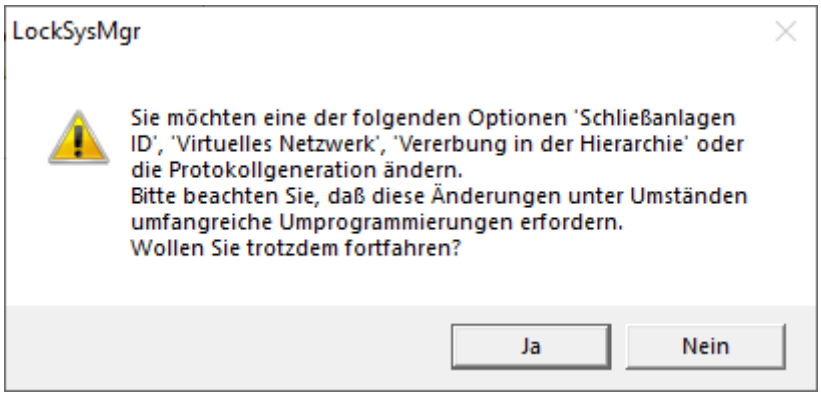
1. Aprire da | Elabora | - Proprietà impianto di chiusura le proprietà del proprio sistema di chiusura.
2. Passate alla scheda di registro [Nome].
3. Nell'area "Creazione di protocollo" attivate la casella di controllo ☑ Rete virtuale (SREL2, funzionalità limitata).

4. Se state usando delle schede: selezionate nella scheda di registro [Gestione schede G2] un modello di scheda AV.



↳ L'impianto di chiusura è predisposto per la rete virtuale con SmartRelè 2 G2.

Se questa impostazione viene applicata a un impianto di chiusura esistente, può essere necessaria una programmazione considerevole.



10.5.2.3 Configurazione del servizio VN

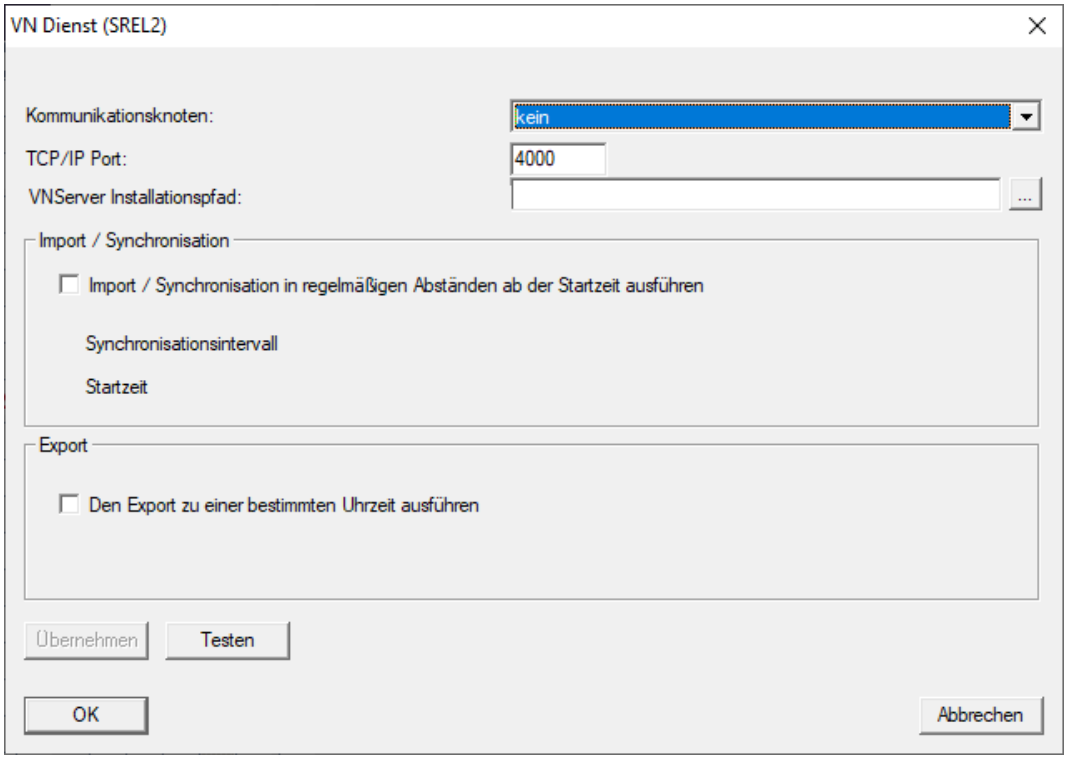
✓ Impianto di chiusura configurato (vedere *Creazione di un nuovo impianto di chiusura [▸ 136]*, *Creazione di un nuovo transponder [▸ 136]* e *Creazione di una nuova chiusura [▸ 195]*).

✓ Casella di controllo ☑ Rete virtuale (SREL2, funzionalità limitata) attivata.

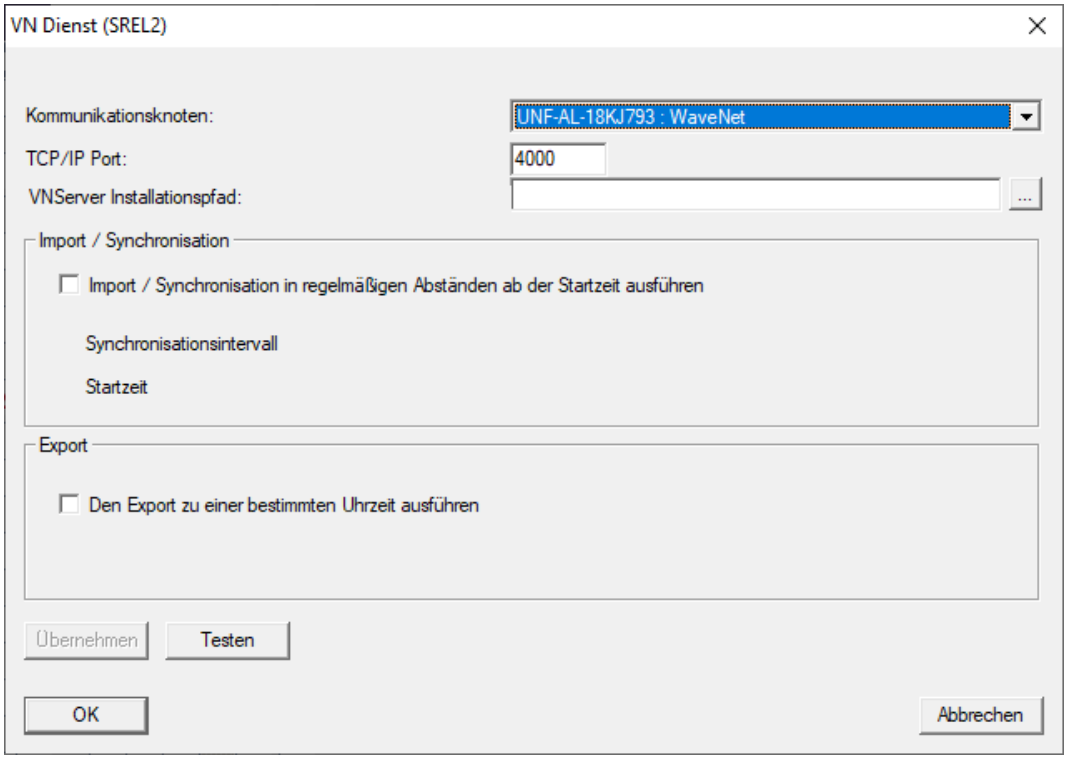
✓ Tutti i componenti programmati (vedere *Programmazione del transponder [▸ 152]* e *Programmazione della chiusura [▸ 196]*).

✓ SmartRelè 2 G2 collegato in rete (vedere manuale WaveNet).

1. Selezionate tramite | Rete | la voce Servizio VN (SREL2) .
   ↳ Si apre la finestra "Servizio VN (SREL2)".

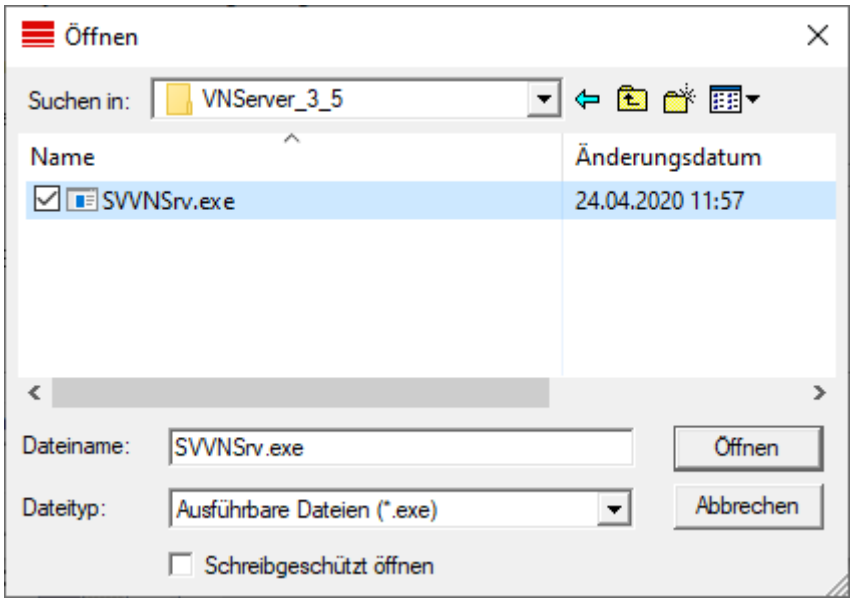


2. Nel menu a discesa ▼ **Nodi di comunicazione** selezionate il nodo di comunicazione a cui è collegata la WaveNet con RouterNode 2 e SmartRelè 2 G2.

