

LSM 3.5 SP3 Basic Online SmartUserGuide

Handbuch

08.12.2023

Inhaltsverzeichnis

1.	Allgemein	4
1.1	Allgemeine Sicherheitshinweise	4
1.2	Produktspezifische Sicherheitshinweise	5
1.3	Rechtliche Hinweise	5
1.4	Systemanforderungen	6
1.5	Informationen zum Handbuch	6
1.6	Datenschutz im System 3060	7
1.6.1	IT-Grundschutz	7
1.6.2	Verschlüsselung	7
2.	Bedeutung der Textformatierung	9
3.	Grundfunktionen	10
3.1	Neue Schließanlage anlegen	10
3.2	Neue Transpondergruppe anlegen	10
3.3	Neuen Transponder anlegen	10
3.4	Transponder nachträglich einer Transpondergruppe zuweisen	11
3.5	Neuen Bereich anlegen	11
3.6	Neue Schließung anlegen	11
3.7	Pin Code Tastatur anlegen	11
3.7.1	Pin Code Tastatur konfigurieren	12
3.7.2	Pin Code Tastatur im Schließplan anlegen	12
3.7.3	Pin Code Tastatur programmieren	13
3.8	Schließung einem Bereich zuweisen	13
3.9	Berechtigung vergeben/entziehen	13
3.10	DoorMonitoring Komponenten einrichten	14
3.11	Übergreifende Schließebene	14
3.11.1	Übergreifende Schließebene anlegen	15
3.11.2	Schließungen verknüpfen	15
3.11.3	Transponder verknüpfen	16
3.11.4	Transponder berechtigen	17
3.12	Feuerwehrtransponder erstellen	17
3.13	Datenbank manuell sichern	18
3.14	Datenschutzkonformes Arbeiten nach DSGVO	19
3.14.1	Daten exportieren	20
3.14.2	Daten löschen	22
3.14.3	Welche personenbezogenen Daten werden in der Software gespeichert?	24

3.14.4	Zu welchem Zweck werden personenbezogene Daten in der Software gespeichert?	25
3.14.5	Wie lange werden personenbezogene Daten in der Software gespeichert?	25
3.14.6	Sind personenbezogene Daten in der Software vor dem Zugriff Dritter geschützt?	25
3.14.7	Können die gespeicherten Daten als Kopie zur Verfügung gestellt werden?	26
3.14.8	Können personenbezogene Daten aus der Software gelöscht werden?	26
3.15	Matrix durchsuchen	26
3.16	Gruppenaktionen ausführen	27
3.17	Transponder programmieren	27
3.18	Schließung programmieren	28
3.19	Programmieren über LSM Mobile	28
3.19.1	Mit Laptop, Netbook oder Tablet	29
3.20	Zeitzone(n)plan (mit Feiertagen und Betriebsferien) definieren	29
3.21	Zurücksetzen von Komponenten	31
3.22	Defekte Schließung ersetzen	31
3.23	Transponder sperren	32
3.23.1	Transponder dauerhaft sperren und Ersatztransponder erstellen	33
3.23.2	Transponder temporär sperren	37
3.24	Batteriezustand der Schließungen überprüfen und auswerten	38
3.25	Lagermodus bei G1-Schließungen zurücksetzen	40
3.26	Freezemode bei G2-Schließungen zurücksetzen	40
3.27	Zutrittslistenadministration	41
3.27.1	Zutrittslisten	42
3.28	Kartenmanagement	42
3.28.1	Konfiguration ändern	43
3.28.2	Übersicht	44
4.	Realisierung gängiger WaveNet basierter Aufgaben in LSM	48
4.1	Virtuelles Netzwerk (VN) verwalten	48
4.1.1	Virtuelles Netzwerk mit SmartRelais 3 Advanced	48
4.1.2	Virtuelles Netzwerk mit SmartRelais 2 G2	54
4.2	Schließung auslesen	73
5.	Hilfe und weitere Informationen	78

1. Allgemein

Dieses Handbuch beschreibt die Funktionen der Locking System Management Software 3.5 SP3. Die Locking System Management Software, kurz LSM-Software, wurde entwickelt, um komplexe Schließanlagen mit SimonsVoss-Schließkomponenten zu verwalten.

Ergänzend zu diesem Handbuch sind noch weitere Dokumente verfügbar:

■ *WaveNet Handbuch*

Beschreibt den Umgang mit dem WaveNet-Funknetzwerk.

■ *SimonsVoss SmartUserGuide*

Grundfunktionen mit der LSM-Software umsetzen.

■ *LSM Update-Handbuch*

Beschreibt den Update-Vorgang von vorherigen Versionen.

1.1 Allgemeine Sicherheitshinweise

Signalwort: Mögliche unmittelbare Auswirkungen bei Nichtbeachtung

WARNUNG: Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)

VORSICHT: Leichte Verletzung

ACHTUNG: Sachschäden oder Fehlfunktionen

HINWEIS: Geringe oder keine



WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.



HINWEIS

Bestimmungsgemäßer Gebrauch

SimonsVoss-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SimonsVoss-Produkte nicht für andere Zwecke.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

1.2 Produktspezifische Sicherheitshinweise

VORSICHT

Verlust des Schließanlagenpassworts

Das Schließanlagenpasswort ist zentraler Bestandteil des Sicherheitskonzepts. Der Verlust des Schließanlagenpassworts schränkt den Betrieb der Schließanlage ein und ist ein Sicherheitsrisiko.

1. Bewahren Sie das Schließanlagenpasswort sicher auf (z.B. in einem Safe)!
2. Machen Sie das Schließanlagenpasswort für Berechtigte jederzeit einsehbar!

1.3 Rechtliche Hinweise

Der Käufer wird ausdrücklich darauf hingewiesen, dass der Einsatz des Schließsystems (z. B. mit Zutrittsprotokollierung und DoorMonitoring Funktionen) gesetzlichen, insbesondere datenschutzrechtlichen Genehmigungspflichten und Mitbestimmungsrechte der Belegschaft unterliegen kann. Die Verantwortung für den rechtskonformen Einsatz des Produkts liegt beim Käufer bzw. Kunden und dem Endnutzer.

Nicht vereinbarungsgemäße bzw. unübliche Verwendung, welche nicht ausdrücklich von der SimonsVoss Technologies GmbH zugelassene Reparaturarbeiten bzw. Modifikationen sowie nicht fachgemäßer Service sind, können zu Funktionsstörungen führen und sind zu unterlassen. Jegliche, nicht ausdrücklich von der SimonsVoss Technologies GmbH zugelassene Änderungen führen zu Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.

1.4 Systemanforderungen

Für ein flüssiges Arbeiten mit der LSM empfiehlt SimonsVoss immer leistungsstarke und aktuelle Hardware einzusetzen, die die Systemanforderungen übertreffen.

Um auch große Schließanlagen mit vielen Komponenten übersichtlich darzustellen, empfiehlt SimonsVoss einen hochauflösenden Breitbildmonitor mit 21" oder mehr.

Allgemein

- Lokale Administratorrechte zur Installation
- TCP/IP
(Bei Verwendung des EventAgent wird NetBios benötigt.)
- LAN (min. 100MBit/s)
- .NET-Framework 4.0 oder neuer
- USB-Schnittstelle(n)
- Keine Unterstützung von ARM-Prozessoren unter System 3060

Client-PC

- Monitor: Min. 48 cm (19")
- Monitorauflösung: Min. 1024x768, empfohlen 1280x1024 oder mehr
- Prozessor: Min. 2,66 GHz mit 2 oder mehr Kernen (Intel/AMD)
- Arbeitsspeicher: Min. 4 GB
- Festplattengröße: Abhängig von der Anlagengröße, min. 500 MB
(während der Installation ca. 1 GB)
- Windows-Betriebssystem:
 - Windows 11 Professional, 64-Bit
 - Windows 10 Professional, 64-Bit



HINWEIS

Sehen Sie in den Release-Notes der LSM Software nach, welche Version der LSM Mobile zu verwenden ist.

1.5 Informationen zum Handbuch

Dieses Handbuch beschreibt die Funktionen der LSM-Software. Dadurch ist es dem Benutzer möglich, SimonsVoss-Schließkomponenten zu programmieren und die Schließanlage zu verwalten.



HINWEIS

Dieses Handbuch beschreibt nicht die Montage einzelner SimonsVoss-Schließkomponenten. Beachten Sie hierfür unbedingt die Kurzanleitungen und Handbücher der jeweiligen Komponenten!

Transponder

In der LSM Software werden grundsätzlich alle Identmedien (Transponder, Tag, Karte, etc.) als Transponder angesehen. Der Begriff "Transponder" steht in diesem Handbuch deshalb auch für alle anderen Identmedien wie Tags und Karten.

1.6 Datenschutz im System 3060

Siehe *Datenschutzkonformes Arbeiten nach DSGVO* [► 19].

1.6.1 IT-Grundschutz

1.6.1.1 Welchen Schutzbedarf haben die im System verarbeiteten Daten?

Generell werden in der Software nur unkritische Daten mit sog. normalem Schutzbedarf verarbeitet und gespeichert. Also Daten, bei deren hypothetischem Verlust weder der Ruf einer Person noch das Image eines Unternehmens geschädigt wird. Auch ein hoher finanzieller Schaden ist nicht zu erwarten.

1.6.1.2 Welche Anforderungen an die IT-Infrastruktur sind empfohlen?

Daher ist der IT-Grundschutz laut Bundesamt für Sicherheit in der Informationstechnik (BSI) für eine SimonsVoss Schließanlage als Sicherheitskonzept ausreichend und gilt als empfohlene Mindestanforderung an Ihre IT-Infrastruktur.

1.6.2 Verschlüsselung

1.6.2.1 Sind die Daten im System 3060 verschlüsselt?

Ja. Innerhalb der systemeigenen Kommunikation sind Datenpakete End-to-End verschlüsselt. Mit den neuesten Versionen unserer Produkte erhöhen Sie den Grad der Sicherheit, da diese stets dem aktuellen Stand der Technik entsprechen. Es kommen mehrstufige Verschlüsselungsmethoden zum Einsatz (AES, 3DES).

1.6.2.2 Welche Daten werden dabei verschlüsselt?

Innerhalb der systemeigenen Kommunikation werden keine personenbezogene Daten verarbeitet, sondern mit Hilfe von Identifikationsnummern pseudonymisiert. Auch ohne Verschlüsselung ist keine Zuordnung zu einer realen Person möglich.

1.6.2.3 Sind die Übertragungswege z.B. per Funk auch verschlüsselt?

Nein. Durch die verwendete End-to-End Verschlüsselung ist keine zusätzliche Verschlüsselung der Übertragungswege nötig.

2. Bedeutung der Textformatierung

Diese Dokumentation verwendet Textformatierung und Gestaltungselemente, um das Verständnis zu erleichtern. Die Tabelle erklärt die Bedeutung möglicher Textformatierungen:

Beispiel	Schaltfläche
<input checked="" type="checkbox"/> Beispiel <input type="checkbox"/> Beispiel	Checkbox
<input type="radio"/> Beispiel	Option
[Beispiel]	Registerkarte/Tab
"Beispiel"	Name eines angezeigten Fensters
Beispiel	Obere Programmleiste
Beispiel	Eintrag in der ausgeklappten oberen Programmleiste
Beispiel	Kontextmenü-Eintrag
▼ Beispiel	Name eines Dropdown-Menüs
"Beispiel"	Auswahlmöglichkeit in einem Dropdown-Menü
"Beispiel"	Bereich
Beispiel	Feld
<i>Beispiel</i>	Name eines (Windows-)Dienstes
<i>Beispiel</i>	Befehle (z.B. Windows-CMD-Befehle)
Beispiel	Datenbank-Eintrag
[Beispiel]	MobileKey-Typauswahl

3. 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.

