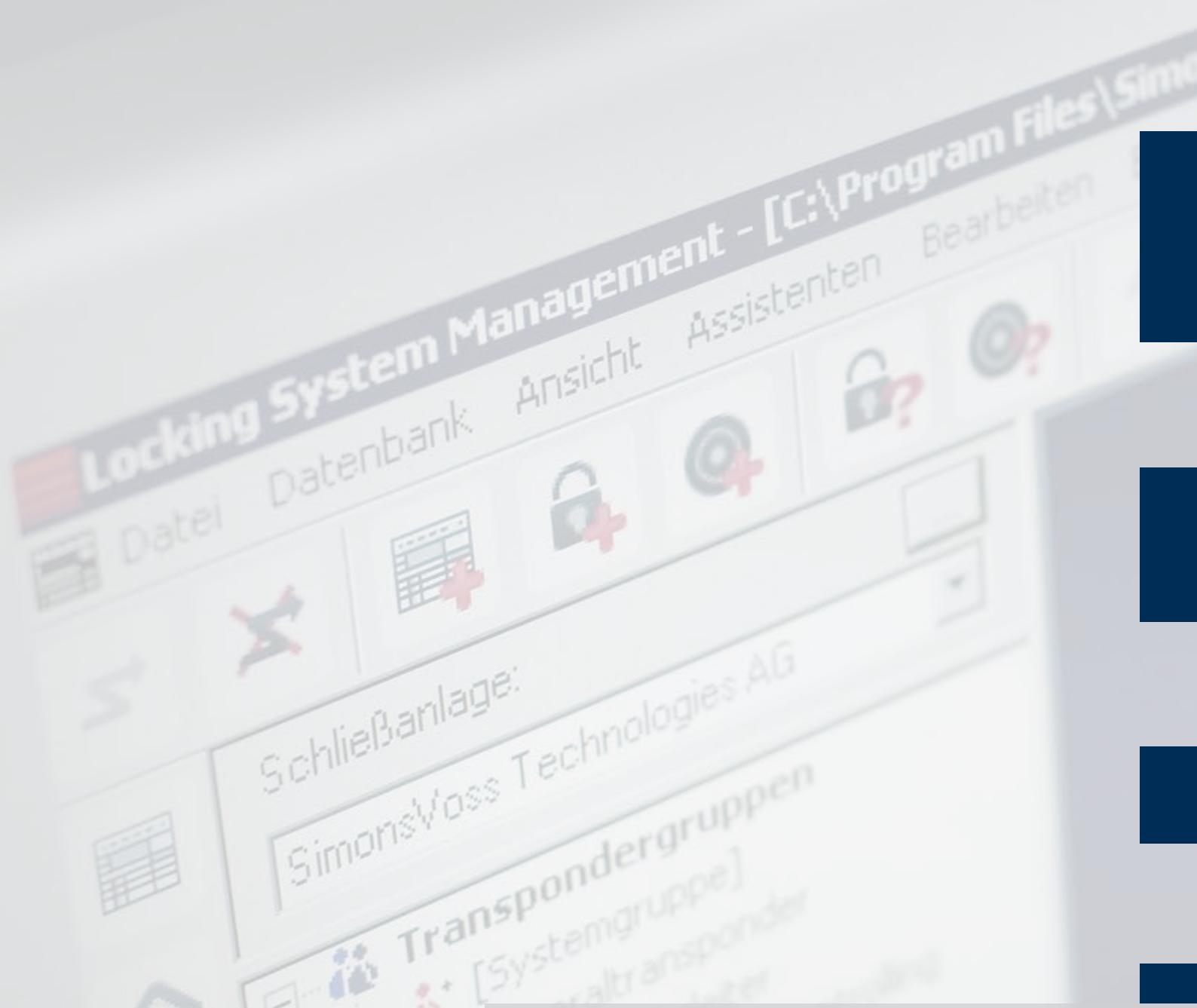


LSM 3.4 SP2 SmartUserGuide

Handbuch

29.10.2019

SimonsVoss technologies

Inhaltsverzeichnis

1 Grundfunktionen

Dieses Kapitel beschreibt grundlegende Vorgänge in der LSM Software. In der LSM Software gibt es oft mehrere Wege, um zur gewünschten Funktion zu gelangen. Diese Grundfunktionen zeigen meist den schnellsten und einfachsten Weg.

Der SimonsVoss SmartUserGuide beschreibt anhand eines verständlichen Beispiels ausführlich, wie eine Schließanlage angelegt und verwaltet werden kann.

1.1 Neue Schließanlage anlegen

✓ Die Installation wurde ordnungsgemäß durchgeführt und ein Backup ist zur Sicherheit eingerichtet.

1. In der Menüleiste *Bearbeiten/Neue Schließanlage* auswählen.
2. Gewünschte Schließanlagenoptionen festlegen.
   ↳ Für übergreifende Schließebenen eine Farbe aus "Als übergreifende Schließebene nutzen" auswählen. *Übergreifende Schließebenen dienen als zusätzliche Ebenen zu bereits existierenden Standard-Schließanlagen. Siehe* Übergreifende Schließebene.
3. Klicken Sie auf die Schaltfläche "Übernehmen".
4. Klicken Sie auf die Schaltfläche "Beenden".

1.2 Neue Transpondergruppe anlegen

✓ Es ist bereits eine Schließanlage angelegt.

1. Rechtsklick auf Transpondergruppen im "Gruppen-Bereich" der LSM Software.
2. Klicken Sie auf "Neu".
3. Vergeben Sie einen Namen für die neue Transpondergruppe und legen Sie ggf. weitere Einstellungen fest.
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

1.3 Neuen Transponder anlegen

✓ Es ist bereits eine Schließanlage angelegt.

1. Wählen Sie *Bearbeiten/Neuer Transponder*.
2. Füllen Sie alle Attribute aus und setzen Sie ggf. weitere Einstellungen über die Schaltfläche "Konfiguration".
3. Klicken Sie auf die Schaltfläche "Speichern & Weiter".
4. Klicken Sie auf die Schaltfläche "Beenden".

1.4 Transponder nachträglich einer Transpondergruppe zuweisen

✓ Der Transponder wurde bereits erstellt und eine Transpondergruppe ist angelegt.

1. Öffnen Sie die Schließanlageneinstellungen, z.B. über die Menüleiste *Bearbeiten/Eigenschaften: Schließanlage*.
2. Wählen Sie die Registerkarte "Transponder".
3. Wählen Sie den Transponder aus der Tabelle aus, dem Sie eine Transpondergruppe zuordnen wollen.
4. Wählen Sie aus der Dropdownliste bei "Zuordnung zu Transpondergruppen ändern" die gewünschte Transpondergruppe aus, welche dem Transponder zugewiesen werden soll.
5. Klicken Sie auf die Schaltfläche "Ausführen".
6. Klicken Sie auf die Schaltfläche "Übernehmen".
7. Klicken Sie auf die Schaltfläche "Beenden".

Wenn ein Transponder neu angelegt wird, kann diesem gleich eine existierende Transpondergruppe zugewiesen werden.

1.5 Neuen Bereich anlegen

✓ Es ist bereits eine Schließanlage angelegt.

1. Rechtsklick auf Bereiche im "Bereiche-Bereich" der LSM Software.
2. Klicken Sie auf "Neu".
3. Vergeben Sie einen Namen für den neuen Bereich und legen Sie ggf. weitere Einstellungen fest.
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

1.6 Neue Schließung anlegen

✓ Es ist bereits eine Schließanlage angelegt.

1. Wählen Sie *Bearbeiten/Neue Schließung*.
2. Füllen Sie alle Attribute aus und setzen Sie ggf. weitere Einstellungen über die Schaltfläche "Konfiguration".
3. Klicken Sie auf die Schaltfläche "Speichern & Weiter".
4. Klicken Sie auf die Schaltfläche "Beenden".

1.7 Schließung einem Bereich zuweisen

✓ Die Schließung wurde bereits erstellt und ein Bereich ist angelegt.

1. Öffnen Sie die Schließanlageneinstellungen, z.B. über die Menüleiste *Bearbeiten/Eigenschaften: Schließanlage*.
2. Wählen Sie die Registerkarte "Türen".

3. Wählen Sie die Tür aus der Tabelle aus, der Sie einem Bereich zuordnen wollen.
4. Wählen Sie aus der Dropdownliste bei "Zuordnung zum Bereich ändern" den gewünschten Bereich aus, welcher der Tür zugewiesen werden soll.
5. Klicken Sie auf die Schaltfläche "Ausführen".
6. Klicken Sie auf die Schaltfläche "Übernehmen".
7. Klicken Sie auf die Schaltfläche "Beenden".

Wenn eine Schließung neu angelegt wird, kann dieser gleich ein existierender Bereich zugewiesen werden.

1.8 Berechtigung vergeben/entziehen

Berechtigungen können über die Matrix vergeben und entzogen werden. In der Standardeinstellung genügt es, ein Berechtigungsfeld einfach anzuklicken, um die Berechtigung zu ändern.

Berechtigungen können nur zwischen einer Schließung und einem Transponder gesetzt oder wiederrufen werden.

Beachten Sie die beiden Ansichten:

- **Ansicht/Türen und Personen**

  In dieser Ansicht werden die Berechtigungen für den gewünschten Transponder geändert.

- **Ansicht/Bereiche und Transpondergruppen**

  In dieser Ansicht werden die Berechtigungen für komplette Gruppen geändert.

1.9 Datenschutzkonformes Arbeiten nach DSGVO

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung europaweit gültig. Sie regelt den Umgang mit personenbezogenen Daten, um deren Schutz und zugleich deren freien Verkehr im europäischen Binnenmarkt sicherzustellen. Zu allererst ist der Zugriff über die grafischen Benutzeroberfläche auf die Datenbank nur mit Passwort und entsprechenden Benutzerrechten möglich. Darüber hinaus werden innerhalb der LSM-Software keine „besonderen Kategorien“ personenbezogener Daten nach Art. 9 DSGVO gespeichert. Die verwendeten Pflichtfelder zu einer Person dienen ausschließlich zur eindeutigen Zuordnung von Identifikationsmedien innerhalb des Schließplans. Die verpflichtenden Daten werden systemseitig nur über die Dauer der Inbesitznahme eines Identifikationsmediums benötigt (z. B. Firmenzugehörigkeit). Die Dauer der Speicherung von Daten in Protokollen kann vom Schließanlagenverwalter selbst beliebig verändert werden (siehe Optionen/Protokollieren).

1.9.1 Daten exportieren

HINWEIS

Fremdsprachige Texte

Für die Texte in den exportierten Dateien wird dieselbe Sprache wie in der LSM-Software verwendet.

Personen

Sie können die gespeicherten personenbezogenen Daten der Personen in der Schließanlage als CSV-Dateien exportieren. Dabei werden drei Dateien erzeugt:

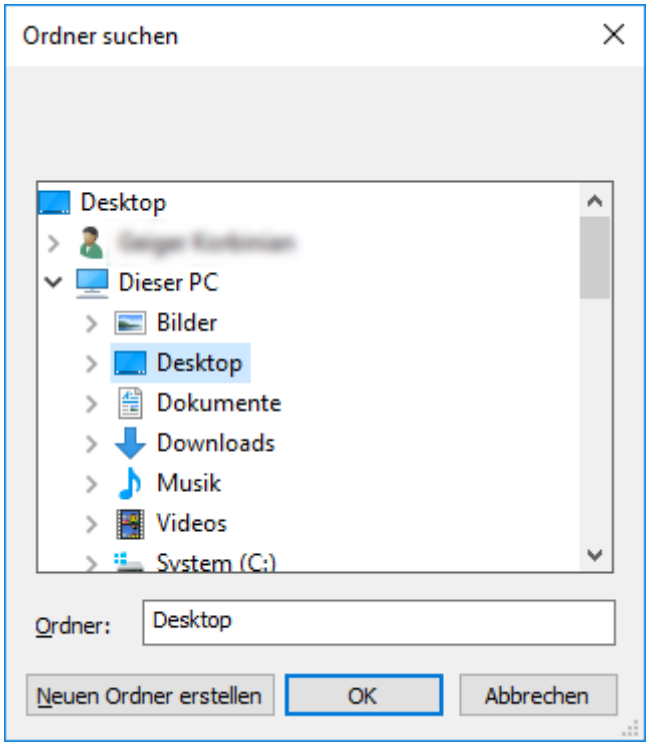
Person	Diese Datei beinhaltet die personenbezogenen Daten, mit denen die Person identifiziert werden kann (zum Beispiel Nachname, Adresse oder Foto).
PersonHistory	Diese Datei beinhaltet das Datum der Erstellung und der Löschung des Datensatzes.
PersonLog	Diese Datei beinhaltet den Verlauf der Bearbeitungen, die an dem Datensatz dieser Person durchgeführt wurden (zum Beispiel Berechtigungsänderungen oder Programmierungen).

HINWEIS

Die DSGVO-Funktionen greifen dazu auf die Personalverwaltung zu. Sie müssen deshalb einer Benutzergruppe zugeordnet sein, die zur Personalverwaltung berechtigt ist.

✓ LSM geöffnet.

1. Wählen Sie über | Optionen | den Eintrag DSGVO Funktionen.
   ↳ Fenster "DSGVO Funktionen" öffnet sich.
2. Markieren Sie im Bereich "Personen" den Eintrag der Person, deren Daten exportiert werden sollen.
3. Klicken Sie im Bereich "Personen" auf die Schaltfläche Personenbezogene Daten exportieren.
   ↳ Fenster "Ordner suchen" öffnet sich.



4. Bestimmen Sie einen Ordner, in den die Dateien exportiert werden sollen.
5. Klicken Sie auf die Schaltfläche OK.

↳ Daten werden exportiert.

Benutzer

Sie können die gespeicherten personenbezogenen Daten der Benutzer der LSM-Software als CSV-Dateien exportieren. Dabei werden zwei Dateien erzeugt:

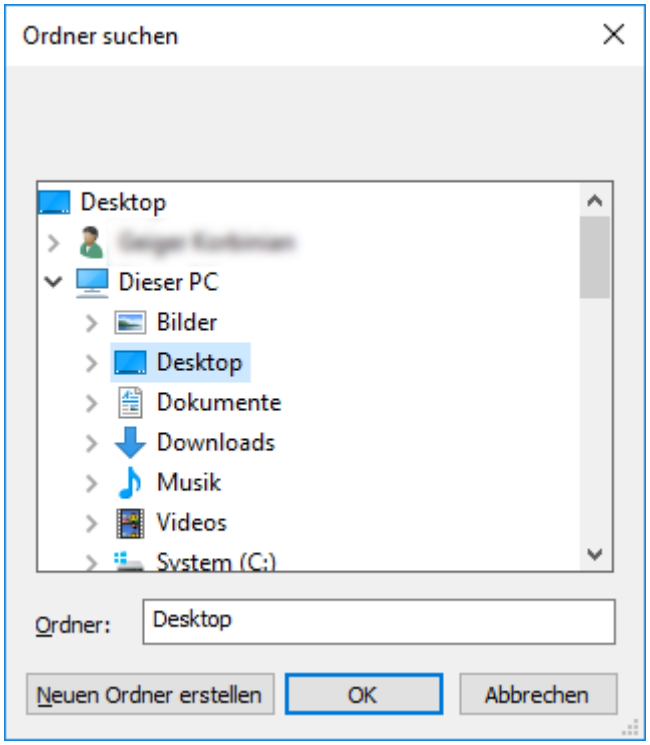
User	Diese Datei beinhaltet die Daten, die auf den Benutzer zutreffen (zum Beispiel Benutzername und Benutzergruppe).
UserLog	Diese Datei beinhaltet den Verlauf der Bearbeitungen, die durch diesen Benutzer durchgeführt wurden (zum Beispiel das Anlegen einer neuen Schließung).

HINWEIS

Die DSGVO-Funktionen greifen dazu auf Administrationsfunktionen zu. Sie müssen deshalb einer Benutzergruppe zugeordnet sein, die zur Administration berechtigt ist.

✓ LSM geöffnet.

1. Wählen Sie über | Optionen | den Eintrag DSGVO Funktionen.
   ↳ Fenster "DSGVO Funktionen" öffnet sich.
2. Markieren Sie im Bereich "Benutzer" den Eintrag des Benutzers, dessen Daten exportiert werden sollen.
3. Klicken Sie im Bereich "Benutzer" auf die Schaltfläche Personenbezogene Daten exportieren.
   ↳ Fenster "Ordner suchen" öffnet sich.



4. Bestimmen Sie einen Ordner, in den die Dateien exportiert werden sollen.
5. Klicken Sie auf die Schaltfläche OK.

↳ Daten werden exportiert.

1.9.2 Daten löschen

Mit dem DSGVO-Modul können Sie personenbezogene Daten auch komfortabel löschen.

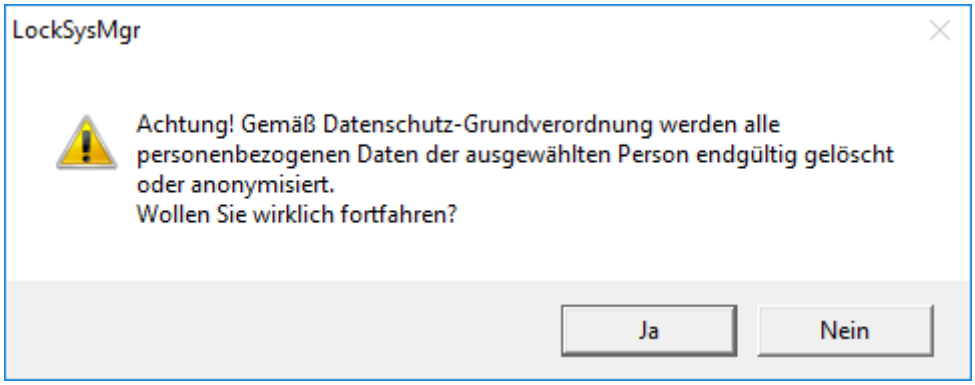
Personen

HINWEIS

Die DSGVO-Funktionen greifen dazu auf die Personalverwaltung zu. Sie müssen deshalb einer Benutzergruppe zugeordnet sein, die zur Personalverwaltung berechtigt ist.

✓ LSM geöffnet.