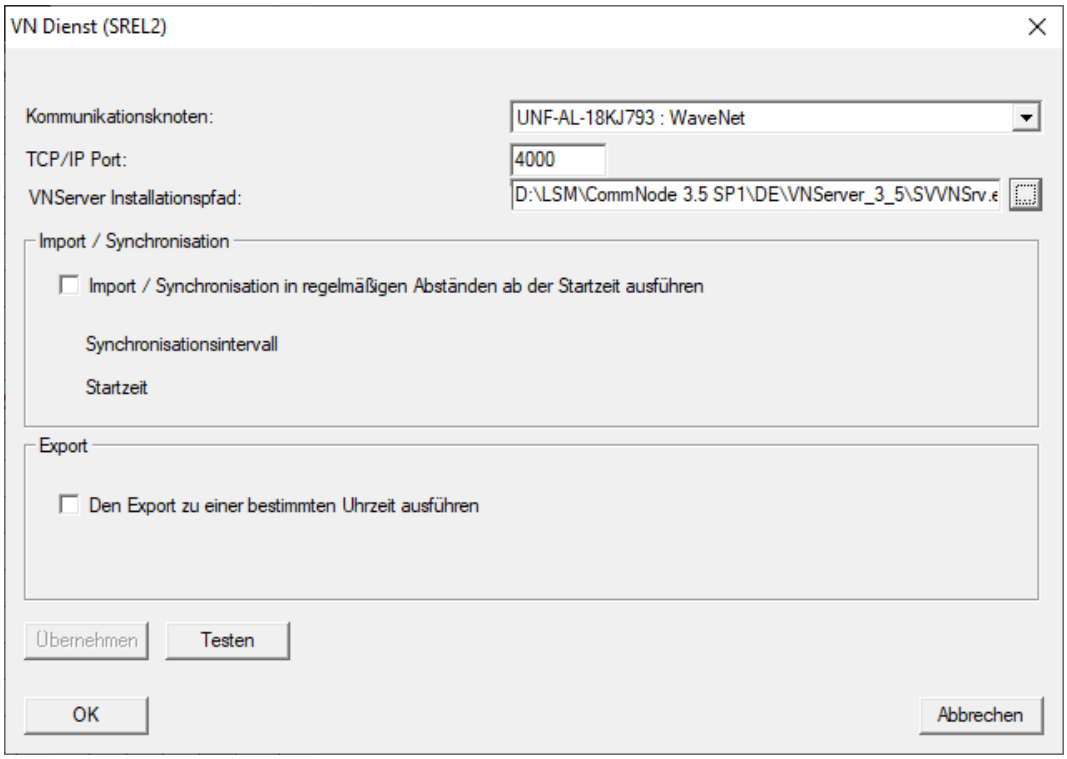


3. Assicuratevi che la porta TCP/IP sia impostata a 4000.
4. Aprire Esplora risorse con il pulsante ... .

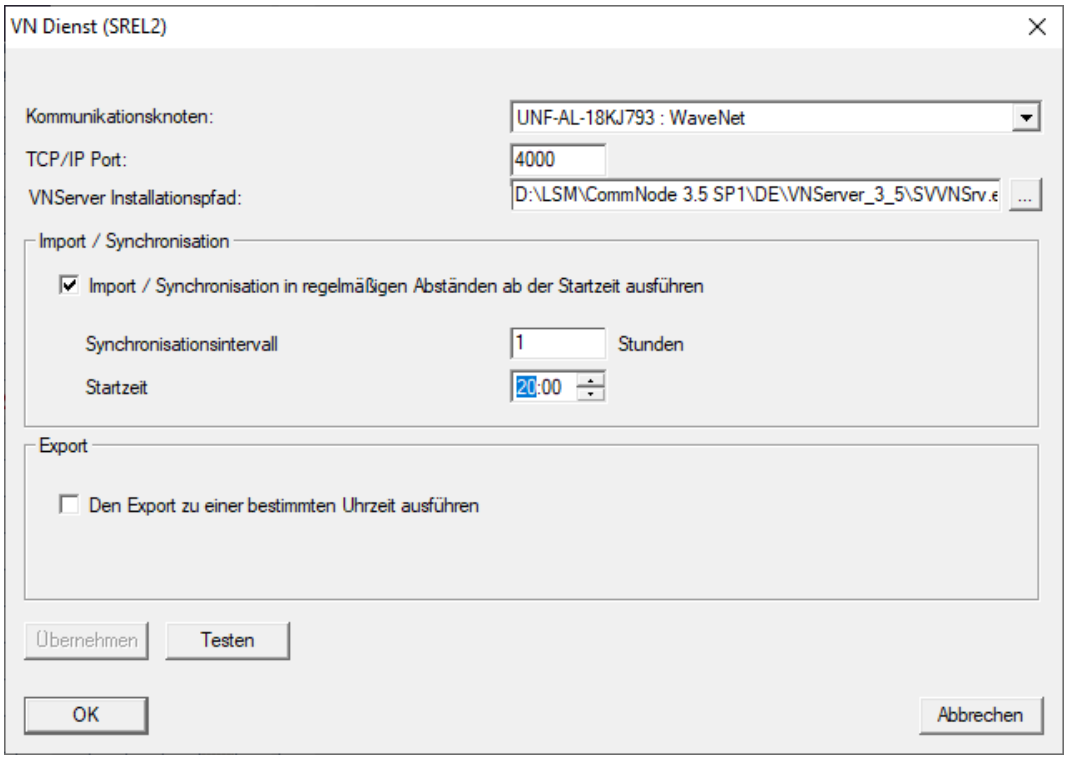
5. Selezionate SVVNSvr.exe.
   SVVNSvr.exe verrà installato insieme al server CommNode. Directory standard: (C:\Programmi(x86)\SimonsVoss\VNServer_x_x)



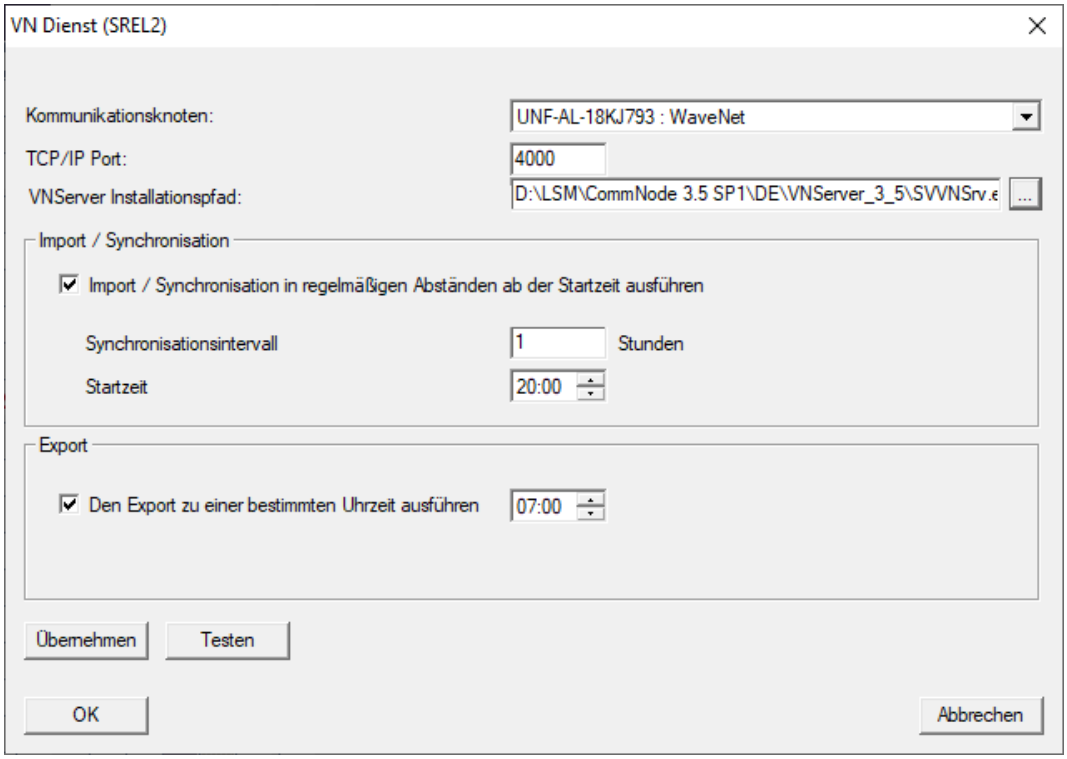
6. Cliccate sul pulsante Apri.
   ↳ La finestra Esplora risorse si chiude.



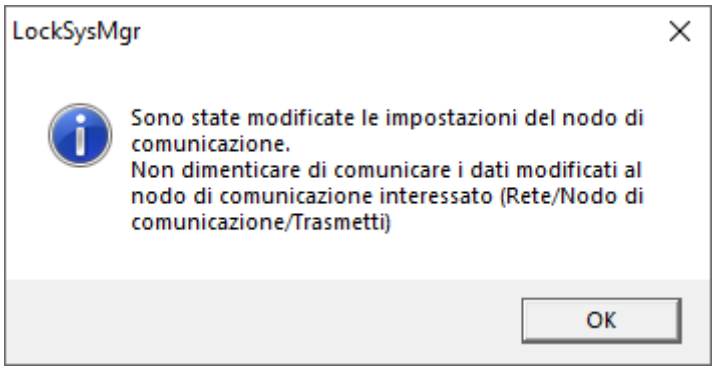
7. Opzionale: nell'area "Importazione / sincronizzazione" impostate quando i dati dello SmartRelè 2 G2 devono essere reimportati automaticamente nell'LSM.



8. Opzionale: nell'area "Esporta" impostate quando dati dell'LSM devono essere trasmesse automaticamente allo SmartRelè 2 G2.



9. Fare clic sul pulsante OK.
   ↳ Si apre la finestra "LockSysMgr".



10. Fare clic sul pulsante OK.
    ↳ Si chiude la finestra "LockSysMgr" .
    ↳ Si chiude la finestra "Servizio VN (SREL2)" .
11. Trasmettete le impostazioni al CommNode (vedere *Trasferimento della configurazione WaveNet [▸ 206]*).

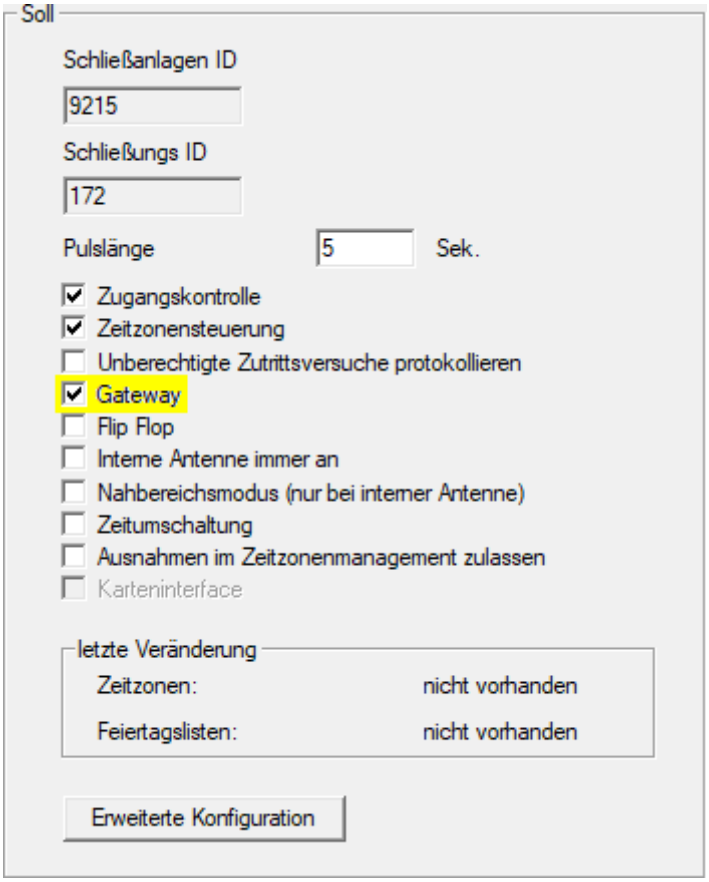
10.5.2.4 Creazione di componenti e configurazione dell'LSM

Prima di iniziare la configurazione, le impostazioni più importanti per il funzionamento di una rete devono essere effettuate nel software LSM e il RouterNode 2 deve essere pronto all'uso.