3.1 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".

3.2 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".

3.3 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".

3.4 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.

3.5 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".

3.6 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".

3.7 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.

3.7.1 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.

3.7.2 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

3.7.3 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.

3.8 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.

3.9 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 widerrufen 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.

3.10 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.

3.11 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!

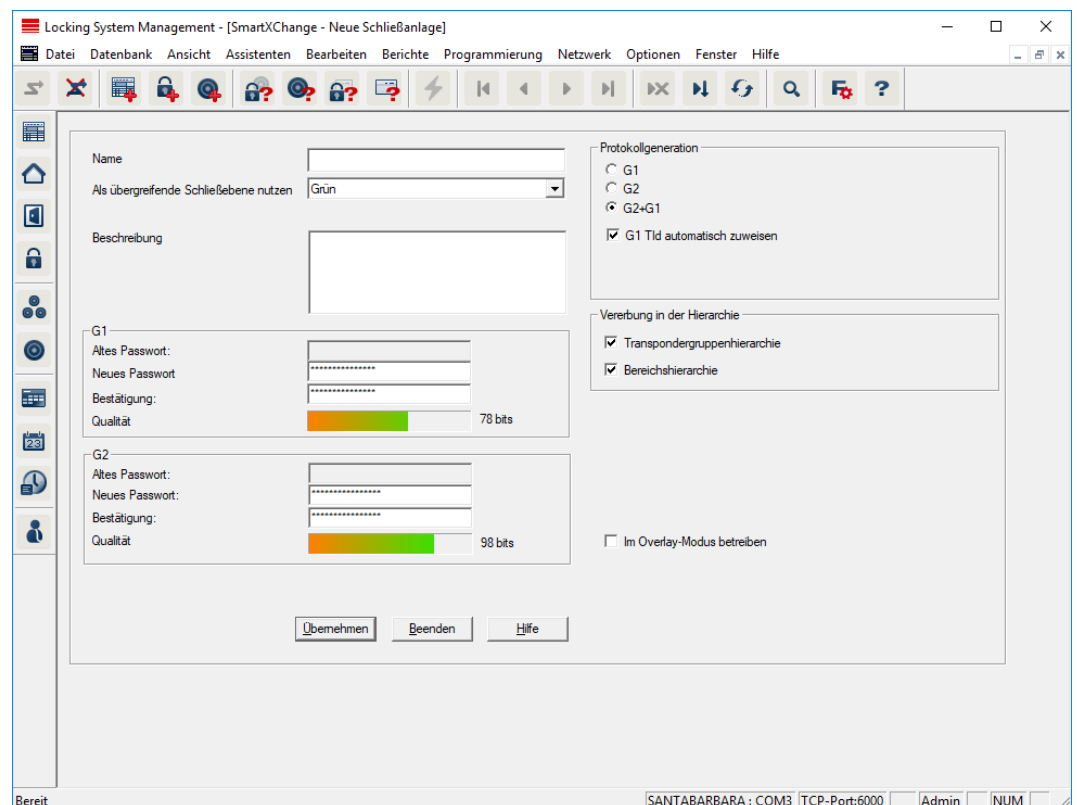
3.11.1 Übergreifende Schließebene anlegen

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.

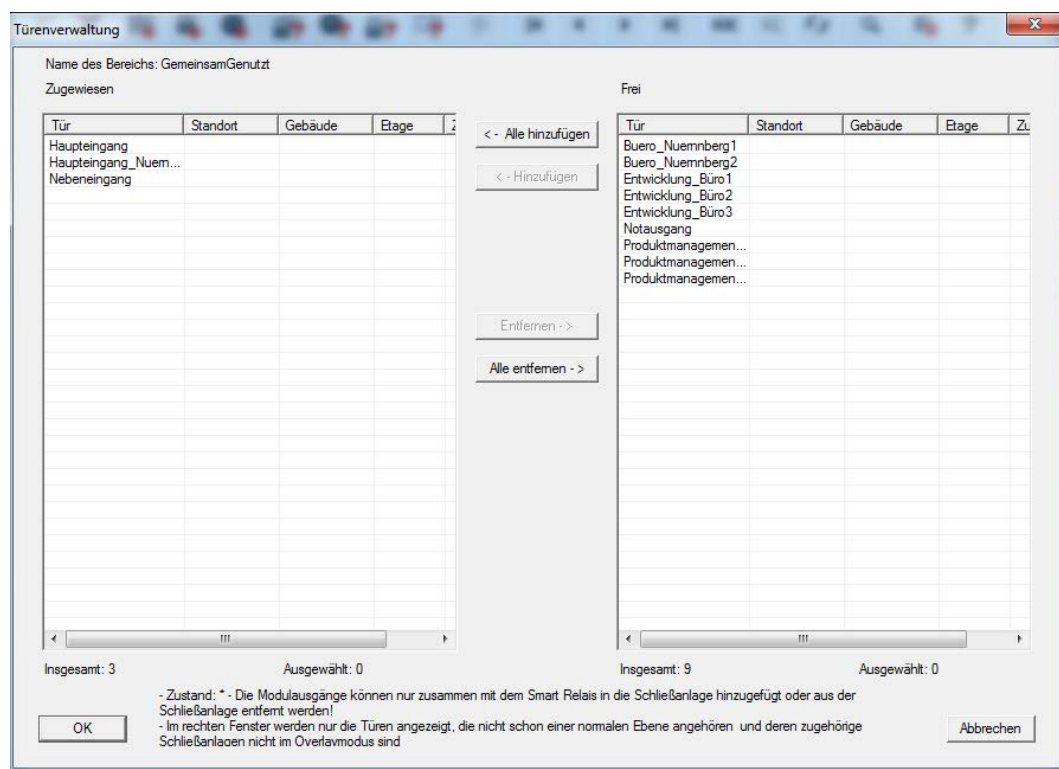


3.11.2 Schließungen verknüpfen

- ✓ 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.

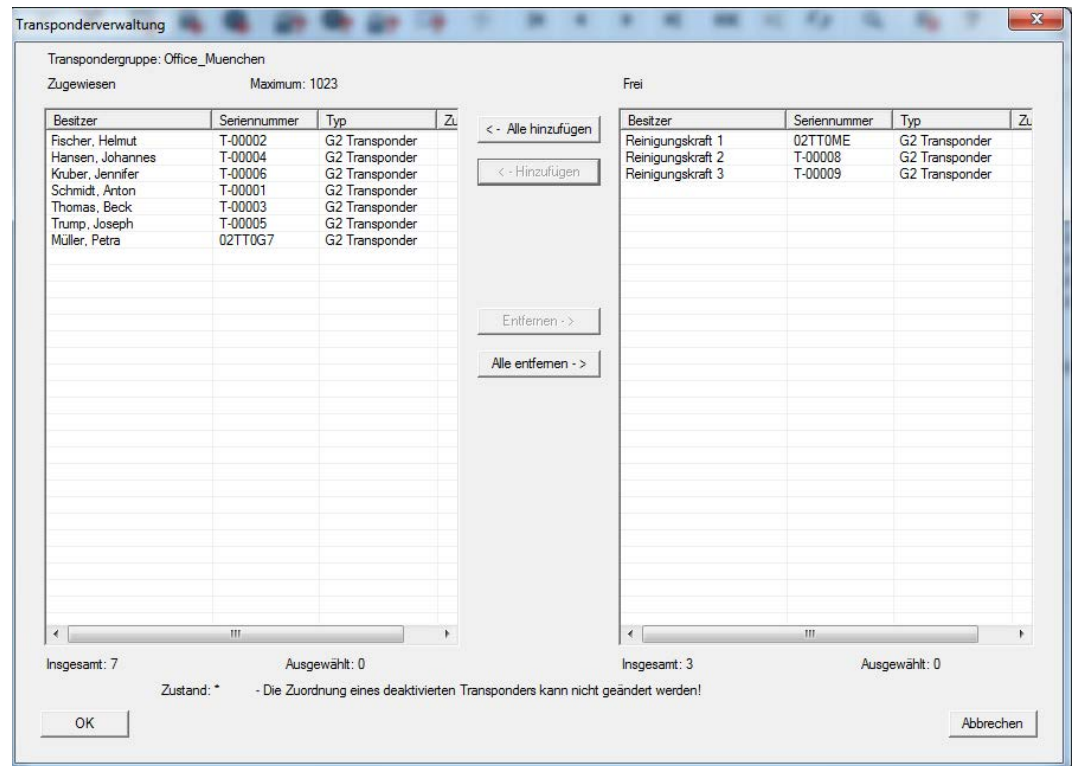


3.11.3 Transponder verknüpfen

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.



3.11.4 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 Checkboxes alle gewünschten Bereiche/Schließungen anwählen, um der Transpondergruppe Zugriff an allen Türen zu gewähren.


3.12 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.

3.13 Datenbank manuell sichern

1. Melden Sie sich als der Windows Benutzer an, der auch sonst die Administration der Schließanlage vornimmt.
2. Starten Sie die LSM.
3. Klicken Sie auf die Setup-Schaltfläche ().
- ↳ Setup öffnet sich.
4. Klicken Sie auf die Schaltfläche **Erweitert**.
- ↳ Fenster "Setup Einstellungen" öffnet sich.

Setup Einstellungen

Datenbank

Backup

Projekt: TestDB

Backup-Dateien für die Wiederherstellung

☒ Alle anzeigen
☐ nur für das ausgewählte Projekt

Neues DB-Projekt:

Datenbankablage

Verzeichnis: D:\LSM 3.5\Lokale LSMDB

Übernehmen Voreinstellung wiederherstellen

OK Abbrechen

5. Wählen Sie im Dropdown-Menü ▼ **Projekt:** Ihr Projekt aus.
6. Klicken Sie auf die Schaltfläche **Backup**
↳ Backup erstellt.
7. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Setup Einstellungen" schließt sich.
8. Kopieren Sie das erstellte Backup (.zip) auf einen separaten Datenträger.



HINWEIS

Das Backup ist standardmäßig in C:\ProgramData\SimonsVoss\Repository gespeichert.

3.14 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 Protokollieren).