1. Wählen Sie über | Optionen | den Eintrag DSGVO Funktionen.
   ↳ Fenster "DSGVO Funktionen" öffnet sich.
2. Markieren Sie im Bereich "Personen" den Eintrag der Person, deren Daten gelöscht werden sollen.
3. Klicken Sie im Bereich "Personen" auf die Schaltfläche Personenbezogene Daten endgültig löschen.
   ↳ Fenster "LockSysMgr" öffnet sich.



4. Klicken Sie auf die Schaltfläche Ja.

↳ Personenbezogene Daten der markierten Person gelöscht oder anonymisiert.

HINWEIS

Löschung von Restdaten aus vorherigen Löschungen

Es ist möglich, die Daten von Personen auch mit der Schaltfläche ✕ in der Registerkarte [Name] der zugeordneten Identifikationsmedien zu löschen. Dabei werden jedoch im Gegensatz zur Löschung über das DSGVO-Modul die Protokolle nicht gelöscht und verbleiben im System. Somit ist nur ein Teil der personenbezogenen Daten gelöscht. Personen, die so gelöscht wurden, werden nicht mehr im DSGVO-Modul angezeigt. Um der DSGVO zu genügen und auch diese Dateien zu entfernen, verwenden Sie bitte die Schaltfläche Löschen im Bereich "Datenbank".

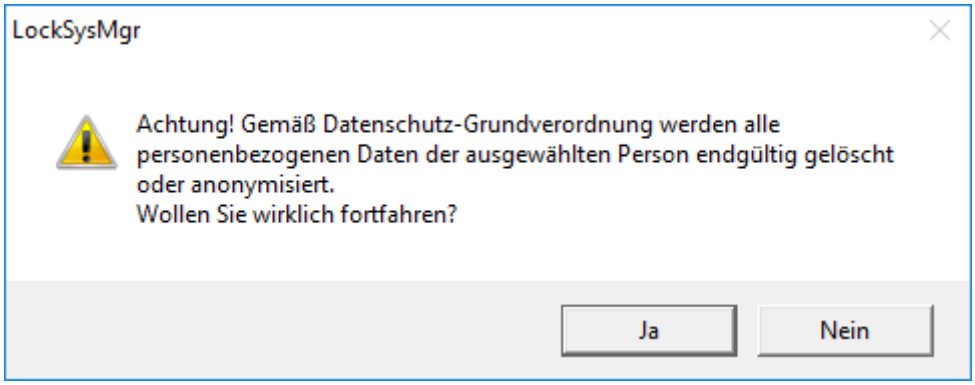
Benutzer

HINWEIS

Die DSGVO-Funktionen greifen dazu auf Administrationsfunktionen zu. Sie müssen deshalb einer Benutzergruppe zugeordnet sein, die zur Administration berechtigt ist.

✓ LSM geöffnet.

1. Wählen Sie über | Optionen | den Eintrag DSGVO Funktionen.
   ↳ Fenster "DSGVO Funktionen" öffnet sich.
2. Markieren Sie im Bereich "Benutzer" den Eintrag des Benutzers, dessen Daten gelöscht werden sollen.
3. Klicken Sie im Bereich "Benutzer" auf die Schaltfläche Personenbezogene Daten endgültig löschen.
   ↳ Fenster "LockSysMgr" öffnet sich.



4. Klicken Sie auf die Schaltfläche Ja.

↳ Personenbezogene Daten des markierten Benutzers gelöscht oder anonymisiert.

1.10 Pin Code Tastatur anlegen

Eine Pin Code Tastatur kann nicht in reinen G2-Schließanlagen betrieben werden. Die drei User-Pins verhalten sich wie G1-Transponder.

1.10.1 Pin Code Tastatur konfigurieren

Master-Pin ändern

Dieser Schritt muss nur ausgeführt werden, wenn noch kein neuer Master-Pin einprogrammiert wurde.

1. Eingabe 0 0 0 0
2. Eingabe alte Master-Pin: 1 2 3 4 5 6 7 8
3. Eingabe neue Master-Pin
   ↳ Die neue Master-Pin muss aus 8 Zeichen bestehen, welche weder fortlaufend noch identisch sind und darf nicht mit 0 beginnen!
4. Eingabe des neuen Master-Pin zur Wiederholung

HINWEIS

Der Master-Pin ist für die Nutzung der Pin Code Tastatur essentiell und kann nicht ausgelesen oder wiederhergestellt werden. Notieren Sie den Master-Pin und bewahren Sie ihn an einem sicheren und geheimen Ort auf. *Wer den Master-Pin kennt, könnte die Schließungen der Pin Code Tastatur öffnen oder versperren, indem er selbst neue User-Pins definiert!*

User-Pin programmieren

In der Pin Code Tastatur können bis zu drei User-Pins vergeben werden. Die Länge des User-Pins kann zwischen 4 und 8 stellen betragen, welche nicht fortlaufend oder identisch sind.

Zum besseren Verständnis: Jeder User-Pin verhält sich wie ein eigener Transponder. Deshalb müssen diese einzelnen User-Pins in den jeweiligen (internen) Transpondern (1, 2 & 3) programmiert werden.

1. Eingabe 0
2. Eingabe Master-Pin
3. Eingabe User Pin - z.B 1 für User-Pin 1
4. Eingabe der Länge des User-Pin - z.B. 4 für einen 4-stelligen User-Pin
5. Eingabe User-Pin

Wiederholen Sie den Vorgang, um weitere User-Pins in der Pin Code Tastatur zu programmieren.

1.10.2 Pin Code Tastatur im Schließplan anlegen

Für jeden User-Pin muss ein eigener Transponder angelegt werden!

1. *Bearbeiten / Neuer Transponder* in der Menüleiste auswählen.
2. Wählen Sie aus der Dropdown-Liste bei Typ den Eintrag "G1 PinCode" und vervollständigen Sie die weiteren Angaben.
   ↳ Der Eintrag kann später wie ein Transponder detailliert nachbearbeitet werden.
3. *Speichern & Weiter* auswählen
4. *Beenden* auswählen

1.10.3 Pin Code Tastatur programmieren

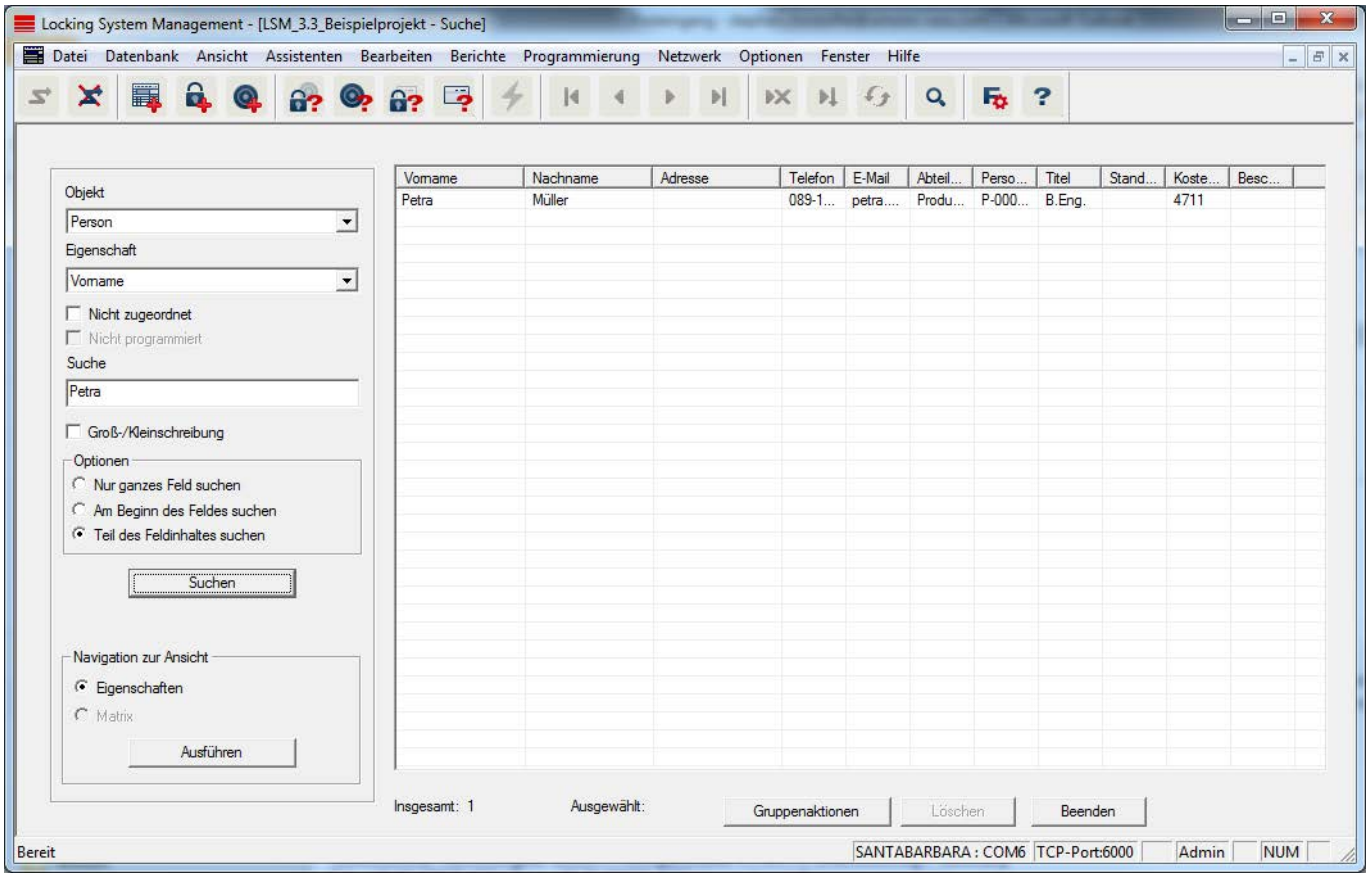
1. LSM: Rechtsklick auf Transponder/Pin Code im Schließplan und *Programmieren* auswählen.
   ↳ Das Fenster "Transponder programmieren" öffnet sich.
2. Pin Code Tastatur: Eingabe 0 0 + Master-Pin
3. LSM: *Programmieren* auswählen.
   ↳ Der Programmiervorgang startet.

4. Pin Code Tastatur: User-Pin z.B. 1 für User-Pin 1 / Interner Transponder 1 drücken, sobald die LSM den Hinweis "Drücken Sie jetzt den Taster des Transponders 1x kurz..." zeigt.
   ↳ Der Programmiervorgang ist jetzt abgeschlossen.

Wiederholen Sie den Vorgang, um weitere User-Pins im Schließplan zu programmieren.

1.11 Matrix durchsuchen

Die Suche ermöglicht es, komfortabel nach verschiedenen Objekten, zum Beispiel einer bestimmten Tür oder einem bestimmten Transponder, zu suchen.



✓ In der Schließanlage wurden bereits Elemente angelegt, nach denen gesucht werden kann.

1. Klicken Sie auf das Lupensymbol in der Symbolleiste.
2. Wählen Sie ein Objekt aus, nachdem Sie suchen möchten. Zur Auswahl stehen z.B. Personen, Transponder, Türen, Schließungen, etc.
3. Wählen Sie eine Eigenschaft des gesuchten Objekts aus, z.B. Nachname oder Vorname.
4. Geben Sie einen Suchbegriff in das Suchfeld ein.
5. Klicken Sie auf die Schaltfläche "Suchen", um den Suchvorgang zu starten.

1.12 Gruppenaktionen ausführen

Für verschiedene Komponenten können Einstellungen gleich an mehreren Komponenten in nur einem Schritt durchgeführt werden. In diesem Beispiel sollen die Eigenschaften *(z.B. Zugangskontrolle aktivieren)* von mehreren G2-Schließungen auf einmal geändert werden.

1. Klicken Sie auf das Lupensymbol in der Symbolleiste.
2. Suchen Sie z.B. nach allen Objekten vom Typ "Schließung".
   ↳ Bei der Suche nach allen Schließungen müssen im Feld "Suche" keine Angaben gemacht werden.
3. Wählen Sie beispielsweise durch Filtern nach Typ oder Bereich mehrere Schließungen aus.
4. Klicken Sie auf die Schaltfläche "Gruppenaktionen".
   ↳ Wenn im vorherigen Schritt nur G2-Schließungen ausgewählt wurden, werden gleich die richtigen Parameter *("Konfigurationsänderungen der G2 Schließungen" und "G2 Schließzylinder aktiv/hybrid")* ausgewählt.
5. Drücken Sie auf die Schaltfläche "Ausführen", um mit den Änderungen der ausgewählten Schließungen zu beginnen.
6. Führen Sie die Änderungen nach Belieben durch.
7. Speichern Sie die neuen Einstellungen über die Schaltfläche "Beenden".

HINWEIS

Dieses Vorgehen erlaubt ein schnelles und einfaches Ändern vieler Einstellungen. Beachten Sie, dass jede geänderte Komponente neu programmiert werden muss.

1.13 Transponder programmieren

✓ Ein Transponder wurde in der Schließanlage angelegt und ist in der Matrix sichtbar.

1. Rechtsklick auf den gewünschten Transponder.
2. Programmieren anklicken.
3. Folgen Sie den Anweisungen der LSM Software.

Achten Sie auf die Auswahl des entsprechenden Programmiergeräts.

Mit der Schaltfläche "TIDs zum Deaktivieren" rufen Sie eine Liste auf, auf der Sie bis zu zwei Transponder-IDs auswählen können, die gesperrt werden sollen (siehe *Defekten, verlorenen oder gestohlenen Transponder ersetzen [▸ 18]*).

HINWEIS

G2-Karten automatisch erkennen

Karten sind als Identifikationsmedium nicht immer voneinander zu unterscheiden. Wenn mehrere Karten vorliegen, dann muss die Karte, die jetzt programmiert werden soll, zuerst ausgelesen werden, um in der LSM die richtige Karte zur Programmierung auszuwählen. Dieser Schritt entfällt, wenn das Häkchen bei "G2 Karte automatisch erkennen" gesetzt ist. Wenn die vorliegende Karte der LSM bereits bekannt ist, dann wird der dazu passende Datensatz automatisch ausgewählt und programmiert.

1.14 Schließung programmieren

✓ Eine Schließung wurde in der Schließanlage angelegt und ist in der Matrix sichtbar.

1. Rechtsklick auf die gewünschte Schließung.
2. Programmieren anklicken.
3. Folgen Sie den Anweisungen der LSM Software.

Achten Sie auf die Auswahl des entsprechenden Programmiergeräts.

HINWEIS

In der Nähe des Programmiergeräts darf sich nur eine Schließung befinden!

1.15 Zeitzonenplan (mit Feiertagen und Betriebsferien) definieren

HINWEIS

Abweichende Zeiten bei G2-Schließungen

Die interne Zeiteinheit der G2-Schließungen hat eine technisch bedingte Toleranz von bis zu ± 15 Minuten pro Jahr.

Es wird empfohlen, Zeitzonenpläne auf ganze Transpondergruppen und Bereiche anzuwenden. Es ist allerdings auch möglich, Zeitzonenpläne direkt mit Schließungen und Transpondern zu verknüpfen.

✓ Es wurden bereits Schließungen (bzw. Bereiche) und Transponder (bzw. Transpondergruppen) erstellt.

1. Klicken Sie in der Menüleiste auf *Bearbeiten/Zeitzonenplan*.
   ↳ Ein "leerer Zeitzonenplan" öffnet sich. Falls ein bestehender Zeitzonenplan angezeigt wird, klicken Sie auf die Schaltfläche "Neu", um einen neuen, leeren Zeitzonenplan zu erstellen.

2. Füllen Sie die Felder "Name" und "Beschreibung" aus.
3. Wählen Sie bei Bedarf eine Feiertagsliste für Ihr Bundesland aus. So gehen Sie vor, wenn Sie beispielsweise einmalige Werksferien definieren möchten:
   - ↳ Klicken Sie auf das "...-Feld" neben der Feiertags-Dropdown-Auswahl.
   - ↳ Klicken Sie auf die Schaltfläche "Neuer Feiertag".
   - ↳ Vergeben Sie einen Namen; z.B. "Werksferien 2017"
   - ↳ Neu definierte Feiertage können einen Zeitraum aufweisen. Dazu muss das Feld "Urlaub" aktiviert werden. Anschließend kann ein Zeitraum (Von - Bis) eingegeben werden.
   - ↳ Wählen Sie, wie der neue Feiertag behandelt werden soll; z.B. als "Sonntag".
   - ↳ Klicken Sie auf die Schaltfläche "Übernehmen" und danach auf die Schaltfläche "Beenden".
   - ↳ Klicken Sie auf die Schaltfläche "Feiertagsverwaltung".
   - ↳ Fügen Sie Ihren neu definierten Feiertag *(in der linken Spalte)* über die Schaltfläche "Hinzufügen" der Feiertagsliste *(in der rechten Spalte)* hinzu.
   - ↳ Klicken Sie auf die Schaltfläche "OK" und danach auf die Schaltfläche "Beenden", um zum Hauptmenü des Zeitzonenplan zurückzukehren.
4. Wählen Sie eine Gruppe in der Tabelle und bearbeiten Sie für diese den Wochenplan.
   - ↳ Ein blauer Balken zeigt eine Berechtigung zu dieser Zeit.
   - ↳ Felder können einzeln angeklickt oder zusammen ausgewählt werden.
   - ↳ Jeder Klick auf ein Feld oder einen Bereich invertiert die Berechtigung.
   - ↳ 
5. Klicken Sie auf die Schaltfläche "Übernehmen".
6. Klicken Sie auf die Schaltfläche "Beenden".

Weisen Sie den Zeitzonenplan einem Bereich zu:

1. Rechtsklick auf den Bereich, dem der Zeitplan zugewiesen werden soll.
2. Wählen Sie "Eigenschaften".
3. Wählen Sie aus der Dropdown-Liste bei "Zeitzone" den entsprechenden Zeitzonenplan.
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

Es wäre auch möglich, den Zeitzonenplan direkt einer Schließung zuzuweisen.

Weisen Sie der Zeitgruppe eine Transpondergruppe zu:

1. Rechtsklick auf die Transpondergruppe, welcher die Zeitgruppe zugewiesen werden soll.
2. Wählen Sie "Eigenschaften".
3. Wählen Sie aus der Dropdown-Liste bei "Zeitzonengruppe" die entsprechende Zeitgruppe.
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

Es wäre auch möglich, die Zeitgruppe direkt einem Transponder zuzuweisen.

1.16 Zurücksetzen von Komponenten

Alle SimonsVoss-Komponenten können jederzeit zurückgesetzt werden. Es können sogar SimonsVoss-Komponenten, welche nicht zur Schließanlage gehören, zurückgesetzt werden. In diesem Fall benötigen Sie das entsprechende Schließanlagenpasswort.