- *Preparazione del software LSM [▸ 195]*
- *Preparazione dell'hardware [▸ 196]*
- *Creazione del nodo di comunicazione [▸ 197]*
- *Impostazione del servizio task [▸ 216]*

1. Create diversi mezzi di identificazione (ad es. *Creazione di un nuovo transponder [▸ 136]*) e chiusure (ad es. *Creazione di una nuova chiusura [▸ 195]*).
2. Eseguire la programmazione iniziale dei componenti creati (*Programmazione del transponder [▸ 152]* e *Programmazione della chiusura [▸ 196]*).
3. Create uno SmartRelè 2 G2 (▼ **Tipo** "SmartRelè G2 attivo/ibrido").
4. Aprite Proprietà della chiusura.
5. Passate alla scheda di registro [Configurazione/dati].

6. Attivate la casella di controllo ☑ Gateway.



7. Tornate alla vista Matrice.
8. Autorizzate sullo SmartRelè 2 G2 tutti i mezzi di identificazione che dovranno ricevere nuove autorizzazioni successivamente.
9. Eseguite la programmazione iniziale dello SmartRelè 2 G2.
10. Assicuratevi che un LockNode sia installato nello SmartRelè 2 G2.
11. Configurate il RouterNode 2 tramite il WaveNet Manager (vedere *Configurazione della rete e importazione nell'LSM [▸ 197]*).
12. Assegnategli il gateway (o lo SmartRelè 2 G2).

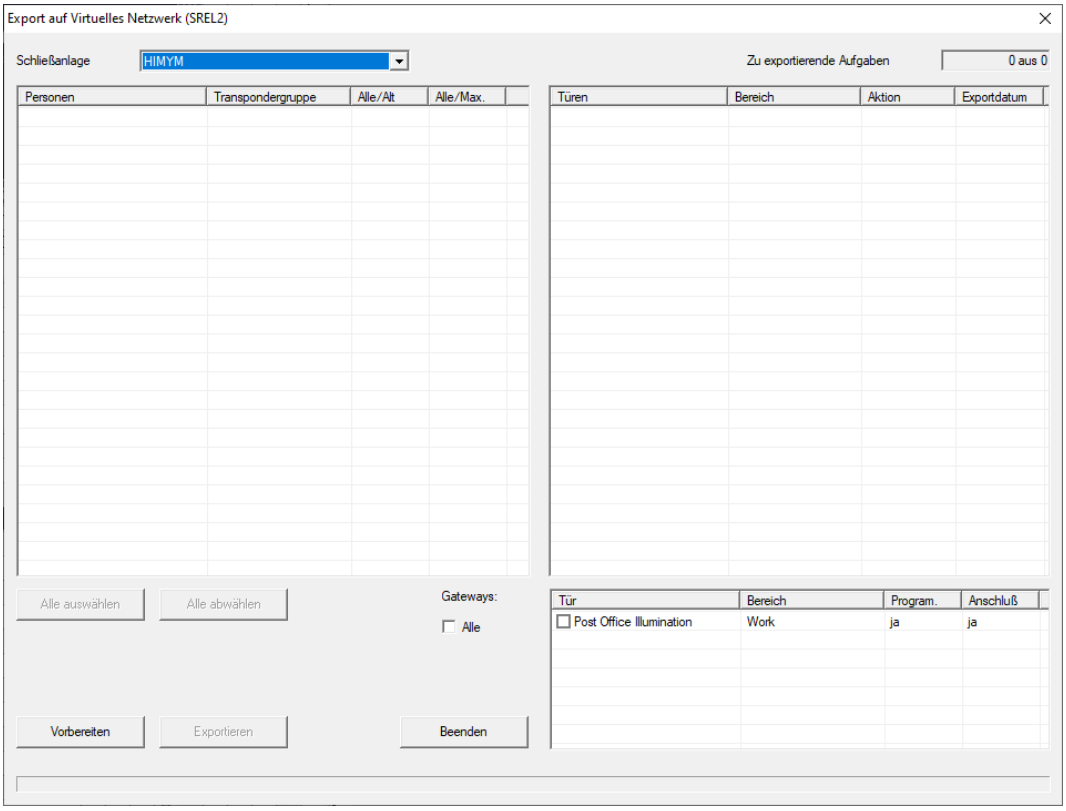
↳ La rete virtuale è pronta per l'uso.

10.5.2.5 Esportazione delle modifiche alle autorizzazioni

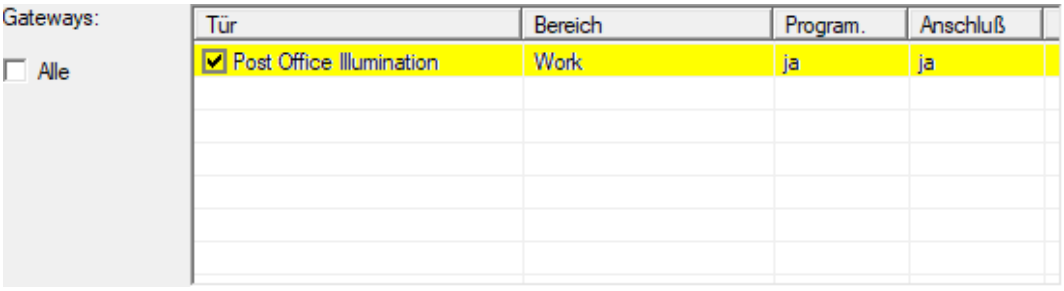
L'esportazione delle modifiche alle autorizzazioni funziona solo se almeno una modifica è stata apportata. Per effettuare una verifica, ritirate ad esempio dal transponder 1 l'autorizzazione per il cilindro di chiusura 1.

1. Eseguite un reset prima della prima esportazione (vedere *Reset dei task nella rete virtuale [▸ 246]*).
2. Selezionate tramite | Programmaz. | - Rete virtuale (SREL2) la voce Esportazione in VNetwork.

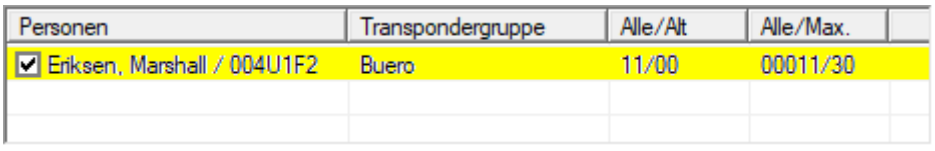
↳ Si apre la finestra "Esportazione su rete virtuale (SREL2)".



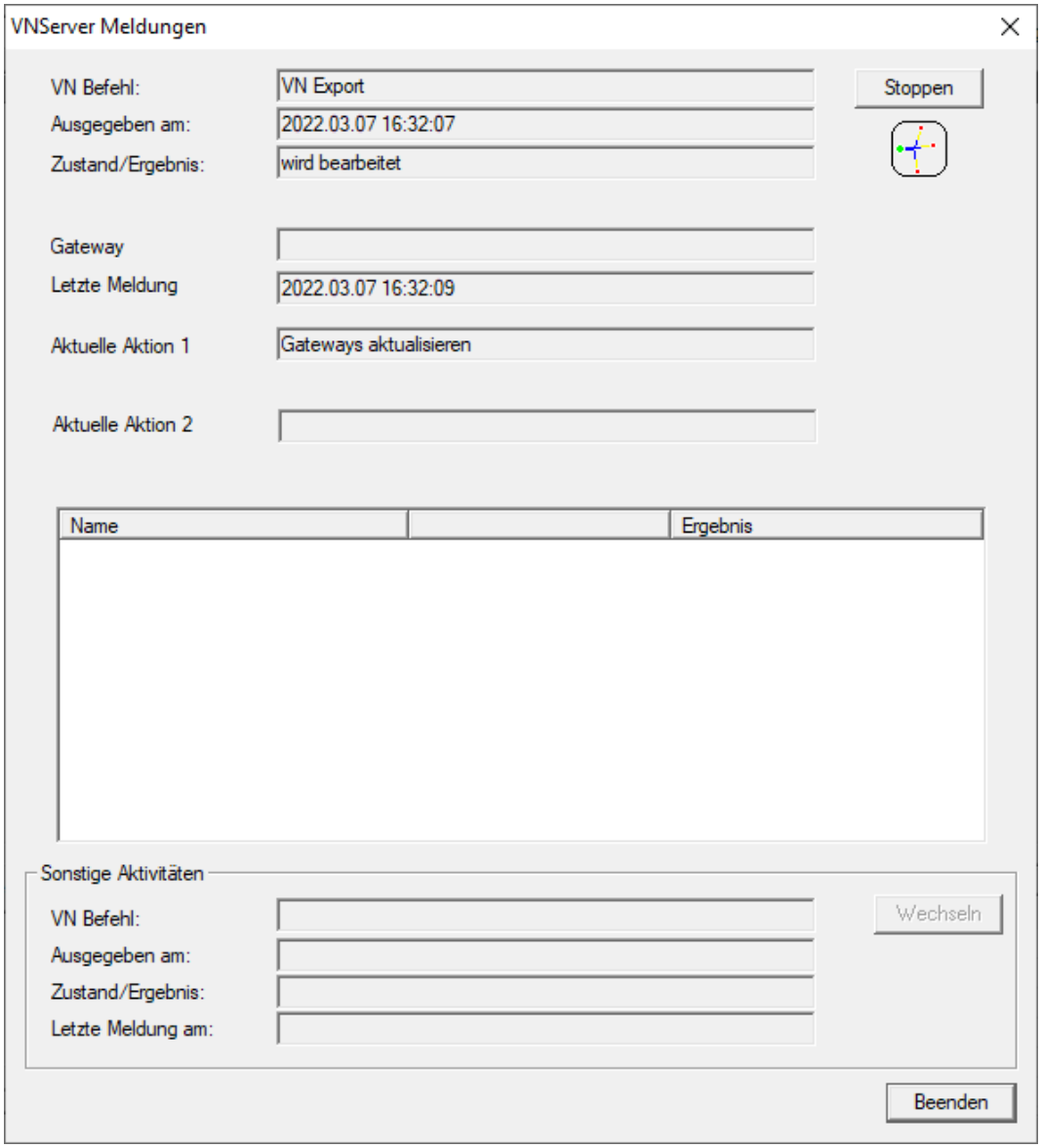
3. Selezionate tutti gli SmartRelè 2 G2, a cui le modifiche devono essere inviate/esportate.