3.14.1 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:

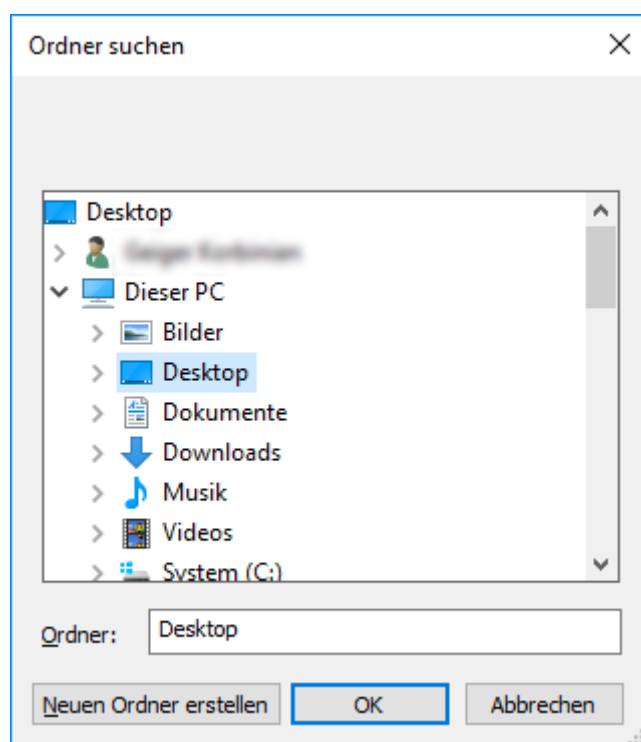
Person	Diese Datei beinhaltet die personenbezogenen Daten, mit denen die Person identifiziert werden kann (zum Beispiel Nachname, Adresse oder Foto).
PersonHistory	Diese Datei beinhaltet das Datum der Erstellung und der Löschung des Datensatzes.
PersonLog	Diese Datei beinhaltet den Verlauf der Bearbeitungen,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

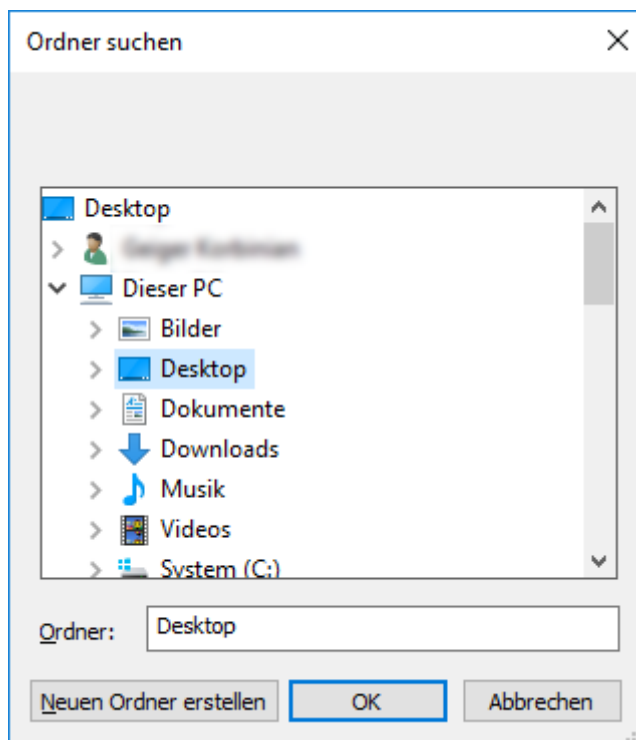
Sie können die gespeicherten personenbezogenen Daten der Benutzer der LSM-Software als CSV-Dateien exportieren. Dabei werden zwei Dateien erzeugt:

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).
---------	--

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.

3.14.2 Daten löschen

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

Personen

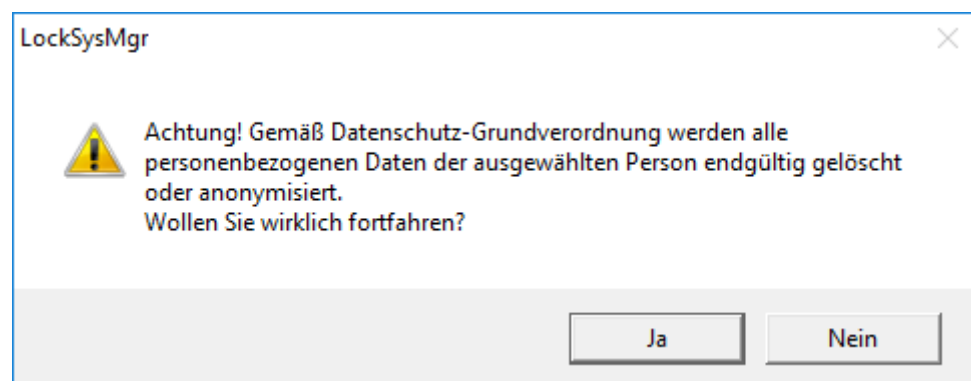


HINWEIS

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

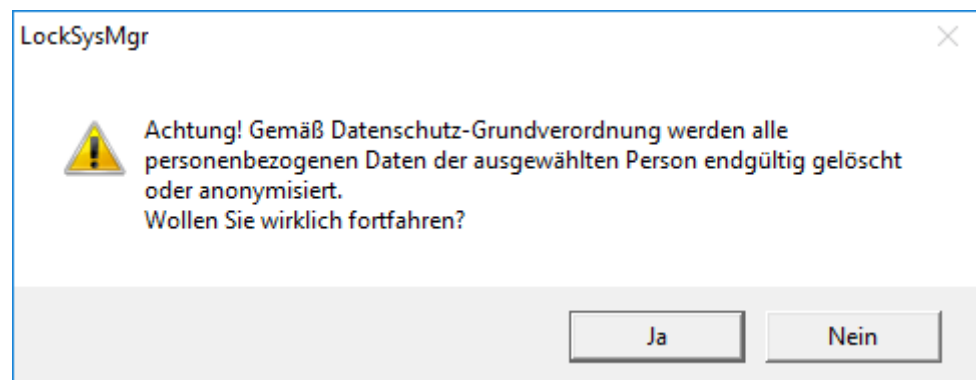
Löschung von Restdaten aus vorherigen Löschungen

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

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.

3.14.3 Welche personenbezogenen Daten werden in der Software gespeichert?

Es besteht die Möglichkeit folgende Daten einer Person in der Software zu speichern:

- Vorname
- Nachname*
- Titel
- Adresse
- Telefon
- E-Mail
- Personalnummer*
- Benutzername
- Abteilung
- Ort/Gebäude

- Eingestellt von/bis
- Geburtsdatum
- Kostenstelle
- Foto

Davon sind nur Nachname und Personalnummer sogenannte *Pflichtfelder und bei der Verwendung der Software erforderlich.

Besonders sensible Kategorien personenbezogener Daten nach Art. 9 DSGVO werden nicht gespeichert.

3.14.4 Zu welchem Zweck werden personenbezogene Daten in der Software gespeichert?

Um die Funktionen einer elektronischen Schließanlage vollumfänglich nutzen zu können, ist es notwendig die verwendeten Identifikationsmedien (z. B. Transponder) einem bestimmten Nutzer (z. B. Mitarbeiter) zuordnen zu können.

3.14.5 Wie lange werden personenbezogene Daten in der Software gespeichert?

Die Daten werden mindestens über die Dauer der Inbesitznahme eines Identifikationsmediums innerhalb der Schließanlage gespeichert (z. B. Firmenzugehörigkeit).

Die Dauer der Speicherung von Daten (z. B. in Protokollen und Zutrittslisten) kann vom Schließanlagenverwalter verändert und an betriebliche Vorgaben angepasst werden.

3.14.6 Sind personenbezogene Daten in der Software vor dem Zugriff Dritter geschützt?

Grundsätzlich ist der Nutzer (Endkunde) der Schließanlage und der Software für die Verwaltung und Sicherstellung der Zugriffsrechte verantwortlich.

Im Schließsystem selbst, werden alle Daten über ein mehrstufiges Verschlüsselungsverfahren gesichert. Ein Öffnen der grafischen Benutzeroberfläche, um auf die Daten zugreifen zu können, ist ohne Passwort und entsprechende Benutzerrechte nicht möglich.

Eine automatische Übermittlung an Dritte, eine Nutzung oder Verarbeitung durch SimonsVoss findet im Rahmen des Geschäftsbetriebes nicht statt.

3.14.7 Können die gespeicherten Daten als Kopie zur Verfügung gestellt werden?

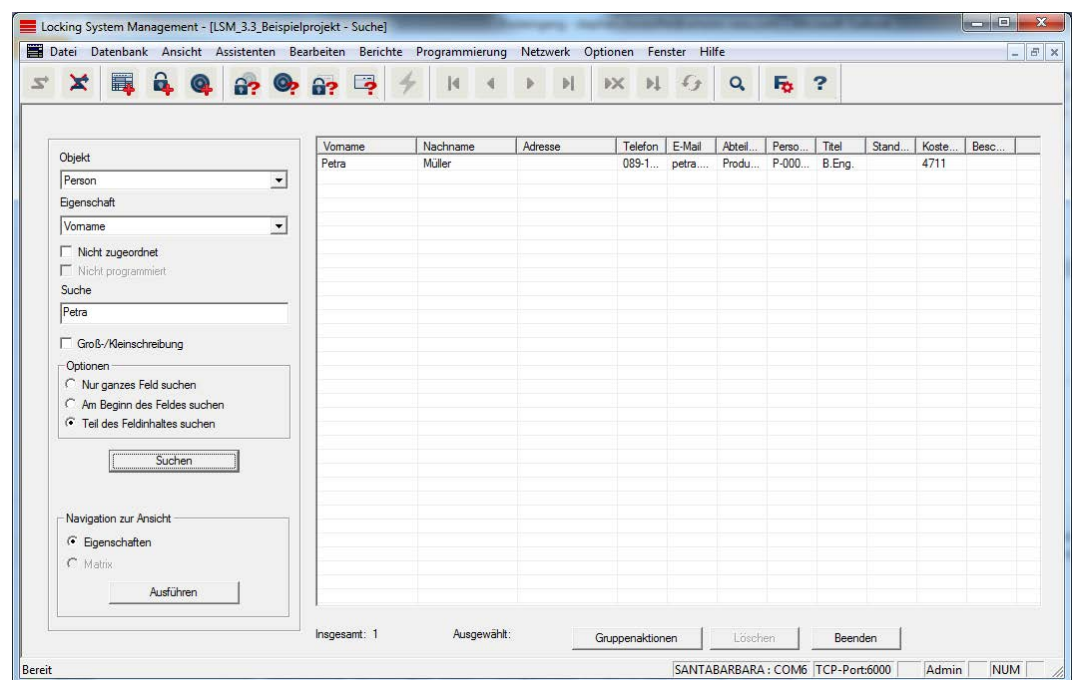
Alle gesammelten Daten zu einer betroffenen Person können (ab Version 3.4), entsprechende Benutzerrechte vorausgesetzt, per Exportfunktion als Kopie durch den Kunden (z.B. im Rahmen eines Audits) zur Verfügung gestellt werden. Dies ermöglicht dem Kunden die Erfüllung des Auskunftsrechts nach Art. 15 DSGVO Absatz 3.

3.14.8 Können personenbezogene Daten aus der Software gelöscht werden?

Personenbezogene Daten können durch den Kunden auf Verlangen einer betroffenen Person nach Art. 17 DSGVO aus der Software (ab Version 3.4 SP1) und der dazugehörigen Datenbank endgültig gelöscht werden.

3.15 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.

3.16 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.

3.17 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 *Transponder dauerhaft sperren und Ersatztransponder erstellen* [► 33]).



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.

3.18 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!

Abweisung der ersten Transponderbetätigung nach Erstprogrammierung von AX-Produkten

Wenn das erste betätigte Identmedium nach der Erstprogrammierung ein Transponder ist, dann wird der Transponder einmalig abgewiesen und im Hintergrund mit der Schließung synchronisiert. Danach funktionieren Transponder wie gewohnt.

3.19 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.

3.19.1 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.

3.20 Zeitzonenplan (mit Feiertagen und Betriebsferien) definieren

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/Zeitzoneplan*.
 - ↳ Ein "leerer Zeitzoneplan" öffnet sich. Falls ein bestehender Zeitzoneplan angezeigt wird, klicken Sie auf die Schaltfläche "Neu", um einen neuen, leeren Zeitzoneplan 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 Zeitzoneplan 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 Zeitzoneplan 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.

3.21 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.

3.22 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!