Ein Zurücksetzen der Komponente bietet sich in vielen Szenarien an. Besonders bei einem möglichen Fehlverhalten ist es ratsam, die entsprechende Komponente zurückzusetzen und erneut zu programmieren.

1. Lesen Sie die entsprechende Komponente über *Programmierung/Komponente auslesen* aus.
2. Wählen Sie die Schaltfläche "Zurücksetzen", um den Rücksetz-Vorgang zu starten.
3. Folgen Sie den Anweisungen der LSM Software.
   ↳ Sie werden ggf. dazu aufgefordert, das Schließanlagenpasswort einzugeben oder den zu löschenden Datensatz auszuwählen.

1.17 Defekte Schließung ersetzen

Es kann vorkommen, dass Schließungen beschädigt werden oder einen Defekt erleiden.

Gehen Sie folgendermaßen vor, um eine defekte Schließung durch eine Neue auszutauschen:

1. Entfernen Sie die defekte Schließung aus der Tür.
   ↳ Es kann unter Umständen schwierig sein, einen Zylinder aus einer verschlossenen Tür zu entfernen. Fragen Sie ggf. den Fachhändler, der Ihnen die SimonsVoss-Produkte installiert hat, um Rat.

2. Besorgen Sie sich eine Ersatzschließung.
   ↳ Über einen Doppelklick auf die defekte Schließung in der LSM Software finden Sie in der Registerkarte "Ausstattung" alle Details zur Schließung.
3. Führen Sie in der LSM Software einen Software Reset der Schließung durch.
   ↳ Die Schaltfläche "Software Reset" erreichen Sie mit einem Doppelklick auf die defekte Schließung über die Registerkarte "Konfiguration/Daten".
   ↳ Nach dem Software Reset wird ein Programmierbedarf bei der defekten Schließung signalisiert.
4. Führen Sie einen Programmiervorgang an der Ersatzschließung durch.
5. Bauen Sie die Ersatzschließung wieder in die Tür ein und testen Sie die Funktionalität.

HINWEIS

Versuchen Sie im Fehlerfall zuerst, die Schließung selbst über einen Auslesevorgang zurückzusetzen! Nach dem Zurücksetzen kann die Schließung möglicherweise neu programmiert werden.

HINWEIS

Setzen Sie defekte Schließungen nach Möglichkeit unbedingt zurück, bevor Sie diese zu einem Händler oder der SimonsVoss Technologies GmbH zurücksenden!

1.18 Defekten, verlorenen oder gestohlenen Transponder ersetzen

Transponder können unter Umständen verloren gehen, beschädigt oder gestohlen werden. Alle Szenarien führen dazu, dass der alte Transponder im Schließplan zurückgesetzt und ein Ersatztransponder angelegt werden muss.

HINWEIS

Aus Sicherheitsgründen müssen in allen Schließungen die Berechtigungen des gelöschten Transponders entfernt werden. Dies erfolgt über eine Neuprogrammierung aller Schließungen.

Gehen Sie folgendermaßen vor, um einen "alten" Transponder durch einen neuen, unprogrammierten Transponder zu ersetzen.

1. Besorgen Sie sich einen Ersatztransponder.
   ↳ Über einen Doppelklick auf den defekten Transponder in der LSM Software finden Sie in der Registerkarte "Ausstattung" alle Details zum jeweiligen Transponder.
2. Rechtsklick auf den defekten, verlorenen oder gestohlenen Transponder und "Transponderverlust" auswählen.
   ↳ Der betroffene Transponder wird zum Sperren vorbereitet.
   ↳ Geben Sie den Grund an, weshalb diese Maßnahme notwendig ist. *Mit der Auswahl "Transponder verloren/gestohlen" kann direkt im Anschluss ein neuer Transponder mit denselben Berechtigungen programmiert werden. Im G2-Protokoll sperrt dieser Transponder bei jeder Betätigung an einer berechtigten Schließung den verlorenen Transponder. Eine Neuprogrammierung aller betroffenen Schließungen ist dennoch nötig.*
3. Führen Sie alle neu entstandenen Programmierbedarfe an allen Komponenten durch.

Nachprogrammieren der Schließungen umgehen

Das Erstellen eines neuen Ersatztransponders bringt Programmierbedarf an allen Schließungen mit sich. Diese speziellen Programmieraufgaben können allerdings auch direkt mit dem neuen Ersatztransponder durchgeführt werden:

✓ Der Ersatztransponder wurde ordnungsgemäß programmiert.

1. Betätigen Sie den neuen Ersatztransponder an jeder Schließung.
2. Programmieren Sie den neuen Ersatztransponder erneut. Aktivieren Sie im Fenster "Transponder programmieren" die Checkbox "Deaktivierungsquittungen / Batteriewarnungen auslesen".
3. Aktualisieren Sie die Matrix. Der Programmierbedarf ist nun verschwunden.

Ab LSM 3.4 SP2 ist es möglich, beliebigen Transpondern bis zu zwei andere Transponder-IDs "mitzugeben", die gesperrt werden sollen.

Zu sperrende TIDs direkt programmieren

Die zu sperrenden IDs werden während des Programmiervorgangs auf dem Transponder gespeichert.

✓ Der Transponder ist physikalisch verfügbar.
✓ Das Programmierfenster des Transponders ist geöffnet.

1. Klicken Sie auf die Schaltfläche "TIDs zum Deaktivieren".
   ↳ Liste öffnet sich.
2. Setzen Sie bis zu zwei Häkchen in der Spalte TID, um die zu löschenden TIDs auf dem Transponder zu speichern.

3. Bestätigen Sie die Eingaben über die Schaltfläche OK.
4. Fahren Sie mit der Programmierung fort.

↳ Die markierten TIDs werden auf dem Transponder als zu löschend hinterlegt. Wenn der Transponder sich an einer betroffenen Schließung authentifiziert, werden die zu löschenden TIDs an der Schließung gesperrt.

Zu sperrende TIDs in den Eigenschaften hinterlegen

Die zu sperrenden IDs werden entweder während des nächsten Programmiervorgangs oder bei der nächsten Buchung an einem Gateway auf dem Transponder gespeichert.

✓ Das Eigenschaften-Fenster des Transponders ist geöffnet.

1. Wechseln Sie zur Registerkarte "Konfiguration".
2. Klicken Sie auf die Schaltfläche "TIDs zum Deaktivieren".
   ↳ Liste öffnet sich.
3. Setzen Sie bis zu zwei Häkchen in der Spalte TID, um die zu löschenden TIDs auf dem Transponder zu speichern.
4. Bestätigen Sie die Eingaben über die Schaltfläche OK.

↳ Die markierten TIDs werden bei der nächsten Programmierung oder der nächsten Buchung an einem Gateway auf dem Transponder gespeichert.

1.19 Batteriezustand der Schließungen überprüfen und auswerten

Es gibt verschiedene Möglichkeiten, den Batteriestatus einer Schließung abzufragen. In regulären Offline-Schließanlagen (und VN) müssen die Batteriezustände zunächst in die LSM-Software übertragen werden, bevor Sie anschließend auf verschiedene Weisen ausgewertet werden können.

Batteriezustände in die LSM-Software übertragen

Schnell & effizient: Batteriezustände über Transponder "sammeln"

1. Nehmen Sie sich einen Transponder, der an jeder Schließung berechtigt ist. Betätigen Sie diesen Transponder zweimal an jeder Schließung.
2. Programmieren Sie den Transponder erneut. Aktivieren Sie im Fenster "Transponder programmieren" die Checkbox "Deaktivierungsquittungen / Batteriewarnungen auslesen".

Batteriezustände über das Auslesen der Schließung importieren

Lesen Sie die gewünschten Schließungen über "Programmieren / Schließung auslesen" separat aus.

Batteriezustände über LSM Mobile in die LSM-Software übertragen

Batteriezustände von Schließungen können über die LSM-Mobile direkt ausgelesen oder an die LSM-Software übertragen werden. Folgen Sie den Anweisungen im Handbuch "LSM-Mobile". Dieses finden Sie auf der SimonsVoss-Homepage (*www.simons-voss.com*) im Supportbereich unter Dokumente.

Batteriezustände anzeigen

Grundsätzliches Vorgehen bei allen LSM-Versionen:

✓ Die aktuellen Batteriewarnungen der jeweiligen Schließungen wurden in die LSM-Software übertragen.

1. Doppelklick auf eine Schließung, um die Schließungseigenschaften anzuzeigen.
2. Wählen Sie die Registerkarte "Zustand".
3. Der Batteriezustand wird im Feld "Zustand bei letzter Auslesung" angezeigt.

Batteriewarnungen gesammelt anzeigen bei LSM BASIC Online und LSM BUSINESS:

Generieren Sie sich eine Liste, welche alle Schließungen mit Batteriewarnungen anzeigt.

✓ Die aktuellen Batteriewarnungen der jeweiligen Schließungen wurden in die LSM-Software übertragen.

1. Wählen Sie in der Menüleiste "Berichte / Gebäudestruktur".
2. Wählen Sie die Eigenschaft "Schließungen mit Batteriewarnungen".
3. Klicken Sie auf die Schaltfläche "Anzeigen".

Batteriewarnungen automatisch anzeigen unter LSM BUSINESS

Erstellen Sie eine Warnung, welche Batteriewarnungen direkt anzeigt.

✓ Die aktuellen Batteriewarnungen der jeweiligen Schließungen wurden in die LSM-Software übertragen.

1. Wählen Sie in der Menüleiste "Berichte / Warnungen verwalten"
2. Erstellen Sie über die Schaltfläche "Neu" eine neue Warnung.
3. Erstellen Sie die Warnung nach Ihren Wünschen. Wählen Sie als Typ "Batteriewarnung Schließung".
4. Vergessen Sie nicht, dieser Warnung entsprechende Schließungen zuzuordnen! Das Feld "Schließungen" sollte nicht leer sein.
5. Bestätigen Sie die Neue Warnung über die Schaltfläche "OK".

6. Beenden Sie den Dialog über die Schaltfläche "Beenden".

1.20 Übergreifende Schließebene

Übergreifende Schließebenen lassen sich nur mit aktiven Komponenten betreiben. Übergreifende Schließebenen können bei der Verwendung von passiver Kartentechnologie bzw. SmartTags nicht realisiert werden!

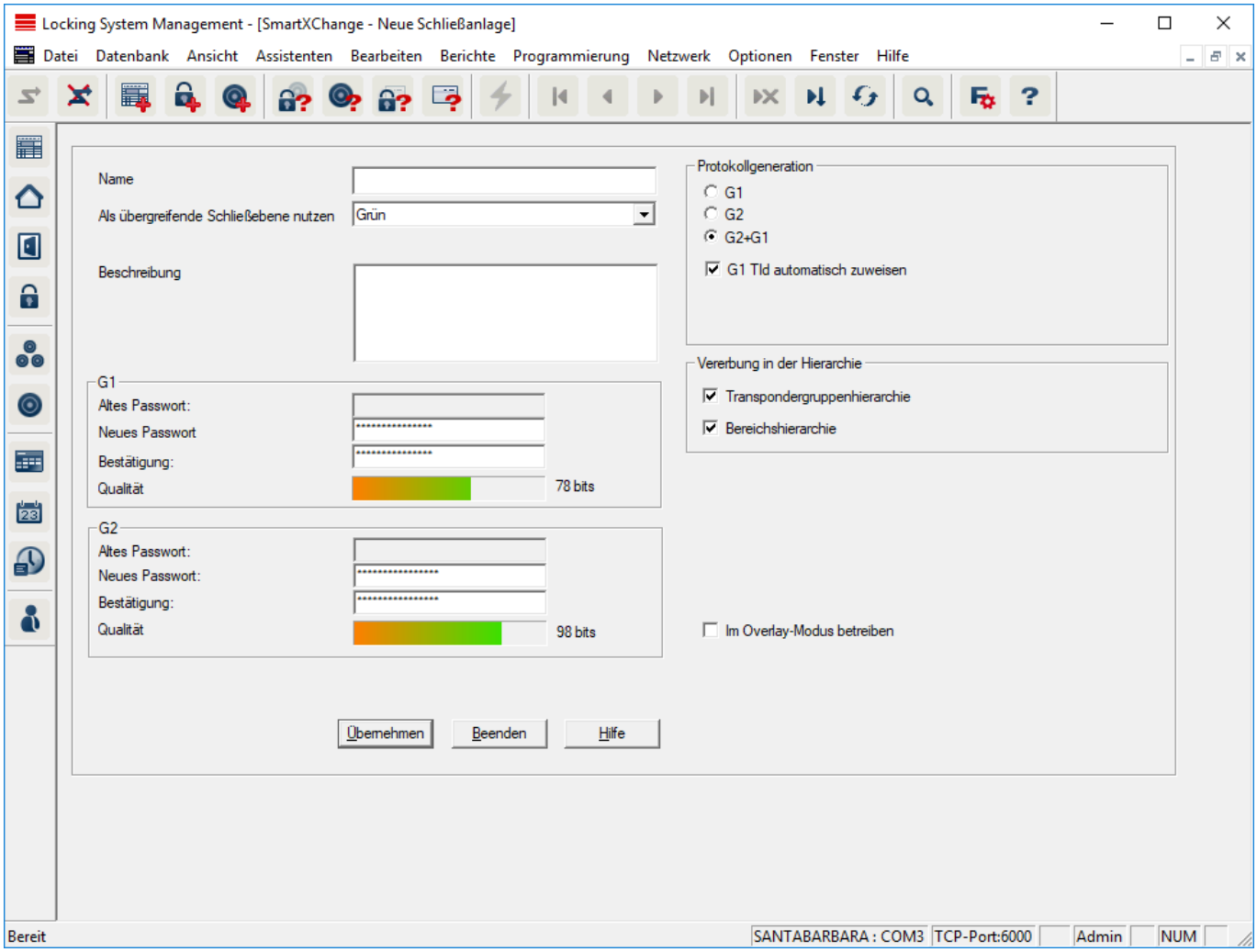
1.20.1 Übergreifende Schließebene anlegen

Beachten Sie bei übergreifende Schließebenen unbedingt:

- Übergreifende Schließebenen müssen die gleichen Protokollgenerationen aufweisen.
- Die rote Schließebene sollte nur für Feuerwehr oder andere Notfall-Einsatzkräfte eingesetzt werden, da diese speziell für diesen Einsatz optimiert wurde.

Eine übergreifende Schließebene wird prinzipiell wie jede andere Schließanlage angelegt, z.B. über die Schaltfläche "Neue Schließanlage" in der Symbolleiste:

- Wählen Sie unter "Als übergreifende Schließebene nutzen" eine beliebige Farbe.

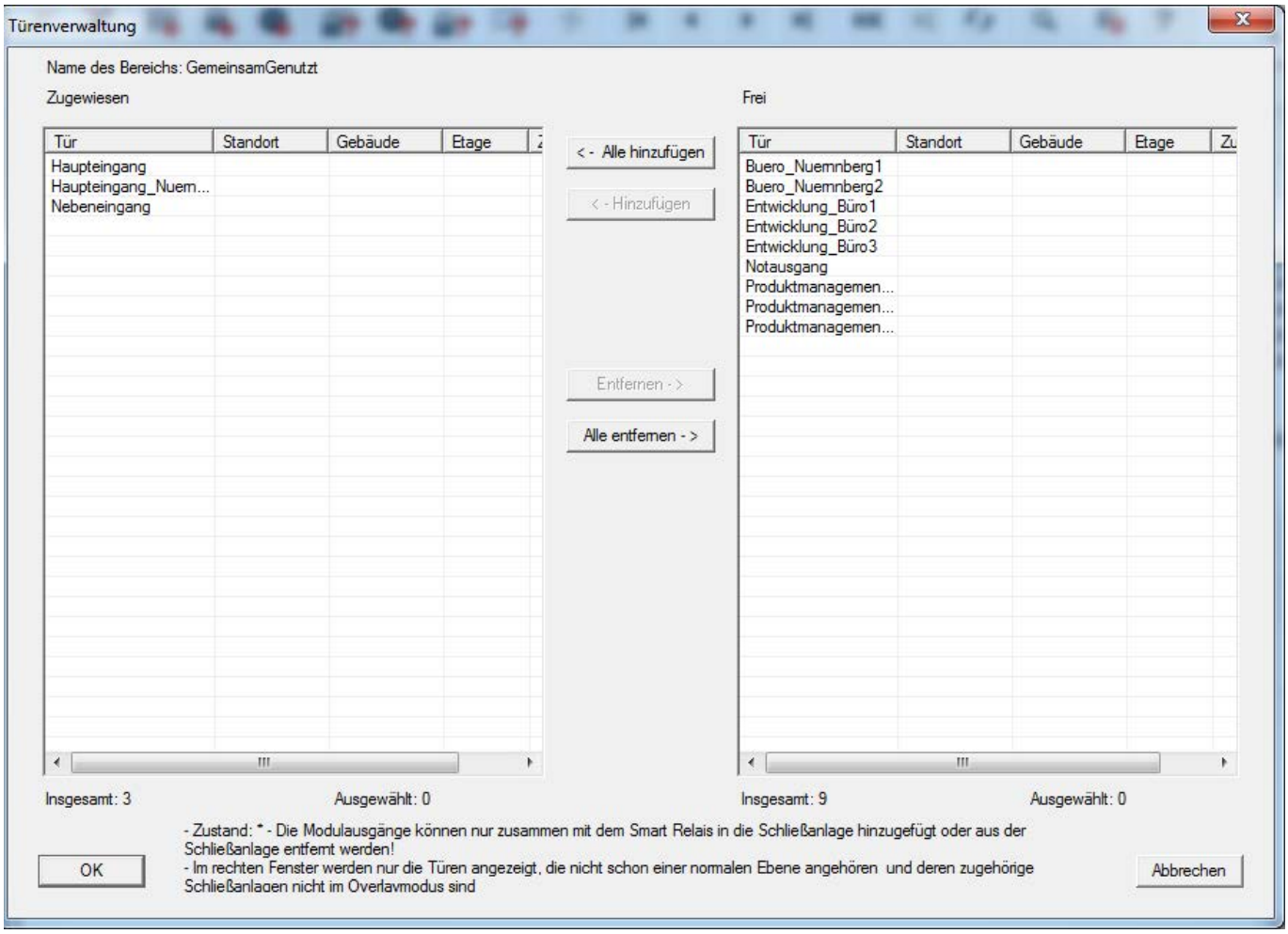


1.20.2 Schließungen verknüpfen

✓ Es wurde bereits eine übergreifende Schließebene angelegt.