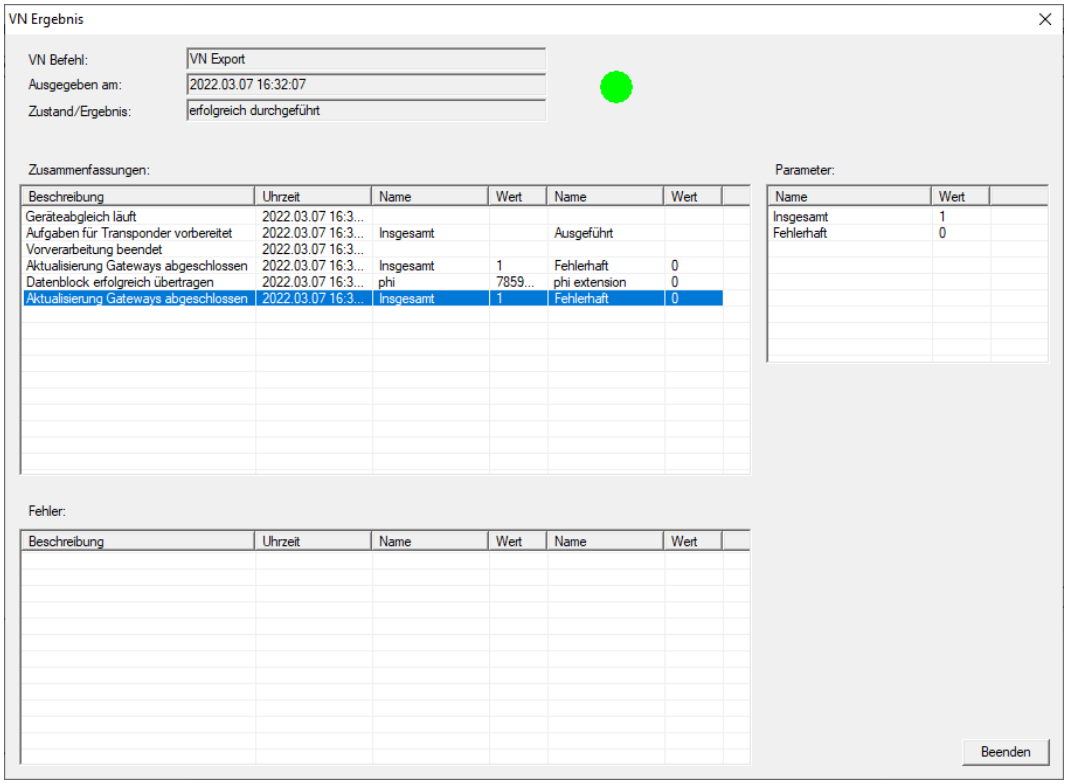
4. Controllate se nel menu a discesa ▼ **Sistema di chiusura** è stato selezionato l'impianto di chiusura corretto.
5. Cliccate sul pulsante Preparazione.
   ↳ Nell'area "Persone" vengono elencate tutte le modifiche esportabili.
6. Contrassegnate tutte le modifiche che volete esportare nello SmartRelè 2 G2 determinato in precedenza.



7. Cliccate sul pulsante Esporta.
   ↳ Il processo di esportazione inizia. Le modifiche vengono inviate al gateway.



↳ Viene visualizzato il riepilogo dell'esportazione.



Ora è possibile tracciare i task esportati nella panoramica (*Stato dei task nella rete virtuale (SREL2.G2) [▸ 245]*).

La modifica dell'autorizzazione è ora pronta nel gateway. Sono ora possibili due scenari:

- Il transponder 1 si prenota sul gateway. La chiusura 1 riconoscerà in seguito che il transponder 1 non è più autorizzato e rifiuterà l'accesso.
- Un altro transponder (non il transponder 1) si prenota per primo sul gateway e si autorizza sulla chiusura 1. L'ID di blocco del transponder 1 viene comunicato al cilindro di chiusura 1.

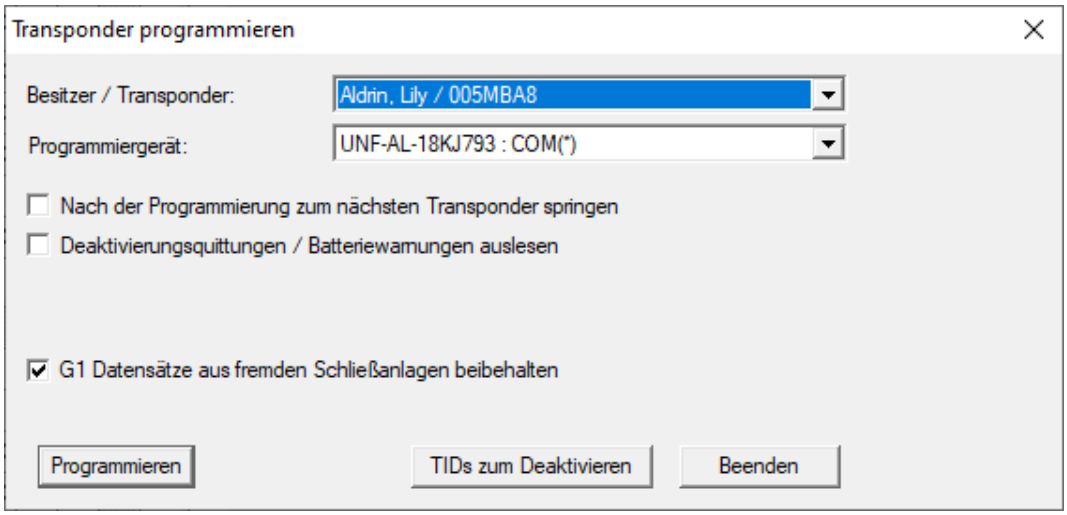
A partire dalla versione LSM 3.5 SP3 è possibile aggiungere ai transponder desiderati fino a due altri ID transponder da bloccare.

Programmazione diretta dei TID da bloccare

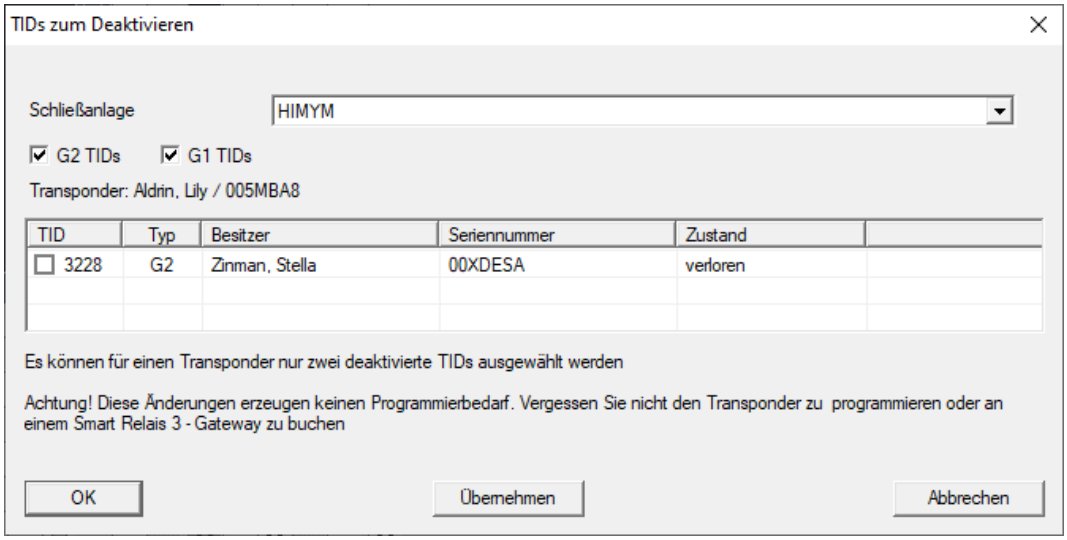
Gli ID da bloccare vengono memorizzati sul transponder durante il processo di programmazione.

✓ Il transponder è fisicamente disponibile.
✓ La finestra di programmazione del transponder è aperta.

1. Cliccate sul pulsante TID da disattivare.



↳ L'elenco si apre.



2. Apponete un massimo di due segni di spunta nella colonna TID per memorizzare i TID da cancellare sul transponder.
3. Confermare l'inserimento con il pulsante "OK".
4. Continuate con la programmazione.

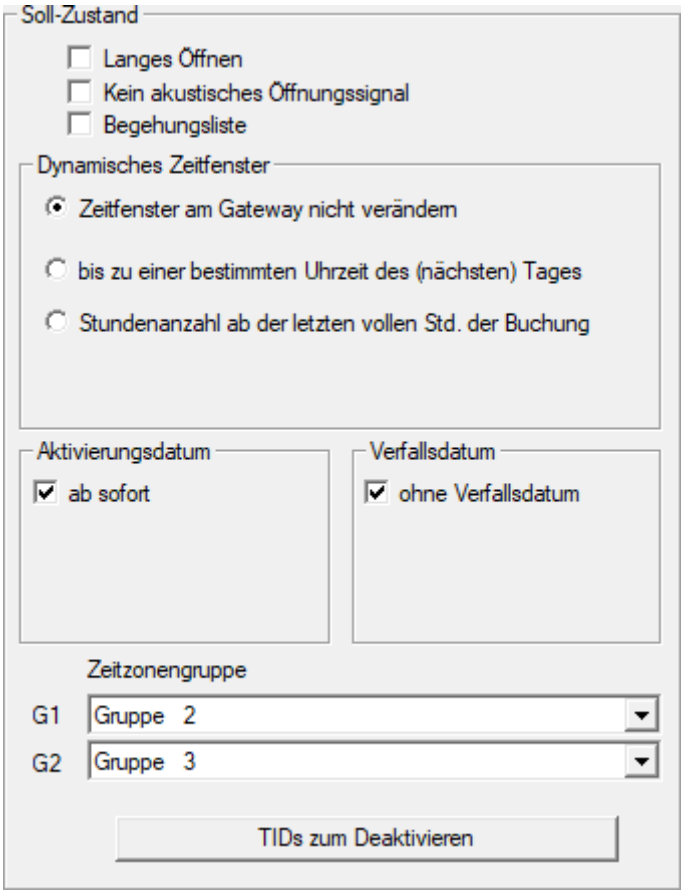
↳ I TID contrassegnati sono memorizzati sul transponder come da cancellare. Quando il transponder si autentica nella chiusura interessata, i TID da cancellare vengono bloccati nella chiusura.