3.23 Transponder sperren

Transponder können unter Umständen verloren gehen, beschädigt oder gestohlen werden. Sie haben dann zwei Möglichkeiten:

- *Transponder dauerhaft sperren und Ersatztransponder erstellen*
[▶ 33]
- *Transponder temporär sperren* [▶ 37]



HINWEIS

Übertragung der Sperr-IDs mit Karten an beidseitig lesenden Schließungen

Karten können nur einzelne Sperr-IDs übertragen, kein vollständiges Programmierprotokoll.

- Halten Sie deshalb die Karte, die die Sperr-IDs überträgt, immer an beide Leser.

3.23.1 Transponder dauerhaft sperren und Ersatztransponder erstellen



HINWEIS

Aus Sicherheitsgründen müssen in allen Schließungen die Berechtigungen des gelöschten Transponders entfernt werden.

- Programmieren Sie dazu alle Schließungen neu.

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 3.5 SP3 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**.

Transponder programmieren

Besitzer / Transponder: Aldrin, Lily / 005MBA8

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

☐ Nach der Programmierung zum nächsten Transponder springen

☐ Deaktivierungsquittungen / Batteriewarnungen auslesen

☒ G1 Datensätze aus fremden Schließanlagen beibehalten

Programmieren TIDs zum Deaktivieren Beenden

↪ Liste öffnet sich.

TIDs zum Deaktivieren

Schließanlage

HIMYM

☒ G2 TIDs
 ☒ G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

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

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

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

OK

Übernehmen

Abbrechen

- Setzen Sie bis zu zwei Häkchen in der Spalte TID, um die zu löschenden TIDs auf dem Transponder zu speichern.
- Bestätigen Sie die Eingaben über die Schaltfläche **OK**.
- 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.

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

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.

3.23.2 Transponder temporär sperren

Die dauerhafte Sperrung eines Identifikationsmediums führt zum Verlust einer TID. Deshalb wurde mit der LSM 3.5 eine Funktion eingeführt, die es ermöglicht einen Transponder oder eine Karte lediglich temporär zu sperren: "Temporäre Sperrung".

The screenshot shows a dialog box titled "Die Begründung" with a close button (X) in the top right corner. The main text asks: "Wollen Sie tatsächlich den Transponder sperren? Falls 'ja', geben Sie bitte den Grund an, z.B. ob der Transponder verlorengegangen oder defekt ist". Below this text is a dropdown menu with "Temporäre Sperrung" selected. Underneath the dropdown is a text area labeled "Zusatzinformation:". At the bottom of the dialog are two buttons: "Ja" on the left and "Nein" on the right.

Die TID wird nicht tatsächlich gesperrt. Stattdessen entziehen Sie der Person per Knopfdruck alle Berechtigungen. Betroffene Türen bekommen natürlich Programmierbedarf und müssen programmiert werden. Sollte der Transponder wieder auftauchen oder an eine neue Person weitergegeben werden, können Sie die Berechtigungen vor der Sperrung einfach wieder herstellen.

Sie sehen die temporär gesperrten Transponder in den Eigenschaften der Schließanlage unter der Registerkarte [Sonder-TIDs].

3.24 Batteriezustand der Schließungen überprüfen und auswerten

Batteriezustände in die LSM-Software übertragen

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".

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".

3.25 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.

3.26 Freezemode bei G2-Schließungen zurücksetzen

Gegenüber der G1-Generation wurde in G2 die Notöffnung der Schließung und die Aufhebung des Noterhaltungsmodus (Freezemode) vereinfacht.

- ✓ Batteriwechsel-Identifikationsmedium angelegt (siehe G2 Batteriwechsel-Transponder).
 - ✓ Batteriwechsel-Identifikationsmedium programmiert.
1. Betätigen Sie das Batteriwechsel-Identifikationsmedium an der Schließung.
 - ↳ Freezemode ist deaktiviert.
 2. Betätigen Sie ein beliebiges berechtigtes Identifikationsmedium.
 - ↳ Schließung öffnet.
 3. Wechseln Sie die Batterie.
 4. Betätigen Sie das Batteriwechsel-Identifikationsmedium an der Schließung.
 - ↳ Freezemode ist deaktiviert.
 5. Testen Sie mit einem beliebigen berechtigten Identifikationsmedium die Funktion der Schließung.
 - ↳ Freezemode zurückgesetzt.

ACHTUNG

Ausfall der Schließung durch Missbrauch

Das Batteriwechsel-Identifikationsmedium ist ausschließlich für die Aufhebung des Freezemode vor einem Batteriwechsel gedacht. Wenn es missbraucht wird, dann können die Batterien vollständig entleert werden. Die Folge ist ein Totalausfall der Schließung.

3.27 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.

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 beliebigen, 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.

3.27.1 Zutrittslisten

Schließungen mit ZK-Funktion protokollieren die Zutritte in einer Zutrittsliste:

- Datum
- Uhrzeit
- ID des Identifikationsmediums
- Name des Nutzers oder der Nutzerin

Sie können die Zutrittsliste mit der LSM-Software auslesen und anzeigen. Die Anzahl der Einträge in der Zutrittsliste hängt von der Schließung und der Konfiguration ab.

	Standard	Gateway
Zylinder	Bis zu 3000	
SmartHandle	Bis zu 3000	
SmartRelais	Bis zu 3600	Bis zu 200

In einer vernetzten Schließanlage können Sie das Auslesen auch automatisieren (siehe [Schließung auslesen \[► 73\]](#)).

3.28 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 empfiehlt 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.

3.28.1 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 \[► 44\]](#)).

Karte einrichten

- ✓ LSM geöffnet.

1. Wechseln Sie zur Schließenanlage, deren Kartenmanagement Sie verändern wollen.
2. Öffnen Sie mit einem Klick auf die Schaltfläche  die Eigenschaften der Schließenanlage.

3. Wechseln Sie zur Registerkarte [Kartenmanagement G2].

Name

Schließungen

Türen

Transponder

Transpondergruppen

Bereiche

Passwort

Sonder-TIDs

PIN-Code Terminal

Kartenmanagement G1

Kartenmanagement G2

Schließanlage: HIMYM

Ebene: Standard

Kartentyp: Mifare Classic

Konfiguration: MC1000L_AV

Speicherbedarf: 528 Bytes

Schließungs IDs: 128-1127 im Kartenprofil

Begehungen im Protokoll: 19

Virtuelles Netzwerk: OK

Parameter:

Name	Wert	Beschreibung
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	Transport Settings

Druckansicht

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).

Name	Wert	Beschreibung
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	Transport Settings

7. Klicken Sie auf die Schaltfläche **Übernehmen**.
- ↳ Sie haben die Konfiguration geändert.

3.28.2 Übersicht

	MIFARE DESFire	MIFARE DESFire Predefined	MIFARE DESFire Predefined DB1
MDBasic	✓	✓	✗
MD1200L	✓	✓	✗
MD3800L	✓	✓	✗
MD2500L_AV	✓	✓	✗
MD4000L_AV	✓	✓	✗

	MIFARE DESFire	MIFARE DESFire Predefined	MIFARE DESFire Predefined DB1
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_A V	✗	✓	✓	✗	✓
MC2400L_A V	✗	✓	✓	✗	✓
MC8000L_A V	✗	✓	✓	✗	✓
MBasic	✗	✗	✗	✓	✗
M1200L	✗	✗	✗	✓	✗
M3800L	✗	✗	✗	✓	✗
M1000L_AV	✗	✗	✗	✓	✗
M4000L_AV	✗	✗	✗	✓	✗
M8000L_AV	✗	✗	✗	✓	✗
M10000L_A V	✗	✗	✗	✓	✗

	G1/G2	Lock-IDs	Anzahl der Schlie- ßungen	Bege- hungslis- te	Sektoren	Benötig- ter Spei- cher- platz	Virtuel- les Netz- werk
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗
MC3800 L	G2	128-3927	3800	✗	2-15	528	✗

	G1/G2	Lock-IDs	Anzahl der Schlie- ßungen	Bege- hungslis- te	Sektoren	Benötig- ter Spei- cher- platz	Virtuel- les Netz- werk
MC1000 L_AV	G2	128-1127	1000	19	2-15	528	✓
MC2400 L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000 L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✗	✗	✗	2-15	48	✗
M1200L	G2	128-1327	1200	✗	2-15	192	✗
M3800L	G2	128-3927	3800	✗	2-15	528	✗
M1000L_ AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_ AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_ AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000 L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✗	✗	✗	2-15	48	✗
MD1200L	G2	128-1327	1200	✗	2-15	192	✗
MD3800 L	G2	128-3927	3800	✗	n.a. (DESFi- re)	528	✗
MD2500 L_AV	G2	128-2627	2500	58	n.a. (DESFi- re)	1024	✓
MD4000 L_AV	G2	128-4127	4000	100	n.a. (DESFi- re)	1600	✓
MD1000 L_AV	G2	128-10127	10000	225	n.a. (DESFi- re)	3048	✓

	G1/G2	Lock-IDs	Anzahl der Schlie- ßungen	Bege- hungslis- te	Sektoren	Benötig- ter Spei- cher- platz	Virtuel- les Netz- werk
MD3200 L_AV	G2	128-3212 7	32000	470	n.a. (DESFi- re)	7000	✓
MD2400 L_AV	G2	128-2527	2400	34	n.a. (DESFi- re)	830	✓
MD3650 L_AV	G2	128-3777	3650	2	n.a. (DESFi- re)	830	✓

4. Realisierung gängiger WaveNet basierter Aufgaben in LSM

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.

4.1 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 Beispiel wird die prinzipielle Einrichtung eines virtuellen Netzwerks gezeigt.

Für alle Arten von virtuellen Netzwerk ist beim Einsatz von Karten ein AV-Kartentemplate erforderlich (AV = **A**udit trail / **V**irtual network).



HINWEIS

LSM Business/Professional für dauerhaften Einsatz des virtuellen Netzwerks

Die LSM Basic Online unterstützt das virtuelle Netzwerk nur eingeschränkt: Sie muss als Administrator gestartet werden und dauerhaft laufen, damit alle Funktionen gewährleistet sind.

- Verwenden Sie für den dauerhaften Einsatz des virtuellen Netzwerks eine LSM Business oder Professional.

4.1.1 Virtuelles Netzwerk mit SmartRelais 3 Advanced

4.1.1.1 Funktionsprinzip

Eine Verwendung als Gateway im virtuellen Netzwerk ist möglich. Dazu stellt der Controller eine Verbindung zum VNHost-Server her. Der VNHost-Server überträgt geänderte Berechtigungen (Programmierbedarf) und Daten von der LSM-Datenbank zum Controller. Damit ist kein vollständiges und zeitintensives Laden der Datenbank mehr erforderlich, sondern der Controller holt bei Erkennung eines Identifikationsmediums die bereitgestellten Daten ab (Pull-Prinzip). Das gesamte System wird nur über eine einzige Schnittstelle – den Controller – programmiert.

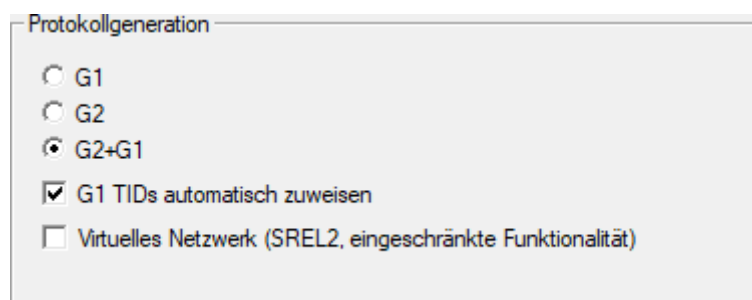
Der VNHost-Server prüft dabei in regelmäßigen Abständen, ob in der LSM-Datenbank Änderungen vorhanden sind, die über das Gateway verteilt werden sollen. Umgekehrt prüft er auch, ob am Gateway Informationen vorhanden sind, die in die Datenbank geschrieben werden sollen (siehe *Status des virtuellen Netzwerks prüfen* [► 53]).