1. In der übergreifenden Schließebene Rechtsklick auf einen Bereich und "Eigenschaften" auswählen.
2. Schaltfläche "Türverwaltung" auswählen.

3. In der rechten Tabelle werden sämtliche Schließungen aller Schließanlagen im Projekt angezeigt. Wählen Sie die gewünschten Schließungen über die Schaltfläche "Hinzufügen" aus.



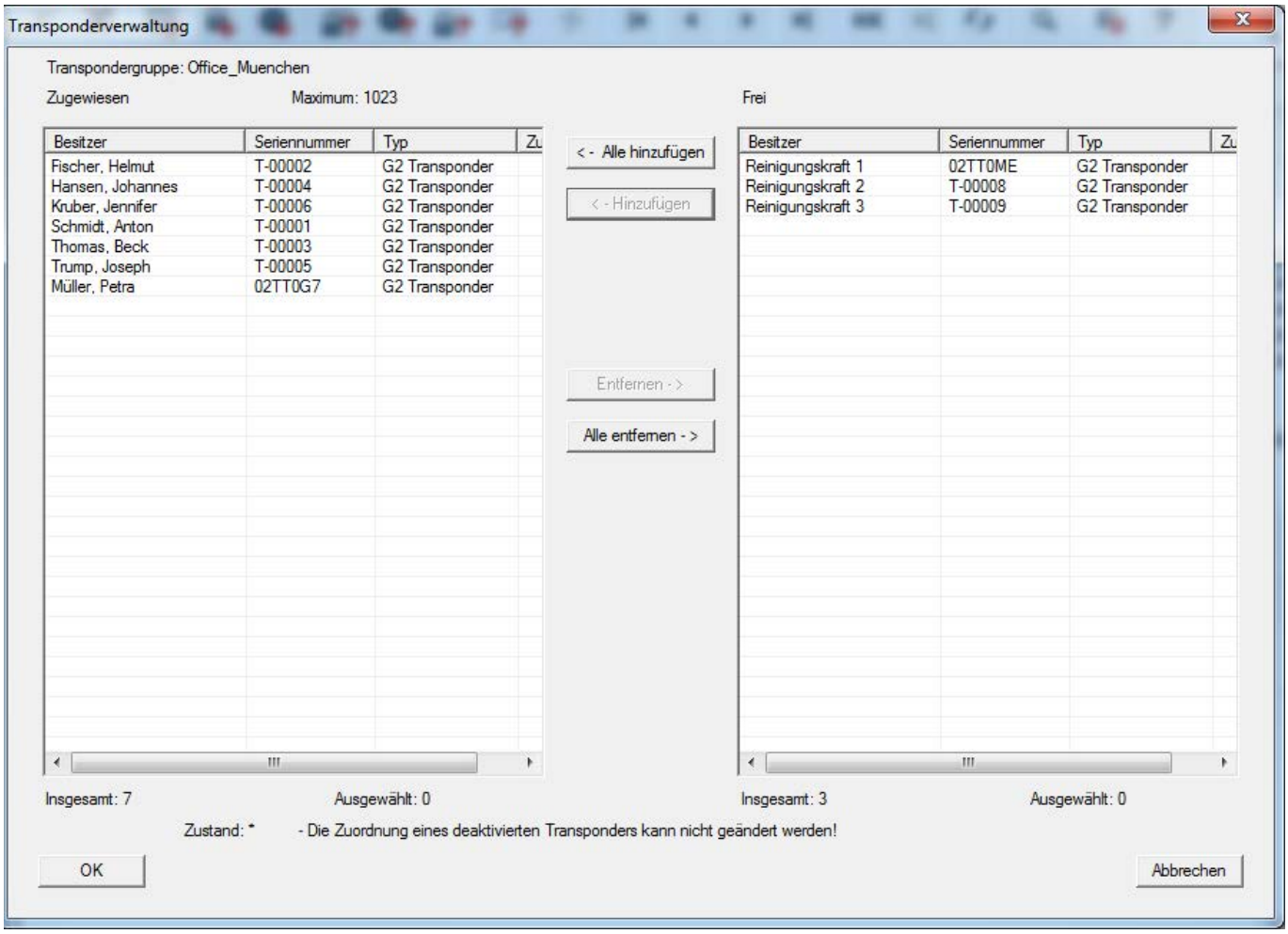
1.20.3 Transponder verknüpfen

Das Verknüpfen von Transpondern sollte nur an nicht übergreifenden Schließebenen erfolgen.

✓ Es wurden bereits Transponder bzw. Transpondergruppen angelegt.

1. Rechtsklick auf eine Transpondergruppe und "Eigenschaften" auswählen.
2. Schaltfläche "Automatisch" bei Transponderzuweisung auswählen.

3. In der rechten Tabelle werden sämtliche Transponder aller anderen Schließanlagen im Projekt angezeigt. Wählen Sie die gewünschten Transponder über die Schaltfläche "Hinzufügen" aus.



1.20.4 Transponder berechtigen

Wie in jeder übergreifenden Schließebene lassen sich auch in der "roten Ebene" ausgewählte Transpondergruppen mit nur wenigen Mausklicks an allen Schließungen berechtigen. Diese Funktion eignet sich insbesondere für Feuerwehrtransponder.

✓ Sie haben bereits eine übergreifende Schließebene in der Farbe "rot" angelegt.

1. Rote übergeordnete Schließanlage öffnen.
2. Transpondergruppe erstellen, die an allen für die Feuerwehr relevanten Bereichen berechtigt sein soll.
3. In den Transpondergruppeneigenschaften auf die Schaltfläche "Berechtigungen" bei Verwaltung klicken.
4. Über die Checkboxen alle gewünschten Bereiche/Schließungen anwählen, um der Transpondergruppe Zugriff an allen Türen zu gewähren.

1.21 Feuerwehrtransponder erstellen

✓ Sie haben bereits mindestens eine Schließanlage erstellt.

1. Erstellen Sie eine neue, übergreifende Schließebene der Farbe "rot", z.B. über *Bearbeiten/Neue Schließanlage*.
2. Fügen Sie einen neuen Bereich, z.B. "Alle Schließungen", ein und weisen Sie diesem alle gewünschten Schließungen über die "Türverwaltung" zu.
3. Legen Sie in der übergreifenden Schließebene eine neue Transpondergruppe "Feuerwehr" an.
4. Klicken Sie in den Eigenschaften der Transpondergruppe "Feuerwehr" auf die Schaltfläche "Berechtigungen".
5. Aktivieren Sie die Checkbox "Alle Anlagen", um diese Transpondergruppe generell an jeder Schließung zu berechtigen.
6. Speichern Sie die Einstellungen über die Schaltfläche "OK".
7. Legen Sie in der Transpondergruppe einen neuen Transponder (z.B. "Feuerwehrtransponder 1") an und programmieren Sie diesen. *Außerdem sind alle Schließungen neu zu Programmieren. Achten Sie auf den neu entstandenen Programmierbedarf.*

Der in diesem Schritt erstellte Feuerwehrtransponder "Feuerwehrtransponder 1" ist an allen Schließungen berechtigt. Selbst deaktivierte Schließungen können (in der roten Ebene) geöffnet werden, was den wesentlichen Unterschied zur "grünen" und "blauen" Schließebene ausmacht.

1.22 DoorMonitoring Komponenten einrichten

Die DoorMonitoring Funktion ist ein Zusatzfeature, um Türzustände in der LSM Software anzuzeigen. SmartHandles und Schließzylinder mit DoorMonitoring-Funktion werden in der LSM Software zunächst genau so eingerichtet wie die regulären Schließkomponenten.

- Neuen DoorMonitoring-Schließzylinder hinzufügen: Wählen Sie als Schließungstyp "G2 DoorMonitoring Zylinder" aus der Dropdownliste.
- Neues DoorMonitoring-SmartHandle hinzufügen: Wählen Sie als Schließungstyp "G2 DoorMonitoring SmartHandle" aus der Dropdownliste.

Registerkarte: Konfiguration/Daten

Nehmen Sie über die Schaltfläche "Monitoring Konfiguration" weitere Einstellungen vor.

Registerkarte: DoorMonitoring Status

In dieser Registerkarte wird der aktuelle Status der Tür angezeigt. Der aktuelle Türstatus wird in Echtzeit angezeigt.

Damit diese Anzeige stets aktuell ist, wird eine direkte Verbindung zwischen LSM Software und Schließkomponente (z.B. WaveNet) vorausgesetzt. Nähere Information zur Einrichtung eines WaveNet-Funknetzwerks finden Sie im WaveNet-Handbuch.

1.23 Programmieren über LSM Mobile

Über LSM Mobile können Programmieraufgaben direkt an der Schließung mit mobilen Geräten durchgeführt werden. Diese Programmierung läuft wie folgt ab:

1. Eine Liste mit Komponenten, die Programmierbedarf aufweisen, wird in der LSM Software zum mobilen LSM Mobile-Gerät exportiert. *Entweder direkt auf den Pocket PC oder als Datei für ein Notebook, Netbook oder Tablet-PC.*
2. Die LSM Mobile wird auf dem mobilen Gerät gestartet. Über den Export der LSM Software kann mit der Programmierung der Komponenten begonnen werden.
3. Der LSM Software muss im Anschluss mitgeteilt werden, welche Komponenten über die LSM Mobile programmiert wurden. Hierfür wird ein Import bzw. eine Synchronisation von der LSM Mobile zur LSM Software durchgeführt.

1.23.1 Mit Pocket PC/PDA

HINWEIS

Das Programmmieren über LSM Mobile mit einen Pocket PC bzw. PDA funktioniert nur im G1 Protokoll.

So führen Sie einen Programmiervorgang mit Hilfe der LSM Mobile durch:

- ✓ Es liegen Komponenten mit Programmierbedarf in der LSM Software vor.
- ✓ An den Komponenten mit Programmierbedarf wurde bereits eine Erstprogrammierung durchgeführt.
- ✓ Auf dem mobilen Gerät wurde die LSM Mobile korrekt installiert. Die Versionsnummern sind identisch.
- ✓ Das SMARTCD.G2 Programmiergerät ist aufgeladen und über Bluetooth mit dem PDA verbunden.
- ✓ Die Treiber vom Pocket PC wurden am Computer korrekt installiert und es besteht eine Verbindung.

1. Wählen Sie *Programmierung/LSM Mobile/Export auf LSM Mobile/LSM Mobile PDA*.
2. Folgen Sie den Anweisungen der LSM Software und übertragen Sie die Programmieraufgaben auf den PDA.
3. Starten Sie die LSM Mobile auf dem PDA und melden Sie sich an der gewünschten Schließanlage an.
4. Führen Sie mit Hilfe des Programmiergeräts die Programmiervorgänge an den gewünschten Komponenten durch.
5. Wählen Sie *Programmierung/LSM Mobile/Import von LSM Mobile/LSM Mobile PDA*.
6. Folgen Sie den Anweisungen der LSM Software und synchronisieren Sie die Programmieraufgaben.

Die Programmieraufgaben wurden über den PDA durchgeführt. Über die Synchronisierung im letzten Schritt sind die Programmierblitze, welchen Programmierbedarf anzeigen, in der LSM Software verschwunden.

1.23.2 Mit Laptop, Netbook oder Tablet

So führen Sie einen Programmiervorgang mit Hilfe der LSM Mobile durch:

- ✓ Es liegen Komponenten mit Programmierbedarf in der LSM Software vor.
- ✓ An den Komponenten mit Programmierbedarf wurde bereits eine Erstprogrammierung durchgeführt.
- ✓ Auf dem mobilen Gerät wurde die LSM Mobile korrekt installiert. Die Versionsnummern sind identisch.
- ✓ Die Treiber der SMARTCD.G2 und SMARTCD.MP Programmiergeräte (je nach Bedarf) sind korrekt installiert.

1. Wählen Sie *Programmierung/LSM Mobile/Export auf LSM Mobile/LSM Mobile PC*.
2. Folgen Sie den Anweisungen der LSM Software und exportieren Sie die Programmieraufgaben in eine Datei.

3. Starten Sie die LSM Mobile auf dem mobilen PC und importieren Sie die Datei mit den Programmieraufgaben in die LSM Mobile.
4. Folgen Sie den Anweisungen der LSM Mobile.
5. Führen Sie mithilfe des Programmiergeräts die Programmiervorgänge an den gewünschten Komponenten durch.
6. Exportieren Sie den Status der Programmieraufgaben.
7. Wählen Sie *Programmierung/LSM Mobile/Import von LSM Mobile/LSM Mobile PC*.
8. Folgen Sie den Anweisungen der LSM Software und importieren Sie die Datei aus LSM Mobile.

Die Programmieraufgaben wurden über das externe Gerät durchgeführt. Über den Import im letzten Schritt sind die Programmierblitze, die Programmierbedarf anzeigen, in der LSM Software verschwunden.

1.24 Lagermodus bei G1-Schließungen zurücksetzen

Werden die Batteriewarnungen bei G1-Schließungen nicht beachtet, wechseln die betroffenen Schließungen in den Lagermodus. Auf diesem Weg wird eine vollständige Entladung der Batterien verhindert. Der Lagermodus kann beendet werden, indem die Schließung neu programmiert wird. Anschließend muss die Schließung sofort mit einem berechtigten Transponder geöffnet und die Batterien gewechselt werden.

1.25 Zutrittslistenadministration

Das Auslesen von Zutritts- und Begehungslisten kann zum Schutz der Privatsphäre stark eingeschränkt werden. In der LSM BASIC ist hierfür bereits standardmäßig ein eigener Benutzer "AdminAL" (Admin Access List) angelegt. In der LSM BUSINESS kann ein entsprechender Benutzer manuell angelegt werden, siehe *Benutzer verwalten (BUSINESS) [▸ 30]*.

In diesem Kapitel wird folgendes Szenario beschrieben: Nur eine befugte Person (z.B. Betriebsrat angemeldet als AdminAL) soll Zutritts- und Begehungslisten auslesen dürfen. Dem allgemeinen Schließanlagenadministrator wird dieses Recht nicht gegeben.

AdminAL einrichten und Auslesen von Zutrittslisten gestatten

1. Melden Sie sich an Ihrem Projekt mit dem Benutzernamen „Admin“ und ihrem Kennwort an.
2. Öffnen Sie die Benutzergruppenverwaltung über „Bearbeiten/Benutzergruppe“.
3. Navigieren Sie über die Navigationspfeile zur Benutzergruppe „Zutrittslisten Administration“ (bzw. in LSM BUSINESS zu einer beliebeigen, zuvor angelegten Benutzergruppe).

4. Stellen Sie sicher, dass im Bereich „Rolle“ die Rechte „Zutrittslisten Administration“ und „Zutrittslisten verwalten“ aktiviert sind.
5. Klicken Sie auf das Feld „Bearbeiten“ unterhalb des Bereichs „Rolle“.
6. Aktivieren Sie in Transpondergruppen und Bereichen jeweils die gewünschten Schließanlagen. Sofern Sie Bereiche bzw. Transpondergruppen angelegt haben, müssen Sie zusätzlich alle gewünschten Bereiche bzw. Transpondergruppen separat aktivieren!
7. Beenden Sie die Maske über die Schaltfläche "OK".
8. Bestätigen Sie Ihre vorgenommenen Einstellungen über die Schaltflächen "Übernehmen" und "Beenden".
9. Melden Sie sich von Ihrem aktuellen Projekt über "Datenbank/Abmelden" ab.

Admin die Rechte zum Auslesen von Zutrittslisten entziehen

HINWEIS

Das Recht „Zutrittslisten Administration“ muss immer bei einem Benutzer/Benutzergruppe liegen und darf nicht beiden entzogen werden!

1. Melden Sie sich an dem Projekt mit dem Benutzernamen „AdminAL“ an.
   ↳ Das Standard-Passwort in LSM BASIC lautet "system3060".
   ↳ Ändern Sie dieses Passwort umgehend!
2. Öffnen Sie die Benutzergruppenverwaltung über „Bearbeiten/Benutzergruppe“.
3. Navigieren Sie über die Navigationspfeile zur Benutzergruppe „Admin“.
4. Deaktivieren Sie die Rollen „Zutrittslisten Administration“ und „Zutrittslisten verwalten“.
5. Bestätigen Sie Ihre vorgenommenen Einstellungen über die Schaltflächen "Übernehmen" und "Beenden".
   ↳ Die Einrichtung ist abgeschlossen. Zutrittslisten und Begehungslisten können zukünftig nur noch durch das Benutzerkonto „AdminAL“ ausgelesen oder eingesehen werden.

1.26 Benutzer verwalten (BUSINESS)

Benutzer einer Benutzergruppe zuweisen

1. Klicken Sie auf "Bearbeiten/Benutzergruppe".
2. Navigieren Sie über die Navigationspfeile zu einer Benutzergruppe (oder erstellen Sie über die Schaltfläche "Neu" eine neue Benutzergruppe.
3. Klicken Sie auf die Schaltfläche "Bearbeiten".

4. Markieren Sie den gewünschten Benutzer und weisen Sie diesen über die Schaltfläche "Hinzufügen" der Benutzergruppe zu.
5. Bestätigen Sie Ihre vorgenommenen Einstellungen über die Schaltfläche "OK".
6. *Korrigieren Sie ggf. die Rollen.*
   - ↳ *Klicken Sie auf das Feld „Bearbeiten“ unterhalb des Bereichs „Rolle“.*
   - ↳ *Aktivieren Sie in Transpondergruppen und Bereichen jeweils die gewünschten Schließanlagen. Sofern Sie Bereiche bzw. Transpondergruppen angelegt haben, müssen Sie zusätzlich alle gewünschten Bereiche bzw. Transpondergruppen separat aktivieren!*
   - ↳ *Beenden Sie die Maske über die Schaltfläche "OK".*
7. Bestätigen Sie Ihre vorgenommenen Einstellungen über die Schaltflächen "Übernehmen" und "Beenden".

Neuen Benutzer anlegen

1. Klicken Sie auf "Bearbeiten/Benutzer".
2. Klicken Sie auf die Schaltfläche "Neu", um einen neuen Benutzer anzulegen.
3. Vergeben Sie einen neuen Benutzernamen und setzen Sie ein Kennwort.
4. Bestätigen Sie ihre vorgenommenen Einstellungen über die Schaltflächen "Übernehmen" und "Beenden".