Memorizzazione dei TID da bloccare nelle Proprietà

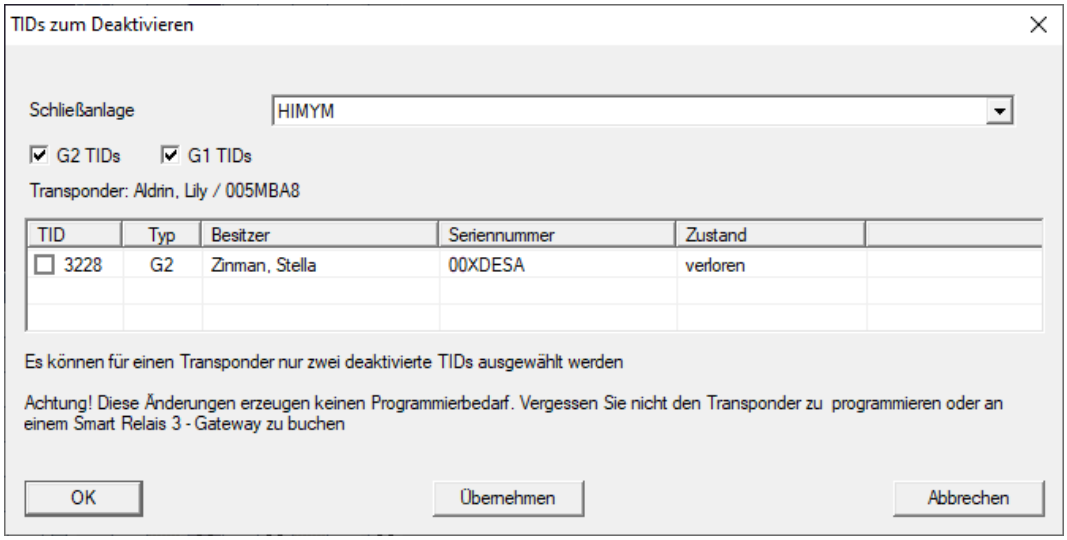
Gli ID da bloccare vengono memorizzati sul transponder durante il successivo processo di programmazione o durante la successiva prenotazione su un gateway.

✓ La finestra Proprietà del transponder è aperta.

1. Passate alla scheda di registro [Configurazione].



2. Cliccate sul pulsante TID da disattivare.
   ↳ L'elenco si apre.



3. Apponete un massimo di due segni di spunta nella colonna TID per memorizzare i TID da cancellare sul transponder.

4. Confermare l'inserimento con il pulsante "OK".

↳ I TID contrassegnati vengono memorizzati sul transponder durante la successiva programmazione o la successiva prenotazione su un gateway.

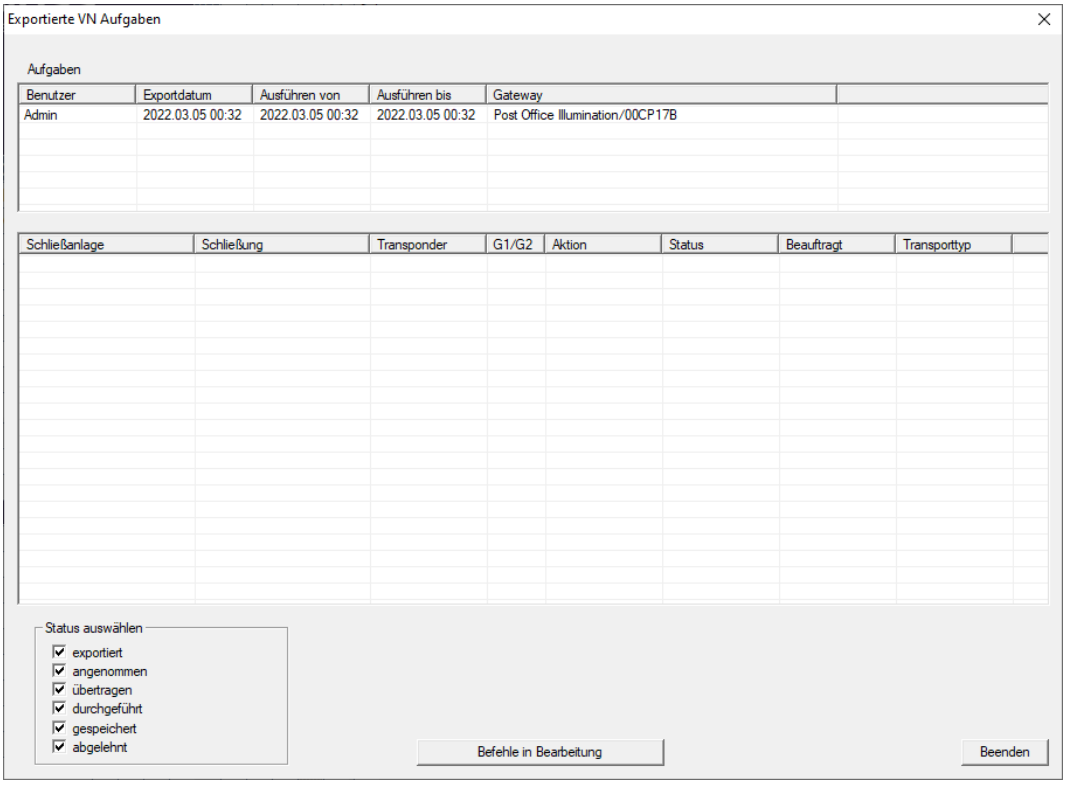
10.5.2.6 Stato dei task nella rete virtuale (SREL2.G2)

Dopo l'esportazione nella rete virtuale, potete vedere i task in una panoramica:

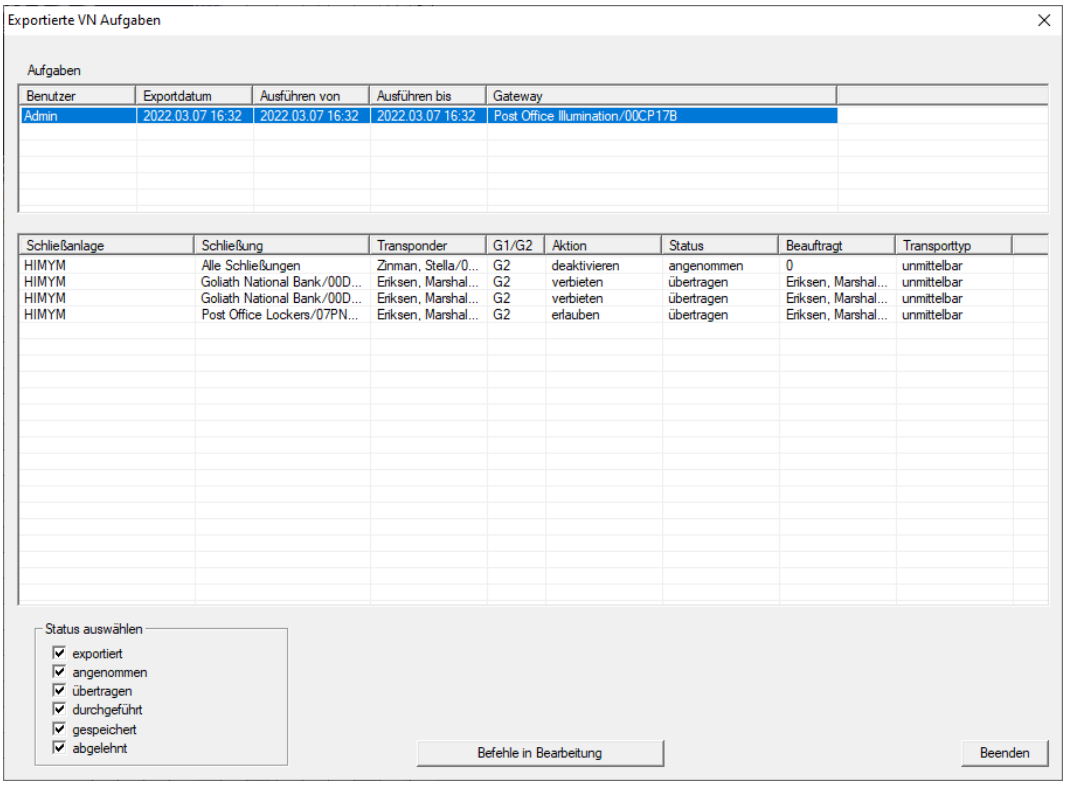
✓ Esportazione dei task nella rete virtuale (vedere *Esportazione delle modifiche alle autorizzazioni [▸ 239]*).

1. Aprite tramite | Programmaz. | - Rete virtuale (SREL2) la voce Task VN esportati.

↳ Si apre la finestra "Task VN esportati".



2. Selezionate un utente per visualizzare i suoi task esportati.

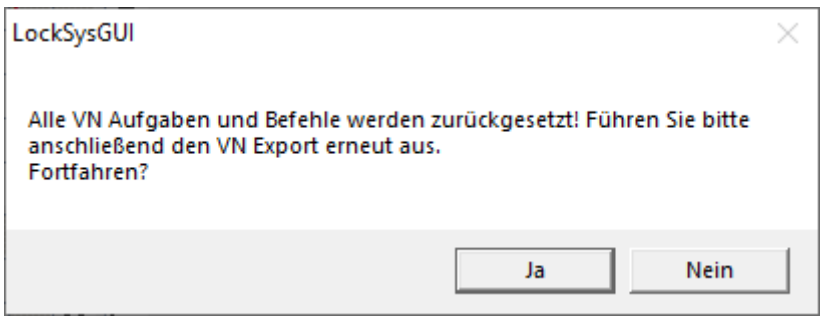


↳ I task esportati vengono visualizzati.