4.1.1.2 Schließanlage einrichten

Für ein virtuelles Netzwerk mit dem SmartRelais 3 Advanced ist keine besondere Vorbereitung notwendig.

In den Schließanlageneigenschaften darf die Checkbox ☐ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) nicht aktiviert sein.

1. Öffnen Sie über | Bearbeiten | - **Eigenschaften: Schließanlage** die Eigenschaften Ihrer Schließanlage.
2. Wechseln Sie zur Registerkarte [Name].
3. Stellen Sie sicher, dass die Checkbox ☐ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) nicht aktiviert ist.



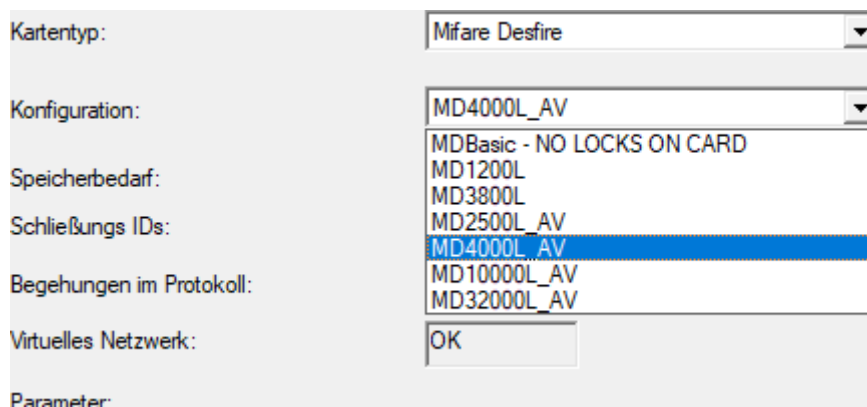
Protokollgeneration

☐ G1
☐ G2
☒ G2+G1

☒ G1 TIDs automatisch zuweisen

☐ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität)

4. Klicken Sie auf die Schaltfläche **Übernehmen**.
5. Wenn Sie Karten verwenden: Wählen Sie ggfs. in der Registerkarte [Kartenmanagement G2] ein AV-Kartentemplate aus.



Kartentyp: Mifare Desfire

Konfiguration: MD4000L_AV

Speicherbedarf:

Schließungs IDs:

Begehungen im Protokoll:

Virtuelles Netzwerk: OK

Parameter:

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

4.1.1.3 Gateway und VNHost-Server einrichten

- ✓ Schließanlage erstellt (siehe *Schließanlage einrichten* [► 49]).
 - ✓ SmartRelais 3 Advanced konfiguriert und vernetzt (siehe Systemhandbuch zum SmartRelais 3 Advanced).
 - ✓ VNHost installiert (siehe VNHost).
1. Öffnen Sie über | Bearbeiten | - **Eigenschaften: Schließung** die Eigenschaften des SmartRelais 3 Advanced (Alternative: Doppelklick).
 2. Wechseln Sie zur Registerkarte [Konfiguration/Daten].

Soll

Schließanlagen ID
9215

Schließungs ID
173

Pulslänge 2 Sek.

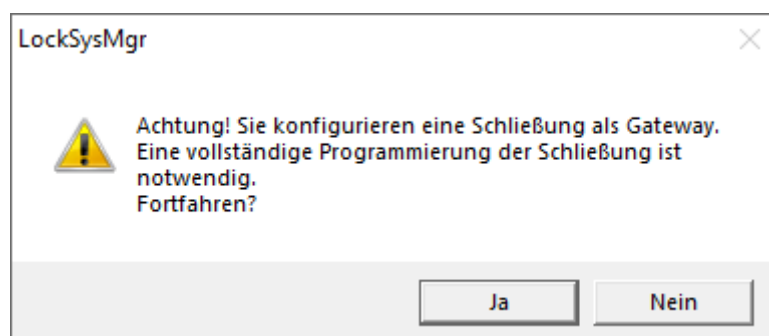
☒ Zugangskontrolle
☐ Zeitzonesteuerung
☒ Unberechtigte Zutrittsversuche protokollieren
☐ Gateway
☐ Flip Flop
☐ Keine Batteriewarnungen
☒ Nahbereichsmodus
☐ Zeitschaltung
☐ Aktivierungs- bzw. Verfallsdatum ignorieren
☒ Karteninterface

letzte Veränderung

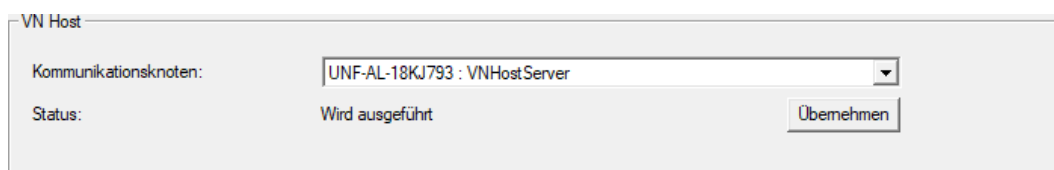
Zeitzone:	21.06.18 17:30:10
Feiertagslisten:	nicht vorhanden

Erweiterte Konfiguration

3. Aktivieren Sie die Checkboxes ☒ Zeitzonesteuerung und ☒ Zugangskontrolle.
4. Aktivieren Sie die Checkbox ☒ Gateway.
→ Warnung über anstehende Programmierung öffnet sich.



5. Klicken Sie auf die Schaltfläche **OK**.
↳ Warnung schließt sich.
6. Klicken Sie auf die Schaltfläche **Ja**.
↳ Programmierbedarf (Blitz) wird angezeigt.
7. Berechtigen Sie alle Identmedien, die später am Gateway neue Berechtigungen erhalten sollen.
8. Programmieren Sie das SmartRelais 3 Advanced.
↳ Programmierbedarf verschwindet.
9. Wählen Sie über | Netzwerk | den Eintrag **Virtuelles Netzwerk**.
↳ Fenster "VN Host Server" öffnet sich.



10. Stellen Sie sicher, dass im Bereich "VNHost" im Dropdown-Menü ▼ **Kommunikationsknoten** der Eintrag "VNHostServer" ausgewählt ist.



HINWEIS

Unterschiedliche Kommunikationsknoten am SmartRelais 3 Advanced

Für das virtuelle Netzwerk am SmartRelais 3 Advanced wird immer der VN-HostServer verwendet. Für Programmierung, Fernöffnung etc. kann dagegen auch ein anderer Kommunikationsknoten verwendet werden.

- Wählen Sie für das virtuelle Netzwerk auch dann den Eintrag "VNHostServer", wenn Ihr SmartRelais 3 Advanced noch einen anderen Kommunikationsknoten nutzt.

11. Klicken Sie ggfs. auf die Schaltfläche **Übernehmen**.
12. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "VN Host Server" schließt sich.
13. Wählen Sie über | Netzwerk | den Eintrag **Kommunikationsknoten**.

14. Wechseln Sie mit den Schaltflächen ◀ und ▶ zum VNHostServer-Kommunikationsknoten.

Name: VNHostServer

Rechnername: [empty]

Vollständiger Rechnername: [empty]

IP Port: 6001 [Port suchen]

Beschreibung: [empty]

Anschlüsse:

Typ	COM-Port

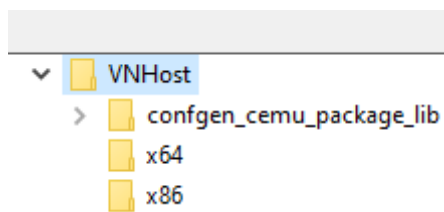
[Ping] [Konfig-Dateien] [Übertragen] [Testen] [Bearbeiten] [Hinzufügen] [Entfernen] [Verschieben]

[Neu] [Bearbeiten] [Übernehmen] [Beenden] [Hilfe]

15. Klicken Sie auf die Schaltfläche Konfig-Dateien.

→ Explorer-Fenster öffnet sich.

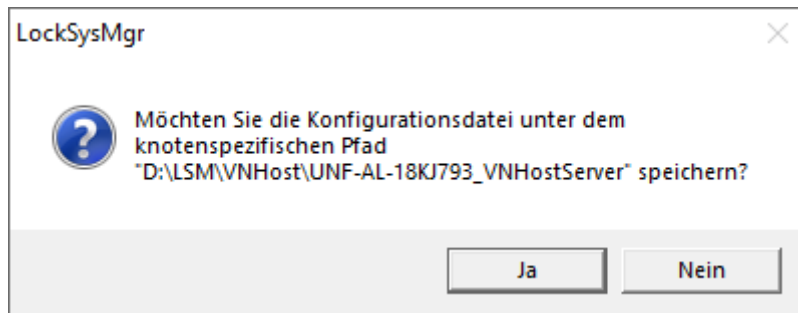
16. Markieren Sie den Installationsordner des VNHost-Servers.



17. Klicken Sie auf die Schaltfläche OK.

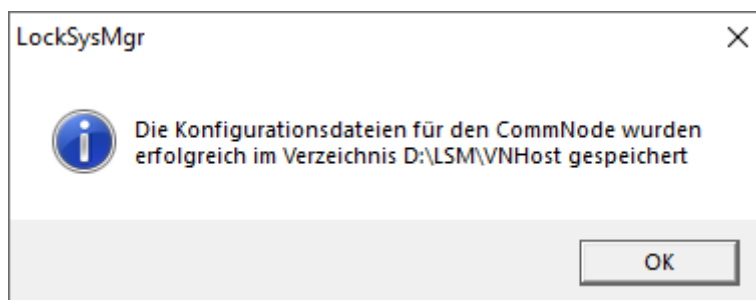
→ Explorer-Fenster schließt sich.

→ Fenster "LockSysMgr" öffnet sich.



18. Klicken Sie auf die Schaltfläche **Nein**.

↳ Konfig-Dateien sind gespeichert.



19. Klicken Sie auf die Schaltfläche **Übertragen**.

↳ Konfig-Dateien sind an den VNHostServer-Kommunikationsknoten übertragen.

20. Wenn Ihr SmartRelais 3 Advanced über einen anderen Kommunikationsknoten angebunden ist: Speichern und übertragen Sie die Konfig-Dateien auch für diesen Kommunikationsknoten.

↳ Virtuelles Netzwerk einsatzbereit.

Sie können jetzt den Status Ihres virtuellen Netzwerks beobachten (siehe *Status des virtuellen Netzwerks prüfen* [► 53]).

4.1.1.4 Status des virtuellen Netzwerks prüfen

Nach der Einrichtung Ihres virtuellen Netzwerks können Sie dessen Status beobachten.

✓ Virtuelles Netzwerk eingerichtet (siehe *Schließanlage einrichten* [► 49] und *Gateway und VNHost-Server einrichten* [► 50]).

■ Wählen Sie über | Netzwerk | den Eintrag **Virtuelles Netzwerk**.

↳ Fenster "VN Host Server" zeigt den aktuellen Status an.