1.27 Kartenmanagement

Nachfolgend sehen Sie die verschiedenen Kartentypen und die Aufteilung des Speichers in Verbindung mit dem SimonsVoss-Schließsystem.

ACHTUNG

MIFARE DESFire empfohlen

MIFARE DESFire verwendet eine gegenüber MIFARE Classic weiterentwickelte mikrocontrollergestützte Verschlüsselung nach AES-128, die auch erhöhten Sicherheitsanforderungen genügt.

- SimonsVoss empfehlt die Verwendung von Transpondern oder MIFARE-DESFire-Produkten.

HINWEIS

Ungleiche Templates für AX-Produkte

Wenn Sie MIFARE-Produkte für SimonsVoss-AX-Produkte verwenden wollen, dann müssen die verwendeten Templates zum Schreiben und zum Lesen identisch sein.

1.27.1 Konfiguration ändern

Sie haben zwei Möglichkeiten, um Karten einzusetzen.

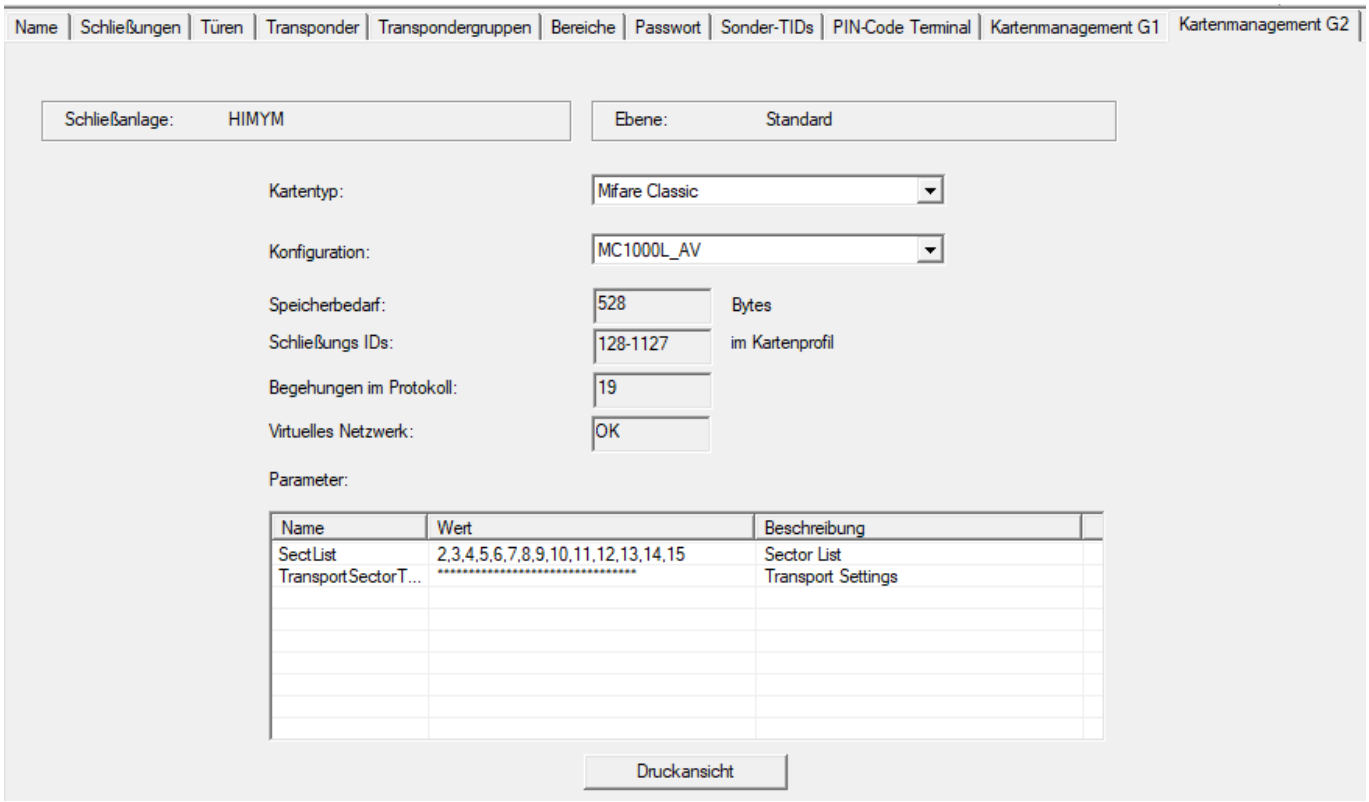
- Sie können bereits eingesetzte Karten verwenden.
- Sie können neue Karten verwenden.

In beiden Fällen geben Sie den Kartentyp, die Konfiguration und ggfs. die zu beschreibenden Sektoren an (siehe *Übersicht [▸ 33]*).

Karte einrichten

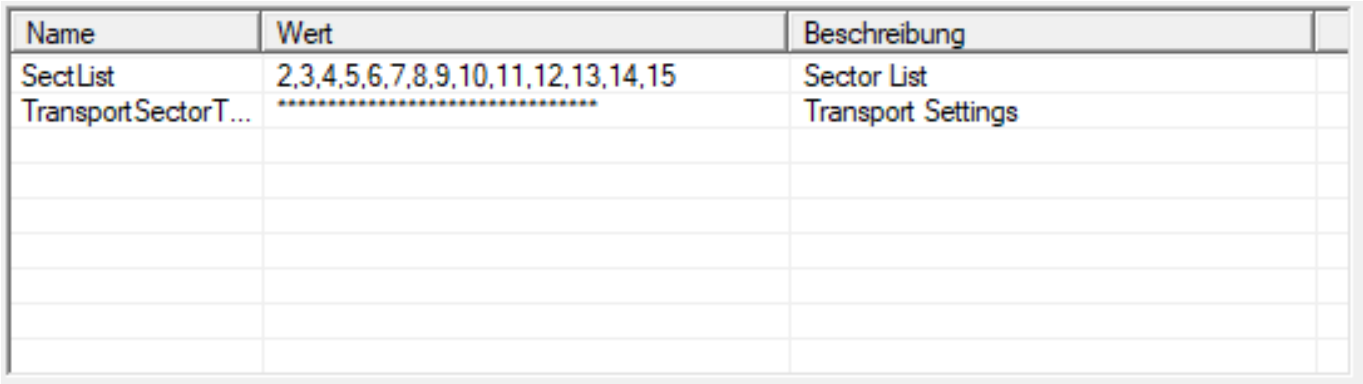
✓ LSM geöffnet.

1. Wechseln Sie zur Schließanlage, deren Kartenmanagement Sie verändern wollen.
2. Öffnen Sie mit einem Klick auf die Schaltfläche … die Eigenschaften der Schließanlage.
3. Wechseln Sie zur Registerkarte [Kartenmanagement G2].



4. Wählen Sie im Dropdown-Menü ▼ **Kartentyp:** Ihren Kartentyp aus.
5. Wählen Sie im Dropdown-Menü ▼ **Konfiguration:** Ihre Konfiguration aus.

6. Geben Sie ggfs. weitere Parameter wie Sektoren an (Bsp: 2,3,4,5,6,7,8,9,10,11,12,13,14,15).



7. Klicken Sie auf die Schaltfläche Übernehmen.

↳ Sie haben die Konfiguration geändert.

1.27.2 Übersicht

	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 Predefined A	MIFARE Classic Predefined B	MIFARE Classic + DESFire	MIFARE Plus S/X
MCBasic	✓	✓	✓	✕	✓
MC1200L	✓	✓	✓	✕	✓
MC3800L	✓	✓	✓	✕	✓
MC1000L_AV	✕	✓	✓	✕	✓
MC2400L_AV	✕	✓	✓	✕	✓
MC8000L_AV	✕	✓	✓	✕	✓

	MIFARE Classic	MIFARE Classic Pre-defined A	MIFARE Classic Pre-defined B	MIFARE Classic + DESFire	MIFARE Plus S/X
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	✓
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	✗

	G1/G2	Lock-IDs	Anzahl der Schließungen	Begehungsliste	Sektoren	Benötigter Speicherplatz	Virtuelles Netzwerk
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	✓

2 Realisierung gängiger WaveNet basierter Aufgaben in LSM Business

In diesem Beispiel werden die wichtigsten Schritte für den Aufbau und die Administration eines WaveNet-Funknetzwerks über die LSM Business gezeigt. Die Beispiele beziehen sich auf bestimmte Installationen und sollen Ihnen dabei helfen, sich mit der WaveNet-Thematik vertraut zu machen.

2.1 Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung

Dieses Ausgangsbeispiel beschreibt, wie Sie ein WaveNet-Funknetzwerk von Grund auf neu erstellen. Das Ziel ist es, eine Schließung über einen aktuellen RouterNode2 anzusprechen.

2.1.1 LSM Software vorbereiten

Beachten Sie, dass für die Vernetzung von SimonsVoss-Schließkomponenten die LSM-Software ordnungsgemäß installiert und ein entsprechendes Network-Modul lizenziert sein muss!

1. Installieren Sie den CommNode-Server und versichern Sie sich, dass der Dienst gestartet ist.
2. Installieren Sie die aktuelle Version des WaveNet-Managers. (Siehe Installation)
3. Öffnen Sie die LSM-Software und wählen Sie "Netzwerk/WaveNet Manager".
   ↳ Geben Sie das Installationsverzeichnis des WaveNet-Managers an und wählen Sie ein Verzeichnis für die Ausgabedatei.
   ↳ Starten Sie den WaveNet-Manager über die Schaltfläche "Starten".
4. Vergeben Sie ein Passwort, um die Sicherheit Ihres Netzwerks zu erhöhen.

↳ Der WaveNet-Manager startet und die Einstellungen sind für die Zukunft gespeichert. Beenden Sie den WaveNet-Manager, um weitere Einstellungen zu vorzunehmen.

2.1.2 Erstprogrammierung der Schließkomponenten

Bevor Schließungen in das Netzwerk eingebunden werden können, müssen diese zuerst programmiert werden.

2.1.2.1 Neue Schließung anlegen

✓ Es ist bereits eine Schließanlage angelegt.

1. Wählen Sie *Bearbeiten/Neue Schließung*.
2. Füllen Sie alle Attribute aus und setzen Sie ggf. weitere Einstellungen über die Schaltfläche "Konfiguration".

3. Klicken Sie auf die Schaltfläche "Speichern & Weiter".
4. Klicken Sie auf die Schaltfläche "Beenden".

2.1.2.2 Schließung programmieren

✓ Eine Schließung wurde in der Schließanlage angelegt und ist in der Matrix sichtbar.

1. Rechtsklick auf die gewünschte Schließung.
2. Programmieren anklicken.
3. Folgen Sie den Anweisungen der LSM Software.

Achten Sie auf die Auswahl des entsprechenden Programmiergeräts.

HINWEIS

In der Nähe des Programmiergeräts darf sich nur eine Schließung befinden!

2.1.3 Hardware vorbereiten

Der aktuelle RouterNode2 kann schnell und einfach in Betrieb genommen werden. Schließen Sie den RouterNode2 anhand der beiliegenden Kurzanleitung an. Der RouterNode2 ist werkseitig so eingestellt, dass dieser seine IP-Adresse von einem DHCP-Server bezieht. Mit Hilfe des OAM-Tools *(kostenlos im Supportbereich unter Infomaterial/Software-Downloads verfügbar)* können Sie diese IP-Adresse schnell ermitteln.

HINWEIS

Standardeinstellungen:

IP-Adresse: 192.168.100.100

Benutzername: SimonsVoss | Passwort: SimonsVoss

Wenn die Schließung noch nicht werkseitig mit einem LockNode (LN.I) ausgestattet ist, müssen Sie diese über entsprechendes Zubehör nachrüsten.

HINWEIS

Notieren Sie sich die IP-Adresse des RouterNode2 und die Chip-ID der Schließung, nachdem Sie die Hardware korrekt vorbereitet haben.

2.1.4 Kommunikationsknoten erstellen

Der Kommunikationsknoten bildet die Schnittstelle zwischen dem CommNode-Server und der LSM-Software. Um die Konfigurations-XMLs anzulegen, muss die LSM-Software als Administrator ausgeführt werden.

1. Öffnen Sie die LSM-Software.
2. Wählen Sie "Netzwerk/Kommunikationsknoten".
3. Ergänzen Sie die Informationen "Name", "Rechnername" und "Beschreibung".
   ↳ *Z.B. WaveNet-Netzwerk_123; Computer_BS21; Kommunikationsknoten für das WaveNet-Funknetzwerk 123*
4. Klicken Sie auf die Schaltfläche "Konfig-Dateien"
5. Vergewissern Sie sich, dass der Pfad auf das Installationsverzeichnis des CommNode-Servers verweist und klicken Sie auf die Schaltfläche "OK".
6. Quittieren Sie die Meldung mit "Nein" und bestätigen Sie die Auswahl mit "OK". *Die drei Konfigurations-XMLs (appcfg, msgcfg und netcfg) müssen direkt im Installationsverzeichnis des CommNode-Servers liegen.*
7. Speichern Sie Ihre Einstellungen über die Schaltfläche "Übernehmen".
8. Quittieren Sie den Hinweis über die Schaltfläche "OK".
9. Beenden Sie den Dialog über die Schaltfläche "Beenden".

2.1.5 Netzwerk einrichten und in LSM importieren

2.1.5.1 WaveNet-Konfiguration anlegen

Sofern alle Voraussetzungen erfüllt sind, können Sie mit dem Konfigurieren des Netzwerks beginnen:

- ✓ Die LSM ist ordnungsgemäß installiert und ein Network-Modul ist lizenziert.
- ✓ Der CommNode-Server wurde installiert und der Dienst ist gestartet.
- ✓ Die Konfigurationsdatein des CommNode-Servers wurden erstellt.
- ✓ Der WaveNet-Manager ist in seiner aktuellen Version installiert.
- ✓ In der LSM-Software wurde ein Kommunikationsknoten erstellt.
- ✓ Die Erstprogrammierung der zu vernetzenden Schließung war erfolgreich.
- ✓ Der RounterNode2 ist über das Netzwerk erreichbar und Sie kennen dessen IP-Adresse.
- ✓ Die programmierte Schließung verfügt über einen montierten LockNode, dessen Chip-ID Sie kennen.

1. Starten Sie den Wavenet-Manager über "Netzwerk/WaveNet Manager" und die Schaltfläche "Starten".

2. Geben Sie das Passwort ein.
3. Rechtsklick auf "WaveNet_xx_x".
4. Initialisieren Sie zuerst den RouterNode2, z.B. über die Option "Hinzufügen: IP oder USB Router".
   ↳ Folgen Sie dem Dialog und binden Sie den RouterNode2 über dessen IP-Adresse in Ihr WaveNet-Funknetzwerk ein.
5. Initialisieren Sie den LockNode der Schließung, indem Sie einen Rechtsklick auf den neu hinzugefügten RouterNode2 durchführen und die Option "Suchen nach ChipID" auswählen.
   ↳ Folgen Sie dem Dialog und weisen Sie die Schließung bzw. den dazugehörigen LockNode über dessen ChipID dem RouterNode2 zu.
6. Klicken Sie nacheinander auf die Schaltflächen "Speichern", "Beenden" und "Ja", um den WaveNet-Manager zu schließen.
7. Importieren Sie die neuen Einstellungen und weisen Sie diese dem entsprechenden Kommunikationsknoten zu.

2.1.5.2 WaveNet-Konfiguration übertragen

Die neuen Einstellungen müssen noch zum CommNode-Server übertragen werden:

1. Wählen Sie "Netzwerk/Kommunikationsknoten".
2. Wählen Sie den RouterNode2 auf der Liste der Anschlüsse aus und klicken Sie auf die Schaltfläche "Übertragen".
3. Speichern Sie Ihre Einstellungen über die Schaltfläche "Übernehmen".
4. Beenden Sie den Dialog über die Schaltfläche "Beenden".

2.1.5.3 LockNode einer Schließung zuweisen

Der initialisierte LockNode muss mit einer Schließung verknüpft werden. Das geschieht (besonders bei mehreren LockNodes) am einfachsten über einen Sammelauftrag:

1. Wählen Sie "Netzwerk/Sammelaufträge/WaveNet-Knoten".
2. Wählen Sie alle LockNodes *(WNNode_xxxx)* aus, welche noch nicht zugewiesen sind. *Noch nicht zugewiesene LockNodes weisen in der Spalte "Tür" keinen Eintrag auf.*
3. Klicken Sie auf die Schaltfläche "Automatisch konfigurieren".
   ↳ Die Autokonfiguration startet sofort.
4. Beenden Sie den Dialog über die Schaltfläche "Beenden".

2.1.5.4 WaveNet-Konfiguration testen

Um die Vernetzung schnell auszuprobieren, können Sie die Schließung jederzeit über das Netzwerk "Rechtsklick/Programmieren" nachprogrammieren. Sofern die Programmierung erfolgreich ist, arbeitet das Netzwerk ordnungsgemäß.

2.2 Inbetriebnahme des DoorMonitoring Schließzylinders

In diesem Beispiel wird gezeigt, welche Einstellungen beim Einrichten eines DoorMonitoring-Schließzylinders vorzunehmen sind. Die Voraussetzungen dafür sind im Kapitel "*Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung [▸ 36]*" zu entnehmen.

2.2.1 DoorMonitoring-Schließzylinder anlegen

Zunächst muss der DM-Schließzylinder korrekt in der LSM angelegt und programmiert werden:

1. Wählen Sie den Button "Schließung anlegen" um den Dialog für eine neue Schließung aufzurufen.
2. Wählen Sie als Schließungstyp "G2 Door Monitoring Zylinder" und ergänzen Sie alle weiteren Angaben nach Belieben.
3. Beenden Sie den Dialog, um die Schließung in der Matrix anzulegen.
4. Öffnen Sie durch einen Doppelklick die Eigenschaften der Schließung und wechseln Sie zur Registerkarte "Konfiguration/Daten".
5. Setzen Sie nach Belieben die Einstellungen im Soll-Bereich der Schließung.
6. Klicken Sie auf die Schaltfläche "Monitoring Konfiguration" und treffen Sie (mindestens) die folgenden Einstellungen:
   - ↳ Abtastintervall Stulpschraube: z.B. 5 Sekunden. In diesem Fall wird der Türzustand alle 5 Sekunden abgefragt.
   - ↳ Tourigkeit des Schlosses: z.B. 1-tourig. Diese Einstellung ist wichtig, um den Riegelzustand korrekt zu erfassen.
7. Speichern Sie die Einstellungen und kehren Sie zur Matrix zurück.
8. Führen Sie eine Erstprogrammierung über ein passendes Programmiergerät durch.