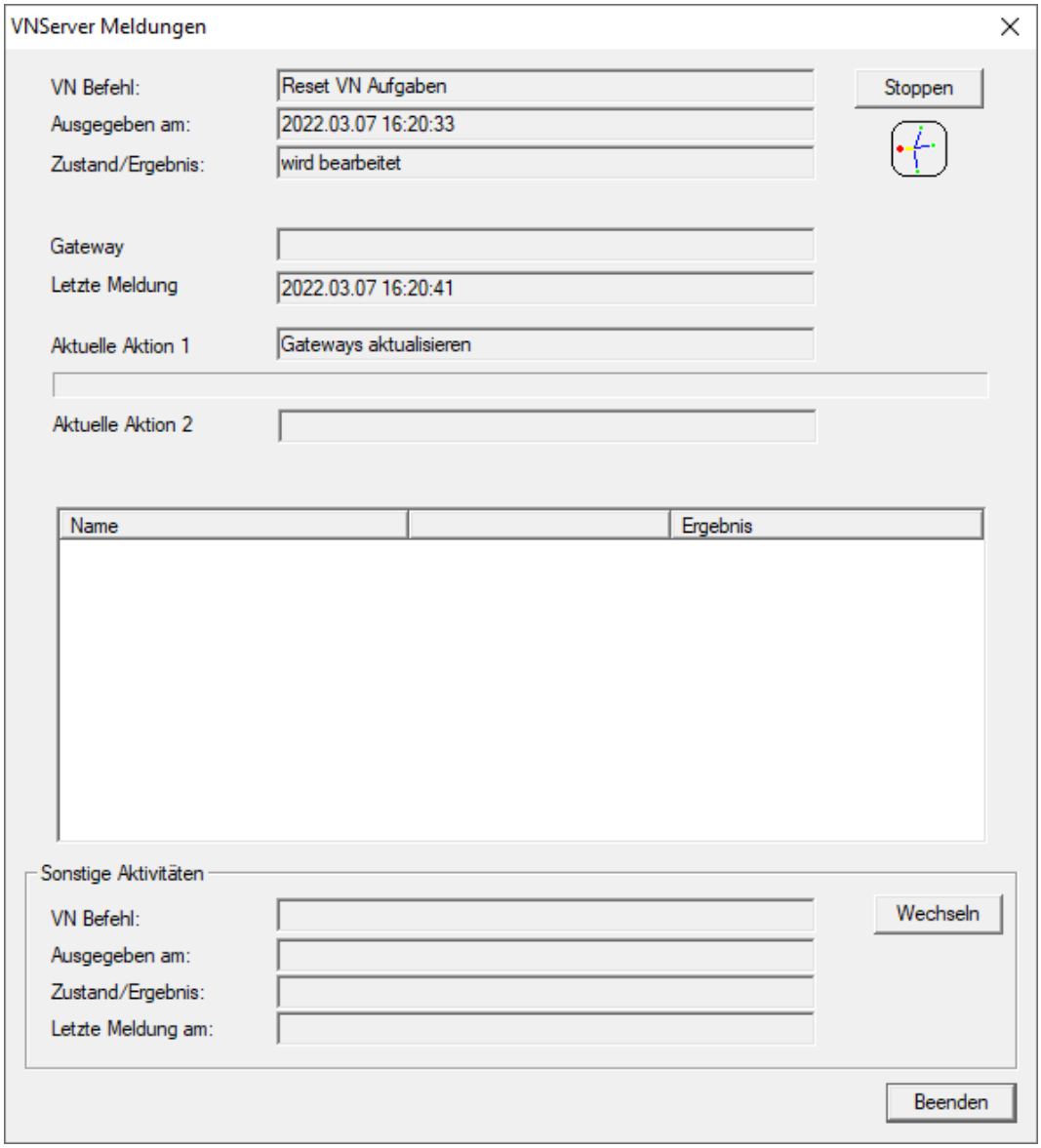
10.5.2.7 Reset dei task nella rete virtuale

I task che avete esportato nella rete virtuale possono anche essere resettati.

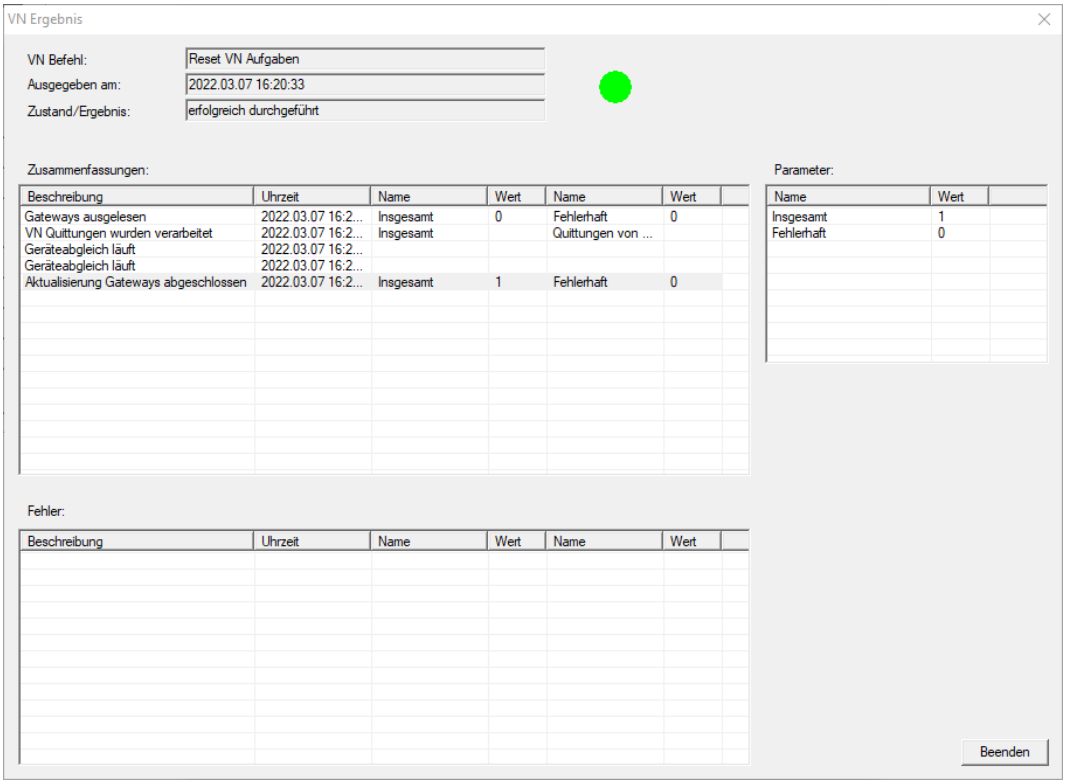
1. Selezionate tramite | Programmaz. | - Rete virtuale (SREL2) la voce Reset task VN.
   ↳ Si apre la nota di reset.



2. Fare clic sul pulsante Sì.
   ↳ I gateway sono programmati per resettare i task esportati.



↳ I task esportati vengono resettati.

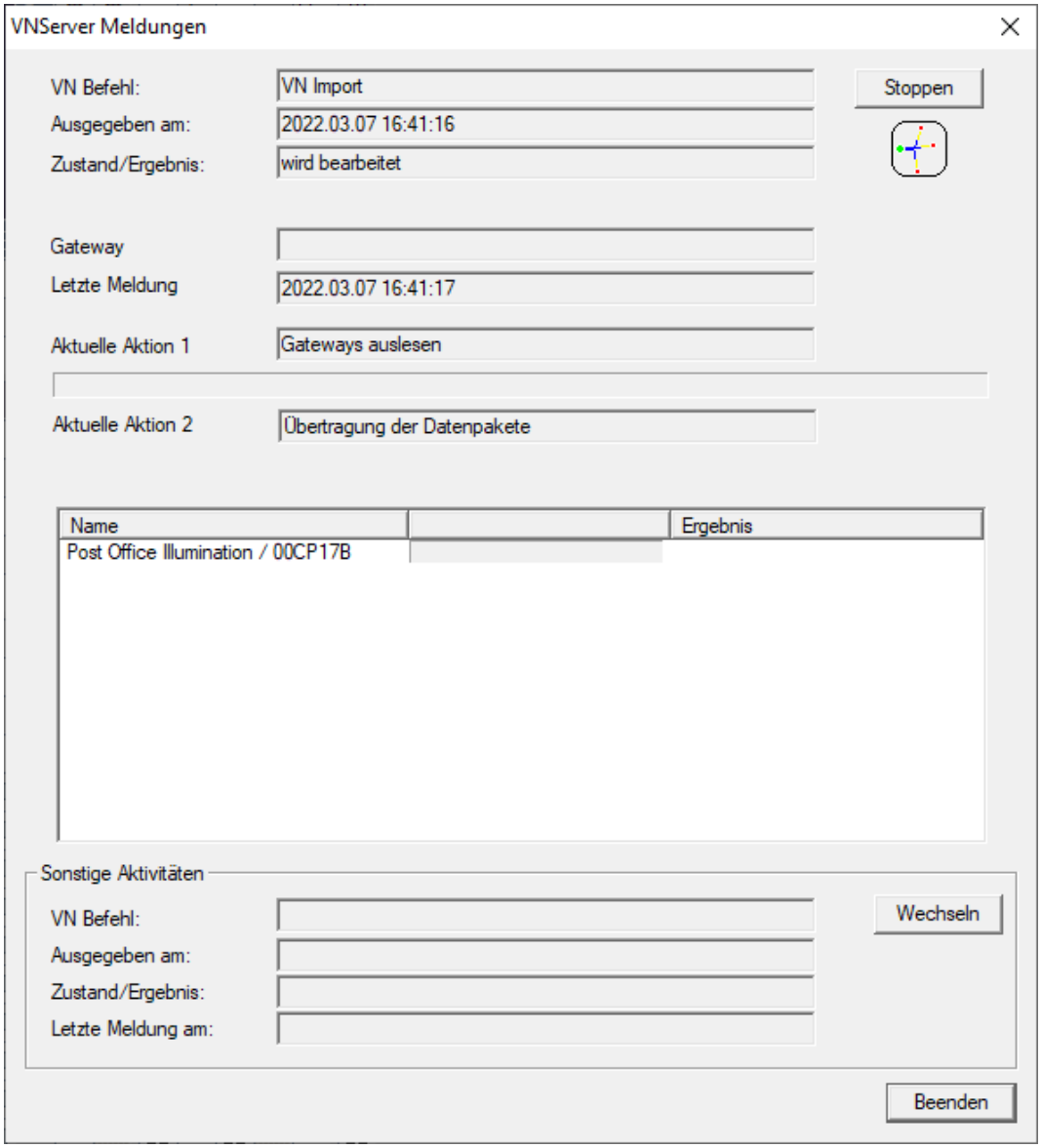


È possibile esportare nuovamente i task desiderati nella rete virtuale (vedere *Esportazione delle modifiche alle autorizzazioni [▸ 239]*).