VN Host Server

VN Host

Kommunikationsknoten: UNF-AL-18KJ793 : VNHostServer

Status: Wird ausgeführt Übernehmen

Aktivitäten

Eigenschaft	Wert
wird ausgeführt seit	2022.03.07 21:16:59
zuletzt aktualisiert	2022.03.07 21:17:04
Dauer der letzten Aktualisierung	0 Min. 4 Sek.
nächste Aktualisierung	2022.03.07 21:32:04
letzte partielle Aktualisierung	2022.03.07 21:23:03
Anzahl Transponder-Programmierungen	1

Neu starten

Gateways

Name	TCP/IP-Adresse	Verbindung	Letzte Kommunikation	Fehler	PHI
Post Office Lockers	192.168.100.56	verbunden	2022.03.07 21:17:10	--	07PN1RM

Anzahl 1

OK Abbrechen

Im Bereich "VNHost" sehen Sie den aktuell verwendeten Kommunikationsknoten (für virtuelles Netzwerk: "VNHostServer").

Im Bereich "Aktivitäten" sehen Sie:

- Start des VNHost-Servers
- Zeitpunkt der letzten Aktualisierung
- Zeitpunkt der nächsten geplanten Aktualisierung
- Anzahl ausstehender Programmierungen

Im Bereich finden Sie eine Auflistung aller als "CheckboxEnable" ☒ Gateway konfigurierten SmartRelais 3 Advanced und deren Status.

4.1.2 Virtuelles Netzwerk mit SmartRelais 2 G2

4.1.2.1 Funktionsprinzip

Im Gegensatz zum SmartRelais 3 wird das SmartRelais 2 G2 (SREL2.G2) nicht über ein Netzkabel angeschlossen, sondern über das WaveNet. Deshalb ist für den Betrieb eines virtuellen Netzwerks mit SmartRelais 2 G2 ein integrierter LockNode und ein RouterNode erforderlich, idealerweise ein RouterNode 2 (siehe [Komponenten anlegen und LSM einrichten \[▶ 60\]](#)).

Die LSM schickt die Daten, die im virtuellen Netzwerk verteilt werden sollen, dann über ein Netzkabel zum RouterNode 2 und anschließend über WaveNet zum SmartRelais 2 G2. Dieses arbeitet dann als Gateway.



Identmedien, die am Gateway betätigt werden, verteilen die Daten dann weiter an die Schließungen.

4.1.2.2 Schließanlage einrichten

In der (reinen) G2-Schließanlage muss die Checkbox ☒ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) aktiviert sein.

1. Öffnen Sie über | Bearbeiten | - **Eigenschaften: Schließanlage** die Eigenschaften Ihrer Schließanlage.
2. Wechseln Sie zur Registerkarte [Name].
3. Aktivieren Sie im Bereich "Protokollgeneration" die Checkbox ☒ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität).

Protokollgeneration

☐ G1

☒ G2

☐ G2+G1

☐ G1 TIDs automatisch zuweisen

☒ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität)

4. Wenn Sie Karten verwenden: Wählen Sie ggfs. in der Registerkarte [Kartenmanagement G2] ein AV-Kartentemplate aus.

Kartentyp: Mifare Desfire

Konfiguration: MD4000L_AV

Speicherbedarf: MD1200L

Schließungs IDs: MD4000L_AV

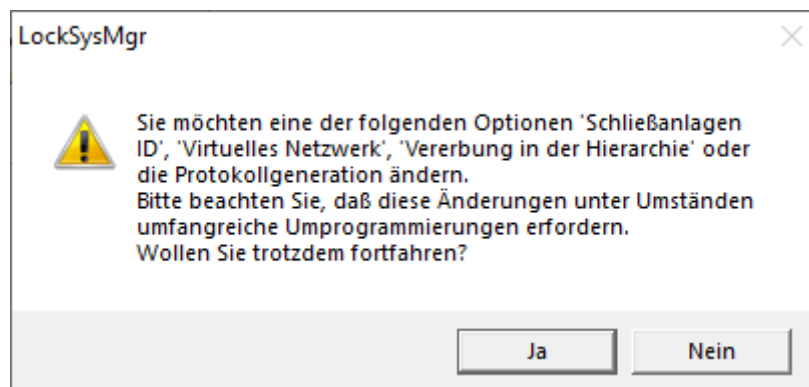
Begehungen im Protokoll: MD10000L_AV

Virtuelles Netzwerk: OK

Parameter:

- ↳ Schließanlage ist für virtuelles Netzwerk mit SmartRelais 2 G2 vorbereitet.

Wird diese Einstellung bei einer bestehenden Schließanlage angewendet, kann erheblicher Programmierbedarf entstehen.



4.1.2.3 VN Dienst einrichten

- ✓ Schließanlage eingerichtet (siehe *Neue Schließanlage anlegen* [► 10], *Neuen Transponder anlegen* [► 10] und *Neue Schließung anlegen* [► 11]).
 - ✓ Checkbox ☒ Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) aktiviert.
 - ✓ Alle Komponenten programmiert (siehe *Transponder programmieren* [► 27] und *Schließung programmieren* [► 28]).
 - ✓ SmartRelais 2 G2 vernetzt (siehe WaveNet-Handbuch).
1. Wählen Sie über | Netzwerk | den Eintrag **VN Dienst (SREL2)**.
- ↳ Fenster "VN Dienst (SREL2)" öffnet sich.

VN Dienst (SREL2)

Kommunikationsknoten: kein

TCP/IP Port: 4000

VNServer Installationspfad: ...

Import / Synchronisation

☐ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

☐ Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

OK Abbrechen

2. Wählen Sie im Dropdown-Menü ▼ **Kommunikationsknoten** den Kommunikationsknoten aus, an dem das WaveNet mit RouterNode 2 und SmartRelais 2 G2 angeschlossen ist.

VN Dienst (SREL2)

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: ...

Import / Synchronisation

☐ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

☐ Den Export zu einer bestimmten Uhrzeit ausführen

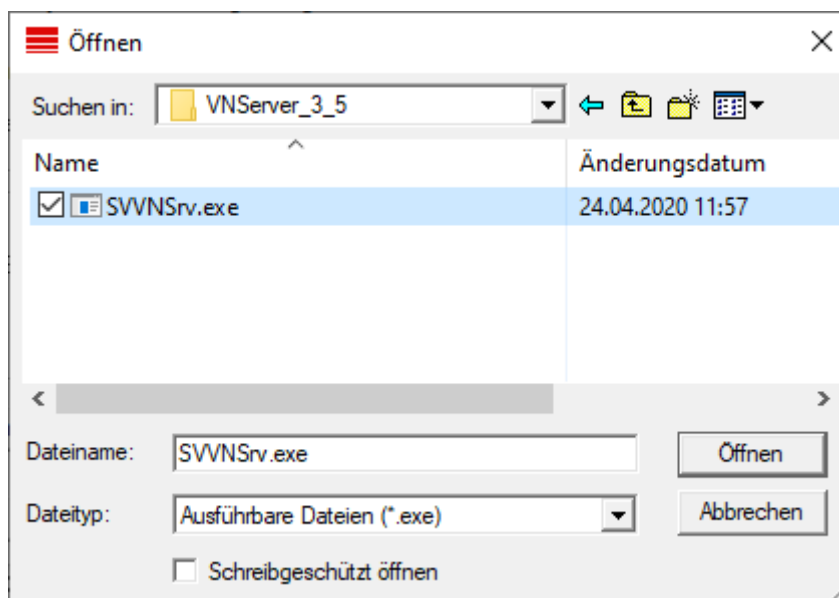
Übernehmen Testen

OK Abbrechen

3. Stellen Sie sicher, dass der TCP/IP-Port auf 4000 eingestellt ist.
4. Öffnen Sie den Explorer über die Schaltfläche ...

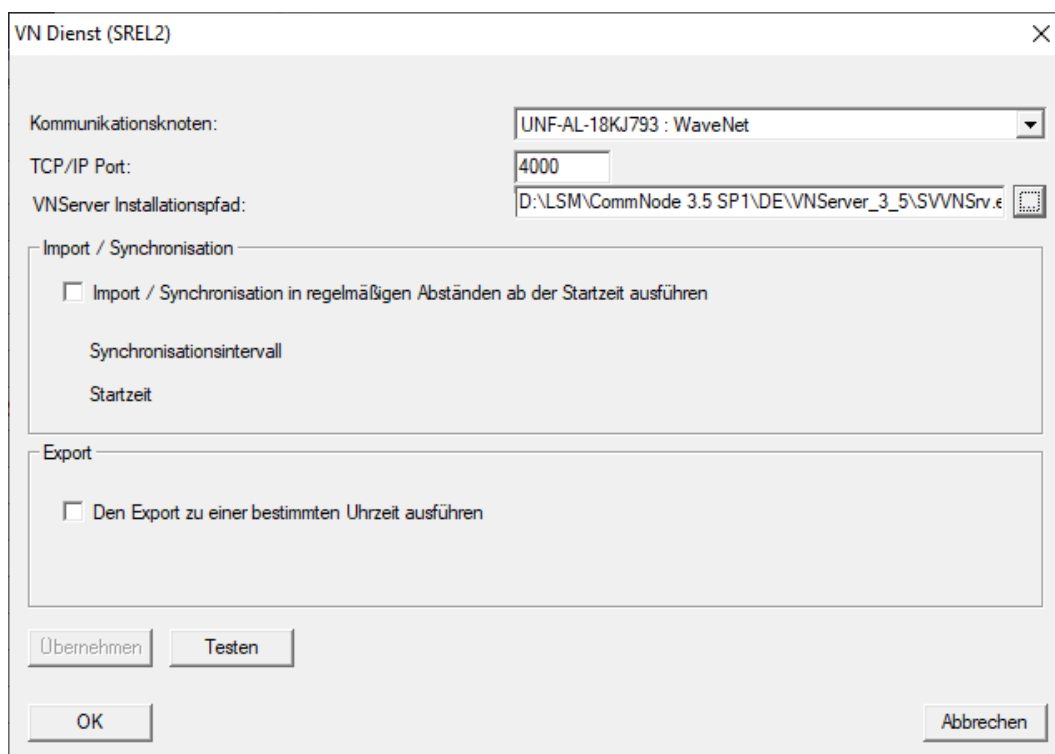
5. Wählen Sie die SVVNSrv.exe aus.

*Die SVVNSrv.exe wird zusammen mit dem CommNode-Server instal-
liert. Standardverzeichnis: (C:\Programme(x86)\SimonsVoss\VNServer_x_x)*



6. Klicken Sie auf die Schaltfläche **Öffnen**.

→ Explorer-Fenster schließt sich.



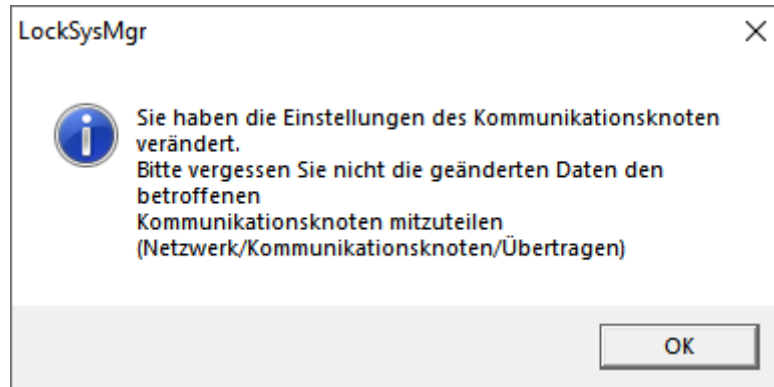
7. Optional: Stellen Sie im Bereich "Import / Synchronisation" ein, wann die Daten vom SmartRelais 2 G2 automatisch wieder in die LSM importiert werden sollen.

The screenshot shows the 'VN Dienst (SREL2)' dialog box. The 'Import / Synchronisation' section is active, with the checkbox 'Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen' checked. The 'Synchronisationsintervall' is set to 1 hour, and the 'Startzeit' is set to 20:00. The 'Export' section is inactive. Buttons at the bottom include 'Übernehmen', 'Testen', 'OK', and 'Abbrechen'.