2.2.2 DoorMonitoring-Schließzylinder im Netzwerk einbinden

So binden Sie den DM-Schließzylinder in das WaveNet-Netzwerk ein:

- ✓ Der WaveNet-Manager ist bereits eingerichtet.
- ✓ Der Router, welchem die neue Schließung zugewiesen werden soll, ist bereits eingerichtet und "online".
- ✓ Ein LockNode ist korrekt auf dem DM-Schließzylinder montiert und Sie kennen die Chip-ID.

1. Starten Sie den WaveNet-Manager.
2. Initialisieren Sie den LockNode der Schließung, indem Sie einen Rechtsklick auf den Router durchführen und die Option "Suchen nach ChipID" auswählen.
   ↳ Folgen Sie dem Dialog und weisen Sie die Schließung bzw. den dazugehörigen LockNode über dessen ChipID dem RouterNode2 zu.
3. Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten DM-LockNode.
4. Aktivieren Sie die CheckBox "I/O-Konfiguration" und klicken Sie auf die Schaltfläche "OK".
5. Aktivieren Sie die CheckBox "Alle Ereignisse zum I/O Router senden" und klicken Sie auf die Schaltfläche "OK".
6. Klicken Sie nacheinander auf die Schaltflächen "Speichern", "Beenden" und "Ja", um den WaveNet-Manager zu schließen.
7. Importieren Sie die neuen Einstellungen und weisen Sie diese dem entsprechenden Kommunikationsknoten zu.

2.2.3 WaveNet-Konfiguration übertragen

Die neuen Einstellungen müssen noch zum CommNode-Server übertragen werden:

1. Wählen Sie "Netzwerk/Kommunikationsknoten".
2. Wählen Sie den RouterNode2 auf der Liste der Anschlüsse aus und klicken Sie auf die Schaltfläche "Übertragen".
3. Speichern Sie Ihre Einstellungen über die Schaltfläche "Übernehmen".
4. Beenden Sie den Dialog über die Schaltfläche "Beenden".

2.2.4 LockNode einer Schließung zuweisen

Der initialisierte LockNode muss mit einer Schließung verknüpft werden. Das geschieht (besonders bei mehreren LockNodes) am einfachsten über einen Sammelauftrag:

1. Wählen Sie "Netzwerk/Sammelaufträge/WaveNet-Knoten".
2. Wählen Sie alle LockNodes *(WNNode_xxxx)* aus, welche noch nicht zugewiesen sind. *Noch nicht zugewiesene LockNodes weisen in der Spalte "Tür" keinen Eintrag auf.*
3. Klicken Sie auf die Schaltfläche "Automatisch konfigurieren".
   ↳ Die Autokonfiguration startet sofort.

4. Beenden Sie den Dialog über die Schaltfläche "Beenden".

2.2.5 Inputereignisse der Schließung aktivieren

Damit die Türzustände ordnungsgemäß in der LSM-Software angezeigt werden, müssen Sie weitere Einstellungen vornehmen:

1. Wählen Sie "Netzwerk/Sammelaufträge/WaveNet-Knoten"
2. Wählen Sie den DoorMonitoring-Zylinder *(oder jeden beliebeigen Schließzylinder, welcher Ereignisse weiterleiten soll)* aus.
3. Klicken Sie auf die Schaltfläche "Inputereignisse aktivieren".
   ↳ Die Programmierung wird umgehend gestartet.
4. Klicken Sie auf die Schaltfläche "Beenden", sobald alle Schließungen programmiert wurden.

2.3 RingCast einrichten

Im Folgenden wird die Konfiguration eines RingCasts beschrieben. Über den RingCast kann ein Input-Ereignis eines RouterNode2 parallel an weitere RouterNode2 im selben WaveNet-Funknetzwerk weitergegeben werden. In diesem Beispiel soll eine Notfreischaltung der Schließungen realisiert werden. Sobald eine Brandmeldeanlage den Input 1 eines RouterNode2 betätigt, sollen alle verbunden Schließungen geöffnet werden. Jede Schließung bleibt danach solange geöffnet, bis sie den expliziten Befehl einer Fernöffnung erhält.

Selbstverständlich können über einen RingCast auch andere Aufgaben wie Blockschlossfunktion, Fernöffnung und Amokfunktion durchgeführt werden.

Dieses Beispiel setzt ein konfiguriertes WaveNet-Funknetzwerk mit zwei RouterNode2 voraus. Mit jedem RouterNode2 ist eine Schließung verbunden. Sobald der Input 1 an einem RouterNode2 kurzzeitig geschaltet wird, sollen alle Schließungen sofort geöffnet werden. Damit können sich Personen Zugang zu allen Räumen verschaffen, um dort Schutz vor Feuer oder Rauch zu suchen.

HINWEIS

Wenn RouterNode2 über Ethernet vernetzt sind, dann wird RingCast erst bei Modellen unterstützt, die ca. ab 2017 ausgeliefert wurden. Ein RouterNode2, dessen Ethernet-Verbindungsversuch zu einem anderen RouterNode2 fehlgeschlagen ist, versucht die neue Verbindung über Funk aufzubauen. Die Reichweite der Funkkommunikation beträgt bis zu 30 m (abhängig vom Umfeld, kann nicht gewährleistet werden).

2.3.1 RouterNode für RingCast vorbereiten

HINWEIS

Firmwareabhängige Verfügbarkeit von RingCast für RouterNodes

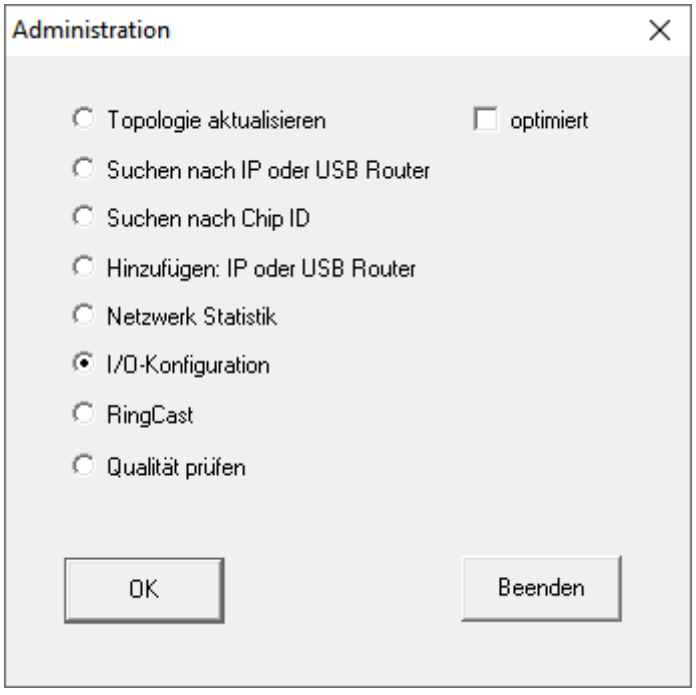
Die Unterstützung von RingCast ist firmwareabhängig (siehe Firmware-Informationen).

- Aktualisieren Sie ggfs. die Firmware (siehe Firmware aktualisieren).

Bereiten Sie die RouterNodes für den RingCast vor:

- ✓ Im Wavenet-Funknetzwerk sind mindestens zwei verschiedene ringcastfähige RouterNodes konfiguriert und "online" (siehe Firmware-Informationen).
- ✓ Jedem RouterNode des geplanten RingCasts ist mindestens eine Schließung zugewiesen. Beide Schließungen sind "online".

1. Öffnen Sie den WaveNet-Manager.
2. Klicken Sie mit der rechten Maustaste auf den ersten RouterNode 2.
   ↳ Fenster "Administration" öffnet sich.



3. Wählen Sie die Option ◉ I/O-Konfiguration.
4. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Administration" schließt sich.
   ↳ Fenster "I/O Konfiguration" öffnet sich.
5. Optional: Wählen Sie beispielsweise für ▼ **Ausgang** 1 "Input Quittung statisch", um während der Deaktivierung ein Signalgerät ansteuern zu können.

6. Wählen Sie im Dropdown-Menü ▼ **Eingang** des gewünschten Eingangs den Eintrag der entsprechenden Reaktion aus (siehe RouterNode: Digitaler Eingang).
7. Wählen Sie im Dropdown-Menü ▼ **Verzögerung [s]** den Eintrag "RingCast" aus.
8. Klicken Sie auf die Schaltfläche LN auswählen.
9. Prüfen Sie, ob alle gewünschten LockNodes ausgewählt sind. *(Beim erstmaligen Einrichten der I/O-Konfiguration des Routers werden alle LockNodes mit einbezogen.)*
10. Wählen Sie im Dropdown-Menü ▼ **Protokollgeneration** Ihre Protokollgeneration.

HINWEIS

Protokollgeneration in der LSM

Die Protokollgeneration wird Ihnen in der LSM in den Schließanlageneigenschaften in der Registerkarte [Name] im Bereich "Protokollgeneration" angezeigt.

11. Geben Sie das Schließanlagenpasswort ein.
12. Klicken Sie auf die Schaltfläche OK.
13. Nehmen Sie die selben Einstellungen auch an den weiteren RouterNodes 2 vor.

2.3.2 RingCast anlegen

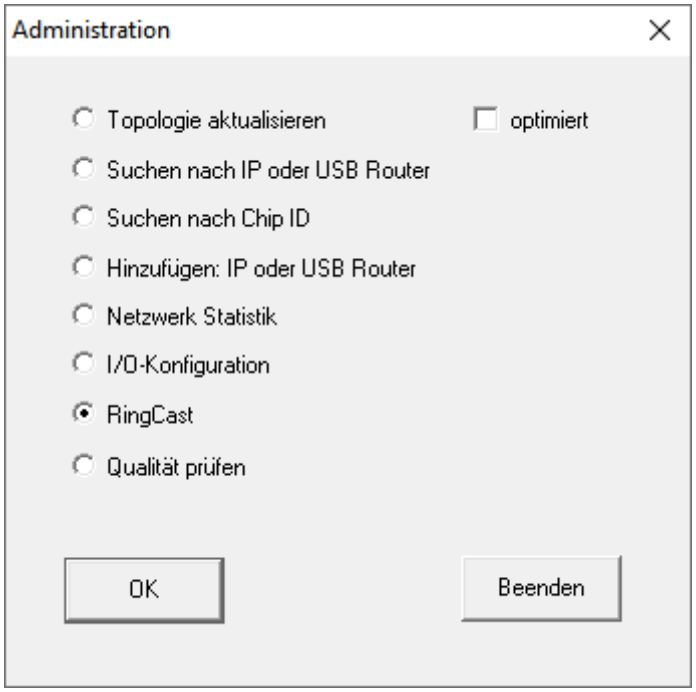
HINWEIS

Neuberechnung des RingCasts

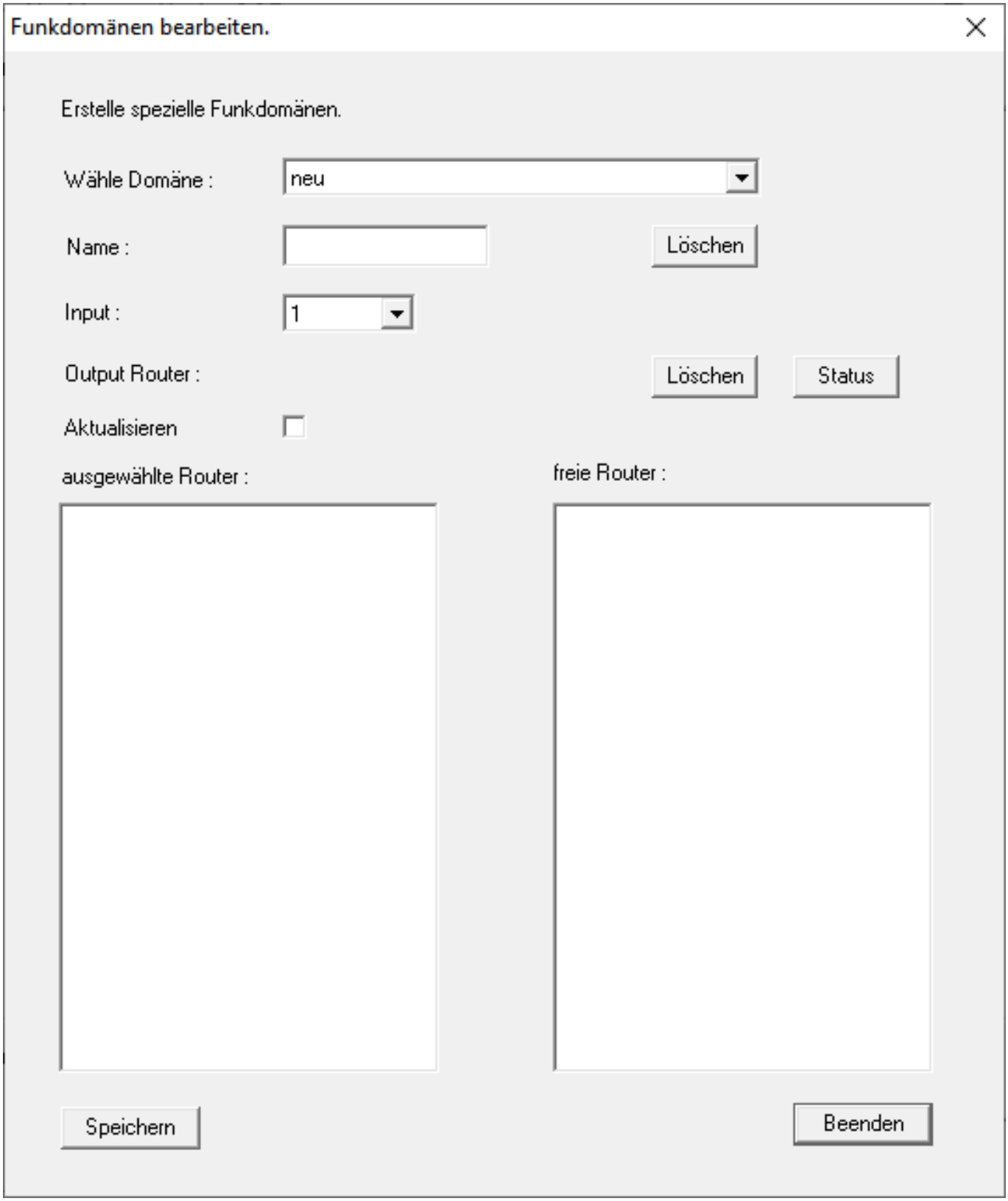
Wenn Sie einen RouterNode im RingCast ersetzen, löschen oder dessen RingCast-relevante IO-Konfiguration ändern, dann wird der RingCast nach dem Speichern der Änderungen und dem Bestätigen der Nachfrage automatisch neu berechnet.

✓ WaveNet-Manager geöffnet (siehe Start).
✓ RouterNodes und LockNodes an Stromversorgung angeschlossen.
✓ RouterNodes und LockNodes in WaveNet-Topologie importiert (siehe Geräte finden und hinzufügen).
✓ RouterNodes für RingCast vorbereitet (siehe *RouterNode für RingCast vorbereiten [▸ 43]*).

1. Klicken Sie mit der rechten Maustaste auf den Eintrag des WaveNets, in dem Sie einen RingCast erstellen wollen.
   ↳ Fenster "Administration" öffnet sich.

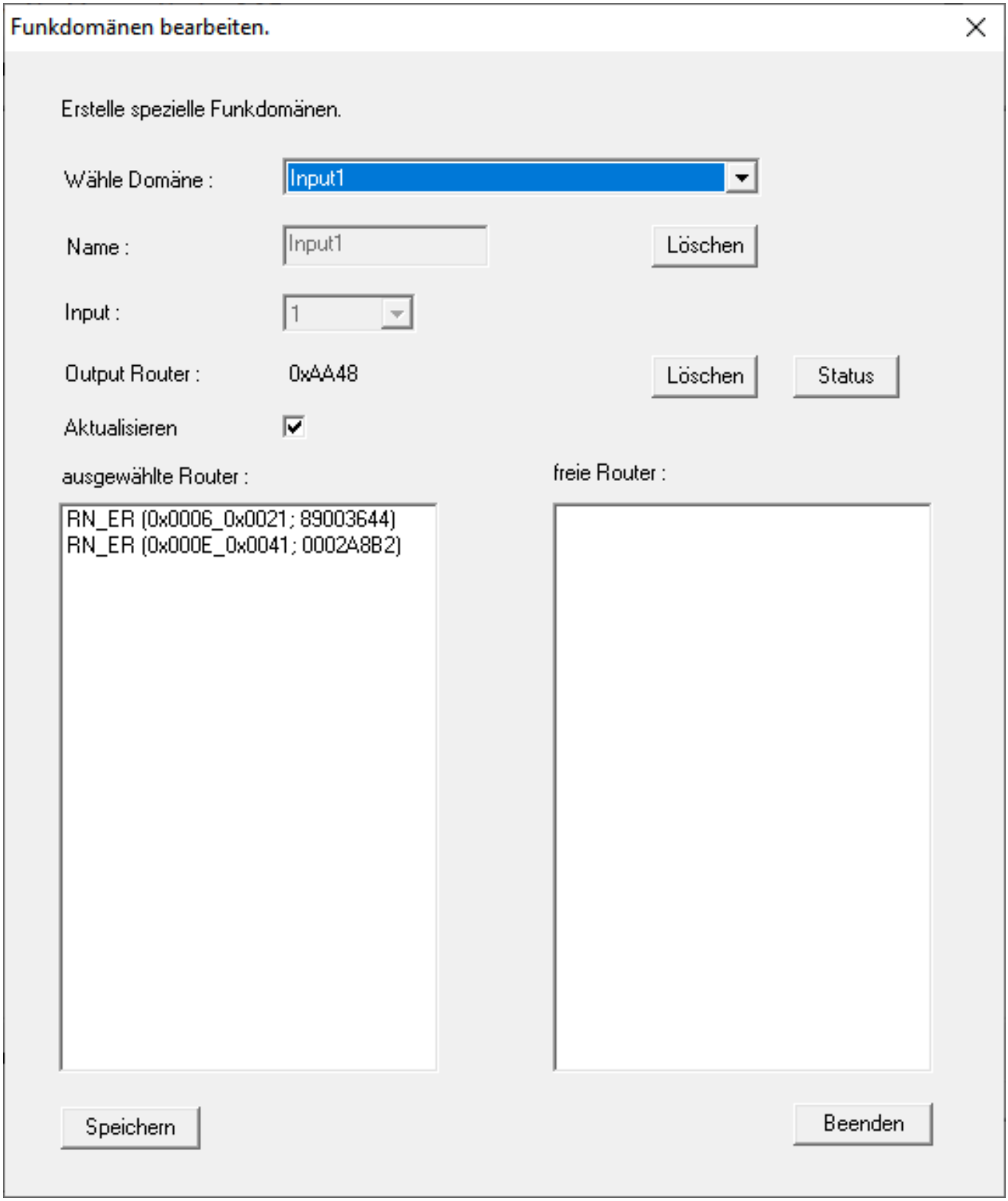


2. Wählen Sie die Option ◉ RingCast.
3. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Administration" schließt sich.
   ↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

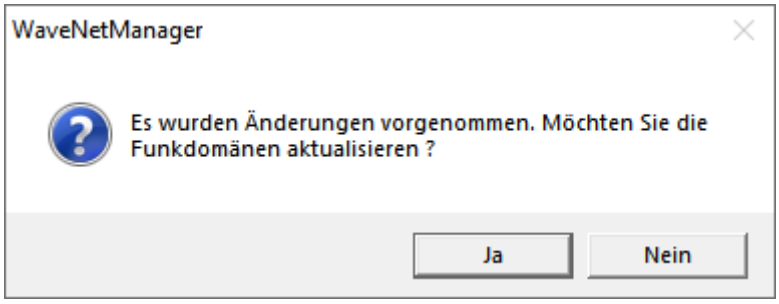

Funkdomänen bearbeiten.
Erstelle spezielle Funkdomänen.
Wähle Domäne :
neu
Name :
Löschen
Input :
1
Output Router :
Löschen
Status
Aktualisieren
ausgewählte Router :
freie Router :
Speichern
Beenden

4. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** einen Eingang aus, für den Sie bei ▼ **Verzögerung [s]** den "RingCast" gewählt haben.

↳ Im Feld "ausgewählte Router" erscheinen alle RouterNode2, bei denen Sie an diesem Eingang bei ▼ **Verzögerung [s]** den Eintrag "RingCast" gewählt haben (=Domäne).

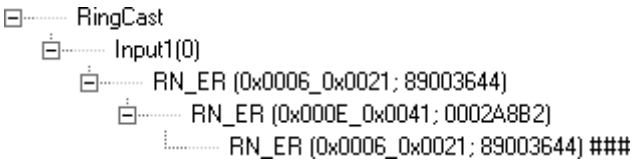


5. Klicken Sie auf die Schaltfläche Speichern.
6. Klicken Sie auf die Schaltfläche Beenden.
   ↳ Fenster "Funkdomänen bearbeiten" schließt sich.
   ↳ Fenster "WaveNetManager" öffnet sich.



7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Fenster "WaveNetManager" schließt sich.
   ↳ Änderungen werden aktualisiert.

↳ Der RingCast wird angelegt und ist nach kurzer Zeit im WaveNet-Manager sichtbar.



Die getätigten Einstellungen wurden bereits in die RouterNode2 geschrieben. Speichern Sie die neuen Einstellungen und beenden Sie den WaveNet-Manager.

2.3.3 RingCast-Funktionstest

Die vorgenommenen Einstellungen sind sofort wirksam. Der RingCast hat keine Selbstprüffunktion.

WARNUNG

Beeinträchtigung oder Ausfall von Schutzfunktionen durch geänderte Bedingungen

Die Aktivierung der Schutzfunktionen im RingCast basiert auf kabellosen Verbindungen und Ethernetverbindungen. Insbesondere kabellose Verbindungen können durch sich ändernde Umgebungsbedingungen beeinflusst werden (siehe Funknetzwerk). Damit wird auch die Aktivierung der Schutzfunktionen im RingCast beeinflusst und die Sicherheit von Personen und Sachwerten, die beispielsweise durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, kann gefährdet sein.

1. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest [▸ 49]*).
2. Beachten Sie ggfs. auch weitere Richtlinien bzw. Verordnungen, die für Ihre Schließanlage relevant sind.

WARNUNG

Veränderung des Ablaufs von Notfallfunktionen durch Fehlfunktionen

SimonsVoss und "Made in Germany" stehen für höchste Sicherheit und Zuverlässigkeit. In Einzelfällen können Fehlfunktionen Ihrer Geräte dennoch nicht ausgeschlossen werden. Damit wird möglicherweise die Sicherheit von Personen und Sachwerten, die durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, gefährdet.

1. Testen Sie Ihre Geräte mindestens einmal pro Monat (siehe Geräte-Funktionstest).
2. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest [▸ 49]*).

Schalten Sie am Initiator den entsprechenden Eingang und überprüfen Sie:

- ob die Schließungen wie gewünscht reagieren (siehe auch RouterNode: Digitaler Eingang).
- ob der ggfs. eingestellte Ausgang am RouterNode die Quittung wie gewünscht durch Schalten anzeigt (siehe auch RouterNode: Digitaler Ausgang).

HINWEIS

Dauerhafte Notöffnung

Ein Brand kann das Inputkabel oder andere Teile beschädigen. Damit würden die Schließungen wieder schließen, obwohl es brennt. Personen könnten im Brandbereich eingesperrt werden und Rettungskräfte am Zutritt gehindert werden.

Deshalb bleiben alle Schließungen im Zustand Notöffnung (und damit passierbar), bis ein expliziter Fernöffnungsbefehl die Schließungen wieder schließt.

Test mit zentralem Output-Router

HINWEIS

Zentraler Output-Router im RingCast mit R/CR-RouterNodes

Der zentrale Output-Router erhält die Inputquittung der beteiligten RouterNodes ausschließlich über eine Ethernetverbindung. Der zentrale Output-Router ignoriert deshalb den Status von RouterNodes, die keine Ethernet-RouterNodes (.ER) sind. Wenn Sie den zentralen Output-Router verwenden und Ihr RingCast auch RouterNodes ohne Ethernetschnittstelle enthält,

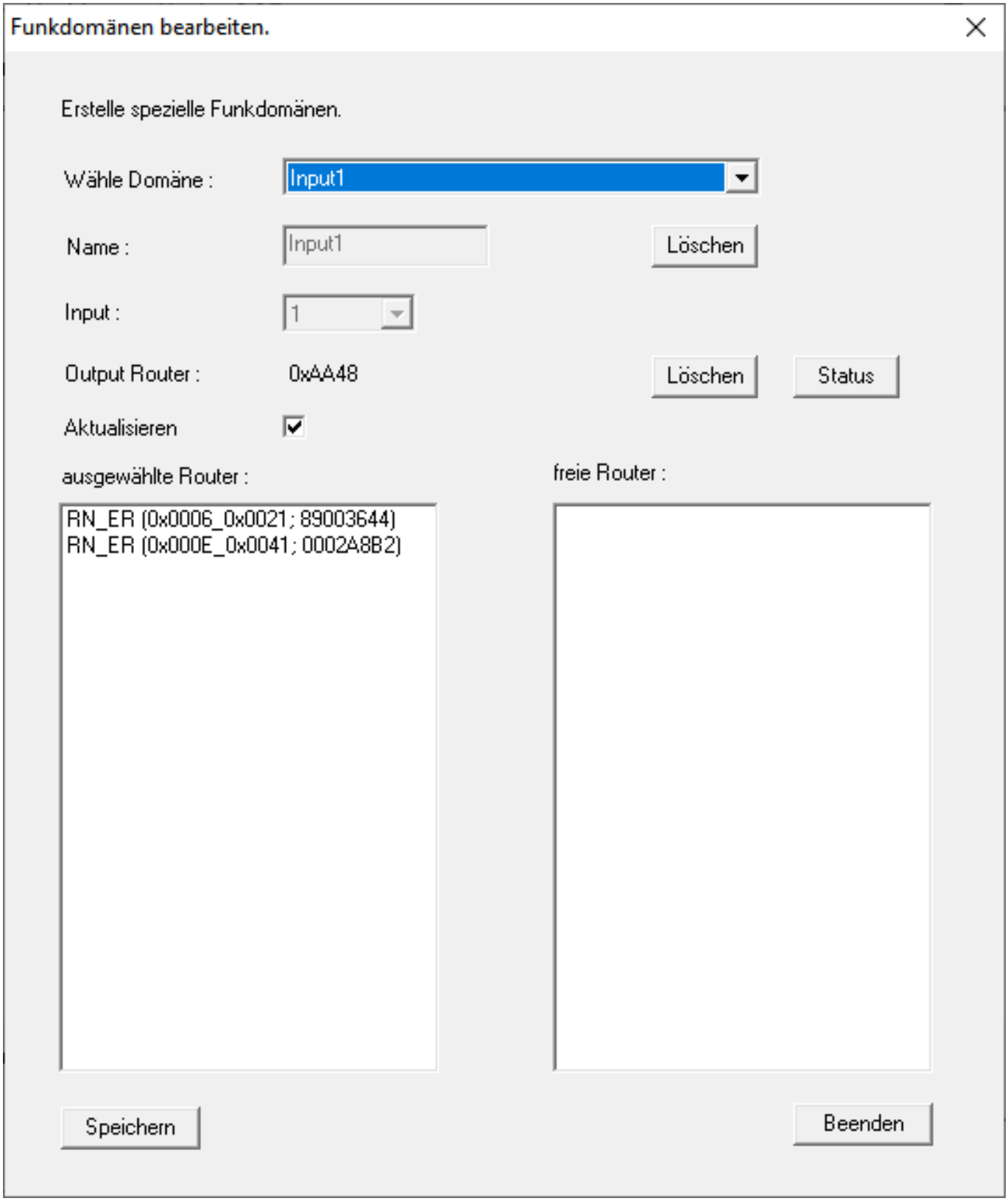
dann bedeutet die Inputquittung des zentralen Output-Routers nur, dass alle Schließungen, die einem Ethernet-RouterNode zugewiesen sind, den Befehl empfangen haben.

- Prüfen Sie den Status von anderen RouterNodes R/CR) unabhängig vom zentralen Output-Router manuell (siehe Erreichbarkeit testen (LSM) und RouterNodes bzw. IO-Status und LockNode-Reaktionsfähigkeit).

Die Verwendung eines zentralen Output-Routers (siehe Zentraler Output-Router) vereinfacht den Test des RingCasts erheblich. Schalten Sie am Initiator den entsprechenden Eingang und prüfen Sie, ob der zentrale Output-Router eine Inputquittung absetzt bzw. den entsprechenden Ausgang schaltet. Wenn der Ausgang schaltet, dann haben alle Schließungen den Befehl empfangen. Wenn der Ausgang nicht schaltet, dann prüfen Sie, welche RouterNodes Probleme verursacht haben:

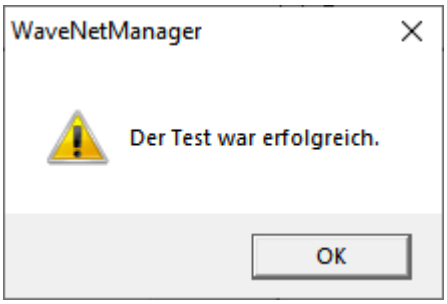
✓ WaveNet-Manager geöffnet (siehe Start).

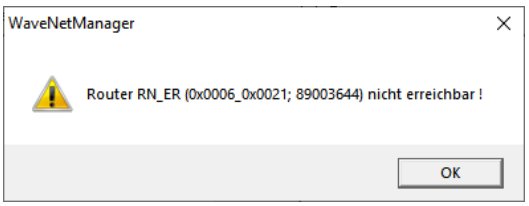
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RingCasts, den Sie testen wollen.
2. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** den Input aus, dessen RingCast Sie testen wollen.
   ↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

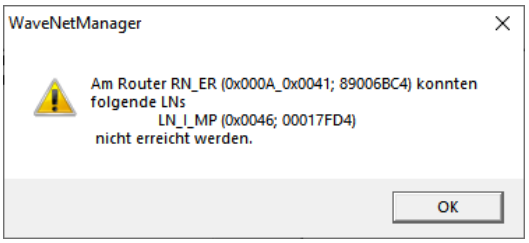


3. Klicken Sie auf die Schaltfläche Status.

↳ RingCast wird getestet.







Der RingCast konnte alle Schließungen ansprechen.	Der RingCast konnte nicht abgeschlossen werden. Mögliche Ursachen (siehe auch Zentraler Output-Router): ■ Ein oder mehrere RouterNodes haben das Datenpaket nicht empfangen. ■ Ein oder mehrere RouterNodes haben einen oder mehrere LockNodes nicht erreicht. ■ Ethernetverbindung zu einem oder mehreren RouterNodes ist unterbrochen. Die RouterNodes könnten das Datenpaket zwar kabellos empfangen haben, aber ihre Inputquittungen wegen der unterbrochenen Ethernetverbindung nicht mehr zurückmelden. 1. Prüfen Sie die Erreichbarkeit der genannten RouterNodes (siehe RouterNodes und Erreichbarkeit testen (LSM)). 2. Prüfen Sie die Erreichbarkeit der LockNodes (siehe LockNodes und Erreichbarkeit testen (LSM)). 3. Prüfen Sie die letzten Reaktionen der LockNodes (siehe IO-Status und LockNode-Reaktionsfähigkeit).

2.4 Eventmanagement (Ereignisse) einrichten

Die Vernetzung von Schließungen über RouterNode2 bietet viele Vorteile. Ein entscheidender Vorteil ist die ständige Kommunikation zwischen RouterNode2 und Schließung.

In diesem Beispiel soll von der LSM-Software eine vordefinierte E-Mail verschickt werden, sobald ein Transponder in der Nacht an einer bestimmten Schließung betätigt wird.

Für diese Anforderung müssen zunächst folgende Voraussetzungen erfüllt sein:

- Ein WaveNet-Funknetzwerk ist wie im Beispiel *Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung [▸ 36]* eingerichtet.
- Außerdem wurde das Weiterleiten von Ereignissen an der Schließung wie im Schritt *Inputereignisse der Schließung aktivieren [▸ 42]* aktiviert.

2.4.1 E-Mail-Server einrichten

In der LSM-Software ist ein rudimentärer E-Mail-Client zum Versenden von E-Mails implementiert. Für das Versenden von E-Mails wird ein eigener E-Mail-Account benötigt, welcher das SMTP-Format unterstützt.

1. Wählen Sie "Netzwerk/E-Mail-Benachrichtigungen"
2. Klicken Sie auf die Schaltfläche "E-Mail".
3. Geben Sie alle SMTP-Einstellungen Ihres E-Mail-Providers an.
4. Klicken Sie auf die Schaltfläche "OK".
5. Klicken Sie auf die Schaltfläche "OK".

2.4.2 Taskdienst einstellen

1. Wählen Sie "Netzwerk/Taskmanager".
2. Wählen Sie unter "Taskdienst" ihren Kommunikationsknoten aus.
3. Klicken Sie auf die Schaltfläche "Übernehmen".
4. Klicken Sie auf die Schaltfläche "Beenden".

2.4.3 Inputereignisse über den RouterNode2 weiterleiten

Sobald Ereignisse *(z.B. ein Transponder bucht an einer vernetzten Schließung)* über den RouterNode2 an den CommNode-Server weitergeleitet werden sollen, muss das in der I/O-Konfiguration des Routers aktiviert werden.

1. Öffnen Sie den WaveNet Manager.
2. Klicken Sie mit der rechten Maustaste auf den Router und wählen Sie "I/O Konfiguration".
3. Legen Sie über die Dropdownleiste bei "Ereignisse an Managementsystem übermitteln" die Option "alle LN Ereignisse" fest.

4. Bestätigen Sie über die Schaltfläche "OK" und beenden Sie den WaveNet-Manager.

2.4.4 Inputereignisse über das SREL3-ADV-System weiterleiten

Das SREL3-ADV-System ermöglicht die Weiterleitung der Input-Eingänge an die LSM.

2.4.4.1 Controller-Inputs auswerten

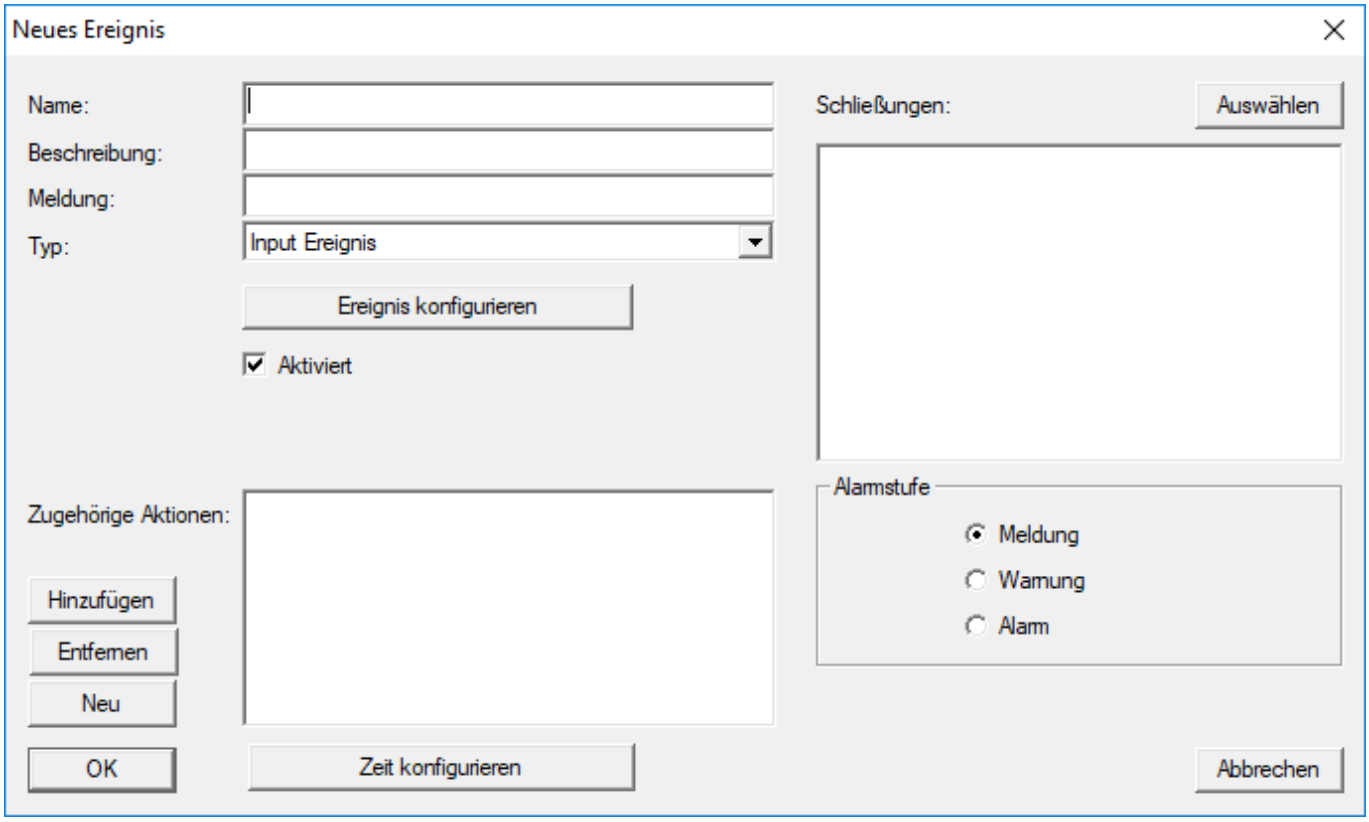
Die digitalen Eingänge am Controller des SREL3-ADV-Systems können an die LSM weitergeleitet werden und dort Aktionen auslösen.

Ereignis anlegen

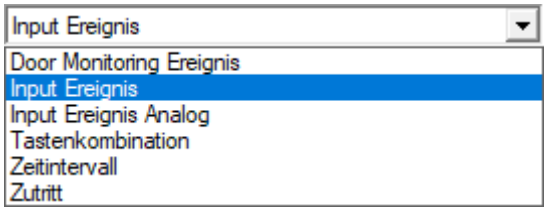
Wenn Sie einen Input durch die LSM oder durch SmartSurveil (siehe SmartSurveil) auswerten wollen, müssen Sie den entsprechenden Input zuerst in der LSM als Ereignis anlegen. Erst dann werden Änderungen am Input auch in der LSM-Datenbank abgelegt.

✓ LSM geöffnet.
✓ SREL3-ADV-System in Matrix angelegt.

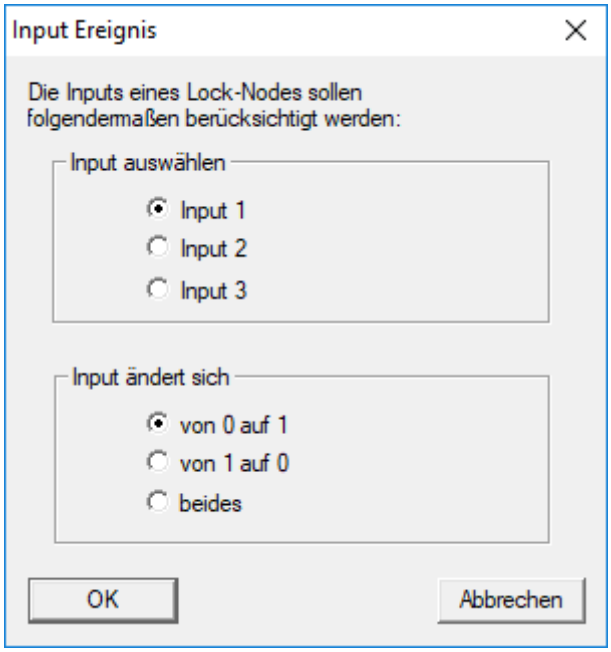
1. Wählen Sie über | Netzwerk | den Eintrag Ereignismanager aus.
   ↳ Fenster "Netzwerkereignis Manager" öffnet sich.
2. Klicken Sie auf die Schaltfläche Neu.
   ↳ Fenster "Neues Ereignis" öffnet sich.



3. Geben Sie einen Namen für das Ereignis ein.
4. Geben Sie optional eine Beschreibung für das Ereignis ein.
5. Geben Sie optional eine Meldung ein.
6. Öffnen Sie das Dropdown-Menü ▼ Typ:.
7. Wählen Sie den Eintrag "Input Ereignis" aus.



8. Klicken Sie auf die Schaltfläche Ereignis konfigurieren.
   ↳ Fenster "Input Ereignis" öffnet sich.



9. Wählen Sie im Bereich "Input auswählen" den gewünschten Input aus.
10. Wählen Sie im Bereich "Input ändert sich" die Zustandsänderung aus, die das Ereignis auslösen soll.
11. Klicken Sie auf die Schaltfläche OK.
12. Klicken Sie auf die Schaltfläche Auswählen, um dem Ereignis eine Schließung zuzuordnen.
    ↳ Fenster "Verwaltung" öffnet sich.
13. Markieren Sie eine oder mehrere Schließungen.
14. Klicken Sie auf die Schaltfläche Hinzufügen.
15. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster schließt sich.
    ↳ Schließung ist dem Ereignis zugeordnet.

16. Wenn Sie eine Aktion festlegen wollen, können Sie mit der Schaltfläche Neu bzw. Hinzufügen eine Aktion zuordnen.
17. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster schließt sich.
    ↳ Ereignis wird im Bereich "Ereignisse" angezeigt.
18. Klicken Sie auf die Schaltfläche Beenden.
    ↳ Fenster schließt sich.

↳ Input ist als Ereignis angelegt und löst je nach Einstellung eine Aktion aus..

2.4.5 Reaktion erstellen

Erstellen Sie zuerst eine Reaktion. Diese Reaktion kann später ausgewählt werden, wenn ein bestimmtes Szenario eintritt.

1. Wählen Sie "Netzwerk/Ereignismanager".
2. Klicken Sie im rechten Bereich unter "Reaktionen" auf die Schaltfläche "Neu".
3. Ergänzen Sie einen Namen und eine Beschreibung für die Reaktion.
4. Wählen Sie den Typ "E-Mail" aus.
5. Klicken Sie auf die Schaltfläche "Reaktion konfigurieren".
6. Klicken Sie auf die Schaltfläche "Neu".
7. Geben Sie die E-Mail-Adresse des Empfängers sowie einen Betreff und einen Nachrichtentext ein. *Über die Schaltfläche "Testen" kann die E-Mail-Konfiguration sofort getestet werden.*
8. Beenden Sie den Dialog, indem Sie dreimal auf die Schaltfläche "OK" drücken. Über die Schaltfläche "Beenden" kehren Sie zur Matrix zurück.

2.4.6 Ereignis erstellen

Wenn bereits eine Reaktion erstellt wurde, kann als nächstes ein Ereignis erstellt werden.

1. Wählen Sie "Netzwerk/Ereignismanager".
2. Klicken Sie im linken Bereich unter "Ereignisse" auf die Schaltfläche "Neu".
3. Ergänzen Sie einen Namen und eine Beschreibung für die Reaktion.
4. Wählen Sie den Typ "Zutritt" aus.
5. Klicken Sie auf die Schaltfläche "Ereignis konfigurieren".
6. Aktivieren Sie die CheckBox "Auf alle Transponder reagieren". *Das Ereignis soll bei jeder Transponderbetätigung eintreten. Alternativ können Sie das Ereignis auf einen einzelnen Transponder beschränken.*
7. Die Aktion kann über den Bereich "Zeiteinstellung" weiter angepasst werden.
8. Klicken Sie auf die Schaltfläche "OK".

9. Klicken Sie im Bereich "Schließungen" auf die Schaltfläche "Auswählen".
10. Fügen Sie alle Schließungen hinzu, welche bei Betätigung des Transponders das Ereignis auslösen sollen und bestätigen Sie die Auswahl über die Schaltfläche "OK".
11. Klicken Sie im Bereich "Zugehörige Aktionen" auf die Schaltfläche "Hinzufügen".
12. Fügen Sie die vorher erstellte Reaktion hinzu.
13. Klicken Sie auf die Schaltfläche "Zeit konfigurieren".
14. Geben Sie die Zeiten der Nachtruhe an. Das Ereignis wird nur in der hier definierten Zeitfenster aktiv ausgeführt.
15. Beenden Sie den Dialog, indem Sie dreimal auf die Schaltfläche "OK" drücken. Über die Schaltfläche "Beenden" kehren Sie zur Matrix zurück.

2.5 Virtuelles Netzwerk (VN) verwalten

Über ein virtuelles Netzwerk (VN-Netzwerk) lassen sich Berechtigungen auch ohne eine volle Vernetzung komfortabel und schnell ändern und regulieren. Die Berechtigung für Schlösser (und Sperr-IDs gesperrter Identmedien) wird direkt im Identmedium gespeichert und bei jeder Betätigung an einer Schließung weitergegeben. Deshalb ist es in virtuellen Netzwerken wichtig, alle Identmedien in regelmäßigen Abständen an einem Gateway zu buchen.

In diesem Bespiel wird die prinzipielle Einrichtung eines virtuellen Netzwerks gezeigt.

2.5.1 Schließanlage einrichten

In der (reinen) G2-Schließanlage muss das die CheckBox "Virtuelles Netzwerk" aktiviert sein. Wird diese Einstellung bei einer bestehenden Schließanlage angewendet, kann erheblicher Programmierbedarf entstehen.

2.5.2 VN Dienst einrichten

1. Wählen Sie "Netzwerk/VN Dienst".
2. Wählen Sie den VN-Server (z.B. der Kommunikationsknoten) aus.
3. Geben Sie den Installationspfad zum VN-Server an. *Der VN-Server wird bei einer LSM Business Installation im Hauptverzeichnis in einem separaten Ordner installiert.*
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

2.5.3 Komponenten anlagen und LSM-Software einrichten.

Bevor Sie mit der Einrichtung beginnen, müssen in der LSM-Software die wichtigsten Einstellungen für den Betrieb eines Netzwerks vorgenommen und der RouterNode2 einsatzbereit sein.

- *LSM Software vorbereiten [▸ 36]*
- *Hardware vorbereiten [▸ 37]*
- *Kommunikationsknoten erstellen [▸ 38]*
- *Taskdienst einstellen [▸ 54]*

1. Legen Sie verschiedene Identmedien (z.B. Transponder) und Schließungen (z.B. aktive Schließzylinder) an.
2. Führen Sie eine Erstprogrammierung der angelegten Komponenten durch.
3. Legen Sie ein SmartRelais2 an und berechtigen Sie alle Identmedien daran, welche dort später neue Berechtigungen erhalten sollen.
   ↳ In den Schließungseigenschaften des SREL2 muss in der Registerkarte unbedingt die CheckBox "Gateway" aktiviert werden!
4. Führen Sie die Erstprogrammierung des SREL2 durch und versichern Sie sich, dass dieses über einen korrekt angeschlossenen LockNode verfügt.
5. Richten Sie den RouterNode2 über den WaveNet-Manager ein und weisen Sie diesem das Gateway (bzw. das SREl2) zu.
   ↳ Siehe *Netzwerk einrichten und in LSM importieren [▸ 38]*.

2.5.4 Berechtigungsänderungen exportieren

Das Exportieren von Berechtigungsänderungen funktioniert nur, wenn mindestens eine Änderung vorliegt. Entziehen Sie zum Test beispielsweise Transponder 1 die Berechtigung für Schließzylinder 1.

1. Wählen Sie "Programmierung/Virtuelles Netzwerk/Export auf VNetzwerk".
2. Wählen Sie alle SREL2s, auf welche die Änderungen geschickt/exportiert werden sollen.
3. Überprüfen Sie, ob Sie die richtige Schließanlage ausgewählt haben.
4. Klicken Sie auf die Schaltfläche "Vorbereiten"
   ↳ In der Liste "Personen" tauchen alle Änderungen auf, die exportiert werden.
5. Klicken Sie auf die Schaltfläche "Exportieren"
   ↳ Der Exportvorgang startet. Die Änderungen werden an das Gateway gesendet.

Die Berechtigungsänderung liegt nun am Gateway bereit. Nun gibt es zwei Szenarien:

- Transponder 1 bucht am Gateway. Schließung 1 wird später erkennen, dass Transponder 1 nicht mehr berechtigt ist und den Zutritt verweigern.
- Ein anderer Transponder (nicht Transponder 1) bucht zuerst am Gateway und berechtigt sich an Schließung 1. Die Sperr-ID von Transponder 1 wird dem Schließzylinder 1 mitgeteilt.

Ab LSM 3.4 SP2 ist es möglich, beliebigen Transpondern bis zu zwei andere Transponder-IDs "mitzugeben", die gesperrt werden sollen.

Zu sperrende TIDs direkt programmieren

Die zu sperrenden IDs werden während des Programmiervorgangs auf dem Transponder gespeichert.

✓ Der Transponder ist physikalisch verfügbar.
✓ Das Programmierfenster des Transponders ist geöffnet.

1. Klicken Sie auf die Schaltfläche "TIDs zum Deaktivieren".
   ↳ Liste öffnet sich.
2. Setzen Sie bis zu zwei Häkchen in der Spalte TID, um die zu löschenden TIDs auf dem Transponder zu speichern.
3. Bestätigen Sie die Eingaben über die Schaltfläche OK.
4. Fahren Sie mit der Programmierung fort.

↳ Die markierten TIDs werden auf dem Transponder als zu löschend hinterlegt. Wenn der Transponder sich an einer betroffenen Schließung authentifiziert, werden die zu löschenden TIDs an der Schließung gesperrt.

Zu sperrende TIDs in den Eigenschaften hinterlegen

Die zu sperrenden IDs werden entweder während des nächsten Programmiervorgangs oder bei der nächsten Buchung an einem Gateway auf dem Transponder gespeichert.

✓ Das Eigenschaften-Fenster des Transponders ist geöffnet.

1. Wechseln Sie zur Registerkarte "Konfiguration".
2. Klicken Sie auf die Schaltfläche "TIDs zum Deaktivieren".
   ↳ Liste öffnet sich.
3. Setzen Sie bis zu zwei Häkchen in der Spalte TID, um die zu löschenden TIDs auf dem Transponder zu speichern.
4. Bestätigen Sie die Eingaben über die Schaltfläche OK.

↳ Die markierten TIDs werden bei der nächsten Programmierung oder der nächsten Buchung an einem Gateway auf dem Transponder gespeichert.

2.5.5 Berechtigungsänderungen importieren

Nach dem Export der Änderungen auf das Gateway ist in der LSM-Software zunächst nicht einsehbar, welche Änderungen bereits vom Gateway abgeholt wurden. Erst ein Import kann das zeigen.

1. Wählen Sie "Programmierung/Virtuelles Netzwerk/Import Synchronisation".
   ↳ Der Importvorgang startet sofort.
2. Klicken Sie auf die Schaltfläche "Beenden"

2.5.6 Tipps zu VN

- Um Änderungen schnell "offline" in der Schließanlage zu verteilen ist es wichtig, sämtliche Transponder in kurzen, regelmäßigen Abständen buchen zu lassen. Hier kann mit Zeitbudgets gearbeitet werden:

  Die Optionen "Dynamische Zeitfenster" in den Schließanlageneigenschaften bieten die Möglichkeit, Transpondern ein Zeitbudget aufzuzwingen. So kann eine Person verpflichtet werden, das Identmedium regelmäßig am Gateway aufzuladen. Andernfalls ist das Identmedium für diese Schließanlage gesperrt.

- Import und Export von Änderungen an ein Gateway können automatisiert werden. Diese Einstellungen können direkt unter "Netzwerk/VN Dienst" vorgekommen werden.

ACHTUNG

Auslastung des WaveNets durch Im- und Export

Wenn viele Änderungen gleichzeitig importiert und exportiert werden, dann wird das WaveNet währenddessen stark ausgelastet. Das kann andere Funktionen, die ebenfalls auf das WaveNet zugreifen, beeinträchtigen.

2.6 Sabotage-Erkennung

Ab der LSM 3.4 SP2 können Sie Sabotageversuche am SmartHandle AX und am SmartRelais 3 Advanced erkennen. Wenn das dort verwendete Gehäuse geöffnet wird, dann erkennt die Elektronik das und sendet die Information an die LSM. Wenn Sie die Information auswerten wollen, dann können Sie ein Ereignis dazu einrichten und darauf reagieren (siehe *Eventmanagement (Ereignisse) einrichten [▸ 54]*).

2.7 DoorMonitoring (SmartHandle) - Türdrücker-Events

Ab der LSM 3.4 SP2 können Sie den Zustand des Drückers am SmartHandle AX erkennen. Wenn der Drücker gedrückt ist, dann erkennt die Elektronik das und sendet die Information an die LSM. Wenn Sie die

Information auswerten wollen, dann können Sie ein Ereignis dazu einrichten und darauf reagieren (siehe (*Eventmanagement (Ereignisse) einrichten [▸ 54]*).

3 Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der SimonsVoss-Homepage im Downloadbereich unter Dokumente (*https://www.simons-voss.com/de/downloads/dokumente.html*).

Software und Treiber

Software und Treiber finden Sie auf der SimonsVoss-Homepage im Downloadbereich unter Software-Downloads (*https://www.simons-voss.com/de/downloads/software-downloads.html*).

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate zu diesem Produkt finden Sie auf der SimonsVoss-Homepage im Zertifikatsbereich (*https://www.simons-voss.com/de/zertifikate.html*).

Hotline

Bei technischen Fragen hilft Ihnen die SimonsVoss Service-Hotline unter +49 (0) 89 99 228 333 (Anruf in das deutsche Festnetz, Kosten variieren je nach Anbieter).

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support@simons-voss.com

FAQ

Informationen und Hilfestellungen zu SimonsVoss-Produkten finden Sie auf der SimonsVoss-Homepage im FAQ-Bereich (*https://faq.simons-voss.com/otrs/public.pl*).

SimonsVoss Technologies GmbH
Feringastraße 4
85774 Unterföhring
Deutschland

Das ist SimonsVoss

SimonsVoss ist Technologieführer bei digitalen Schließsystemen.

Der Pionier funkgesteuerter, kabelloser Schließtechnik bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, mittlere und Großunternehmen sowie öffentliche Einrichtungen.

SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design made in Germany. Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs. Das Unternehmen mit Hauptsitz in Unterföhring bei München und Produktionsstätte in Osterfeld (Sachsen-Anhalt) beschäftigt rund 300 Mitarbeiter in acht Ländern.

SimonsVoss ist ein Unternehmen der ALLEGION Group - ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com)

ALLEGION

SimonsVoss technologies