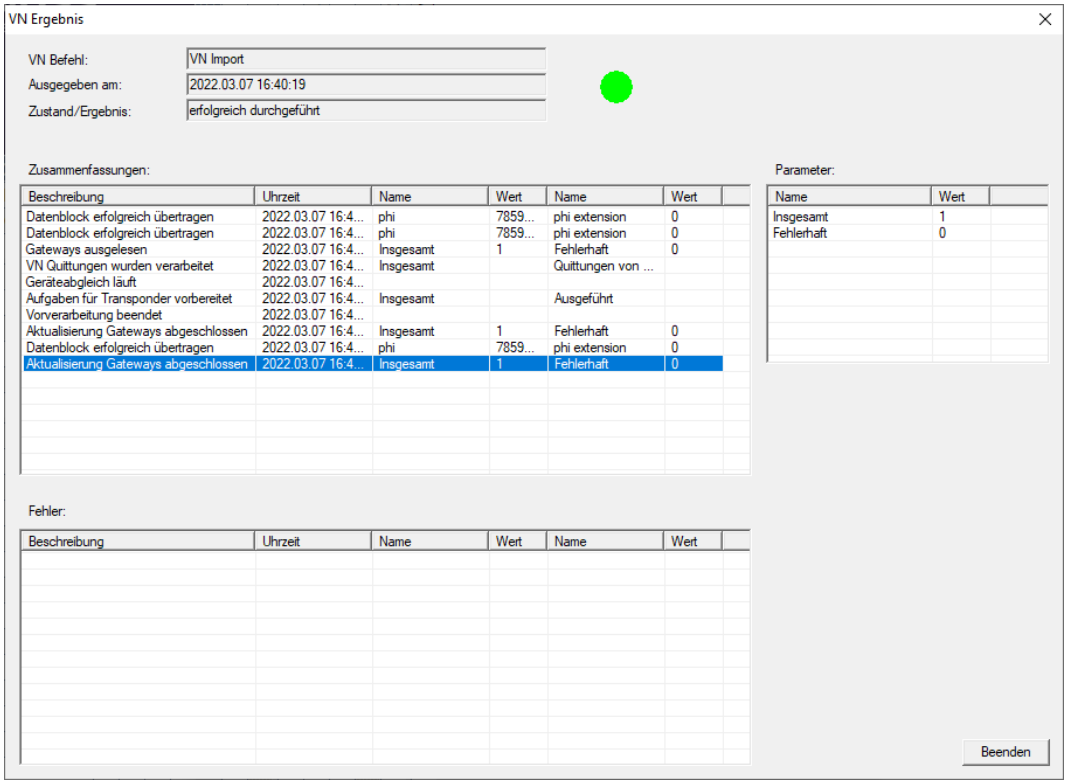
10.5.2.8 Importazione delle modifiche alle autorizzazioni

Dopo aver esportato le modifiche sul gateway, inizialmente non è possibile vedere nel software LSM quali modifiche sono già state recuperate dal gateway. Per fare questo, è necessario prima reimportare le modifiche:

1. Selezionate tramite | Programmaz. | - Rete virtuale (SREL2) la voce Importazione / sincronizzazione.
   ↳ Il processo di importazione inizia immediatamente.



↳ Viene visualizzato il rapporto di importazione.



2. Fare clic sul pulsante Esci.

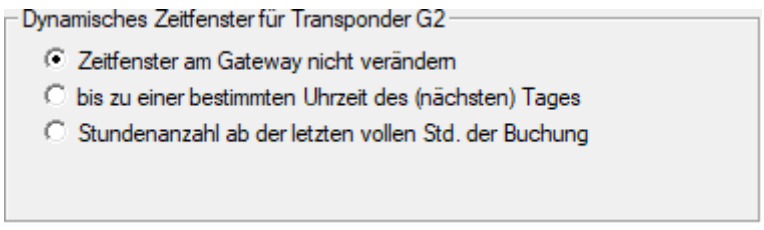
Ora è possibile controllare lo stato dei task (vedere *Stato dei task nella rete virtuale (SREL2.G2) [▸ 245]*).

10.5.2.9 Consigli sulla rete VN

Budget temporali

Per distribuire rapidamente le modifiche "offline" nell'impianto di chiusura, è importante che tutti i transponder siano prenotati a intervalli brevi e regolari. Qui è possibile lavorare con i budget temporali.

L'area "Fascia oraria dinamica per transponder G2" nelle Proprietà dell'impianto di chiusura vi offre la possibilità di imporre un budget temporale ai transponder. In questo modo, una persona può essere obbligata a caricare regolarmente il mezzo di identificazione sul gateway. Altrimenti, il mezzo di identificazione è bloccato per questo impianto di chiusura.



Importazione/esportazione automatica

Potete automatizzare l'importazione e l'esportazione delle modifiche su una gateway qui: | Rete | - Servizio VN (SREL2) .

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.

10.6 Lettura della chiusura

Uno dei grandi vantaggi delle chiusure collegate in rete è la possibilità di controllare lo stato comodamente dalla propria postazione di lavoro.

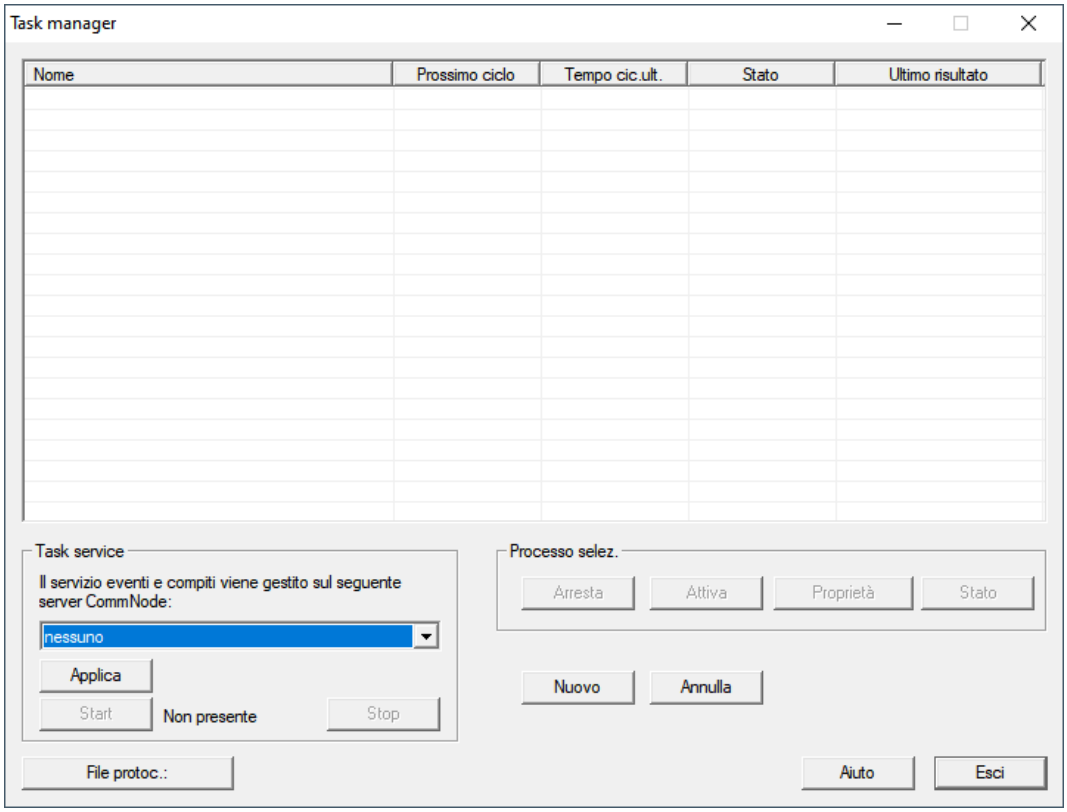
Task Manager consente inoltre di automatizzare questo processo.

Si può quindi rielaborare le informazioni nell'LSM, per esempio, utilizzando avvisi e segnalazioni (vedere *Videata allarmi [▸ 113]* e *Gestione avvisi [▸ 111]*).

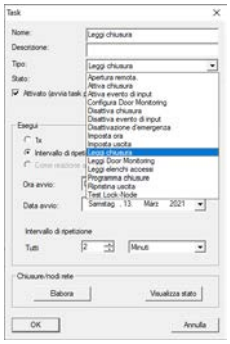
✓ LSM aperto.

✓ Chiusure da visualizzare programmate e collegate in rete (vedere *Creazione di una rete radio WaveNet e integrazione di una chiusura [▸ 195]*).

1. Selezionare in | Rete | la voce Task manager .
   ↳ Si apre la finestra "Task manager" .



2. Fare clic sul tasto Nuovo, per creare un nuovo task.
   ↳ Si apre la finestra "Task" .
3. Inserire un nome per il Task.
4. Selezionare nel menu a discesa ▼ **Tipo** la voce "Leggi chiusura".