8. Optional: Stellen Sie im Bereich "Export" ein, wann die Daten von der LSM automatisch an das SmartRelais 2 G2 übertragen werden sollen.

The screenshot shows the 'VN Dienst (SREL2)' dialog box. The 'Export' section is active, with the checkbox 'Den Export zu einer bestimmten Uhrzeit ausführen' checked. The time is set to 07:00. The 'Import / Synchronisation' section is inactive. Buttons at the bottom include 'Übernehmen', 'Testen', 'OK', and 'Abbrechen'.

9. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "LockSysMgr" öffnet sich.



10. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "LockSysMgr" schließt sich.
↳ Fenster "VN Dienst (SREL2)" schließt sich.
11. Übertragen Sie die Einstellungen zum CommNode (siehe WaveNet-Konfiguration übertragen).

4.1.2.4 Komponenten anlegen und LSM einrichten

Bevor Sie mit der Einrichtung beginnen, müssen in der LSM-Software die wichtigsten Einstellungen für den Betrieb eines Netzwerks vorgenommen und der RouterNode 2 einsatzbereit sein.

- LSM Software vorbereiten
- Hardware vorbereiten
- Kommunikationsknoten erstellen
- Taskdienst einstellen

1. Legen Sie verschiedene Identmedien (z.B. *Neuen Transponder anlegen* [► 10]) und Schließungen (z.B. *Neue Schließung anlegen* [► 11]) an.
2. Führen Sie eine Erstprogrammierung der angelegten Komponenten durch (*Transponder programmieren* [► 27] und *Schließung programmieren* [► 28]).
3. Legen Sie ein SmartRelais 2 G2 (▼ Typ "G2 Smart Relais aktiv/hybrid") an.
4. Öffnen Sie die Schließungseigenschaften.
5. Wechseln Sie zur Registerkarte [Konfiguration/Daten].

6. Aktivieren Sie die Checkbox ☒ Gateway.

Soll

Schließanlagen ID
9215

Schließungs ID
172

Pulslänge 5 Sek.

☒ Zugangskontrolle
☒ Zeitzonesteuerung
☐ Unberechtigte Zutrittsversuche protokollieren
☒ Gateway
☐ Flip Flop
☐ Interne Antenne immer an
☐ Nahbereichsmodus (nur bei interner Antenne)
☐ Zeitzumschaltung
☐ Ausnahmen im Zeitzone management zulassen
☐ Karteninterface

letzte Veränderung

Zeitzone:	nicht vorhanden
Feiertagslisten:	nicht vorhanden

Erweiterte Konfiguration

7. Wechseln Sie wieder zur Matrixansicht.
 8. Berechtigen Sie alle Identmedien am SmartRelais 2 G2, welche dort später neue Berechtigungen erhalten sollen.
 9. Führen Sie die Erstprogrammierung des SmartRelais 2 G2 durch.
 10. Stellen Sie sicher, dass im SmartRelais 2 G2 ein LockNode eingebaut ist.
 11. Richten Sie den RouterNode 2 über den WaveNet-Manager ein (siehe Netzwerk einrichten und in LSM importieren).
 12. Weisen Sie diesem das Gateway (bzw. das SmartRelais 2 G2) zu.
- ➔ Virtuelles Netzwerk ist einsatzbereit.

4.1.2.5 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. Führen Sie vor dem ersten Export einen Reset durch (siehe *Aufgaben im virtuellen Netzwerk zurücksetzen* [▶ 68]).
2. Wählen Sie über | Programmierung | - **Virtuelles Netzwerk (SREL2)** den Eintrag **Export auf VNetzwerk**.
➔ Fenster "Export auf Virtuelles Netzwerk (SREL2)" öffnet sich.

[illegible]

3. Wählen Sie alle SmartRelais 2 G2 aus, an welche die Änderungen geschickt/exportiert werden sollen.

[illegible]

- Überprüfen Sie, ob Sie im Dropdown-Menü ▼ **Schließenlage** die richtige Schließenlage ausgewählt haben.
- Klicken Sie auf die Schaltfläche **Vorbereiten**.
↳ Im Bereich "Personen" werden alle exportierbaren Änderungen aufgelistet.
- Markieren Sie alle Änderungen, die Sie auf die vorher bestimmten SmartRelais 2 G2 exportieren wollen.

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

7. Klicken Sie auf die Schaltfläche **Exportieren**.
↳ Der Exportvorgang startet. Die Änderungen werden an das Gateway
gesendet.

The screenshot shows a window titled "VNServer Meldungen" with a close button (X) in the top right corner. The window is divided into several sections:

- Top Section:** Contains three input fields: "VN Befehl:" with the value "VN Export", "Ausgegeben am:" with the value "2022.03.07 16:32:07", and "Zustand/Ergebnis:" with the value "wird bearbeitet". To the right of these fields is a "Stoppen" button and a small icon of a network switch.
- Middle Section:** Contains three input fields: "Gateway" (empty), "Letzte Meldung" with the value "2022.03.07 16:32:09", and "Aktuelle Aktion 1" with the value "Gateways aktualisieren". Below these is an empty input field for "Aktuelle Aktion 2".
- Table Section:** A table with two columns: "Name" and "Ergebnis". The table is currently empty.
- Bottom Section:** A section titled "Sonstige Aktivitäten" containing four input fields: "VN Befehl:", "Ausgegeben am:", "Zustand/Ergebnis:", and "Letzte Meldung am:". To the right of these fields is a "Wechseln" button.
- Bottom Right:** A "Beenden" button.

- ↳ Zusammenfassung des Exports wird angezeigt.

VN Ergebnis

VN Befehl: VN Export

Ausgegeben am: 2022.03.07 16:32:07

Zustand/Ergebnis: erfolgreich durchgeführt

Zusammenfassungen:

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

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
--------------	---------	------	------	------	------

Beenden

Die exportierten Aufgaben können Sie jetzt in der Übersicht nachverfolgen (*Status der Aufgaben im virtuellen Netzwerk (SREL2.G2)* [► 67]).

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 3.5 SP3 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**.

Transponder programmieren

Besitzer / Transponder: Aldrin, Lily / 005MBA8

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

☐ Nach der Programmierung zum nächsten Transponder springen

☐ Deaktivierungsquittungen / Batteriewarnungen auslesen

☒ G1 Datensätze aus fremden Schließanlagen beibehalten

Programmieren TIDs zum Deaktivieren Beenden

↪ Liste öffnet sich.

TIDs zum Deaktivieren

Schließanlage: HIMYM

☒ G2 TIDs ☒ G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

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

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

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

OK Übernehmen Abbrechen

2. 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.

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

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.

4.1.2.6 Status der Aufgaben im virtuellen Netzwerk (SREL2.G2)

Nach dem Export in das virtuelle Netzwerk können Sie die Aufgaben in einer Übersicht sehen:

- ✓ Aufgaben in das virtuelle Netzwerk exportiert (siehe *Berechtigungsänderungen exportieren* [► 61]).
- 1. Öffnen Sie über | Programmierung | - **Virtuelles Netzwerk (SREL2)** den Eintrag **Exportierte VN Aufgaben**.
 - ➡ Fenster "Exportierte VN Aufgaben" öffnet sich.

[illegible]

- ↳ Gateways werden programmiert, um die exportierten Aufgaben zurückzusetzen.

VNServer Meldungen

VN Befehl:

Reset VN Aufgaben


Ausgegeben am:

2022.03.07 16:20:33

Zustand/Ergebnis:

wird bearbeitet

Stoppen



Gateway

Letzte Meldung

2022.03.07 16:20:41

Aktuelle Aktion 1

Gateways aktualisieren

Aktuelle Aktion 2

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

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

➞ Exportierte Aufgaben sind zurückgesetzt.

VN Ergebnis

VN Befehl:

Reset VN Aufgaben

Ausgegeben am:

2022.03.07 16:20:33

Zustand/Ergebnis:

erfolgreich durchgeführt

Zusammenfassungen:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
Gateways ausgelesen	2022.03.07 16:2...	Insgesamt	0	Fehlerhaft	0
VN Quittungen wurden verarbeitet	2022.03.07 16:2...	Insgesamt		Quittungen von ...	
Geräteabgleich läuft	2022.03.07 16:2...				
Geräteabgleich läuft	2022.03.07 16:2...				
Aktualisierung Gateways abgeschlossen	2022.03.07 16:2...	Insgesamt	1	Fehlerhaft	0

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
--------------	---------	------	------	------	------

Beenden

Sie können die gewünschten Aufgaben erneut ins virtuelle Netzwerk exportieren (siehe [Berechtigungsänderungen exportieren \[► 61\]](#)).

4.1.2.8 Berechtigungsänderungen importieren

Nach dem Export der Änderungen auf das Gateway sehen Sie in der LSM-Software zunächst nicht, welche Änderungen bereits vom Gateway abgeholt wurden. Dazu müssen Sie die Änderungen erst wieder importieren:

1. Wählen Sie über | Programmierung | - **Virtuelles Netzwerk (SREL2)** den Eintrag **Import / Synchronisation**.
 ↳ Der Importvorgang startet sofort.

VNServer Meldungen

VN Befehl:

VN Import


Ausgegeben am:

2022.03.07 16:41:16

Zustand/Ergebnis:

wird bearbeitet

Stoppen



Gateway

Letzte Meldung

2022.03.07 16:41:17

Aktuelle Aktion 1

Gateways auslesen

Aktuelle Aktion 2

Übertragung der Datenpakete

Name	Ergebnis
Post Office Illumination / 00CP17B	

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

→ Importbericht wird angezeigt.

VN Ergebnis

VN Befehl: VN Import

Ausgegeben am: 2022.03.07 16:40:19

Zustand/Ergebnis: erfolgreich durchgeführt

Zusammenfassungen:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
Datenblock erfolgreich übertragen	2022.03.07 16:4...	phi	7859...	phi extension	0
Datenblock erfolgreich übertragen	2022.03.07 16:4...	phi	7859...	phi extension	0
Gateways ausgelesen	2022.03.07 16:4...	Insgesamt	1	Fehlerhaft	0
VN Quittungen wurden verarbeitet	2022.03.07 16:4...	Insgesamt		Quittungen von ...	
Geräteabgleich läuft	2022.03.07 16:4...	Insgesamt		Ausgeführt	
Aufgaben für Transponder vorbereitet	2022.03.07 16:4...	Insgesamt			
Vorverarbeitung beendet	2022.03.07 16:4...	Insgesamt	1	Fehlerhaft	0
Aktualisierung Gateways abgeschlossen	2022.03.07 16:4...	phi	7859...	phi extension	0
Datenblock erfolgreich übertragen	2022.03.07 16:4...	Insgesamt	1	Fehlerhaft	0
Aktualisierung Gateways abgeschlossen	2022.03.07 16:4...	Insgesamt	1	Fehlerhaft	0

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
--------------	---------	------	------	------	------

Beenden

2. Klicken Sie auf die Schaltfläche **Beenden**.

Sie können jetzt den Status der Aufgaben prüfen (siehe *Status der Aufgaben im virtuellen Netzwerk (SREL2.G2)* [▶ 67]).

4.1.2.9 Tipps zu VN

Zeitbudgets

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.

Der Bereich "Dynamisches Zeitfenster für Transponder G2" in den Schließanlageneigenschaften bietet Ihnen 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.

Dynamisches Zeitfenster für Transponder G2

☒ Zeitfenster am Gateway nicht verändern

☐ bis zu einer bestimmten Uhrzeit des (nächsten) Tages

☐ Stundenanzahl ab der letzten vollen Std. der Buchung

Automatischer Import/Export

Import und Export von Änderungen an ein Gateway können Sie hier automatisieren: | Netzwerk | - **VN Dienst (SREL2)**.

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.

4.2 Schließung auslesen

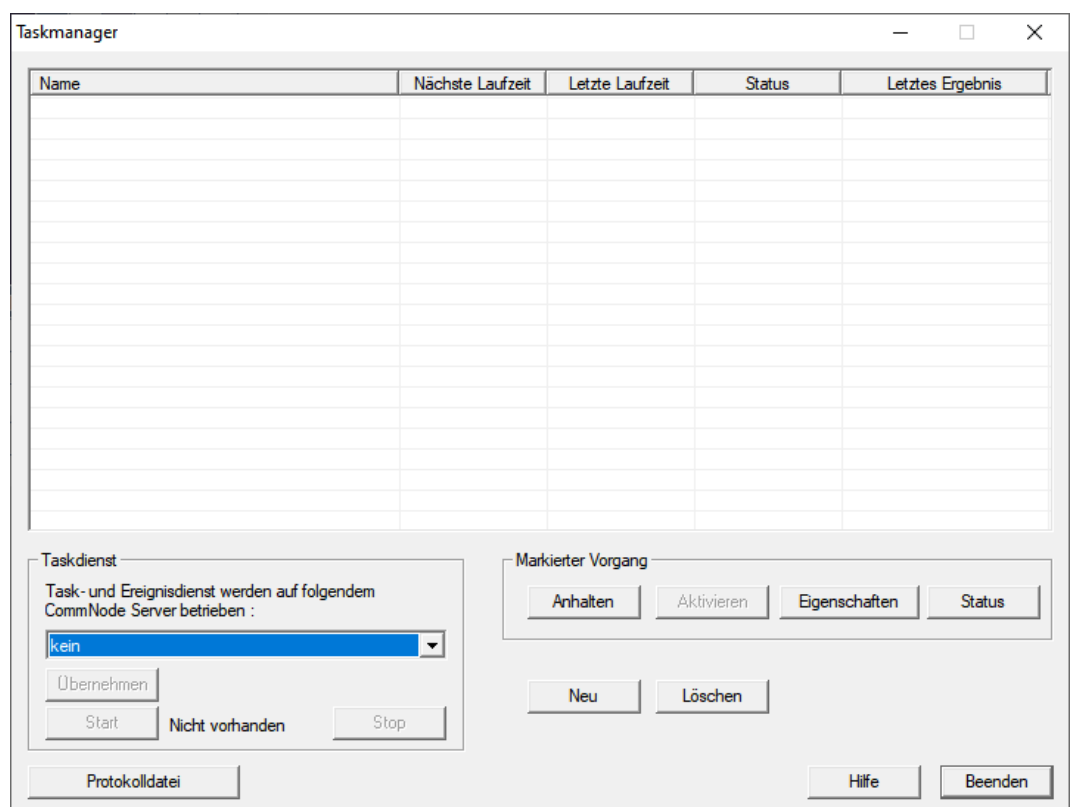
Einer der großen Vorteile von vernetzten Schließungen ist der, dass Sie den Zustand bequem von Ihrem Arbeitsplatz aus abfragen können.

Mit dem Taskmanager können Sie das sogar automatisieren.

Anschließend können Sie die Informationen in der LSM weiter verarbeiten, zum Beispiel mithilfe von Warnungen und Meldungen (siehe Warnungsmonitor und Warnungen verwalten).

- ✓ LSM geöffnet.
- ✓ Auszulesende Schließungen programmiert und vernetzt (siehe Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung).


1. Wählen Sie über | Netzwerk | den Eintrag **Taskmanager**.
↳ Fenster "Taskmanager" öffnet sich.



2. Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Task anzulegen.
↳ Fenster "Task" öffnet sich.

3. Geben Sie einen Namen für den Task ein.
4. Wählen Sie im Dropdown-Menü ▼ **Typ:** den Eintrag "Schließungsstatus auslesen" aus.



5. Wählen Sie im Bereich "Ausführen" die Option  Wiederholungsintervall aus.
6. Stellen Sie das gewünschte Intervall ein.



HINWEIS

Einfluss des Wiederholungsintervall auf die Batterielaufzeit

Je häufiger Sie die Schließung auslesen, desto öfter wird die Schließung aus dem stromsparenden Standby-Modus aufgeweckt. Die Batterielaufzeit kann deshalb kürzer sein.

Task

Name: Schließungsstatus auslesen

Beschreibung:

Typ: Schließungsstatus auslesen

Status:

☒ Aktiviert (geplanten Task wie angegeben starten)

Ausführen

☐ Einmal

☒ Wiederholungsintervall

☐ Als Reaktion auf ein Ereignis

Startzeit: 22:48

Startdatum: Freitag, 12. März 2021

Wiederholungsintervall:

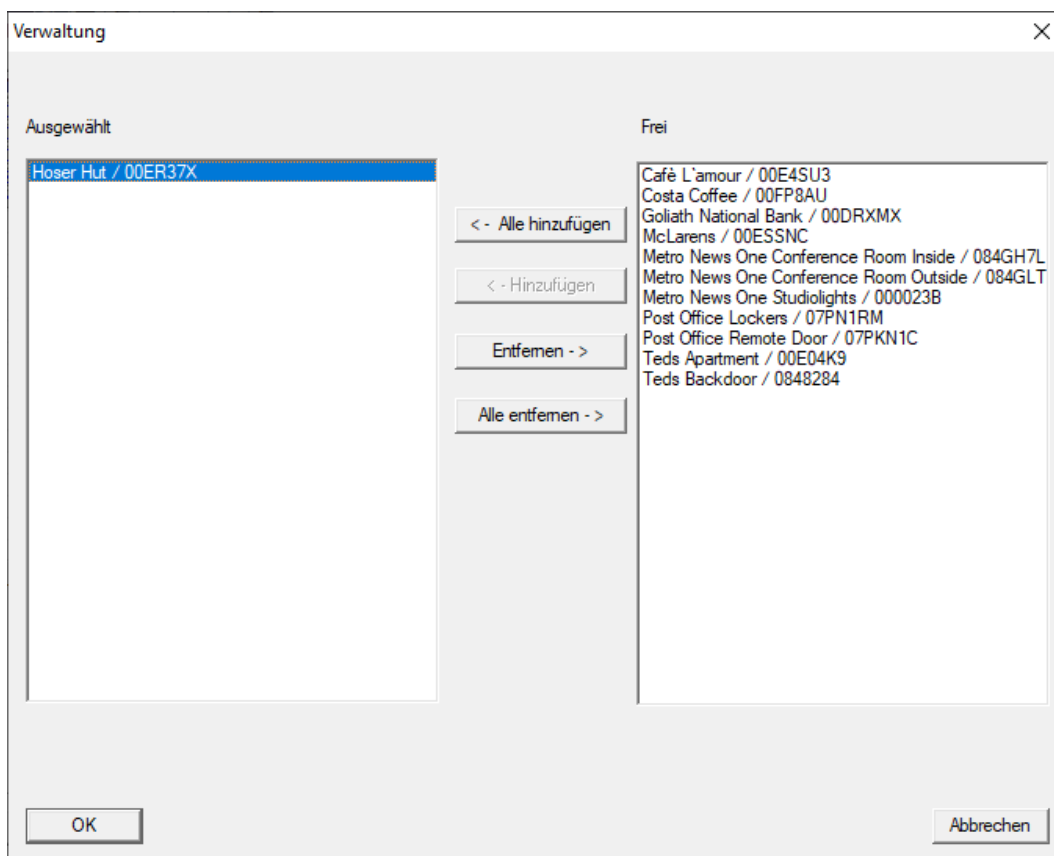
Alle 2 Minuten


Schließungen/Netzwerkknoten

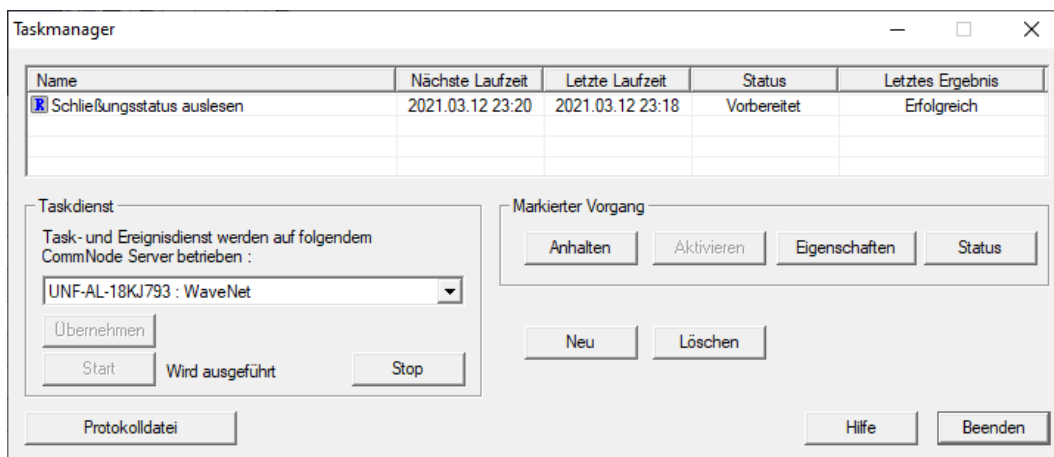
Bearbeiten Status anzeigen

OK Abbrechen

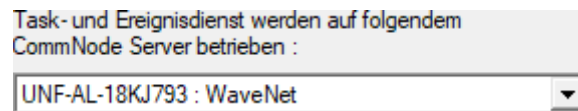
7. Klicken Sie im Bereich "Schließungen/Netzwerkknoten" auf die Schaltfläche **Bearbeiten**.
 - Fenster "Verwaltung" öffnet sich.



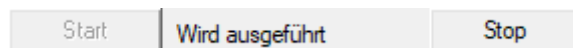
8. Wählen Sie die Schließungen aus, die Sie auslesen wollen.
9. Verschieben Sie die Schließungen anschließend mit der Schaltfläche  **Hinzufügen** in die linke Spalte.
10. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Verwaltung" schließt sich.
11. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Task" schließt sich.
↳ Task wird im Taskmanager aufgelistet.



12. Stellen Sie sicher, dass im Bereich "Taskdienst" im Dropdown-Menü ▼ Task- und Ereignisdienst werden auf folgendem CommNode Server betrieben der passende CommNode ausgewählt ist.



13. Stellen Sie sicher, dass der Taskdienst auch ausgeführt wird.



14. Klicken Sie auf die Schaltfläche **Beenden**.
- ↳ Fenster "Taskmanager" schließt sich.
 - ↳ Schließungsstatus der eingestellten Schließungen wird automatisch abgefragt.

5. Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

<https://www.simons-voss.com/de/dokumente.html>

Software und Treiber

Software und Treiber finden Sie auf der Website:

<https://www.simons-voss.com/de/service/software-downloads.html>

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

<https://www.simons-voss.com/de/zertifikate.html>

Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

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

Adresse

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Deutschland



Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen 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. Damit wird SimonsVoss als ein

Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

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).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

© 2023, SimonsVoss Technologies GmbH, Unterföhring

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts.

Der Inhalt dieses Dokuments darf nicht kopiert, verbreitet oder verändert werden. Technische Änderungen vorbehalten.

SimonsVoss und MobileKey sind eingetragene Marken der SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF