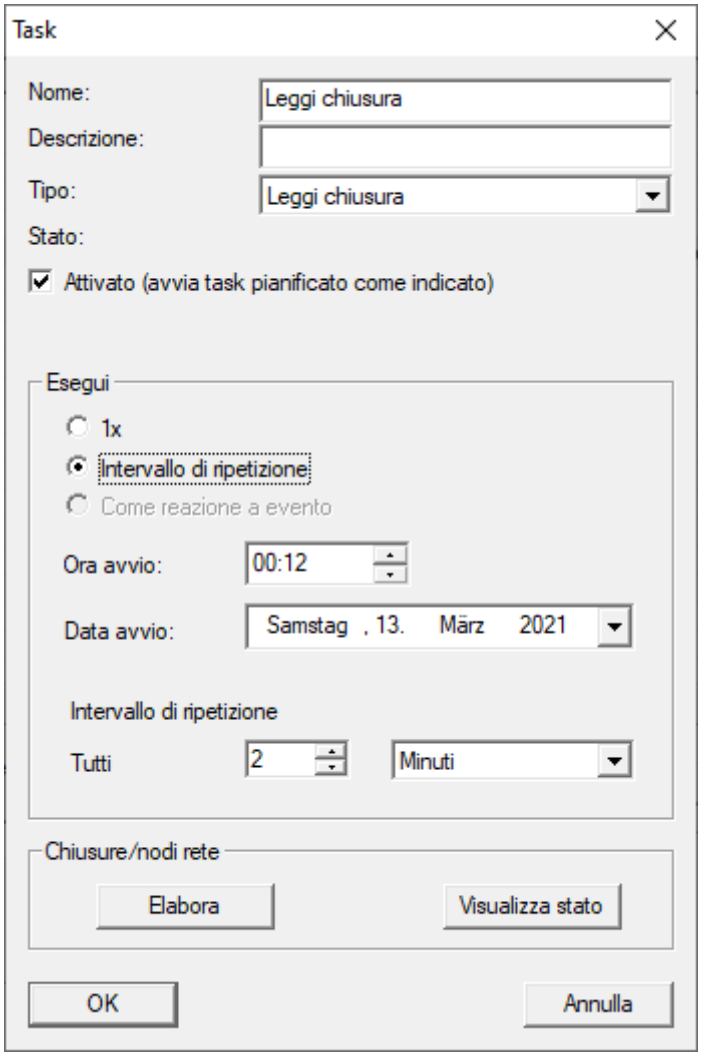


5. Selezionare nell'area "Eseguire" l'opzione ◉ Intervallo di ripetizione.
6. Impostare l'intervallo desiderato.

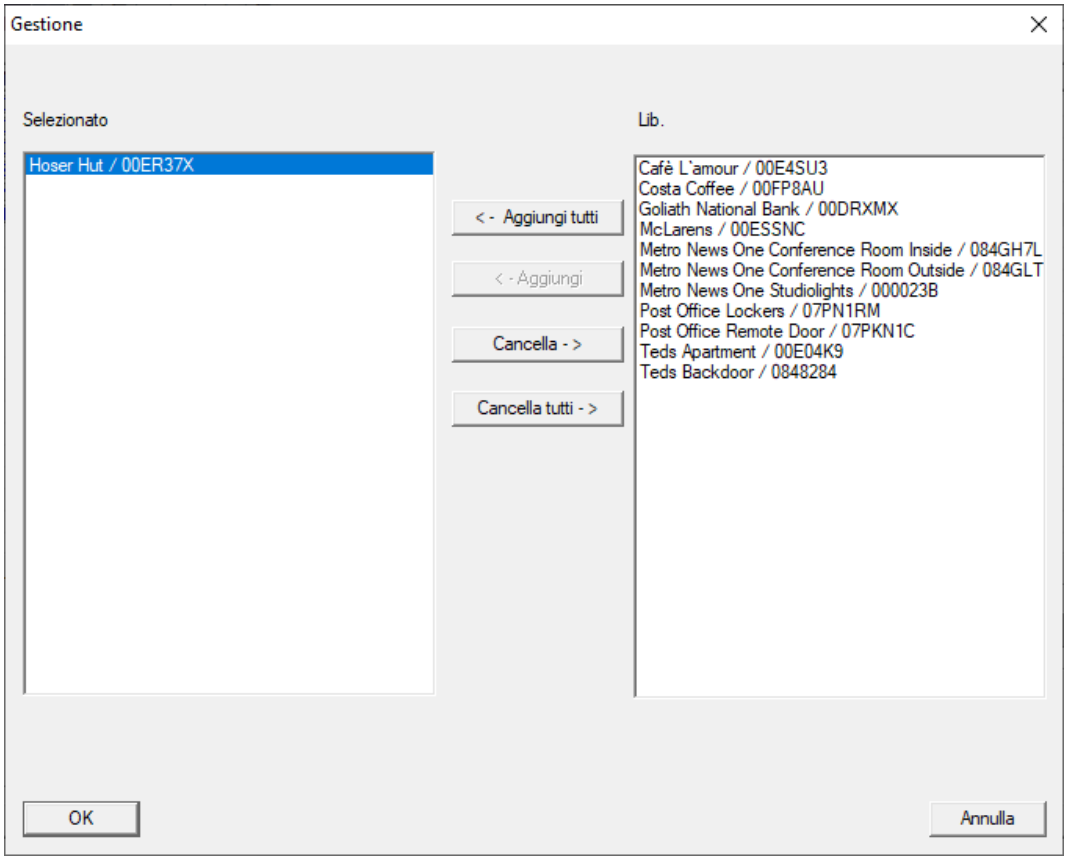
NOTA

Influenza dell'intervallo di ripetizione sulla durata della batteria

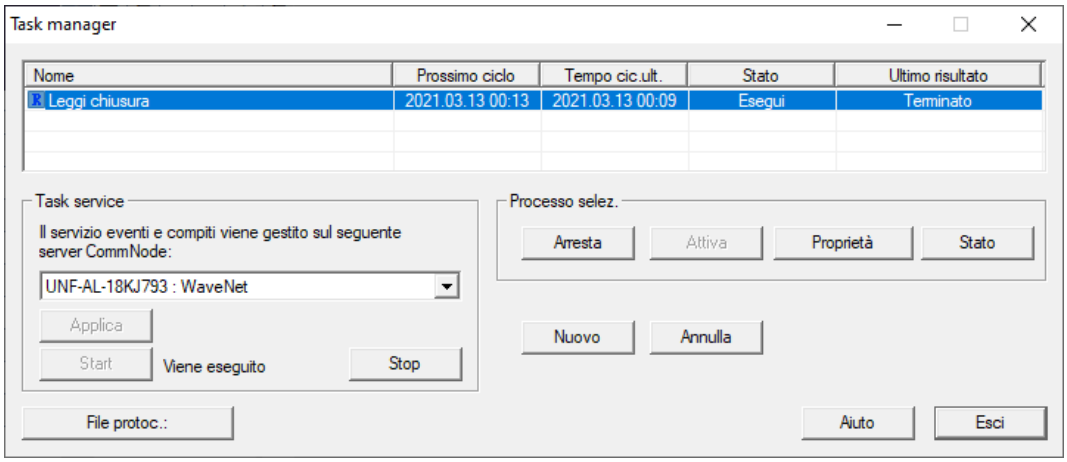
Quanto più frequentemente viene effettuata la lettura della chiusura, tanto più frequentemente la chiusura viene risvegliata dalla modalità di standby a risparmio energetico. La durata della batteria può quindi accorciarsi.



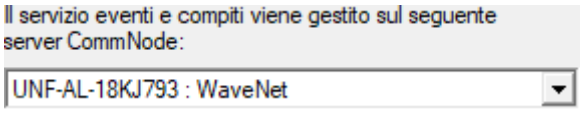
7. Fare clic nell'area "Chiusure/nodi rete" sul tasto Elabora .
   ↳ Si apre la finestra "Gestione" .



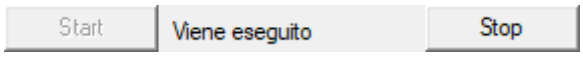
8. Selezionare le chiusure di cui si desidera effettuare la lettura.
9. Infine spostare le chiusure con il tasto Aggiungi nella colonna di sinistra.
10. Fare clic sul pulsante OK.
    ↳ Si chiude la finestra "Gestione" .
11. Fare clic sul pulsante OK.
    ↳ Si chiude la finestra "Task" .
    ↳ Il task è elencato nel Task Manager.



12. Assicurarsi che nell'area "Task service" nel menu a discesa ▼ **Il servizio eventi e compiti viene gestito sul seguente server CommNode** sia selezionato il CommNode appropriato.



13. Assicurarsi che anche il Task Service sia in esecuzione.



14. Fare clic sul pulsante Esci.
    ↳ Si chiude la finestra "Task manager" .

↳ Lo stato di chiusura delle chiusure impostate viene interrogato automaticamente.

11. Glossario & Acronimi

Nel seguito vengono precisati singoli termini. Le spiegazioni sono facilmente comprensibili, anche se forse non includono tutti i particolari.

Termine	Acronimo	Spiegazione
Advantage Database Server	ADS-Server	Servizio server essenziale, che risulta necessario per operare con LSM BUSINESS e PROFESSIONAL.
File CSV		Formato corrente di file per l'import e l'export di valori, quali ad esempio elenchi di personale, impianti di chiusura, ecc.
DoorMonitoring	DM	Opzione di componenti di chiusura, che comunica caratteristiche importanti dello stato di una porta (es. porta chiusa e doppiamente bloccata) al software LSM.
Modalità Freeze		Con batteria in condizioni critiche, le chiusure passano in modalità Freeze, per permettere ancora un'ultima apertura della porta.
Generazione protocollo G1	G1	Prima generazione di protocolli, in cui comunicano chiusure e sistemi di identificazione.
Generazione protocollo G2	G2	Seconda generazione di protocolli, che comporta maggior comfort funzionale.
Lightweight Directory Access Protocol	LDAP	Protocollo di rete per interrogare e modificare informazioni. Nel software LSM possono ad esempio venire caricati, direttamente via LDAP, dati personali.
Locking Data Base Software	LDB	La versione precedente del software LSM.
Lock-ID	LID	Identifica la chiusura all'interno dell'impianto di chiusura. (Paragonabile a una targa automobilistica.)
Local Operating Network	Rete LON	La Local Operating Network (LON) è uno standard più datato, che viene/veniva impiegato prevalentemente nell'automazione di edifici.

Termine	Acronimo	Spiegazione
Locking System Management	LSM	Software attuale, che permette flessibilità di gestione di componenti di chiusura SimonsVoss.
Matrice		La matrice offre una panoramica dei sistemi di identificazione e delle chiusure per cui sono autorizzati.
MIFARE		MIFARE definisce uno standard mondiale per uno dei sistemi di schede più utilizzato. (La chiusura viene azionata con “schede passive”)
Personal Digital Assistant	PDA	Piccolo computer dalle dimensioni che si avvicinano a uno smartphone. Con l'ausilio di un palmare (PDA) si possono programmare in mobilità componenti attivi di chiusura G1.
Physical Hardware Identifier	PHI	Il numero PHI è impresso sul componente SimonsVoss e archiviato all’interno. Il numero PHI è univoco e non può essere modificato.
Cilindro profilato	PZ	Il cilindro profilato è la forma più utilizzata di serrature di sicurezza per porte, ed è una tipologia del cilindro di chiusura.
Router (CentralNode)		Su router speciali si possono interpellare direttamente in rete corrispondenti chiusure.
SMART.SURVEIL		SMART.SURVEIL è un programma stand-alone di monitoraggio. Può essere eseguito su computer privi di software LSM e richiede un user client libero. (Da LSM 3.4 SP1)
Transponder-ID	TID	Identifica il transponder all’interno dell’impianto di chiusura. (Paragonabile a una targa automobilistica.)
Rete virtuale	VN	Su una “rete virtuale” si possono conseguire diversi vantaggi di rete, senza impiego di router speciali.

Termine	Acronimo	Spiegazione
Controllo di accesso	ZK	I componenti SimonsVoss con funzione ZK protocollano tutti gli accessi (o “registrazioni”) nell’impianto di chiusura.

12. Supporto e ulteriori informazioni

Materiale informativo/Documenti

Maggiori informazioni sul funzionamento e sulla configurazione nonché ulteriori documenti sono riportati nella homepage:

https://www.simons-voss.com/it/documenti.html

Software e driver

Software e driver sono disponibili sulla homepage:

https://www.simons-voss.com/it/assistenza/download-software.html

Dichiarazioni di conformità

Le dichiarazioni di conformità e altri certificati sono riportate nella homepage:

https://www.simons-voss.com/it/certificati.html

Supporto tecnico

Il nostro supporto tecnico sarà lieto di aiutarvi (linea fissa, i costi dipendono dal provider):

+49 (0) 89 / 99 228 333

E-mail

Se si preferisce contattarci via e-mail, scrivere all'indirizzo:

support-simonsvoss@allegion.com

FAQ

Per informazioni e consigli utili, consultare l'area FAQ:

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

Indirizzo

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germania

Ecco a voi SimonsVoss

SimonsVoss, pioniere della tecnologia di chiusura radiocomandata senza fili, offre soluzioni di sistema con un'ampia gamma di prodotti per il settore SOHO, per le piccole e grandi imprese e le istituzioni pubbliche. Gli apparati SimonsVoss racchiudono funzionalità intelligenti, alta qualità e design pluripremiato Made in Germany.

Come fornitore di prodotti innovativi, SimonsVoss punta su scalabilità, alta sicurezza, affidabilità, software potenti e facilità d'uso. Questo rende SimonsVoss un leader tecnologico riconosciuto nell'ambito dei sistemi di chiusura digitali wireless.

Coraggio di innovare, mentalità e agire sostenibile e grande attenzione verso collaboratori e clienti: questa è la chiave del nostro successo.

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

Qualità "made in Germany"

Per SimonsVoss, il "Made in Germany" è un impegno serio: Tutti i prodotti sono sviluppati e realizzati esclusivamente in Germania.

© 2024, SimonsVoss Technologies GmbH, Unterföhring

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

Il contenuto di presento 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.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION