

LSM 3.5 SP3 Business + Prof.

Handbuch

24.01.2024

Inhaltsverzeichnis

1. Allgemein	6
1.1 Allgemeine Sicherheitshinweise	6
1.2 Produktspezifische Sicherheitshinweise.....	7
1.3 Rechtliche Hinweise.....	7
1.4 Systemanforderungen.....	8
1.5 Informationen zum Handbuch.....	9
1.6 Datenschutz im System 3060.....	9
1.6.1 IT-Grundschutz	10
1.6.2 Verschlüsselung.....	10
2. Bestimmungsgemäße Verwendung.....	11
3. Bedeutung der Textformatierung.....	12
4. Installation.....	13
4.1 Software	13
4.1.1 LSM Business/Professional	13
4.1.2 VNHost	22
4.1.3 CommNode	24
5. Erste Schritte nach Neuinstallation.....	26
5.1 Empfohlener Umgang mit Kennwörtern	26
5.2 LSM registrieren.....	26
5.3 Schließanlage anlegen	31
5.3.1 Protokollgenerationen im Überblick.....	34
5.3.2 G1 Schließanlage	36
5.3.3 G2 Schließanlage	36
5.3.4 G2+G1 Mischanlage	36
5.3.5 Overlay-Modus.....	37
5.4 Datenbank automatisch sichern	37
6. Programmiergeräte.....	40
6.1 Programmiergeräte erkennen und richtig einsetzen.....	40
6.1.1 SmartCD.G2.....	40
6.1.2 SmartCD.MP	41
6.1.3 SmartCD.HF.....	41
6.1.4 SmartStick AX	42
6.2 Programmierdistanzen	43
6.2.1 Hybride Schließungen programmieren	44
6.3 Verbindung überprüfen.....	44
7. Benutzeroberfläche	45

7.1	Menüleiste.....	46
7.1.1	Datei	46
7.1.2	Datenbank.....	46
7.1.3	Ansicht.....	47
7.1.4	Assistenten.....	54
7.1.5	Bearbeiten	54
7.1.6	Berichte	104
7.1.7	Programmierung.....	113
7.1.8	Optionen.....	116
7.1.9	Netzwerk	121
7.1.10	Fenster.....	123
7.1.11	Hilfe	123
7.2	Menüband.....	124
7.3	Schließanlage.....	125
7.4	Gruppen und Bereiche	125
7.5	Matrix.....	126
8.	Hintergrundwissen zur LSM.....	129
8.1	Gruppenberechtigungen.....	129
8.1.1	Gruppenvorräte (nur G1)	130
8.1.2	Vererbung.....	130
8.2	Berechtigungen im G2 Protokoll	130
8.3	Zeitzonepläne.....	131
8.4	Übergreifende Schließebene	132
8.5	Verschlüsselung (WaveNet)	134
9.	Grundfunktionen.....	136
9.1	Neue Schließanlage anlegen.....	136
9.2	Neue Transpondergruppe anlegen.....	136
9.3	Neuen Transponder anlegen.....	136
9.4	Transponder nachträglich einer Transpondergruppe zuweisen.....	137
9.5	Neuen Bereich anlegen.....	137
9.6	Neue Schließung anlegen	137
9.7	Pin Code Tastatur anlegen.....	137
9.7.1	Pin Code Tastatur konfigurieren.....	138
9.7.2	Pin Code Tastatur im Schließplan anlegen	138
9.7.3	Pin Code Tastatur programmieren	139
9.8	Schließung einem Bereich zuweisen.....	139
9.9	Berechtigung vergeben/entziehen.....	139
9.10	DoorMonitoring Komponenten einrichten	140

9.11	Übergreifende Schließebene	140
9.11.1	Übergreifende Schließebene anlegen	141
9.11.2	Schließungen verknüpfen	141
9.11.3	Transponder verknüpfen	142
9.11.4	Transponder berechtigen.....	143
9.12	Feuerwehrtransponder erstellen	143
9.13	Datenbank manuell sichern	144
9.14	Datenschutzkonformes Arbeiten nach DSGVO.....	145
9.14.1	Daten exportieren	145
9.14.2	Daten löschen.....	148
9.14.3	Welche personenbezogenen Daten werden in der Software gespeichert?	149
9.14.4	Zu welchem Zweck werden personenbezogene Daten in der Software ge- speichert?	150
9.14.5	Wie lange werden personenbezogene Daten in der Software gespeichert?	150
9.14.6	Sind personenbezogene Daten in der Software vor dem Zugriff Dritter ge- schützt?	151
9.14.7	Können die gespeicherten Daten als Kopie zur Verfügung gestellt werden?	151
9.14.8	Können personenbezogene Daten aus der Software gelöscht werden?	151
9.15	Matrix durchsuchen.....	151
9.16	Gruppenaktionen ausführen.....	152
9.17	Transponder programmieren.....	153
9.18	Schließung programmieren.....	154
9.19	Programmieren über LSM Mobile	154
9.19.1	Mit Laptop, Netbook oder Tablet.....	154
9.20	Zeitzone(n)plan (mit Feiertagen und Betriebsferien) definieren	155
9.21	Zurücksetzen von Komponenten	157
9.22	Defekte Schließung ersetzen.....	157
9.23	Transponder sperren	158
9.23.1	Transponder dauerhaft sperren und Ersatztransponder erstellen.....	159
9.23.2	Transponder temporär sperren.....	163
9.24	Batteriezustand der Schließungen überprüfen und auswerten	164
9.25	Lagermodus bei G1-Schließungen zurücksetzen.....	166
9.26	Freezemode bei G2-Schließungen zurücksetzen.....	166
9.27	Zutrittslistenadministration.....	167
9.27.1	Zutrittslisten.....	168
9.28	Benutzer verwalten	168
9.29	Kartenmanagement	169

9.29.1	Konfiguration ändern.....	170
9.29.2	Übersicht	171
9.30	Weiterleitung von USB-Programmiergeräten zu Terminal-Servern (LSM Professional)	173
9.30.1	SmartCD.G2 / SmartCD2.G2.....	173
9.30.2	SmartCD MP / HF	178
9.30.3	SmartStick AX	190
10.	Realisierung gängiger WaveNet basierter Aufgaben in LSM.....	197
10.1	Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung	197
10.1.1	LSM Software vorbereiten.....	197
10.1.2	Erstprogrammierung der Schließkomponenten.....	197
10.1.3	Hardware vorbereiten	198
10.1.4	Kommunikationsknoten erstellen.....	199
10.1.5	Netzwerk einrichten und in LSM importieren	200
10.2	Inbetriebnahme der DoorMonitoring Schließungen.....	201
10.2.1	Mögliche (Tür-)zustände.....	201
10.2.2	DoorMonitoring-Schließungen im Netzwerk einbinden.....	202
10.2.3	DoorMonitoring-SmartHandle	203
10.2.4	DoorMonitoring-Zylinder	205
10.2.5	Controller-Inputs auswerten.....	206
10.2.6	WaveNet-Konfiguration übertragen.....	208
10.2.7	LockNode einer Schließung zuweisen	209
10.2.8	Inputereignisse der Schließung aktivieren.....	209
10.3	RingCast einrichten.....	209
10.3.1	RouterNode für RingCast vorbereiten.....	210
10.3.2	RingCast anlegen	212
10.3.3	RingCast-Funktionstest	215
10.4	Eventmanagement (Ereignisse) einrichten.....	219
10.4.1	E-Mail-Server einrichten.....	219
10.4.2	Taskdienst einstellen	219
10.4.3	Inputereignisse über den RouterNode2 weiterleiten	219
10.4.4	Inputereignisse über das SREL3-ADV-System weiterleiten.....	220
10.4.5	Reaktion erstellen	222
10.4.6	Ereignis erstellen.....	222
10.5	Virtuelles Netzwerk (VN) verwalten	228
10.5.1	Virtuelles Netzwerk mit SmartRelais 3 Advanced.....	229
10.5.2	Virtuelles Netzwerk mit SmartRelais 2 G2.....	235
10.6	Schließung auslesen.....	254
11.	Glossar & Abkürzungen	259
12.	Hilfe und weitere Informationen.....	262

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.

Abweichende Zeiten bei G2-Schließungen

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

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 Schließenanlagenpassworts

Das Schließenanlagenpasswort ist zentraler Bestandteil des Sicherheitskonzepts. Der Verlust des Schließenanlagenpassworts schränkt den Betrieb der Schließenanlage ein und ist ein Sicherheitsrisiko.

1. Bewahren Sie das Schließenanlagenpasswort sicher auf (z.B. in einem Safe)!
2. Machen Sie das Schließenanlagenpasswort 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)
- Windows-Domäne (nicht nötig bei Einzelplatzinstallationen)
- Namensauflösung (nicht nötig bei Einzelplatzinstallationen)
- .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

Server

- Prozessor: Min. 2,66 GHz mit 2 oder mehr Kernen (Intel/AMD)
(Virtuelles Netzwerk mit SmartRelais 3 Advanced und VNHost: Min. 4 Kerne, Takt abhängig von Gateway-Anzahl)

- Arbeitsspeicher: Min. 4 GB
- Festplattengröße: Anwendung ca. 500 MB
(während der Installation ca. 1 GB)
Datenbank abhängig vom Umfang der verarbeiteten Daten
- Windows Server:
 - Windows Server 2019
 - Windows Server 2022
- Virtuelle Umgebungen:
 - VMware ESXi (Version 7.0 U2) mit Windows Server 2022 und 2019
 - VMware ESXi (Version 6.5.0) mit Windows Server 2019
- Wenn CommNode-Server genutzt wird: .NET-Framework 4.0 oder neuer
- Wenn Anwendung serverbasiert genutzt wird. Freigabe auf dem Advantage-Database-Server für ein Datenbankverzeichnis



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* [► 145].

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. Bestimmungsgemäße Verwendung

Die LSM 3.5 SP3 steht für Locking System Management und ist eine datenbankgestützte Software. Mit dieser können Sie Schließpläne anlegen, verwalten und steuern.

3. 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

4. Installation

Dieses Kapitel beschreibt eine Erstinstallation der LSM Software auf einem System, auf dem noch keine ältere LSM-Version installiert ist. Für ein Update von Vorgängerverionen beachten Sie bitte das LSM Update-Handbuch. Vor jeder Änderung an einer bestehenden Installation führen Sie bitte ein aktuelles Backup durch. Es empfiehlt sich vorher ausstehenden Programmierbedarf zu bereinigen.

Die LSM Business und die LSM Professional setzen zudem den Advantage Database Server in der Version 12.x oder neuer voraus.

Das LSM Update-Handbuch dokumentiert die Aktualisierung der LSM Software.

4.1 Software

4.1.1 LSM Business/Professional

Die Installation der LSM Professional ist vergleichbar.

4.1.1.1 ADS-Server installieren und konfigurieren

Der Advantage Database Server ist ein essenzielles Tool für den Betrieb der LSM Business. Nur mit Hilfe dieses ADS-Servers kann sichergestellt werden, dass mehrere Personen simultan auf die Schließpläne in der Datenbank zugreifen können und dabei ein sicherer Datenaustausch erfolgt.

Dieses Kapitel zeigt alle notwendigen Schritte, die auf dem Server ausgeführt werden müssen.

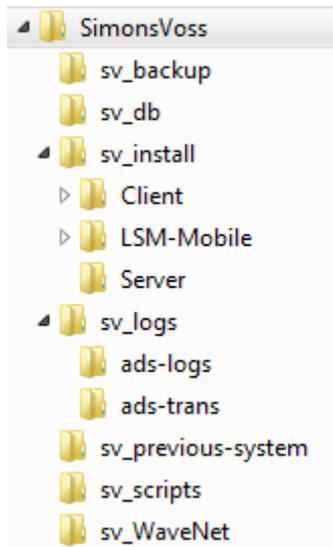


HINWEIS

Die Installation des ADS-Servers setzt einen gültigen Lizenzschlüssel (*Validation Code und Replication Code*) voraus. Wenden Sie sich mit dem SimonsVoss-Lieferschein der LSM Business Software an Ihren Bezugspartner, falls Sie noch keinen Lizenzschlüssel besitzen. Auf dem SimonsVoss Lieferschein befindet sich ein Zertifikat mit Seriennummer und Validierungscode, mit dem sich die ADS-Lizenz registrieren lässt.

Ordnerstruktur anlegen

Legen Sie bei der Installation folgende Ordnerhierarchie im Hauptverzeichnis (z.B. **C:\SimonsVoss**) an:



Ordner	Inhalt
sv_backup	Lokale Backup-Dateien zur Wiederherstellung eines früheren Stands der Schließanlage
sv_db	Schließplan
sv_install	Installationsdateien (bei Bedarf)
sv_logs	Log-Dateien des ADS-Servers
sv_previous_system	Dateien älterer LSM-Versionen
sv_scripts	Backup-Skript, das der Windows-Aufgabenplanung hinzugefügt wird
sv_WaveNet	Dateien des WaveNet-Managers

ADS-Server installieren

Installieren Sie den ADS-Server auf dem Server:

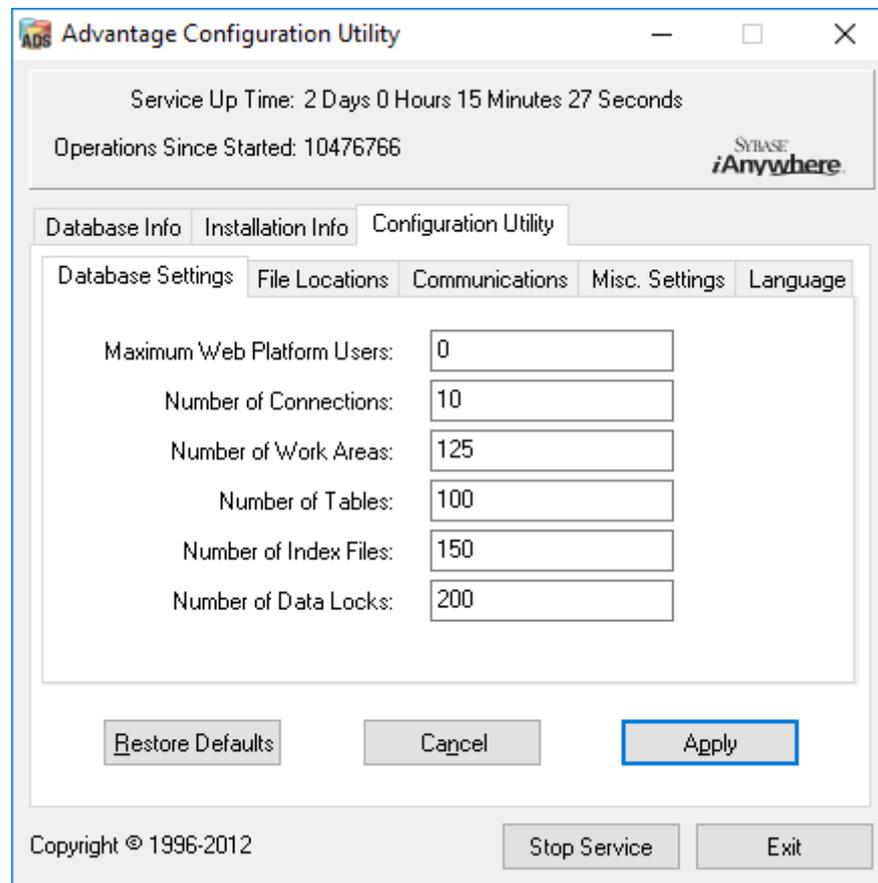
1. Starten Sie die Setup-Datei als Administrator.
2. Folgen Sie den Anweisungen der Installation.
 - ↳ Sie müssen die Lizenzbedingungen akzeptieren, um die Installation durchzuführen.
 - ↳ Geben Sie nach Aufforderung die benötigten Codes ein, um den ADS-Server ordnungsgemäß zu registrieren.

ADS-Server konfigurieren

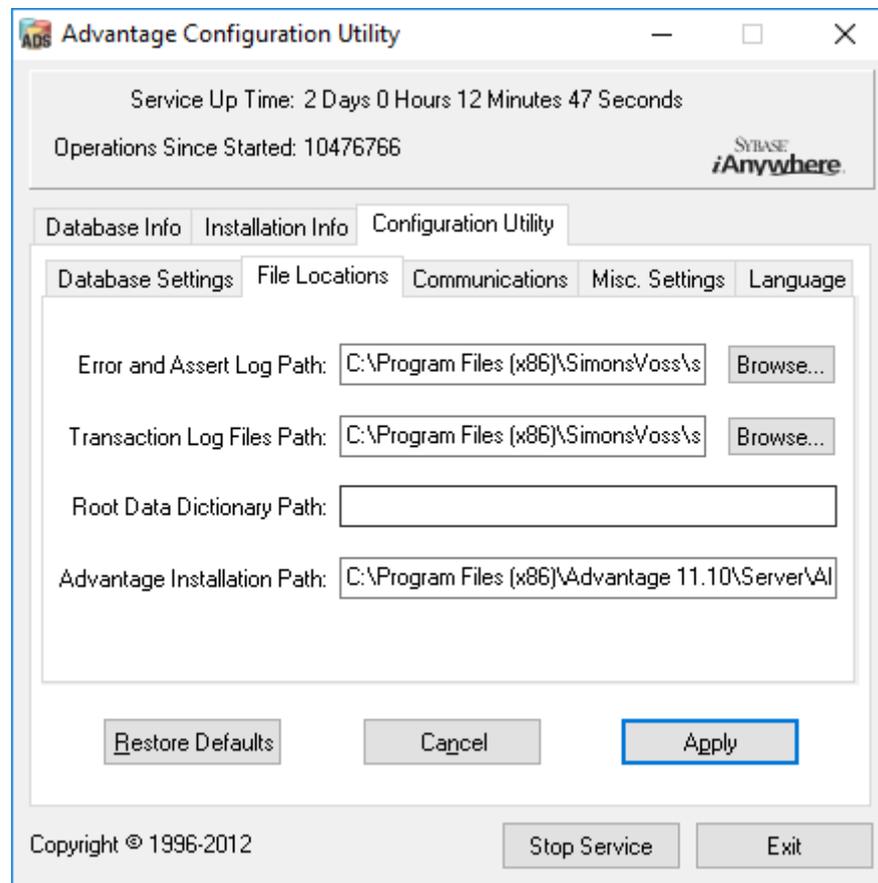
Konfigurieren Sie den ADS-Server mit Hilfe der Advantage Configuration Utility:

1. Starten Sie das Advantage Configuration Utility, z.B. über *Start/Programme/Advantage Database Server/Advantage Configuration Utility*. (Ggf. ist das Configuration Utility bereits gestartet.)

2. Wählen Sie die Registerkarte "Configuration Utility".
3. Ändern Sie folgende Eigenschaften in der Registerkarte "Database Settings" und speichern Sie diese über die Schaltfläche "Apply":

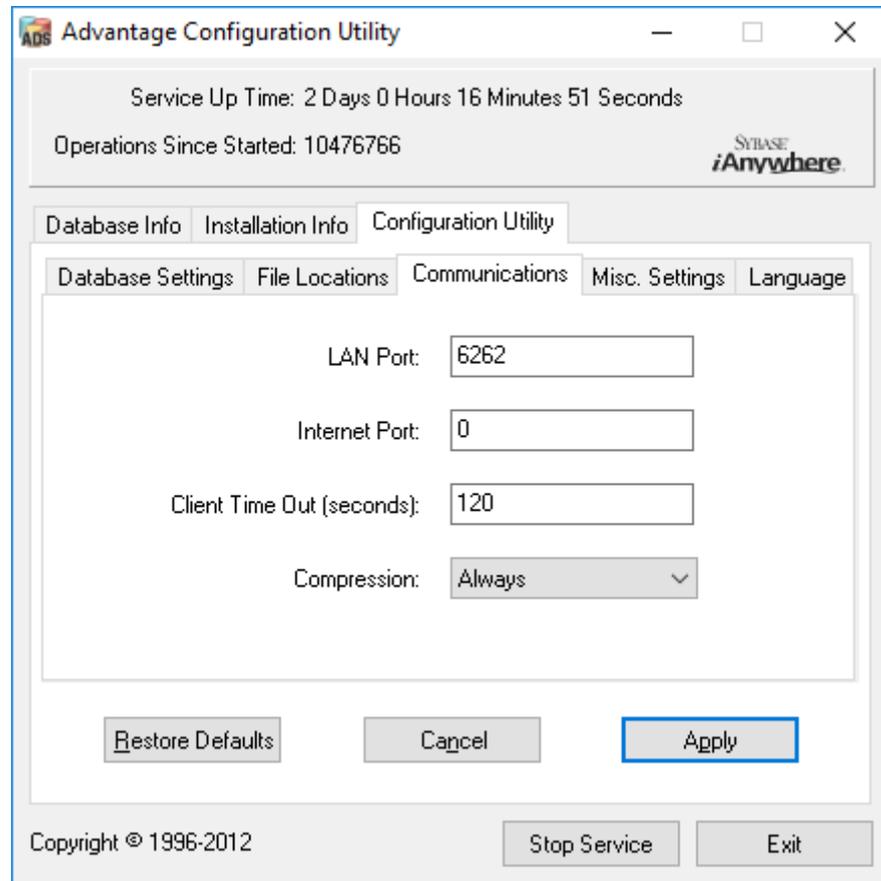


4. Ändern Sie folgende Eigenschaften in der Registerkarte "File Locations" und speichern Sie diese über die Schaltfläche "Apply":

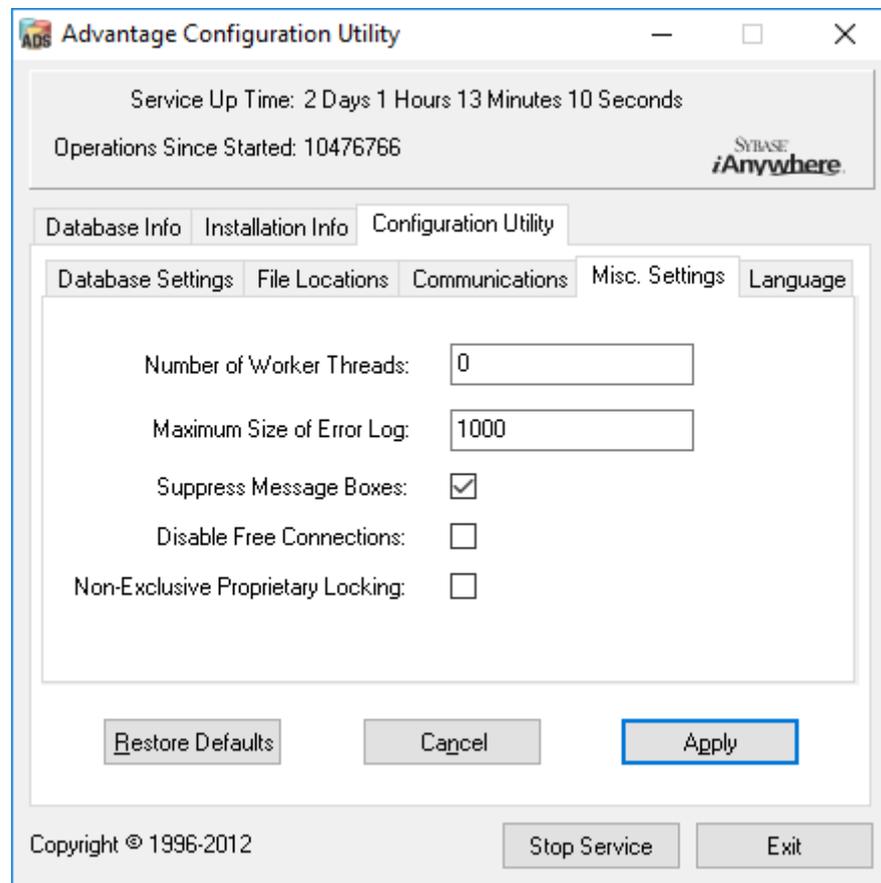


- ↳ Beachten Sie, dass der Laufwerkspfad (hier C:) von dem des Servers abweichen kann!

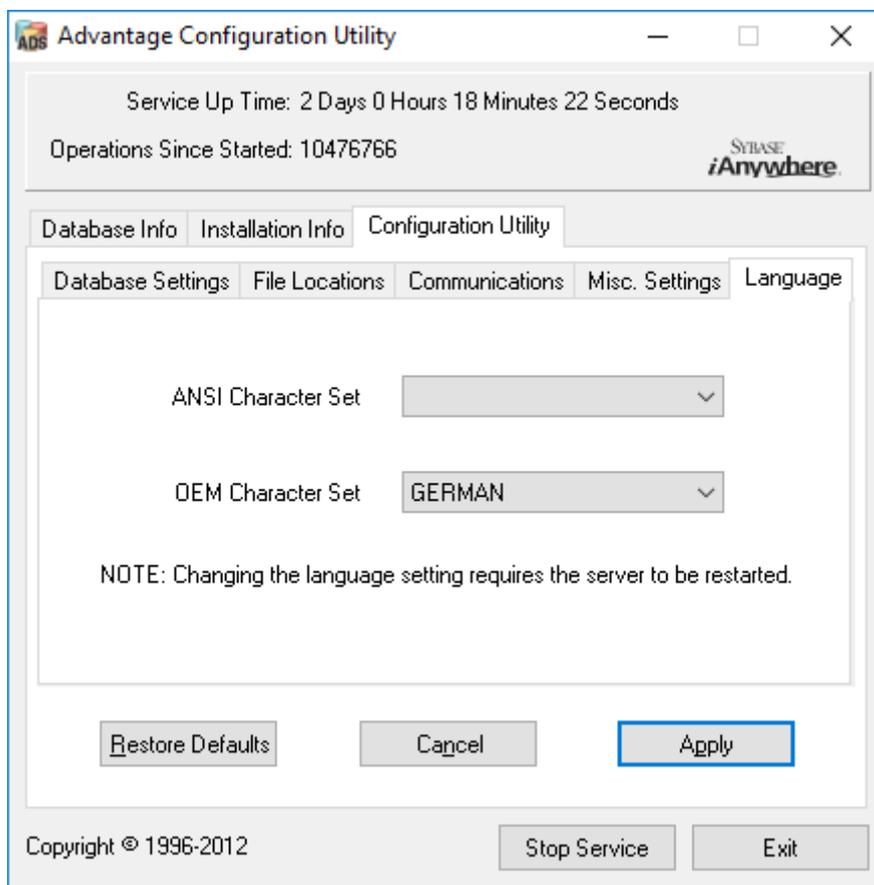
5. Ändern Sie folgende Eigenschaften in der Registerkarte "Communications" und speichern Sie diese über die Schaltfläche "Apply":



6. Ändern Sie folgende Eigenschaften in der Registerkarte "Misc. Settings" und speichern Sie diese über die Schaltfläche "Apply":



7. Ändern Sie die Spracheinstellungen in der Registerkarte "Language" nach Ihren Bedürfnissen und speichern Sie diese über die Schaltfläche "Apply":



ADS-Serverdienst überprüfen

Überprüfen Sie, ob der ADS-Serverdienst als Systemdienst automatisch ausgeführt wird:

1. Öffnen Sie die Systemsteuerung, z.B. über *Start/Systemsteuerung*.
2. Öffnen Sie den Ordner "Verwaltung".
3. Öffnen Sie den Ordner "Dienste"
4. Überprüfen Sie, ob der Dienst "Advantage Database Sever" den Status "Gestartet" besitzt und der Starttyp auf "Automatisch" eingestellt ist.
 - ↳ Ändern Sie die Werte über einen Doppelklick auf den ADS-Dienst, um ggf. Änderungen vorzunehmen.

Freigabe der Datenbank im Netzwerk

Das Verzeichnis der Datenbank "sv_db" muss im Netzwerk freigegeben werden. Richten Sie eine entsprechende Freigabe mit Leserechten ein. Es wird empfohlen, eine "Versteckte Freigabe" einzurichten. *Freigaben können versteckt werden, indem am Ende des Freigabepfades das \$-Zeichen eingefügt wird.*

4.1.1.2 LSM Business installieren und konfigurieren



VORSICHT

VNHost nach LSM installieren

Der VNHost kann nicht auf die Datenbank zugreifen, wenn die LSM noch nicht installiert ist und eine Schließanlage eingerichtet wurde. Wenn der VNHost bei der Installation keine Datenbank findet, auf die er zugreifen kann, können Probleme auftreten.

1. Installieren Sie die LSM vor dem VNHost.
2. Legen Sie eine Schließanlage an.
3. Installieren Sie den VNHost.

LSM Business installieren

Die LSM Business wird auf den gewünschten Client-Computern installiert. Diese greifen auf den ADS-Server im Netzwerk zu, welcher die Schließpläne verwaltet.



HINWEIS

Es wird empfohlen, die LSM Software direkt in einem lokalen Administrator-Benutzerprofil zu installieren! *Melden Sie sich an einem Administrator-Benutzerprofil an und wählen Sie nicht nur als einfacher Benutzer "als Administrator ausführen".*

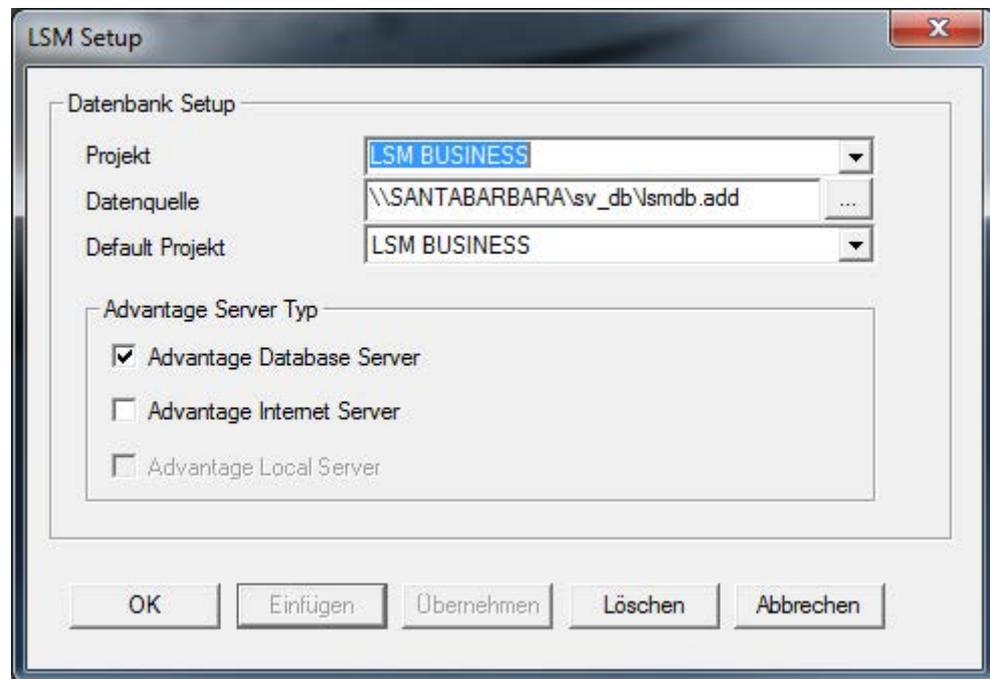
1. Starten Sie die Setup-Datei als Administrator.
2. Folgen Sie den Anweisungen der Installation.
 - ↳ Sie müssen die Lizenzbedingungen akzeptieren, um die Installation durchzuführen.
3. Starten Sie die LSM Business (*Desktopsymbol oder Start/Programme/SimonsVoss/LSM BUSINESS*)

LSM Business konfigurieren

Die LSM Business muss einmalig konfiguriert werden. In diesem Schritt wird ein leerer Schließplan auf den Server kopiert und die LSM Business so eingerichtet, dass sie auf diesen Schließplan zugreifen kann.

1. Entpacken Sie den Schließplan, welcher im LSM-Business Installationsverzeichnis (z.B. C:\Programme (x86)\SimonsVoss\LockSysMgr_3_5\db) gespeichert ist, in das Serververzeichnis "sv_db".
2. Starten Sie die LSM Business (z.B. über *Start/Programme/SimonsVoss/LSM Business*).
3. Wählen Sie "Setup".

- Bei erstmaliger Ausführung erscheint ein Fenster, in dem der Pfad der Datenbank eingestellt wird.



- ↳ Vergeben Sie einen beliebigen Projektnamen.
- ↳ Wählen Sie über die Schaltfläche "..." den Pfad auf dem Server und verweisen Sie direkt auf die lsmdb.add-Datei. Bei versteckten Freigaben muss der Pfad zur lsmdb.add direkt mit \$-Zeichen eingegeben werden; z.B.: \\<SERVER>\sv_db\$\lsmdb.add
- ↳ *In der LSM Business kann kein lokales Verzeichnis ausgewählt werden!*

- Übernehmen Sie die Einstellungen.

4.1.1.3 Crystal-Reports-Hotfix installieren

Crystal Reports wird im Hintergrund als Reportingwerkzeug eingesetzt. Das Tool wird bei der Installation der LSM Basic Online, Business und Professional automatisch installiert. Für den korrekten Betrieb ist die Installation eines aktuellen Hotfixes erforderlich.

- Starten Sie das Hotfix im .exe-Format.
- Folgen Sie den Anweisungen der Installation.
 - ↳ Sie müssen die Lizenzbedingungen akzeptieren, um die Installation durchzuführen.



HINWEIS

Installation ohne Java-Komponenten

Die Java-Komponenten (JCE) des Hotfixes werden für den Betrieb mit der LSM nicht benötigt.

- Deaktivieren Sie während der Installationsroutine die Checkbox JCE.

4.1.2 VNHost

Der VNHost greift auf die LSM-Datenbank zu und stellt verschiedene Funktionen bereit, ohne dass die LSM selbst ausgeführt wird (u.a. Gateway).



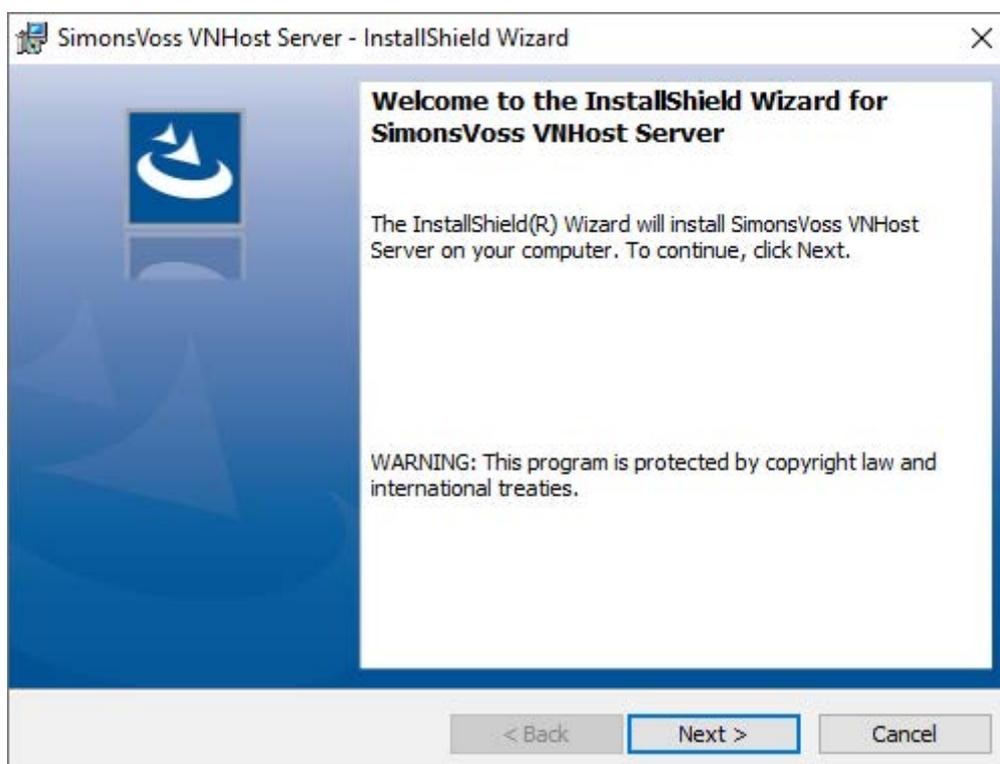
VORSICHT

VNHost nach LSM installieren

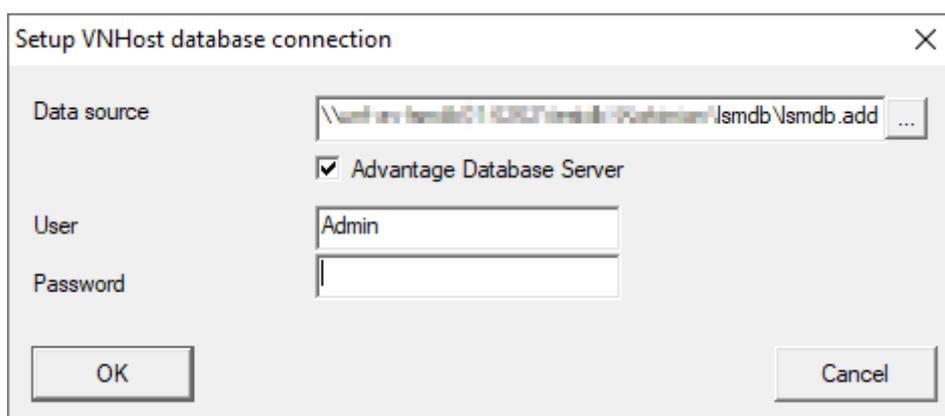
Der VNHost kann nicht auf die Datenbank zugreifen, wenn die LSM noch nicht installiert ist und eine Schließanlage eingerichtet wurde. Wenn der VNHost bei der Installation keine Datenbank findet, auf die er zugreifen kann, können Probleme auftreten.

1. Installieren Sie die LSM vor dem VNHost.
2. Legen Sie eine Schließanlage an.
3. Installieren Sie den VNHost.

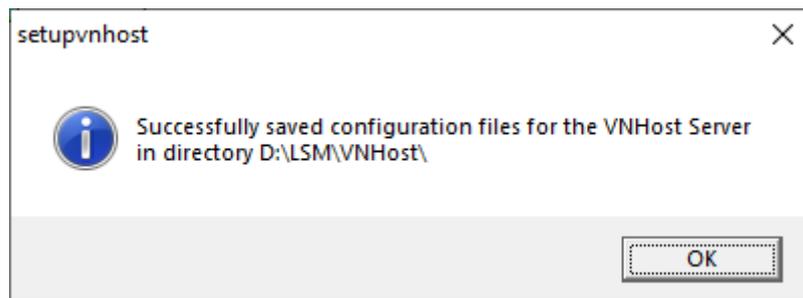
1. Führen Sie die Setup-Datei aus (vnhost_setup_3_5_sp3.exe).



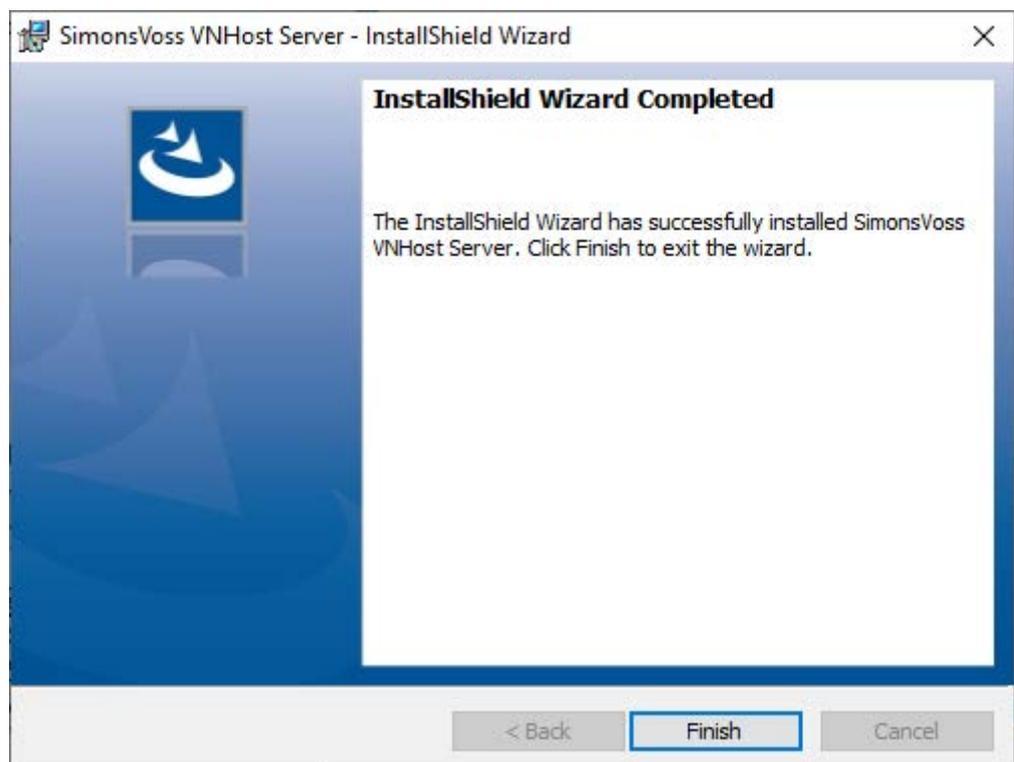
2. Folgen Sie den Installationsanweisungen und installieren Sie den VN-Host auf dem Server.
3. Geben Sie im Fenster "Setup VNHost database connection" den UNC-Pfad zu Ihrer lsmdb.add an (kann aus dem LSM-Anmeldefenster kopiert werden).



4. Geben Sie Ihren LSM-Benutzernamen und Ihr LSM-Benutzerpasswort an.
5. Wenn Ihre lsmdb.add lokal installiert ist: Deaktivieren Sie die Checkbox Advantage Database Server.
6. Klicken Sie auf die Schaltfläche **OK**.
↳ Verbindung zwischen VNHost und Datenbank wird hergestellt.



↳ Installation abgeschlossen.



4.1.3 CommNode

Sie installieren den CommNode-Server mithilfe der Setup-Datei. Sollte der CommNode-Dienst anschließend nicht unter den Windows-Diensten gelistet sein (SimonsVoss CommNode-Server), dann müssen Sie die Installation mit einer Batch-Datei ausführen.

1. Rufen Sie das Installationsverzeichnis des CommNode-Servers (**C:\Program Files (x86)\SimonsVoss\CommNodeSvr_3_5**) auf.
 2. Führen Sie die Batch-Datei `install_CommNodeSvr` mit Administratorrechten aus.
 - ↳ Kommandozeile öffnet sich.
 - ↳ CommNode-Server wird installiert.
- ↳ CommNode-Server ist installiert und unter den Windows-Diensten gelistet.

4.1.3.1 Kommunikationsknoten erstellen

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

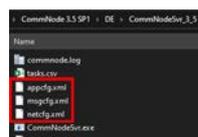
1. Öffnen Sie die LSM-Software.
2. Wählen Sie | Netzwerk | **Kommunikationsknoten**.
3. Ergänzen Sie die Informationen "Name", "Rechnername" und "Beschreibung".

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

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

↳ z.B. UNF-AL-18KJ793; UNF-AL-18KJ793.ALLEGION.COM;
Kommunikationsknoten für das WaveNet-Funknetzwerk 123

4. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.
5. Vergewissern Sie sich, dass der Pfad auf das Installationsverzeichnis des CommNode-Servers verweist und klicken Sie auf die Schaltfläche **OK**.
6. Quittieren Sie die Meldung mit **Nein** und bestätigen Sie die Auswahl mit **OK**. Die drei Konfigurations-XMLs (appcfg, msgcfg und netcfg) müssen direkt im Installationsverzeichnis des CommNode-Servers liegen.



7. Speichern Sie Ihre Einstellungen über die Schaltfläche **Übernehmen**.
8. Quittieren Sie den Hinweis über die Schaltfläche **OK**.
9. Beenden Sie den Dialog über die Schaltfläche **Beenden**.

5. Erste Schritte nach Neuinstallation

5.1 Empfohlener Umgang mit Kennwörtern

In der LSM Software werden grundsätzlich zwei Arten von Kennwörtern eingesetzt:

■ Benutzerkennwort

Das Benutzerkennwort wird zur Anmeldung am Schließplan bzw. der Datenbank benötigt.

■ Schließanlagenpasswort

Das Schließanlagenpasswort wird in alle SimonsVoss-Komponenten einprogrammiert. Dieses Schließanlagenpasswort ist im Schließplan bzw. der Datenbank in einem verschlüsselten Bereich gespeichert und kann nicht ausgelesen werden. Programmierte SimonsVoss-Komponenten können nur neu programmiert werden, wenn der Datenbank das Schließanlagenpasswort bekannt ist!

Nachfolgend zwei Empfehlungen zum sicheren Verwalten von Kennwörtern:

- Für eine erhöhte Sicherheit der gesamten Schließanlage sollte das Schließanlagenpasswort in mindestens zwei Teile aufgeteilt werden, die von den einzelnen Personen individuell vergeben werden.
- Es wird dringend empfohlen, das Administrator- und Schließanlagenpasswort aufzuschreiben und an unterschiedlichen Orten sicher und für Dritte unzugänglich aufzubewahren!

Der Schließanlagenbetreiber sollte sich stets über eine Frage im Klaren sein: was passiert, wenn die einzige Person, die das Schließanlagenpasswort (oder einen Teil davon) kennt, auf einmal nicht mehr zur Verfügung steht.

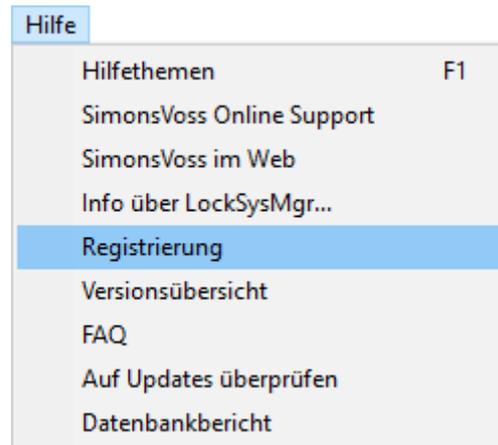
5.2 LSM registrieren

Die LSM muss registriert werden. Dazu wird eine Registrierungsdatei erstellt und an eine dafür bereitstehende E-Mail-Adresse geschickt. Sie erhalten automatisch eine Antwort, die Ihre persönliche Lizenzdatei enthält. Mit dieser Lizenzdatei können Sie die LSM mit den von Ihnen bestellten Modulen registrieren.

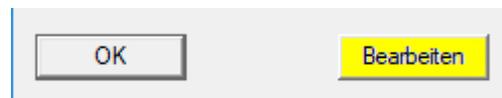
Vorgehen

- ✓ LSM-Installation ist durchgeführt.
- ✓ Lieferschein mit Registrierungsinformationen liegt vor.
- ✓ E-Mail-Versand möglich.

1. Klicken Sie im Reiter | Hilfe | auf den Eintrag **Registrierung**.
↳ Fenster "Registrierung" öffnet sich.



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

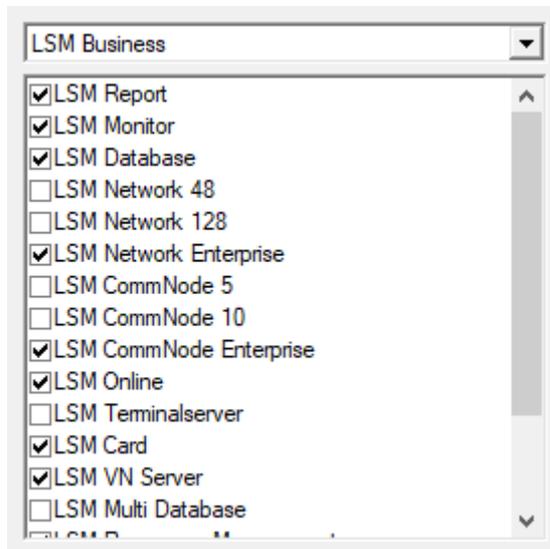


- ↳ Fenster "Registrierung bearbeiten" öffnet sich.

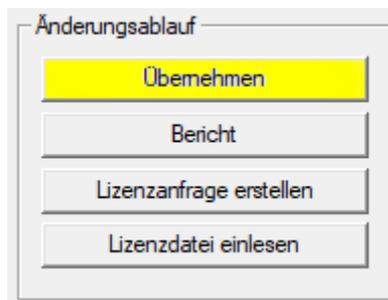
3. Füllen Sie das Formular aus.

Firma:	SimonsVoss		
Adresse:	FeringasträÙe 4		
Stadt:	Untereöhing	PLZ:	85774
Land:	Deutschland		
Ansprechpartner:			
Tel:		Fax:	
E-Mail:			

4. Stellen Sie sicher, dass die richtige Edition ausgewählt ist (Beispiel: Business).

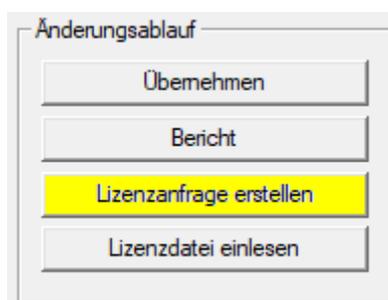


5. Klicken Sie auf die Schaltfläche **Übernehmen**.

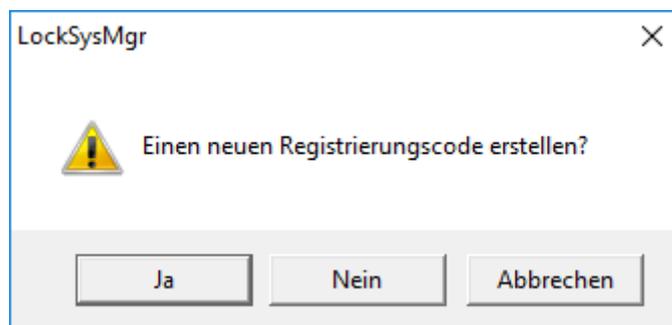


↳ Datensatz ist gespeichert.

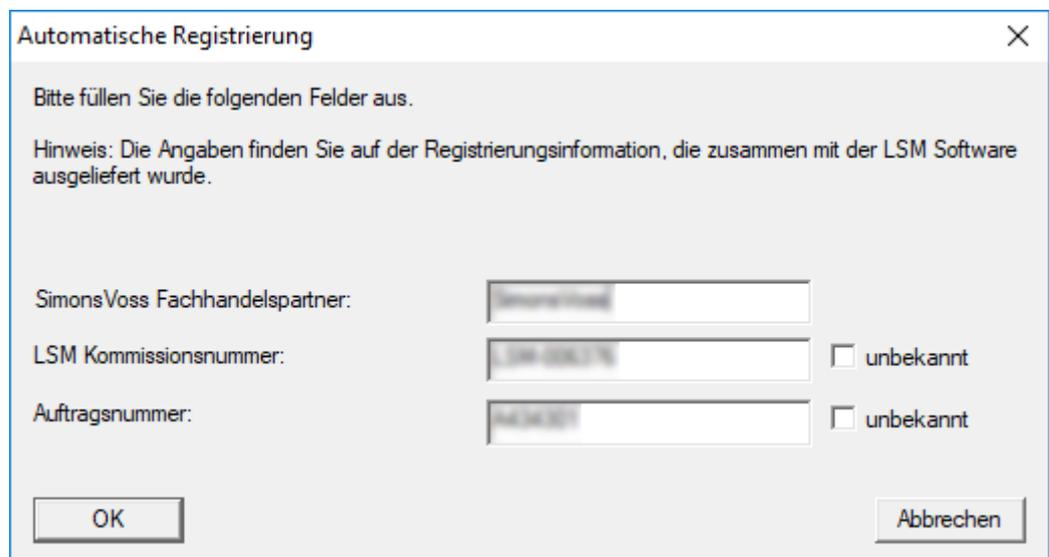
6. Klicken Sie auf die Schaltfläche **Lizenzanfrage erstellen**.



7. Klicken Sie auf die Schaltfläche **Ja**, um die Rückfrage zu bestätigen.



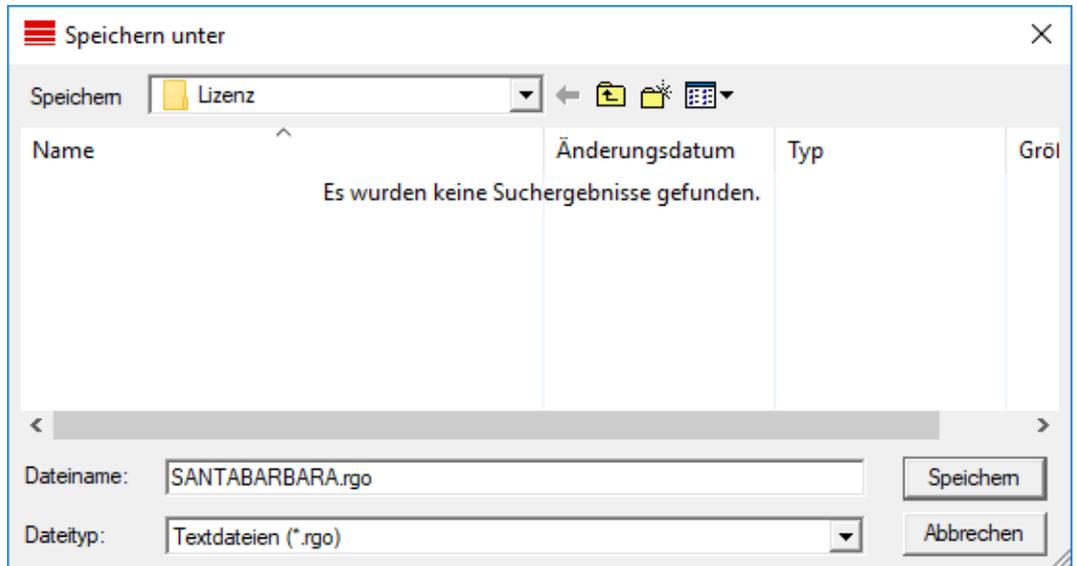
8. Füllen Sie das Formular aus (LSM-Kommissionsnummer im Format LSM-xxxxxx, Auftragsnummer im Format Axxxxxx).



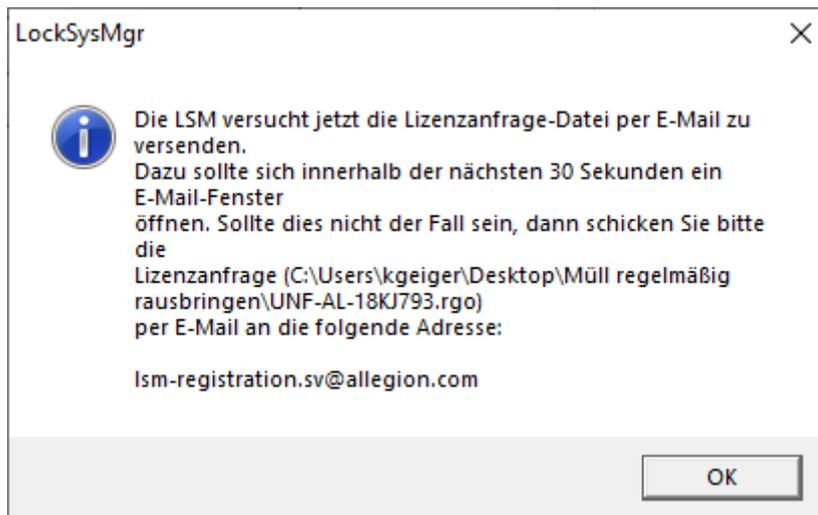
9. Klicken Sie auf die Schaltfläche **OK**.

- ↳ RGO-Datei wird erstellt.
- ↳ Explorer-Fenster öffnet sich.

10. Speichern Sie die RGO-Datei in einem Verzeichnis Ihrer Wahl.



11. Klicken Sie auf die Schaltfläche **OK**.



↳ Standard-E-Mail-Client öffnet sich. Eine entsprechende E-Mail mit der RGO-Datei im Anhang ist vorgefertigt.

12. Wenn die RGO-Datei nicht angehängt ist, dann hängen Sie sie manuell an.

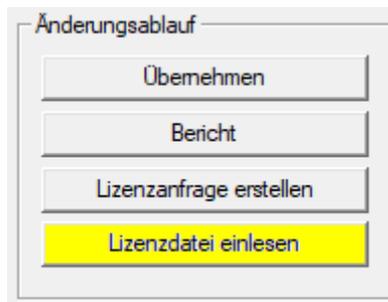
13. Versenden Sie eine E-Mail mit der RGO-Datei an lsm-registrati-on.sv@allegion.com.

↳ Antwort mit angehängter LIC-Datei trifft automatisch ein.

14. Speichern Sie die LIC-Datei in einem Verzeichnis Ihrer Wahl.

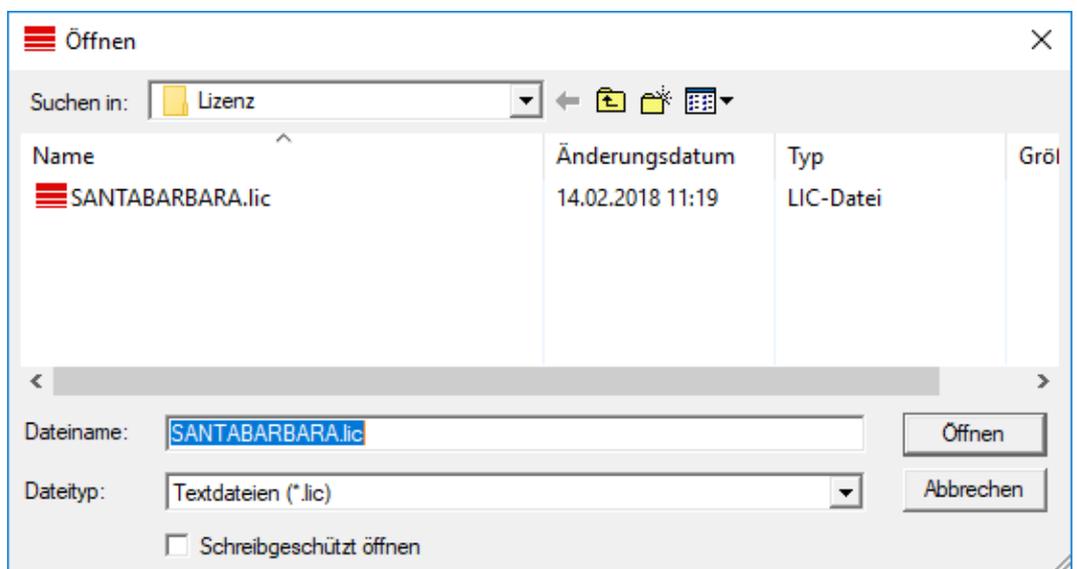
15. Wechseln Sie zurück zur LSM.

16. Klicken Sie auf die Schaltfläche **Lizenzdatei einlesen**.



↳ Explorer-Fenster öffnet sich.

17. Wählen Sie die LIC-Datei aus.



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

19. Klicken Sie auf die Schaltfläche **OK**, um den Hinweis zu bestätigen.

20. Starten Sie die LSM neu.

↳ Registrierung ist durchgeführt.

5.3 Schließenanlage anlegen

Passwort festlegen

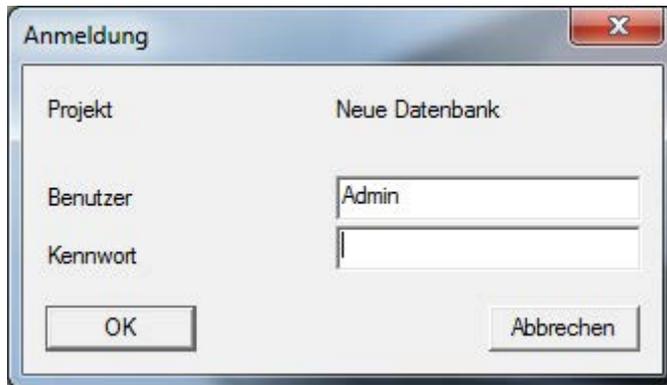
Wenn Sie bereits ein Projekt erstellt haben, können Sie nun eine Schließenanlage anlegen.



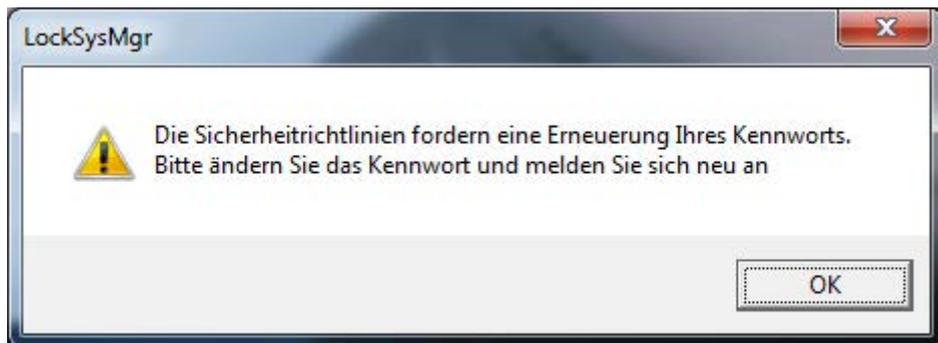
HINWEIS

Beim Anlegen des ersten Schließplans in der LSM BUSINESS oder LSM PROFESSIONAL wird dieser Prozess durch die Lizenzierung unterbrochen. Die Lizenzierung weiterer Module ist bei der LSM BASIC optional.

1. Klicken Sie auf "Anmelden" im Hauptmenü der LSM Software. Vergewissern Sie sich ggf. unter "Setup", ob das richtige Projekt ausgewählt ist.
2. Geben Sie das Default-Passwort "system3060" ein.



3. Bestätigen Sie den Warnhinweis mit einem Klick auf "OK".



4. Geben Sie das Default-Passwort "system3060" erneut ein und legen Sie danach ein neues Benutzerkennwort fest.





HINWEIS

Das Benutzerkennwort wird bei jedem Anmeldevorgang an der Datenbank abgefragt. Bei der LSM Business können mehrere Benutzer mit verschiedenen Kennwörtern und Rechten angelegt werden.

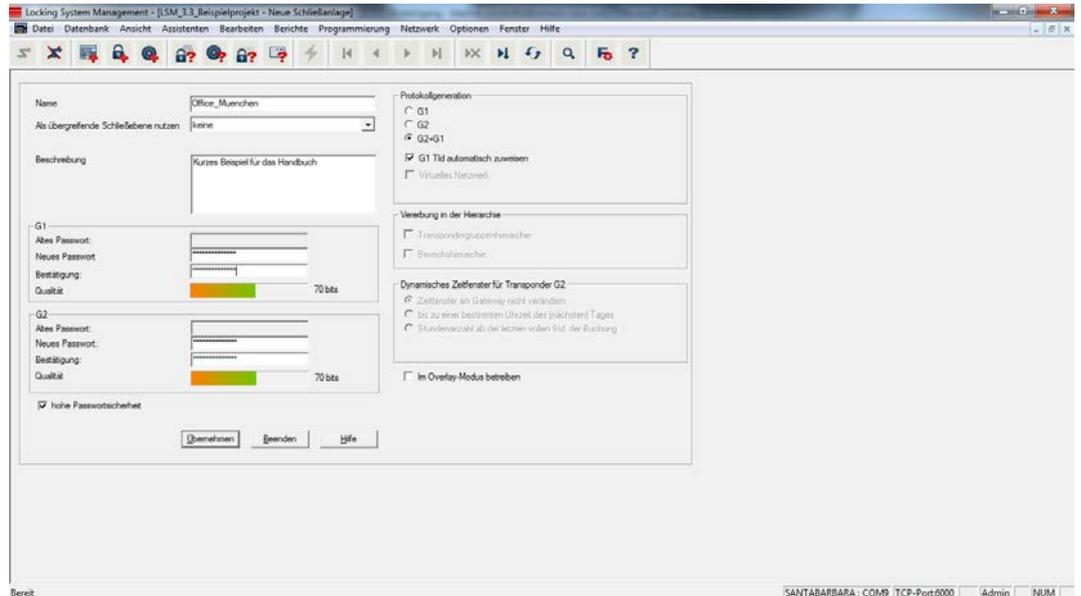
Schließanlage erstellen

1. Gleich nach der Vergabe eines neuen Passworts meldet sich ein Einrichtungsassistent:



2. Wählen Sie "eine neue Schließanlage anlegen", um eine komplett neue Schließanlage anzulegen. Bestätigen Sie mit "OK".

- Legen Sie die Charakteristiken der neuen Schließanlage fest und vergeben Sie sichere Passwörter. *Nachträgliche Änderungen sind zu einem späteren Zeitpunkt jederzeit möglich; nach einer Erstprogrammierung der Komponenten aber wegen der entstehenden Programmierbedarfe sehr aufwändig.*



- Legen Sie die neue Schließanlage durch einen Klick auf "Übernehmen" an.
- Klicken Sie auf "OK", um direkt zur neuen Schließanlage zu gelangen.



HINWEIS

Das Schließanlagenpasswort wird in alle SimonsVoss-Komponenten einprogrammiert und mit der LSM Software verwaltet! Ohne dieses Schließanlagenpasswort können keine Änderungen an programmierten Komponenten vorgenommen werden, was von der LSM Software auch angezeigt wird. *Beachten Sie das Kapitel [Empfohlener Umgang mit Kennwörtern](#) [▶ 26], um einen reibungslosen Betrieb der Schließanlage zu gewährleisten.* Wird das Schließanlagenpasswort geändert, müssen alle programmierten Komponenten neu programmiert werden!

5.3.1 Protokollgenerationen im Überblick

	G1	G2
Verwaltung von Zutrittsrechten:	Schließungen	Schließung und Identmedium (VN nur Identmedium)
Anzahl Schließungen:	16.000	64.000

	G1	G2
Zahl Transponder:	8.000	64.000
Anzahl SLA auf einem Transponder:	3	4 x G2 + 3 x G1
Zeitzonengruppen:	5+1	100+1
Speicherbare Zutritte auf einer Schließung:	Zylinder 1.000	Zylinder 3.000 Smart-Relais 3.600 (200 als Gateway)
Begehungsliste auf Transponder:	Nein	1,000 pro G2-Schließplan(inkl. Datum, Zeit, Schließungs-ID)
Vorgehen Gruppenverwaltung:	Einstellbar; Anzahl wird in der Gruppe definiert	Keine Voreinstellung nötig; Rechte und Ausnahmen werden auf TRAIgetragen
Ersatztransponder:	7 Ersatz-TRA via Overlay-Modus	Keine Voreinstellung notwendig
Netzwerkfähig:	Ja	Ja
Virtuelles Netzwerk:	Nein	Ja, SperrIDs in VN mitgeben
Einkuppeldauer:	5 Sek. oder 10 Sek.	1 Sek. bis 25 Sek.; Einkuppelzeit beim TRA kann individuell verdoppelt werden, max. 25 Sek.
Zeitbefristete Berechtigung:	Ja	Ja
Batteriewarnung:	Stufe 1; Stufe 2; Lagermodus	Stufe 1; Stufe 2; Freeze-Modus
Batteriewechsel:	SmartCD	Batteriewechsel-TRA zusammen mit berechtigtem TRA oder SmartCD
LSM/LDB:	Alle Versionen	Ab LSM3.0
Aktiv / Passiv:	Ja / Ja	Ja / Ja

5.3.2 G1 Schließanlage

Der G1-Standard stellt die erste Protokollgeneration von SimonsVoss dar. Dieser Standard ist kompatibel mit dem Vorgänger der LSM Software: Der LDB Locking Database Software.



HINWEIS

Nutzen Sie dieses mittlerweile veraltete Protokoll nur, wenn Sie bereits bestehende Schließanlagen in der G1-Welt verwalten müssen. Für eine zeitgemäße Schließanlage wird der Einsatz von G2-Protokollen mit aktuellen G2-Komponenten empfohlen.

5.3.3 G2 Schließanlage

G2 steht für die aktuelle Protokollgeneration für SimonsVoss Komponenten. Das G2-Protokoll bietet viele Verbesserungen gegenüber dem Vorgängerprotokoll G1.



HINWEIS

Nutzen Sie nach Möglichkeit immer das G2-Protokoll. Nur mit diesem Protokoll und den dazu passenden G2-Komponenten kann eine Schließanlage nach aktuellem Stand der Technik realisiert und verwaltet werden.

5.3.4 G2+G1 Mischanlage

Die Vorteile einer Mischanlage (*G1- und G2-Komponenten in einer Schließanlage gleichzeitig zu nutzen*) gehen zunächst mit kleineren Nachteilen (*schlechte Übersicht über eingesetzte Komponenten, keine richtige G2-Experience*) einher.

Mischanlagen operieren grundsätzlich in der G1-Welt. Der einzige Vorteil einer Mischanlage ist, dass hier gleichzeitig G2-Komponenten eingesetzt werden können. Die G2-Komponenten werden durch die Mischanlage jedoch in ihrem Einsatz eingeschränkt.

Das gleichzeitige Betreiben von älteren G1-Komponenten und aktuellen G2-Komponenten kann über die Mischanlage grundsätzlich ermöglicht werden. Die abwärtskompatible Unterstützung von älteren Komponenten ermöglicht eine effiziente Nutzung bereits bestehender bzw. eingesetzter Komponenten. Gerade für solche Sonderfälle ist diese Funktion prädestiniert. Auf einzelne, besonders komfortable Eigenschaften von G2-Komponenten, muss jedoch verzichtet werden.

5.3.5 Overlay-Modus

Der Overlay-Modus kann nur in der Protokollgeneration "G1" oder "G2 + G1" aktiviert werden.

Der Overlay-Modus ermöglicht eine sehr komfortable Eigenschaft in der eingeschränkten G1-Protokollgeneration: Die Tatsache, neu programmierte Transponder direkt ohne Neuprogrammierung der Schließung einzusetzen. Diese Eigenschaft funktioniert nur bedingt für bis zu 7 neu angelegte Transponder.

In der G2-Protokollgeneration können solche Programmierungen grundsätzlich beliebig über den Transponder oder die Schließung vorgenommen werden.

Bei aktiviertem Overlay-Modus werden für jede Transponder-ID zusätzlich 7 weitere Transponder-IDs angelegt:

Transponder-IDs starten ab ID 64

- Transponder 1 mit Transponder-ID 64: Die Transponder-IDs 65 - 71 werden zusätzlich reserviert.
- Transponder 2 mit Transponder-ID 72: Die Transponder-IDs 73 - 79 werden zusätzlich reserviert.
- Transponder 3 mit Transponder-ID 80: Die Transponder-IDs 81 - 87 werden zusätzlich reserviert.
- (usw.)

Beispiel - Ersatztransponder: Für Transponder 2 mit Transponder-ID 72 muss wegen Verlust oder Diebstahl ein Ersatztransponder programmiert werden. Diesem Ersatztransponder wird die reservierte Transponder-ID 73 zugewiesen. Wird der neu programmierte Ersatztransponder an einer berechtigten Schließung betätigt, kuppelt die Schließung ein und der "alte" Transponder 2 mit Transponder-ID 72 wird an der Schließung gesperrt. Über eine entsprechende Rückmeldung in der LSM Software kann der Vorgang abgeschlossen werden.

Insgesamt ist es möglich, bis zu 1.000 Transponder auf diese Weise zu reservieren.

5.4 Datenbank automatisch sichern

Erstellen bzw. bearbeiten Sie das Batch-Skript mit einem Texteditor, um die Datenbank automatisch zu sichern. Verwenden Sie alternativ die LSM-Installations-Toolbox.

Die Befehle und der Timeout zu Smart.XChange und dem Transponderterminal sind optional:

■ net stop Smart.XChangeService /y bzw. net start Smart.XChangeService /y

■ net stop TransTermSvr /y bzw. net start TransTermSvr /y

Sie sind nur erforderlich, wenn Sie diese Dienste verwenden. Speichern Sie das Batch-Skript anschließend mit der Dateiendung .bat im SimonsVoss-Ordner ab. Dieses Batch-Skript macht Folgendes:

1. Dienste anhalten, die auf die Datenbank zugreifen
2. Altes Backup entfernen
3. Datenbank in Backup-Verzeichnis kopieren
4. Dienste wieder starten

Inhalt des Batch-Skripts:

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

Tragen Sie anstelle der Pfade *C:\SimonsVoss\sv_backup* und *C:\SimonsVoss\sv_db*.** ggfs. eigene Pfade bzw. Netzwerkpfade zur Datenbank bzw. zum Backup-Verzeichnis ein.

Über die Windows-Aufgabenplanung können Sie mit diesem Batch-Skript regelmäßige (ideal: täglich) Backups durchführen. Wählen Sie das erstellte Skript aus. Weitere Parameter sind nicht nötig.

Beachten Sie dazu:

Standardeinstellungen für die Sicherheitsoptionen

- Ausführung über das Konto "System" und nicht über einen Admin-Login
- Enable: Unabhängig von der Benutzeranmeldung ausführen
- Enable: Kennwort nicht speichern
- Enable: Mit höchsten Privilegien ausführen

Sprechen Sie mit Ihrer IT. Sie ist als Systembesitzer verantwortlich für die korrekte Ausführung der geplanten Backups und für die sichere Archivierung.

6. Programmiergeräte

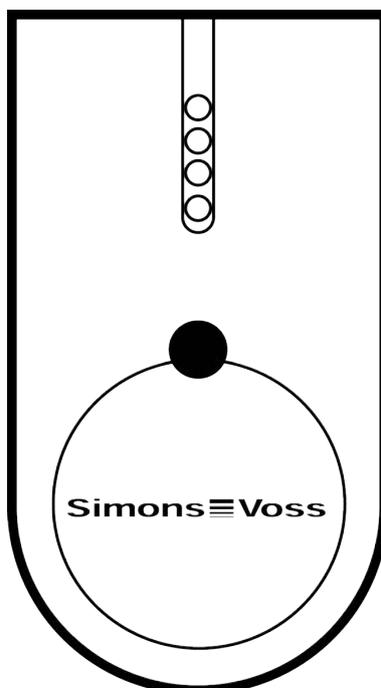
An jedem Computer mit installierter LSM Software besteht die Möglichkeit, ein Programmiergerät anzuschließen. Dazu muss der Computer über eine USB-Schnittstelle verfügen. Mit dem Programmiergerät werden vorgenommene Einstellungen und Berechtigungen an die SimonsVoss-Schließkomponenten übertragen. Außerdem können alle Komponenten komfortabel ausgelesen werden. Für bereits programmierte Komponenten ist dies auch über die LSM Mobile Edition oder das SimonsVoss-WaveNet-Netzwerk möglich.

6.1 Programmiergeräte erkennen und richtig einsetzen

SimonsVoss Programmiergeräte sind derzeit in folgenden Ausführungen erhältlich:

6.1.1 SmartCD.G2

Das SmartCD.G2 ist das Standardprogrammiergerät für aktive und hybride Komponenten. Mit Hilfe des SmartCD.G2 können alle aktiven SimonsVoss-Komponenten programmiert werden. Dieses Programmiergerät verfügt über ein Bluetooth-Modul und einen Akku. Damit kann es in Verbindung mit einem PDA/PocketPC auch komfortabel mit LSM Mobile verwendet werden. Das Smart.G2 ist am SimonsVoss-Logo zu erkennen.





HINWEIS

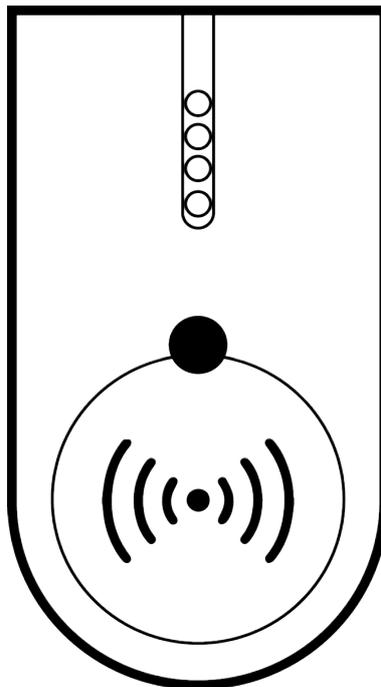
Erstaufladung der eingebauten Akkus.

Die eingebauten Akkus sind im Auslieferungszustand leer.

- Laden Sie das Programmiergerät mindestens drei Stunden, bevor Sie es verwenden.

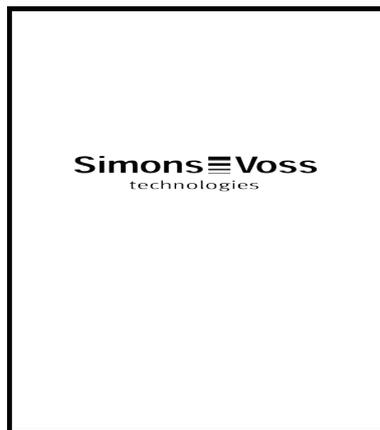
6.1.2 SmartCD.MP

Über das SmartCD.MP-Programmiergerät können passive Komponenten programmiert und ausgelesen werden. Im Gegensatz zum aktiven SmartCD.G2 ist das SmartCD.MP am Funk-Symbol zu erkennen. Das SmartCD.MP kann nur über eine direkte USB-Verbindung eingesetzt werden.



6.1.3 SmartCD.HF

Passive Tags und Karten können zusätzlich mit dem SmartCD.HF Kartenprogrammiergerät programmiert und ausgelesen werden.



6.1.4 SmartStick AX



Der SmartStick AX ist das Standard-Programmiergerät für alle Komponenten mit BLE-Schnittstelle. Mit Hilfe des SmartStick AX können alle SimonsVoss-AX-Komponenten programmiert werden.

Dieses Programmiergerät wird über ein USB-Kabel angeschlossen und mit Strom versorgt.

Vor der Programmierung müssen die zu programmierenden AX-Komponenten zuerst mit dem SmartStick AX angetippt werden, um die BLE-Schnittstelle aufzuwecken. Dann werden die AX-Komponenten für etwa 30 Sekunden vom SmartStick AX erkannt und können programmiert werden.

6.2 Programmierdistanzen

Für erfolgreiche Programmier- und Auslesevorgänge müssen bestimmte Distanzen zwischen dem Programmiergerät und den Komponenten eingehalten werden.

SmartStick AX

Nach dem Aufwecken der Schließung hat der SmartStick AX bis zu 300 cm Reichweite.

SMARTCD.G2

- Der Abstand zwischen SMARTCD.G2 und aktiver Komponente (z.B. Schließzylinder oder Transponder) sollte ca. 20 cm betragen.
- Achten Sie darauf, dass sich keine anderen aktiven Komponenten während des Programmier- oder Auslesevorgangs in unmittelbarer Nähe (Radius ca. 1,5 m zum SMARTCD.G2) befinden.



HINWEIS

Der Programmierabstand zwischen SMARTCD.G2 und **SmartRelais 1 oder 2** bzw. **Biometrieleser** muss 40 cm betragen!

SMARTCD.MP

- Der Knauf auf der Elektronikseite des Schließzylinders (*schwarzer Ring zwischen Knauf und Profilzylinder-Gehäuse*) muss direkt auf das Antennensymbol des SMARTCD.MP gehalten werden.
- Halten Sie den Schließzylinder während des kompletten Vorgangs auf das Antennensymbol.
- Mit dem SMARTCD.MP können auch Karten programmiert werden, indem diese direkt auf das Programmiergerät gelegt werden.



SMARTCD.HF

- Platzieren Sie die Karte oder den Tag bündig zur unteren, linken Ecke des SMARTCD.HF.

6.2.1 Hybride Schließungen programmieren

Hybride Schließungen werden über das SmartCD.G2 programmiert. Für die Programmierung muss jedoch gleichzeitig auch ein SmartCD.MP oder SmartCD.HF angeschlossen (und installiert) sein.

Ausnahme: Das SmartHandle AX kann auch mit dem SmartCD.MP erstprogrammiert werden.

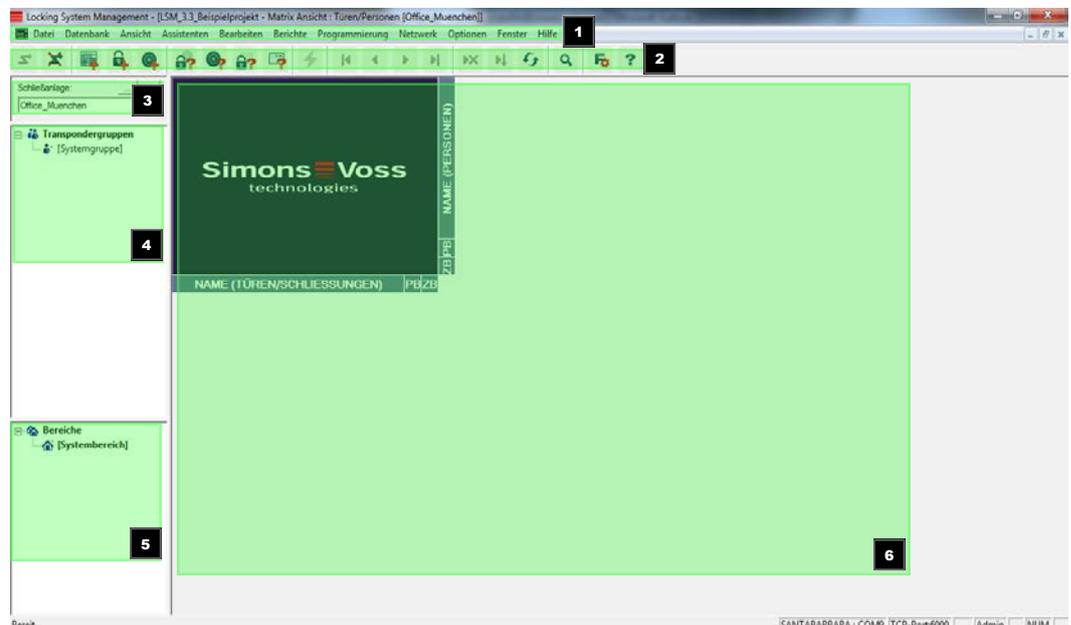
6.3 Verbindung überprüfen

Ob das Programmiergerät korrekt angeschlossen und installiert wurde, lässt sich in der LSM Software überprüfen:

1. Wählen Sie in der Menüleiste den Punkt "Programmierung".
2. Wählen Sie das zu überprüfende Programmiergerät, z.B. "SmartCD Aktiv testen" um das SMARTCD.G2 zu testen.
 - ↳ Der Test startet direkt.

7. Benutzeroberfläche

Die Benutzeroberfläche der LSM Software ist in folgende Bereiche aufgeteilt:



1. Menüleiste

Nutzen Sie die Menüleiste, um grundlegende Funktionen aufzurufen.

2. Menüband

Im Menüband können wichtige und häufig verwendete Funktionen direkt aufgerufen werden.

3. Schließanlage

Hier kann schnell zwischen verschiedenen Schließanlagen im Projekt umgeschaltet werden.

4. Gruppen

Fassen Sie Benutzer in Gruppen zusammen, um effektiver zu arbeiten.

5. Bereiche

Fassen Sie Schließungen in Bereiche zusammen, um effektiver zu arbeiten.

6. Matrix

Die Matrix zeigt eine Übersicht der ausgewählten Schließanlage.



HINWEIS

Je nach verwendeter LSM Software sind einige Funktionen/Einträge möglicherweise nicht verfügbar.

7.1 Menüleiste

Datei Datenbank Ansicht Assistenten Bearbeiten Berichte Programmierung Netzwerk Optionen Fenster Hilfe

7.1.1 Datei

7.1.1.1 Matrix drucken

Ausdrucken der ausgewählten Schließanlage.

7.1.1.2 Seitenansicht

Zeigt die Matrix als Vorschau vor dem Drucken.

7.1.1.3 Druckereinrichtung

Legen Sie erweiterte Druckoptionen wie z.B. die Seitengröße fest.

7.1.1.4 Benutzerkennwort ändern

An dieser Stelle kann das Kennwort des aktuell angemeldeten Benutzers geändert werden.

7.1.1.5 Beenden

Abmeldung vom Projekt und Beenden der LSM Software.

7.1.2 Datenbank

7.1.2.1 Anmelden

Melden Sie sich an einem Projekt an. *Diese Funktion ist nur verfügbar, wenn Sie aktuell in keinem Projekt angemeldet sind.*

7.1.2.2 Abmelden

Durch einen Klick auf "Abmelden" melden Sie sich aus dem aktuellen Projekt ab.

7.1.2.3 Setup

Hier können Sie die Projekte bzw. Datenbanken verwalten. Es stehen folgende Möglichkeiten zur Auswahl:

- Ein bestehendes Projekt bearbeiten.
- Ein bestehendes Projekt löschen.
- Ein neues Projekt erstellen.
- Zur Voreinstellung kann ein Default-Projekt ausgewählt werden, welches automatisch geladen wird.

7.1.2.4 Backup

Mit dieser Funktion können Sie eine Sicherung Ihrer Datenbank erstellen und gesicherte Datenbanken wiederherstellen.

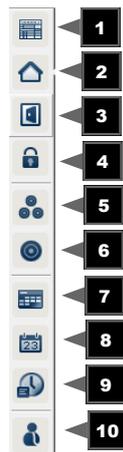
7.1.3 Ansicht

7.1.3.1 Statusleiste

Blendet eine Statusleiste am unteren Bildschirmrand ein bzw. aus. Die Statusleiste ist standardmäßig eingeblendet. In der Statusleiste werden unter anderem der aktuelle Schließanlagenstatus, Computernamen und der Anschluss des Programmiergerätes angezeigt.

7.1.3.2 Bearbeiten

Über *Ansicht/Bearbeiten* kann ein zusätzliches Menüband eingeblendet werden, welches Schnellzugriffe auf folgende Funktionen erlaubt:



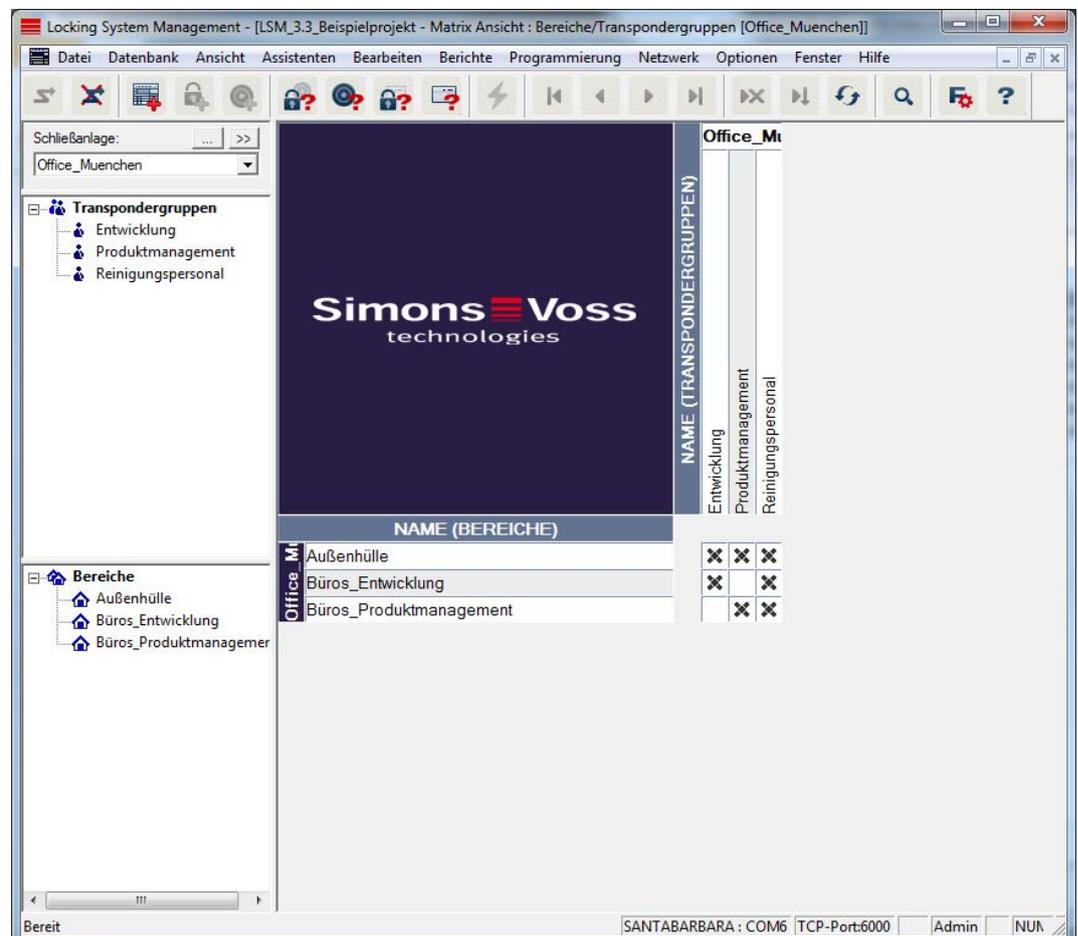
1. Schließanlageneigenschaften
2. Bereich
3. Tür
4. Schließung
5. Transpondergruppe
6. Transponder
7. Feiertagsliste
8. Feiertag
9. Zeitzonen
10. Person

7.1.3.3 Bereiche/Transpondergruppen

Diese Ansicht bildet eine Matrix, die sowohl die hierarchischen Personal- und Raumstrukturen visualisiert, als auch in der Lage ist, komplette Transpondergruppen gegen komplette Bereiche zu berechtigen. In dieser Matrix wird dadurch das schnelle und einfache Herstellen der Grundberechtigungen ermöglicht. Sollen davon abweichende Berechtigungen in Form von individuellen Erweiterungen oder Einschränkungen vergeben werden, so ist dies in der Ansicht Türen/ Personen möglich.

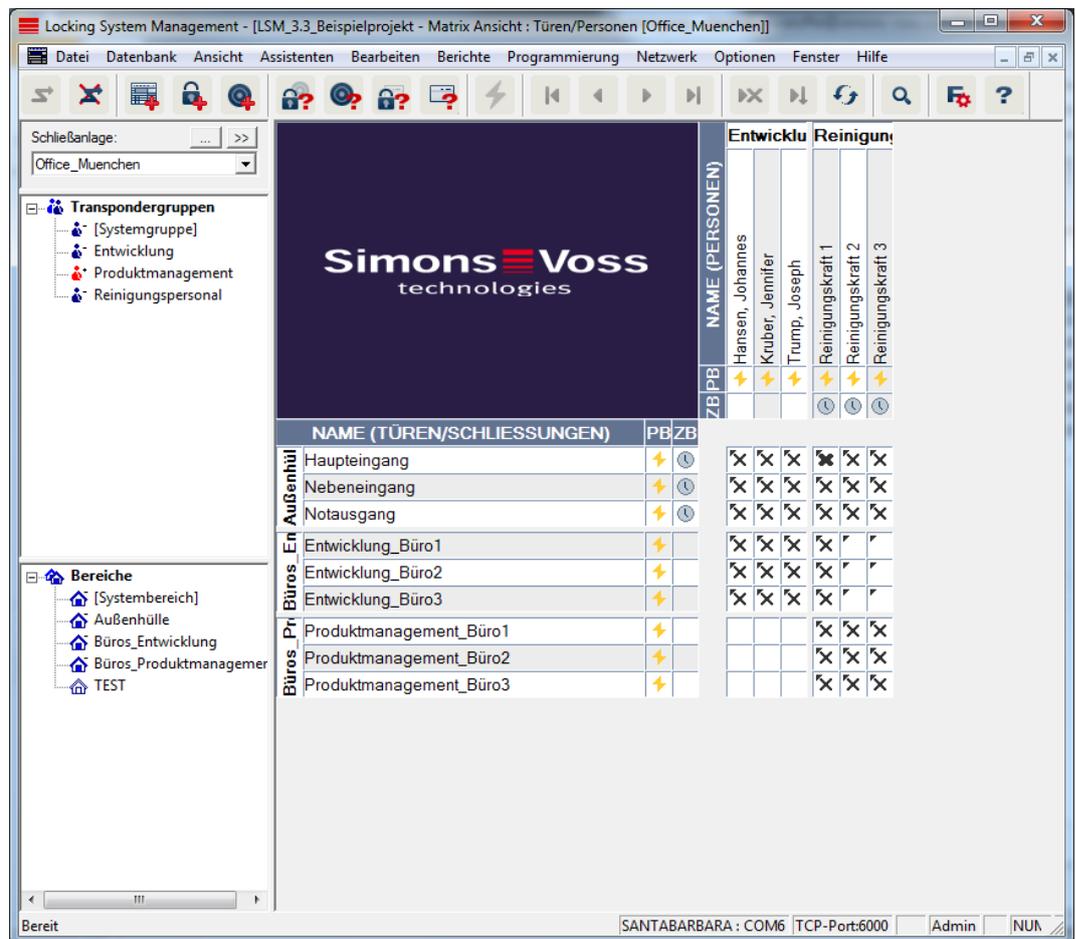
Wenn in der Schließanlage mit Transpondergruppen und Bereichen gearbeitet wird, bietet diese Option unter anderem diese entscheidenden Vorteile:

- Reduzierung der Ansicht, indem nur noch Transpondergruppen und Bereiche angezeigt werden. Diese ermöglicht ein einfacheres Zurechtfinden in der Matrix.
- Ganzen Gruppenberechtigungen für komplette Bereiche erteilen bzw. entziehen.
- Personen, die nachträglich einer Gruppe hinzugefügt werden, bekommen automatisch alle Gruppenrechte.



7.1.3.4 Türen/Personen

In dieser Ansicht werden die Einzelberechtigungen aller Personen auf einzelne Türen gezeigt. Die Matrix wird dadurch natürlich entsprechend umfangreich, erlaubt aber präzises Einstellen von Ausnahmeberechtigungen, wobei zuvor eingestellte Gruppenberechtigungen erweitert oder auch reduziert werden können. So ist diese Ansicht z.B. dafür geeignet, individuelle Erweiterungen oder Einschränkungen vorzunehmen, nachdem zuvor die Grundstruktur unter *Ansicht Bereiche/Transpondergruppen* festgelegt wurde.



7.1.3.5 Alle untergeordneten Bereiche/Gruppen öffnen

In dieser Ansichtseinstellung werden alle Bereiche und Gruppen geöffnet und somit alle Schließungen angezeigt; selbst wenn zuvor einzelne Bereiche ausgeblendet wurden.

7.1.3.6 Protokoll

Über das Protokoll können sämtliche Aktionen eingesehen werden, welche an der Datenbank durchgeführt wurden. Welcher Benutzer eine bestimmte Schließung erstellt oder geändert hat, kann genauso nachgefolgt werden wie beispielsweise die Anmeldungen in der Datenbank.

- Protokolle können beliebig eingegrenzt werden, z.B. nach einem Zeitraum, eines Benutzers oder einer Aktion.
- Die Liste kann wiederum durch einen Klick auf den gewünschten Spaltentitel sortiert werden, z.B. nach Datum, der Uhrzeit oder einem Namen.

7.1.3.7 Matrix Einstellungen

Jeder Benutzer hat die Möglichkeit, seine bevorzugte Ansicht als Standardansicht einzurichten. Diese wird nach der Anmeldung angezeigt. Weiterhin können hier verschiedene Grundeinstellungen getätigt werden.

Einstellungen zur Standardansicht können über die Menüleiste unter *Ansicht/Matrix Ansicht Eigenschaften* angepasst werden.

Matrix Ansicht Eigenschaften

Schriftart:

Feldhöhe:

Höhe an die Schrift anpassen

Transponder in die Horizontalleiste

Fadenkreuz anzeigen

deaktivierte Transponder ausblenden

Logo

Breite:

Höhe:

Vergeben der Berechtigungen

einfacher Mausklick

Doppelklick

Strg + einfacher Mausklick

Sofort speichern

Matrix Ansicht beim Start laden

Keine

Bereiche/Transpondergruppen

Türen/Personen

■ Schriftart

Sie können beliebige Schriftarten auswählen.

■ Feldhöhe

Sie können die Höhe der Felder in Punkten anpassen.

■ Höhe an Schriftart anpassen

Höhe automatisch an die Schriftart anpassen.

■ Transponder in der Horizontalleiste

Transponder werden standardmäßig in der Horizontalen angezeigt. Sie können diese Einstellung ändern, wenn Sie beispielsweise mehr Schließungen als Transponder verwalten möchten.

■ **Fadenkreuz anzeigen**

Zeigt ein Fadenkreuz zur genaueren Navigation.

■ **Deaktivierte Transponder ausblenden**

Blendet deaktivierte Transponder aus.

■ **Logo**

Größe des Logos verändern.

■ **Vergeben der Berechtigungen**

Gerade bei großen Schließanlagen kann es schnell zu einem unachtsamen Mausklick kommen. In diesen Fällen wird empfohlen, diese Einstellung zu ändern.

Aktivieren Sie "Sofort speichern", wenn Sie die Berechtigungsänderungen unmittelbar durch einen einfachen Mausklick übernehmen möchten.

7.1.3.8 Zusätzliche Spalten

Horizontal- und Vertikalleiste der Matrix lassen sich mit weiteren Spalten ausstatten, die dem Anwender nützliche Zusatzinformationen bieten. Die getroffenen Einstellungen gelten nur für die jeweilige Ansicht, in der sie eingestellt wurden. Je nach Ansichtstyp stehen so unterschiedliche Informationen zur Verfügung. Die Reihenfolge der angezeigten Daten kann ebenfalls individuell eingestellt werden und wird nutzerspezifisch (Windowsbenutzer) gespeichert.

So blenden Sie zusätzliche Spalten in die Matrix ein:

1. Wählen Sie in der Menüleiste *Ansicht/Zusätzliche Spalten* gefolgt von der jeweiligen Ansicht, z.B. *Transponder/Personen*.
2. Markieren Sie alle Informationen, die zusätzlich eingeblendet werden sollen.
3. Sortieren Sie über "Nach oben" bzw. "Nach unten" die Reihenfolge.
4. Bestätigen Sie die Auswahl über die Schaltfläche "OK".

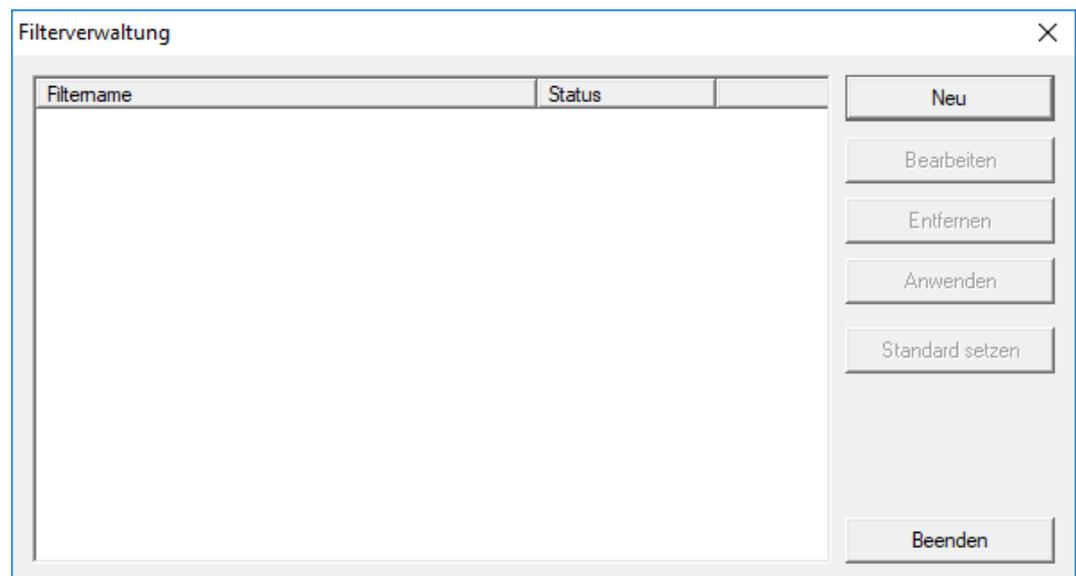
7.1.3.9 Aktualisieren

Aktualisiert die Matrixansicht.

Besonders bei umfangreichen Schließanlagen oder besonderen Einstellungen kann es nötig sein, die Matrix in Ausnahmefällen manuell zu aktualisieren.

7.1.3.10 Filter verwalten

Mit der Einführung von Filtern ist es noch komfortabler geworden, eine Schließanlage zu administrieren. Sie können verschiedenste Filteroptionen auswählen und diese Filter verschiedensten Personen oder Personengruppen zur Verfügung zu stellen. Nicht nur, dass Sie über die Einblendung optionaler Zusatzspalten weitere Informationen bekommen - mit der Filterfunktion halten Sie Ihre Ansichten zudem sehr übersichtlich.



- **Neu**
Erstellen eines neuen Filters
- **Bearbeiten**
Bearbeiten eines ausgewählten Filters
- **Entfernen**
Entfernen eines ausgewählten Filters
- **Anwenden**
Anwenden des ausgewählten Filters. Wird ein Filter angewendet, ändert sich die Schaltfläche zu "**Ausschalten**".
- **Standard setzen**
Dieser Filter wird standardmäßig verwendet
- **Beenden**
Beenden der Filterverwaltung und Rückkehr zur Matrix



HINWEIS

Ein Filter bleibt solange aktiv, bis dieser wieder ausgeschaltet wurde!

Über die Schaltfläche "Neu" können Sie einen neuen Filter erstellen:

Filtername

Geben Sie einen aussagekräftigen Namen für den neuen Filter ein.

Benutzereinschränkung

Benutzer oder Benutzergruppe, die den Filter anwenden kann.

Transpondertyp

Art des Transponders, der angezeigt werden soll.

Transpondereigenschaften

Einschränkungen, welche die Eigenschaften des Transponders betreffen (z.B. Gültigkeitsbereich oder Programmierbedarf).

Transpondergruppenliste

Einschränkungen, welche die Zugehörigkeit des Transponders betreffen (z.B. Transpondergruppe „Geschäftsführung“).

Schließungstyp

Art der Schließung, die angezeigt werden soll.

Türen/Schließanlageneigenschaften

Einschränkungen, welche die Eigenschaften der Schließung betreffen (z.B. Mit Netzwerk oder Programmierbedarf).

■ **Bereichsliste**

Einschränkungen, welche die Zugehörigkeit der Schließung betreffen (z.B. Bereich „Pforte“).

7.1.4 Assistenten

Die Assistenten erleichtern den Einstieg in die LSM Software für neue Benutzer. Auch erfahrende Benutzer profitieren von den Assistenten, mit denen prinzipiell alle Einstellungen auf einmal zentral hintereinander getätigt werden können.

7.1.4.1 Assistenten/Tür

Über diesen Assistenten kann Schritt für Schritt eine neue Tür angelegt werden.

7.1.4.2 Assistenten/Person

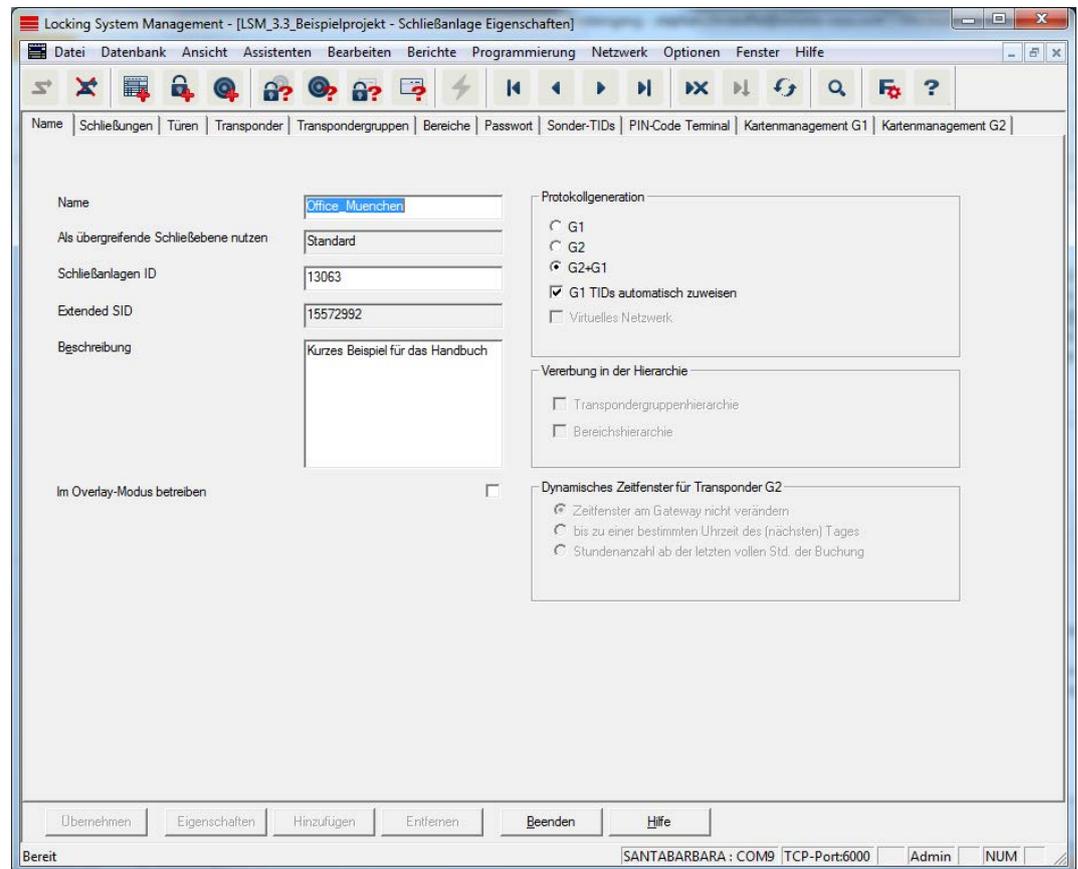
Über diesen Assistenten kann Schritt für Schritt eine neue Person angelegt werden.

7.1.5 Bearbeiten

7.1.5.1 Eigenschaften: Schließanlage

Einstellungen für die aktuell ausgewählte Schließanlage.

Name



❖ Name

Bezeichnung der Schließanlage

❖ Als übergreifende Schließebene nutzen

Festlegung der übergreifenden Schließebene

❖ Schließanlagen ID

Systemnummer der Schließanlage

❖ Extended SID

Zusätzliches Unterscheidungsmerkmal der Schließanlage

❖ Beschreibung

Freies Feld zur Beschreibung der Schließanlage

❖ Im Overlay-Modus betreiben (nur G1)

Aktiviert den Overlay Modus. *Diese Funktion muss bereits beim Anlegen der Schließanlage aktiviert werden. Eine nachträgliche Änderung ist nicht möglich.*

❖ Protokollgeneration

Auswahl der Ausbauparallele der Hardwarekomponenten

❖ Vererbung in der Hierarchie [LSM BUSINESS]

Bereiche der Vererbung wählen

■ **Dynamisches Zeitfenster für Transponder G2**

Erweiterte Zeiteinstellungen für die Verwendung mit Gateways:

■ **Zeitfenster am Gateway nicht verändern**

Alle am Gateway buchenden G2 Transponder werden in ihrer Gültigkeit zeitlich nicht befristet.

■ **bis zu einer bestimmten Uhrzeit des (nächsten) Tages**

Alle am Gateway buchenden G2 Transponder werden in ihrer Gültigkeit bis zu einer bestimmten Uhrzeit beschränkt.

■ **Stundenzahl ab der letzten vollen Stunde der Buchung**

Alle am Gateway buchenden G2 Transponder werden in ihrer Gültigkeit um die festgelegte Dauer in Stunden verlängert.



HINWEIS

Virtuelles Netzwerk nicht erforderlich

Die Konfiguration eines virtuellen Netzwerks ist für die Verwendung eines Gateways zur Verwaltung der Zeitfenster nicht zwingend erforderlich.

Schließungen

The screenshot shows the 'Schließanlage Eigenschaften' window in the Locking System Management software. The window title is 'Locking System Management - [LSM_3.3_Beispielprojekt - Schließanlage Eigenschaften]'. The menu bar includes 'Datei', 'Datenbank', 'Ansicht', 'Assistenten', 'Bearbeiten', 'Berichte', 'Programmierung', 'Netzwerk', 'Optionen', 'Fenster', and 'Hilfe'. The toolbar contains various icons for file operations, navigation, and search. The main area is divided into several sections:

- Navigation:** 'Name', 'Schließungen', 'Türen', 'Transponder', 'Transpondergruppen', 'Bereiche', 'Passwort', 'Sonder-TIDs', 'PIN-Code Terminal', 'Kartenmanagement G1', 'Kartenmanagement G2'.
- Configuration:** 'Schließanlage: Office_Muenchen', 'Ebene: Standard'.
- Table:** A table with columns: 'Seriennummer', 'Schließungs ID', 'Tür', 'Bereich', and 'Typ'. It lists 8 locks with their respective IDs and locations.
- Actions:** 'Druckansicht', 'Insgesamt: 8', 'Ausgewählt: 0'.
- Buttons:** 'Übernehmen', 'Eigenschaften', 'Hinzufügen', 'Entfernen', 'Beenden', 'Hilfe'.
- Status:** 'Bereit', 'SANTABARBARA : COM9 | TCP-Port:6000', 'Admin', 'NUM'.

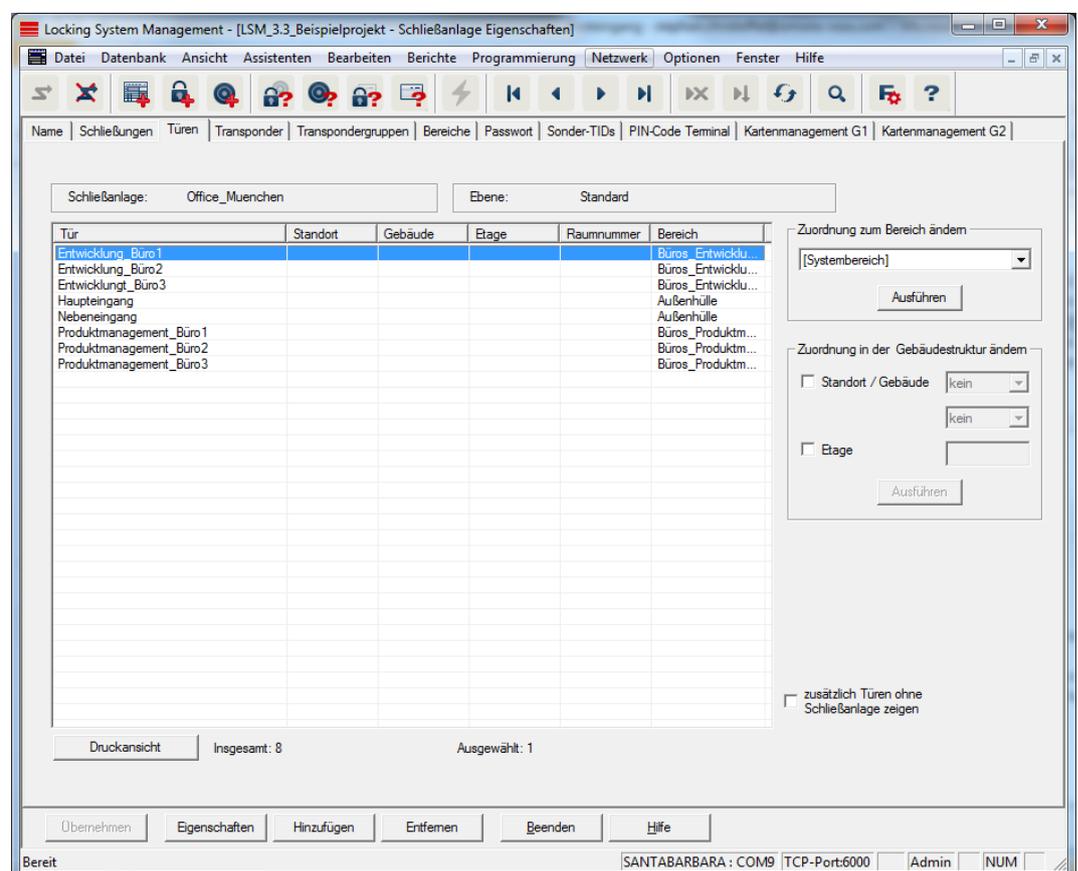
Seriennummer	Schließungs ID	Tür	Bereich	Typ
L-00001	128	Haupteingang	Außenhülle	G2 Door Monitor...
L-00002	129	Produktmanagement_Büro3	Büros_Produktmanagement	G2 Smart Handl...
L-00003	130	Produktmanagement_Büro2	Büros_Produktmanagement	G2 Smart Handl...
L-00004	131	Produktmanagement_Büro1	Büros_Produktmanagement	G2 Smart Handl...
L-00005	132	Entwicklung_Büro2	Büros_Entwicklung	G2 Smart Handl...
L-00006	133	Entwicklung_Büro3	Büros_Entwicklung	G2 Smart Handl...
L-00007	134	Entwicklung_Büro1	Büros_Entwicklung	G2 Smart Handl...
L-00008	135	Nebeneingang	Außenhülle	G2 Smart Handl...

Diese Registerkarte verschafft einen Überblick über die in der Schließanlage eingesetzten Schließungen. Diese werden alle detailliert in einer Tabelle angezeigt.

Außerdem können Hinweise zum Batteriewechsel festgehalten werden:

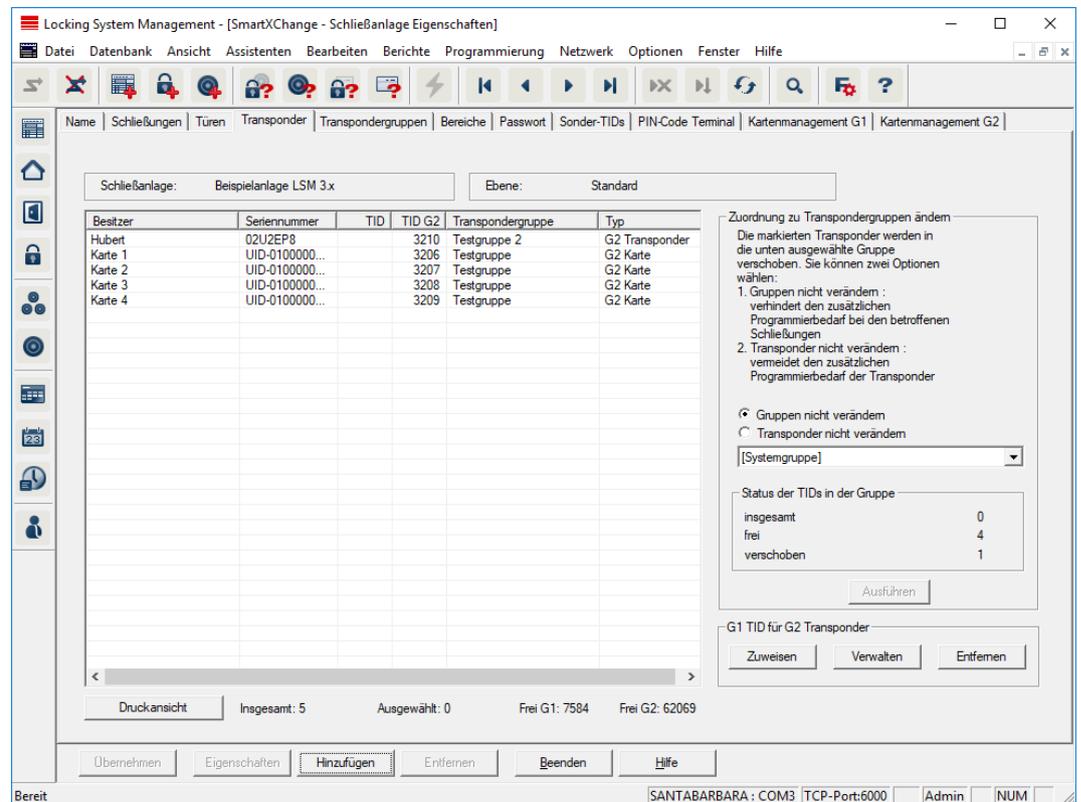
Der „Planmäßige“ Batteriewechsel wird im Warnungsmonitor und in der Aktionsliste der jeweiligen Schließung angezeigt. Zusätzlich hat man die Möglichkeit, in der Aktionsliste der jeweiligen Schließung den planmäßigen Batteriewechsel über mehrere Schließungen gleichzeitig einzutragen. Unter „Letzter“ kann für eine oder mehrere Schließungen ein durchgeführter Batteriewechsel eingetragen werden.

Türen



Diese Registerkarte zeigt den Zusammenhang der in der Schließanlage enthaltenen Türen und zugeordneten Bereiche. Diese werden alle detailliert in einer Tabelle angezeigt. Es ist möglich, eine oder mehrere Türen auszuwählen und einem bestimmten Bereich, Standort oder Etage zuzuordnen. Beachten Sie, dass Bereiche, Standorte oder Etagen bereits angelegt sein müssen.

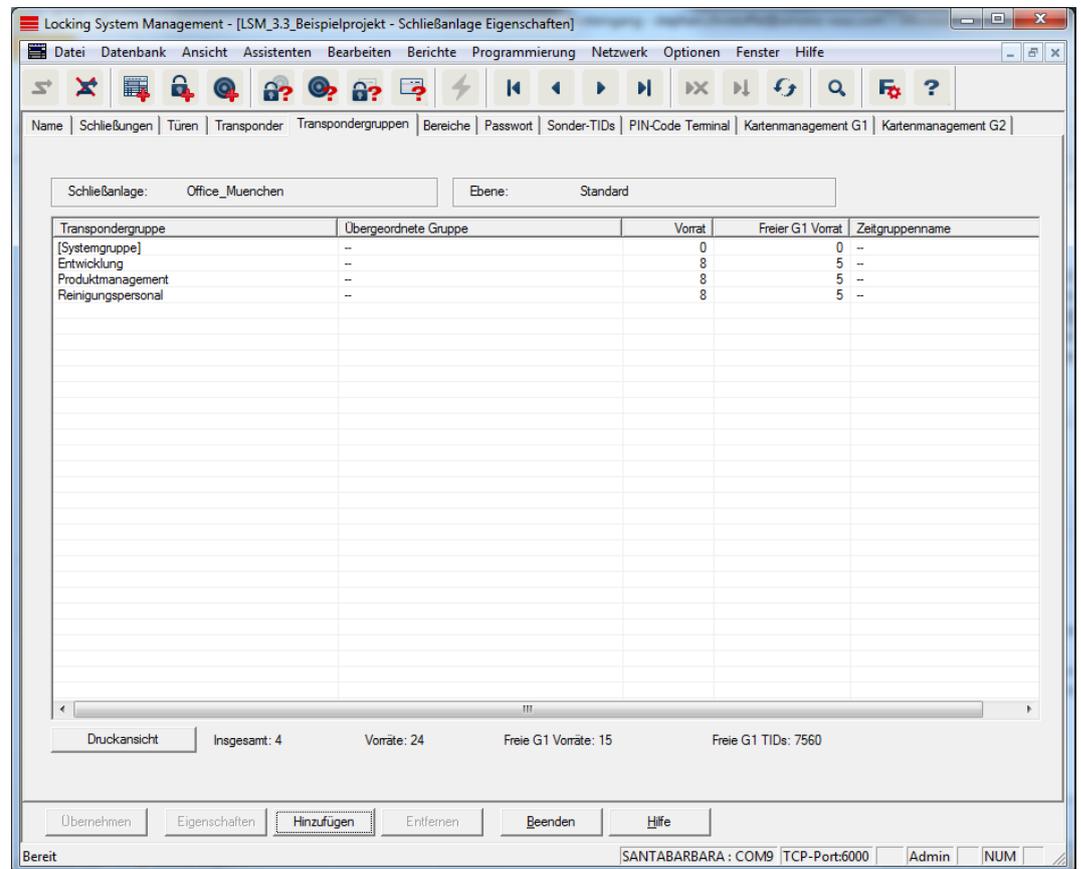
Transponder



Diese Registerkarte verschafft einen Überblick über die in der Schließanlage enthaltenen Transponder. Diese werden alle detailliert in einer Tabelle angezeigt.

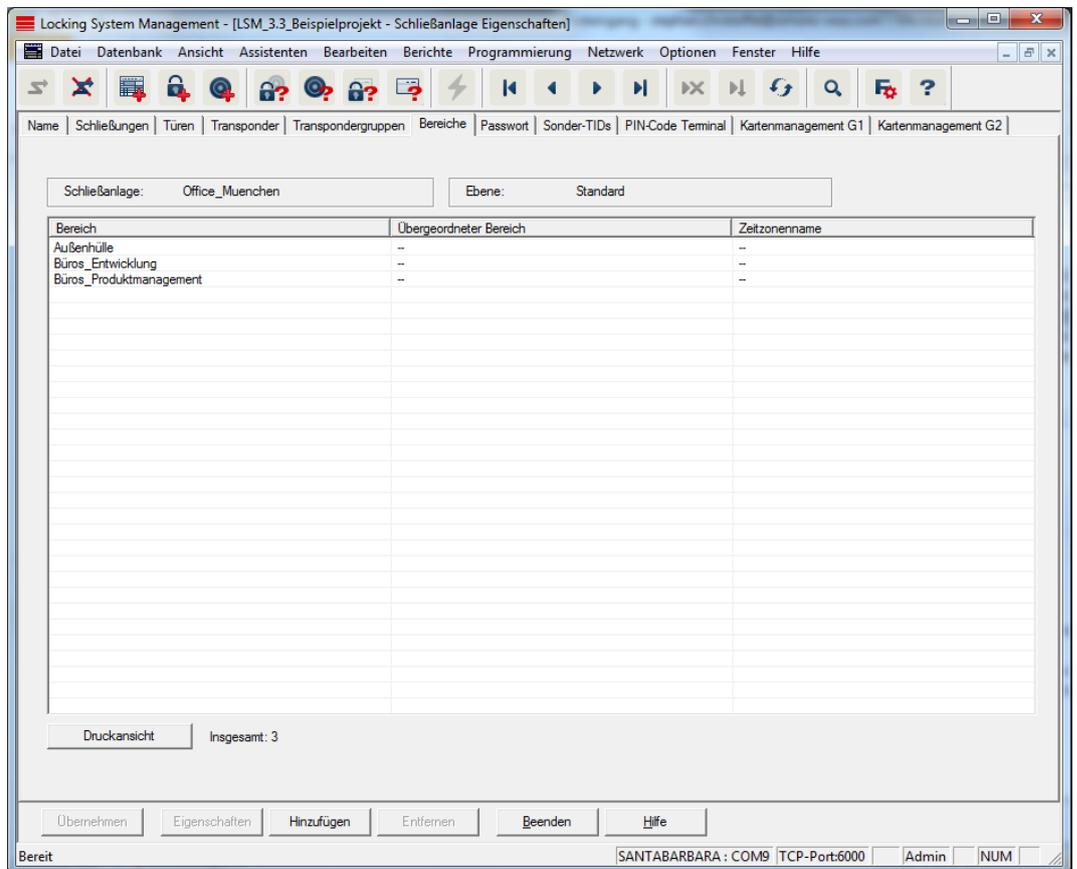
Es ist möglich, einen oder mehrere Transponder auszuwählen und einer anderen Gruppe zuzuordnen. Beachten Sie, dass die Transpondergruppen bereits angelegt sein müssen.

Transpondergruppen



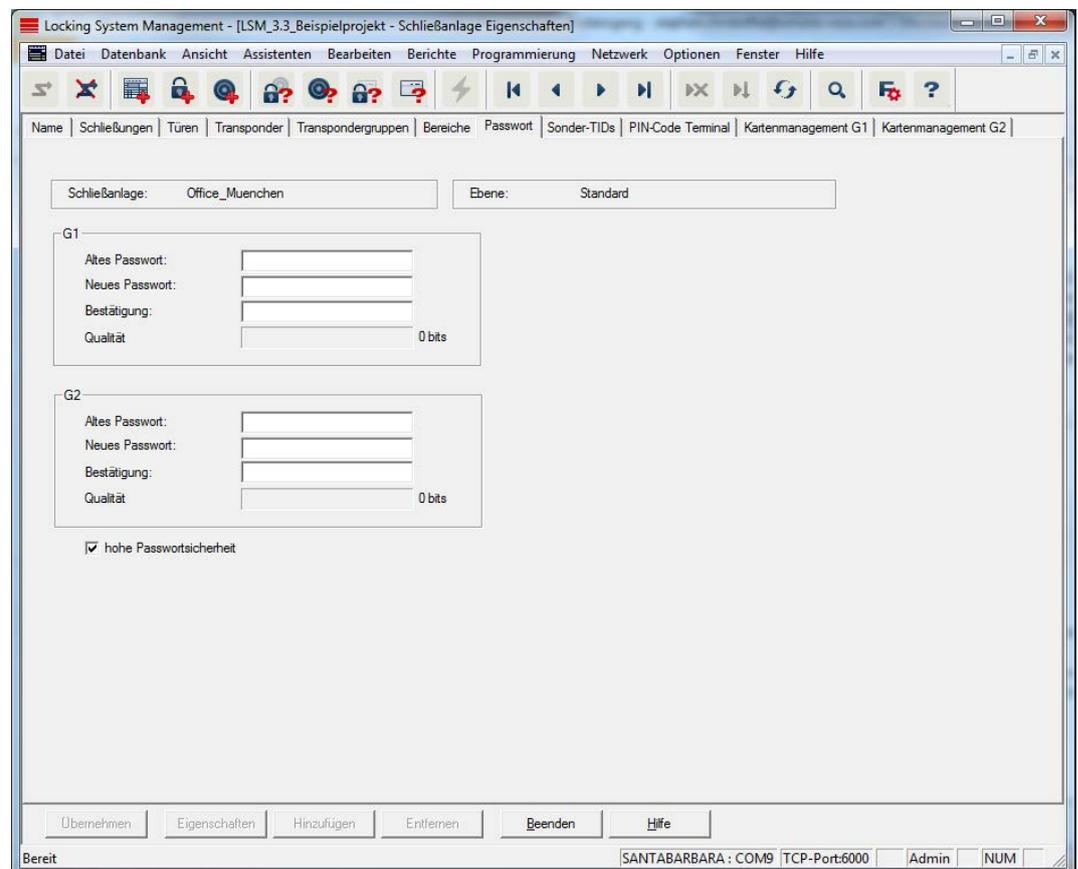
Diese Registerkarte verschafft einen Überblick über die in der Schließanlage eingesetzten Transpondergruppen. Diese werden alle detailliert in einer Tabelle angezeigt.

Bereiche



Diese Registerkarte verschafft einen Überblick über die in der Schließanlage eingesetzten Bereiche. Diese werden alle detailliert in einer Tabelle angezeigt.

Passwort



Hier können die Schließanlagenpasswörter, die zur Programmierung der Komponenten verwendet werden, geändert werden.

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.

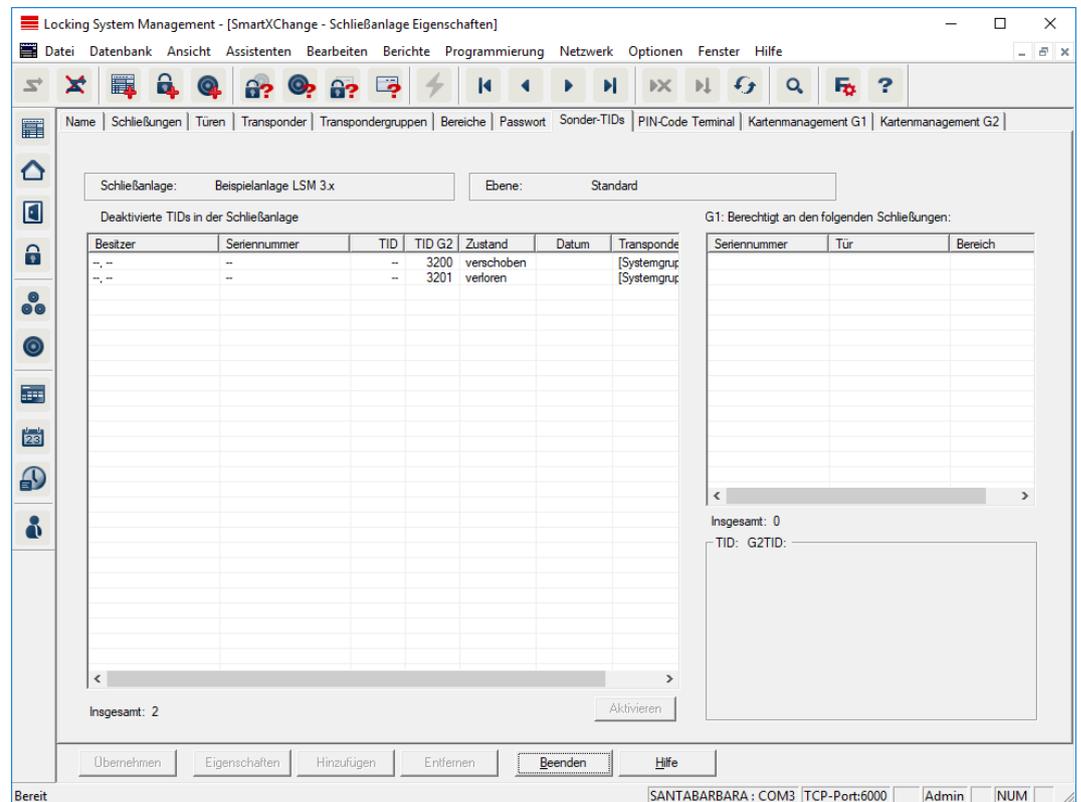
1. Bewahren Sie das Schließanlagenpasswort sicher auf (z.B. in einem Safe)!
2. Machen Sie das Schließanlagenpasswort für Berechtigte jederzeit einsehbar!



HINWEIS

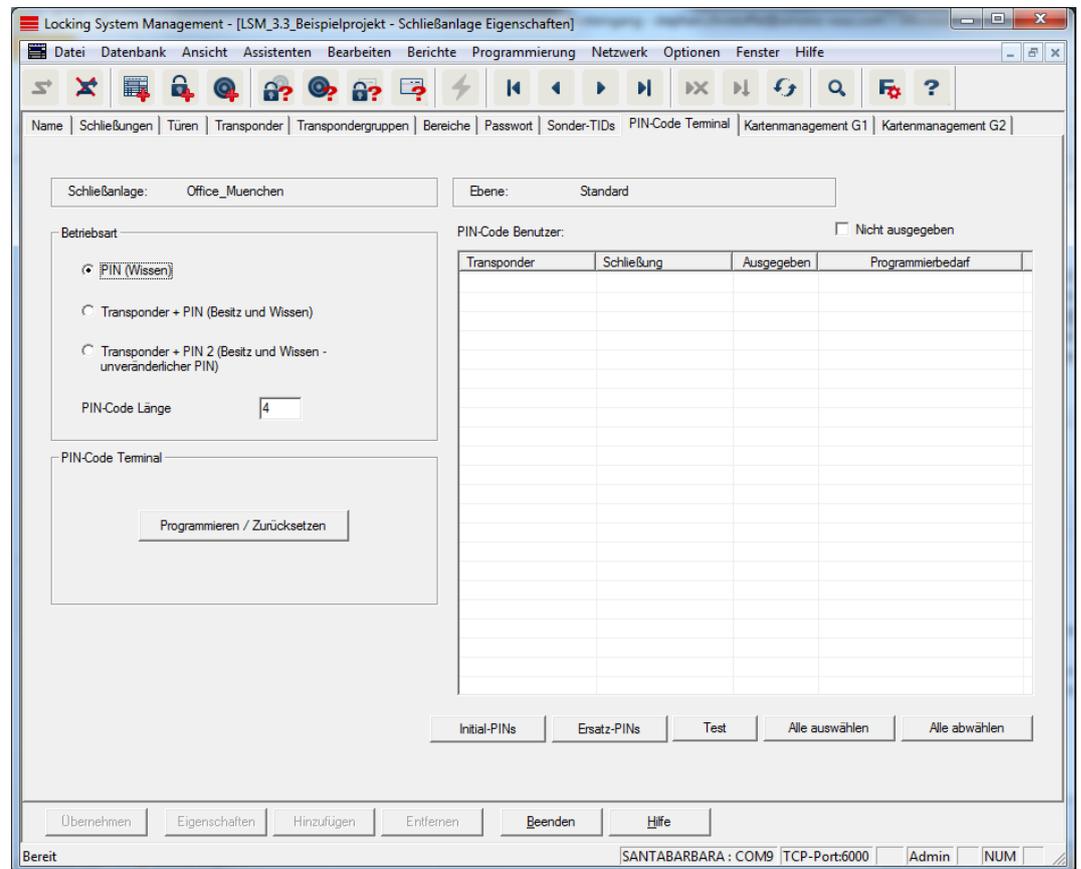
Komponenten mit unterschiedlichen Schließanlagenpasswörtern können nicht miteinander kommunizieren!

Sonder-TIDs



- Die große, linke Tabelle zeigt eine Übersicht folgender Transponder:
 - Deaktivierte Transponder
 - Entfernte Transponder
 - Verlorene Transponder
 - Nicht zurückgegebene Transponder
 - Temporär gesperrte Transponder
- Die kleinere, rechte Tabelle zeigt alle Schließungen an, an denen die in der linken Tabelle ausgewählten Transponder berechtigt sind.
- Im Anzeigebereich unter der kleinen, rechten Tabelle werden Informationen und Bemerkungen zum deaktivierten Transponder angezeigt.
- Über die Schaltfläche "Aktivieren" kann ein ausgewählter Transponder (je nach gesetztem Zustand) wieder aktiviert werden. Im G2-Protokoll wird dem Transponder in diesem Fall eine neue TID zugewiesen, was Programmierbedarf an den berechtigten Schließungen erzeugen kann.

PIN-Code Terminal



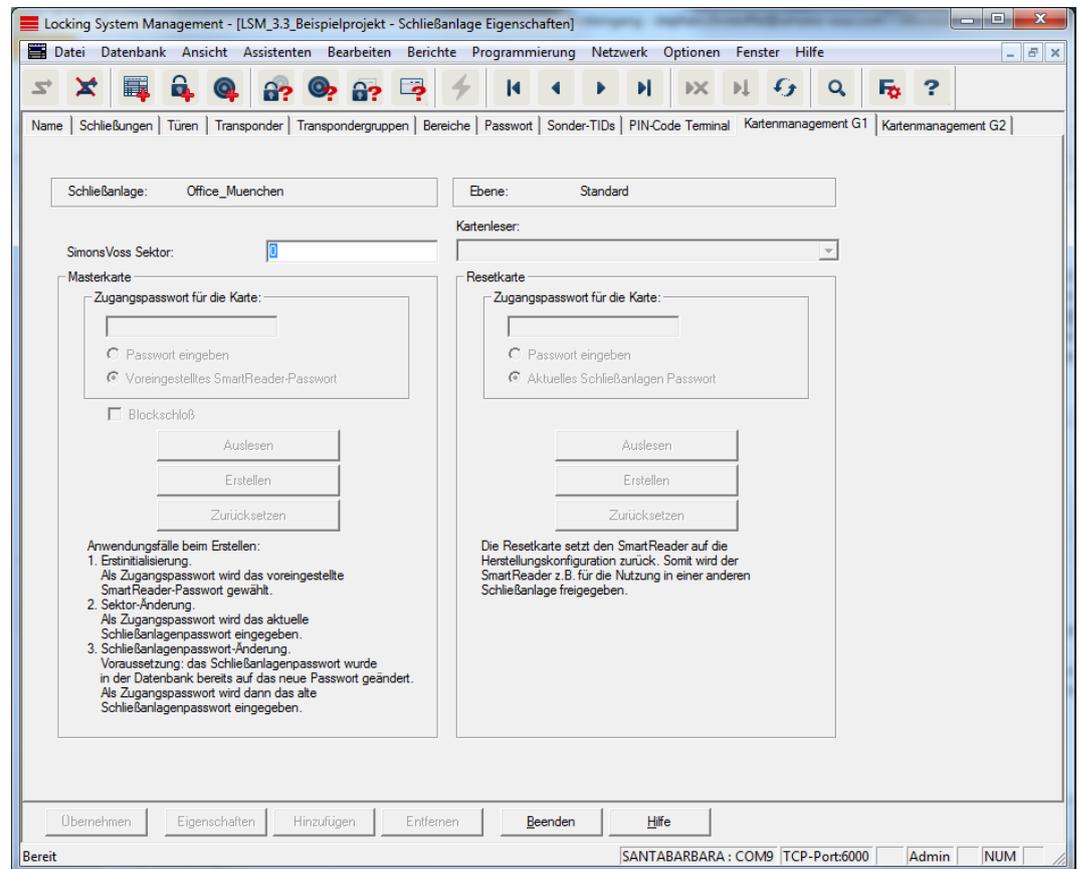
In dieser Registerkarte können Pin Code Terminals angelegt und erweiterte Konfigurationen getätigt werden.

Beachten Sie für die Einrichtung des Pin Code Terminal die Dokumentation "Pin Code Terminal Handbuch", welche Sie auf der Homepage finden:

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

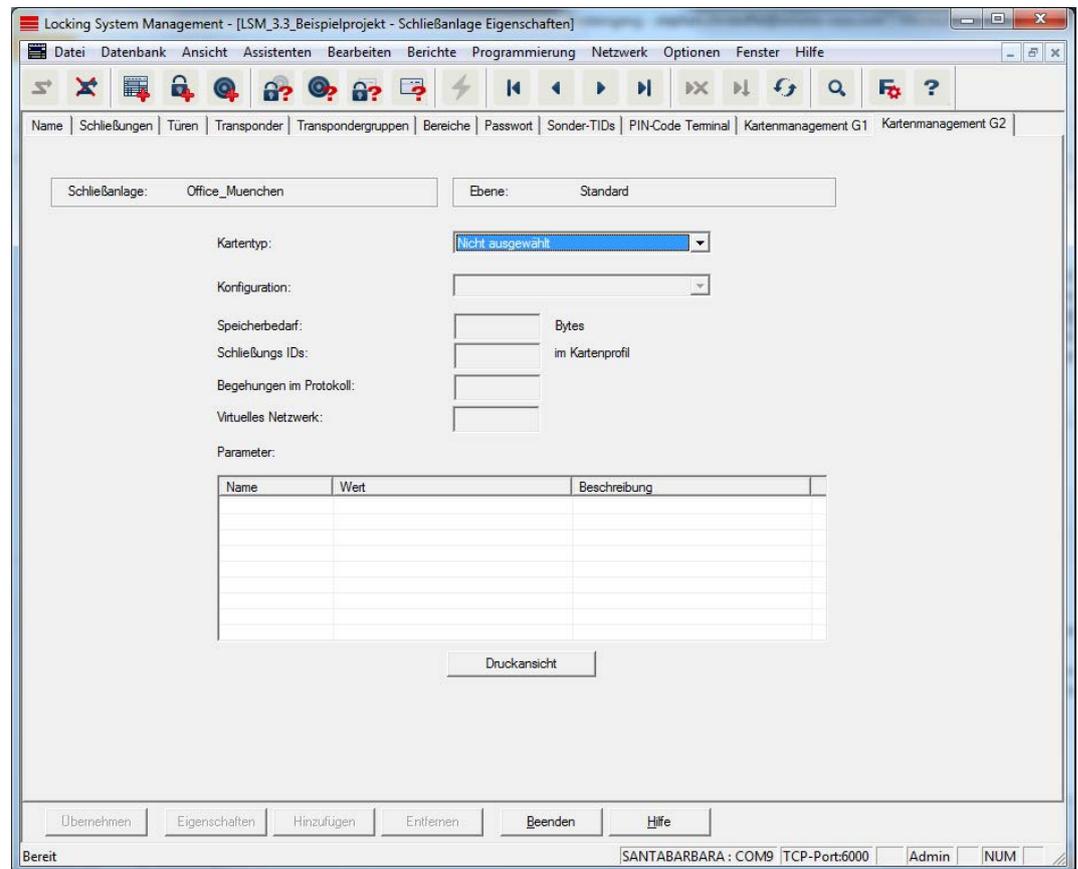
Siehe *Hilfe und weitere Informationen* [▶ 262].

Kartenmanagement G1



Legen Sie erweiterte Eigenschaften und Einstellungen Ihrer G1-Karten fest (siehe *Kartenmanagement* [▶ 169]).

Kartenmanagement G2



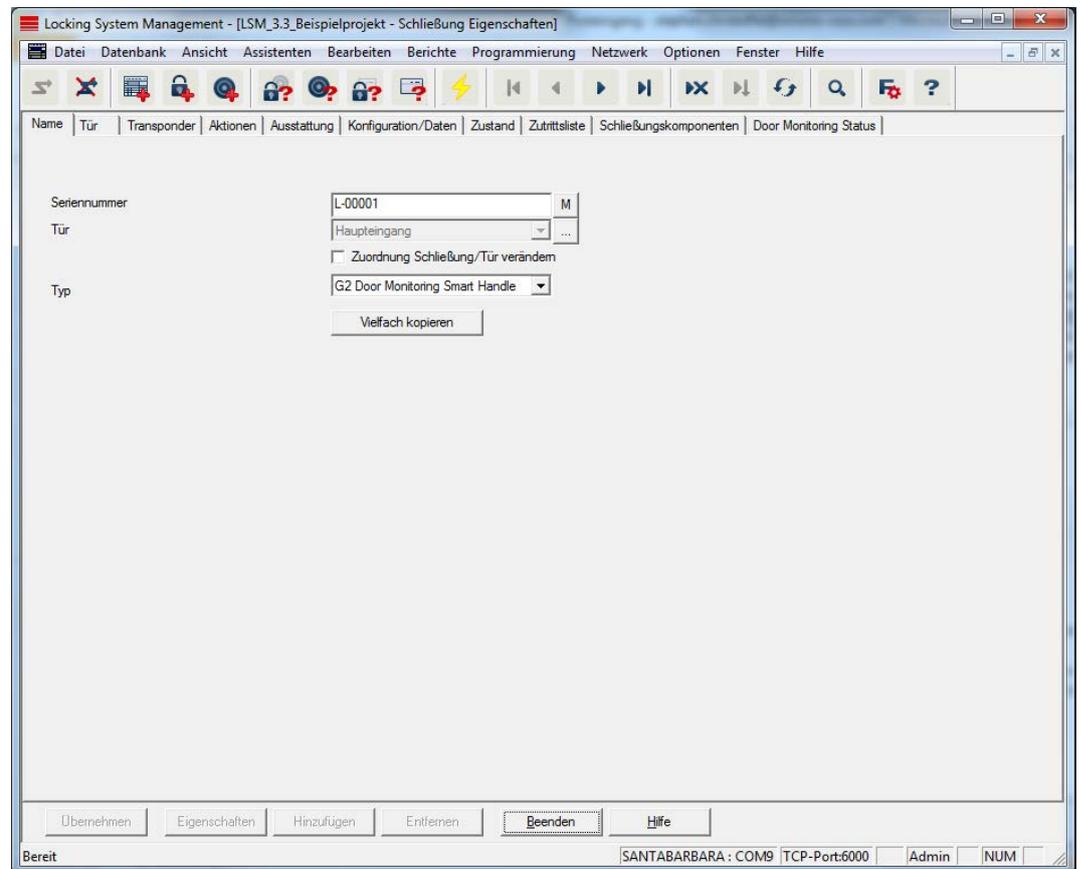
Legen Sie erweiterte Eigenschaften und Einstellungen Ihrer G2-Karten fest (siehe *Kartenmanagement* [▶ 169]).

7.1.5.2 Eigenschaften: Schließung

Eigenschaften der aktuell markierten Schließung anzeigen und bearbeiten.

Ein Doppelklick auf eine Schließung öffnet direkt die Eigenschaften der entsprechenden Schließung!

Name



■ Seriennummer

Zeigt die Seriennummer der Schließung an. Die Schaltfläche "..." zeigt die Eigenschaften der Tür an.

■ Tür

Sobald die Checkbox "Zuordnung der Schließung/Tür verändern" aktiviert wird, ist es möglich, die der Schließung zugewiesenen Tür zu ändern. Die Schaltfläche "M" zeigt die Schließung in der Matrix an.

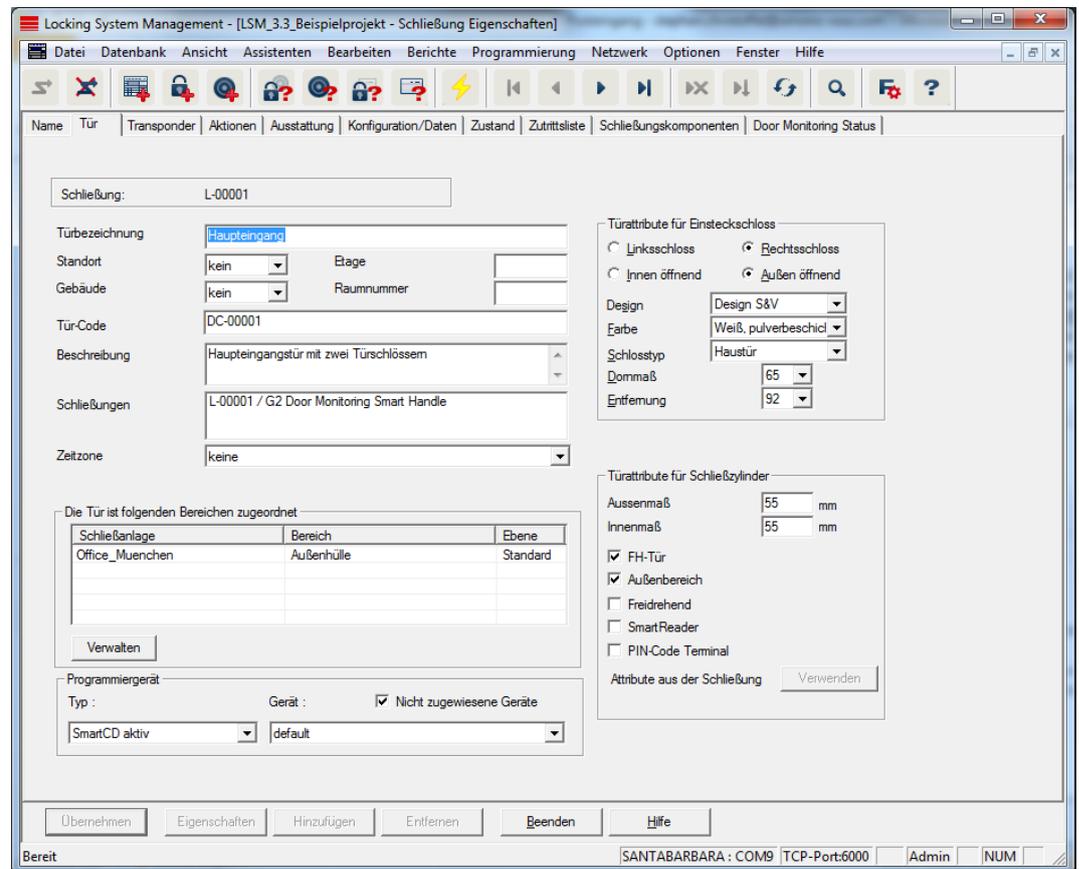
■ Typ

Art der Schließung.

■ Vielfach kopieren

Erzeugt beliebig viele Kopien der Schließung mit denselben Eigenschaften. Zusätzlich zum Namen der Schließung wird eine fortlaufende Nummer angefügt.

Tür



■ Türbezeichnung

Name der Tür.

■ Standort

Standort, an dem sich die Tür befindet. (Standorte müssen bereits vorher angelegt worden sein.)

■ Gebäude

Gebäude, in dem sich die Tür befindet. (Gebäude müssen bereits vorher angelegt worden sein.)

■ Etage

Etage, in der sich die Tür befindet.

■ Raumnummer

Raumnummer der Tür.

■ Türcode

Interne Bezeichnung der Tür.

■ Beschreibung

Freies Feld zur Beschreibung der Tür.

■ Schließungen

Schließungen, die der Tür zugewiesen sind.

■ Zeitzone

Zeitzone der Tür.

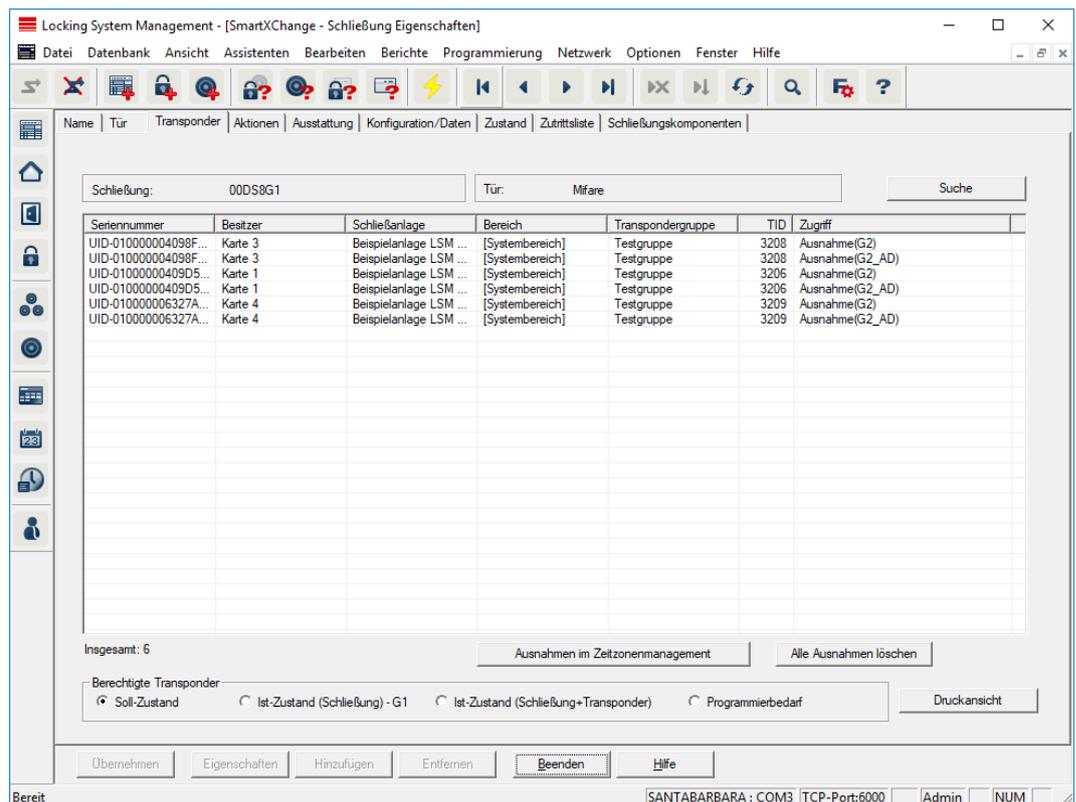
■ Programmiergerät

Auswahl eines bestimmten Programmiergerätes. (Vor allem bei LON und WaveNet notwendig. Schließungen, denen LON oder WaveNet zugeordnet ist, können zusätzlich per Funk "online" ohne Programmiergerät programmiert werden.)

■ Türattribute

Informationen zu Einsteckschloss und Schließung. Im Bedarfsfall ist direkt ersichtlich, welche Ersatzkomponenten benötigt werden.

Transponder



■ Tabelle

Zeigt alle an der Schließung berechtigten Transponder in einer detaillierten Liste.

■ Berechtigte Transponder

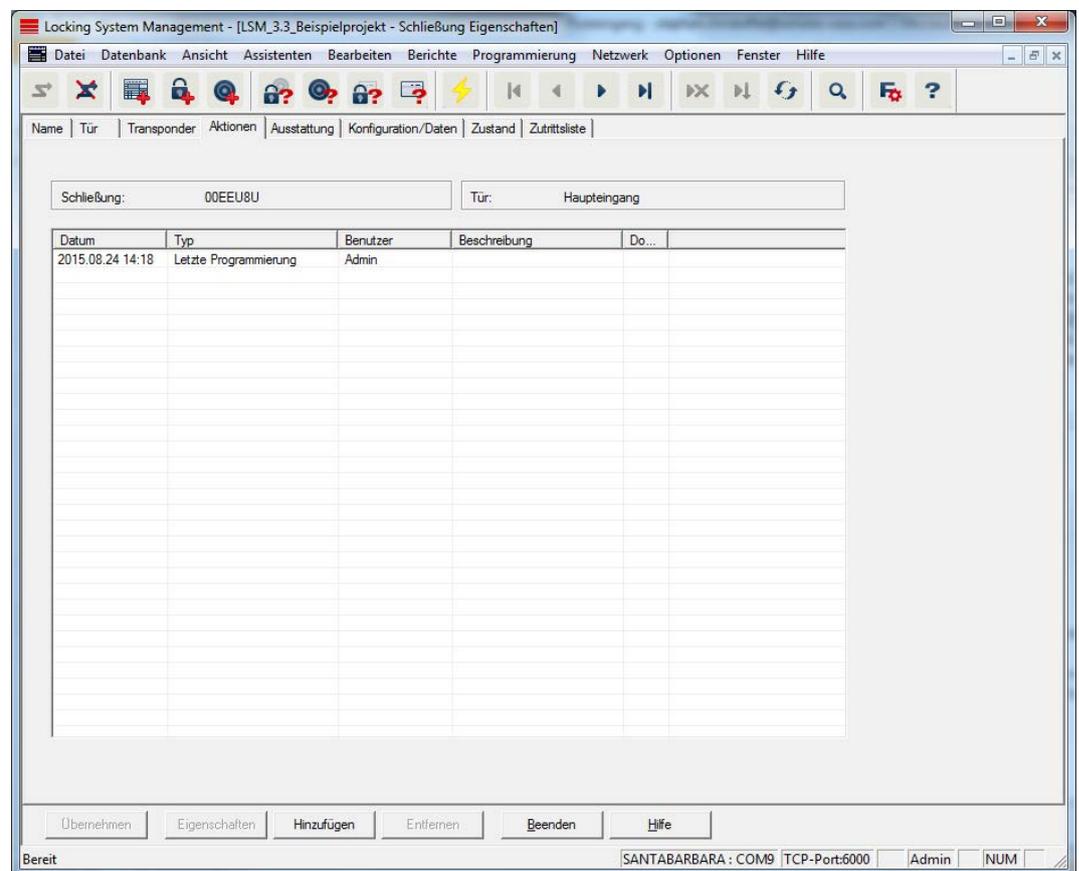
Über die einzelnen Radio-Buttons kann die Tabelle gefiltert werden.

■ Soll Zustand

Zeigt den gewünschten Zustand an.

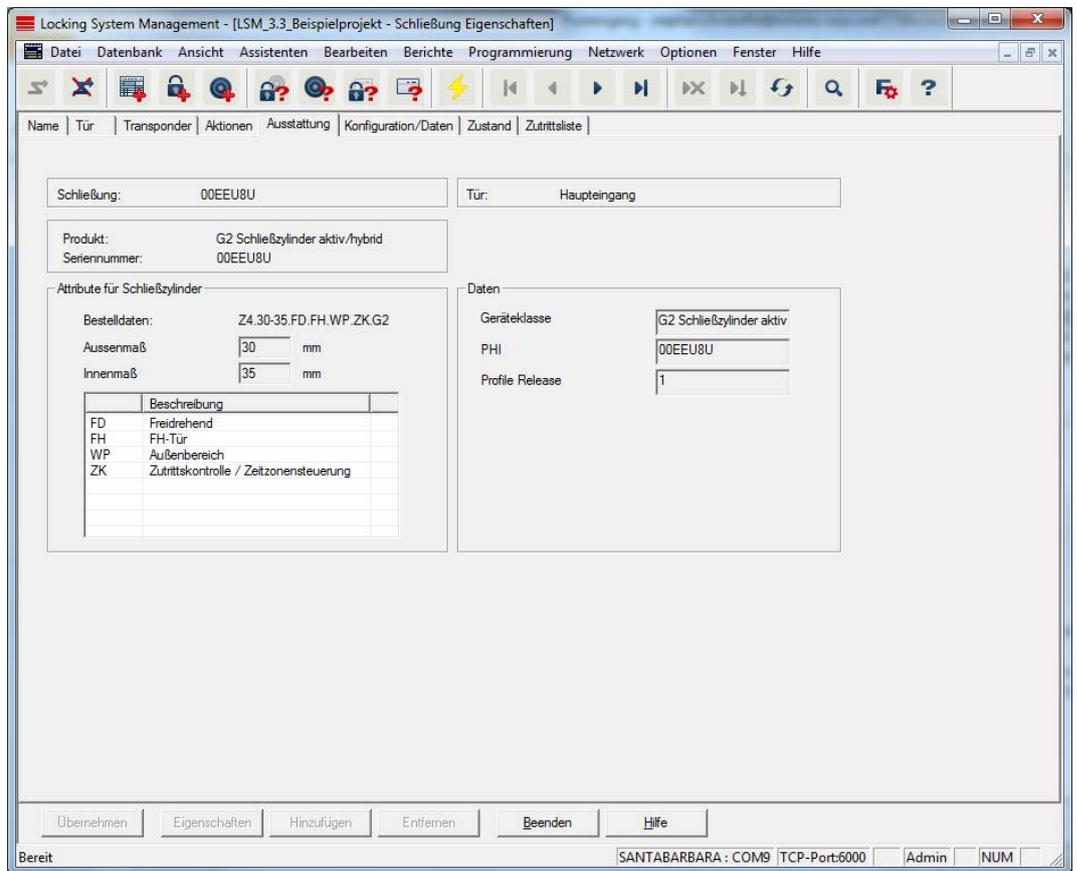
- **Ist Zustand (...)**
Zeigt den aktuell programmierten Zustand an.
- **Programmierbedarf**
Zeigt alle Transponder mit Programmierbedarf an.
- **Zusätzliche Schaltfläche "Ausnahmen im Zeitzonenmanagement":**
Hier können Ausnahmen des Transponders im Zeitzonenmanagement angezeigt werden.

Aktionen



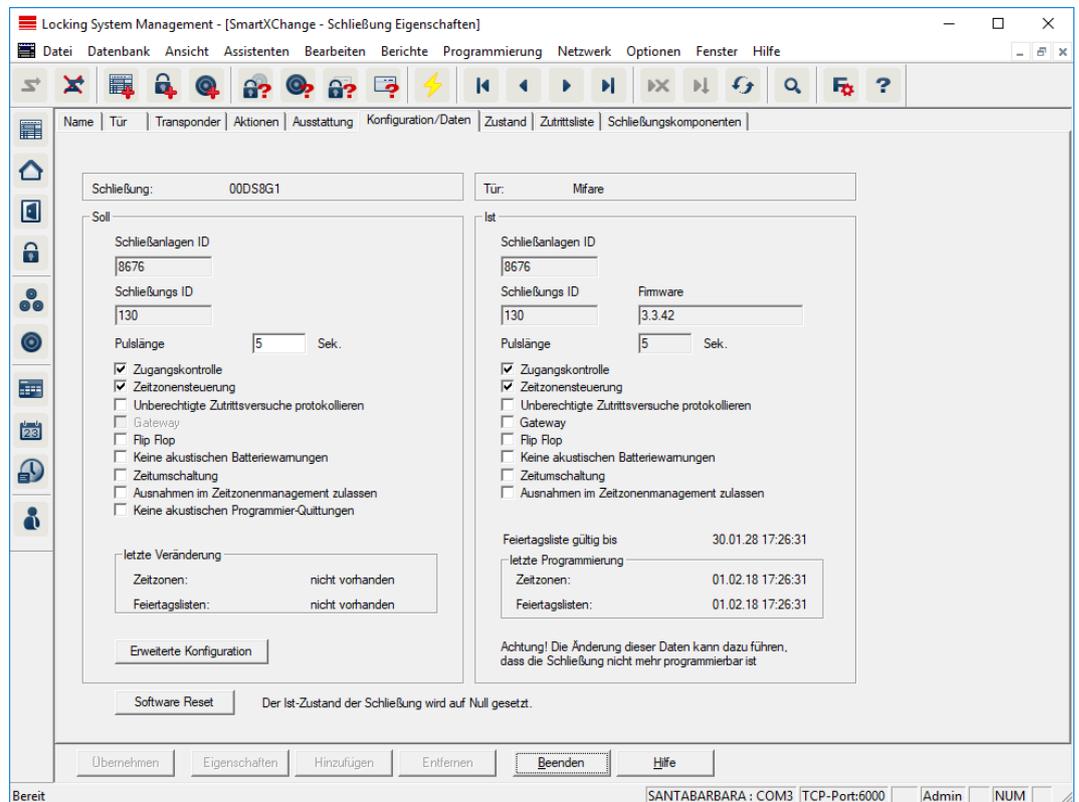
Diese Tabelle zeigt, welche Aktionen (z.B. Programmierung, Berechtigungsänderung, etc.) bei der Schließung durchgeführt wurden. Verschiedene Aktionen, wie z.B. "Letzter Batteriewechsel" lassen sich auch manuell über die Schaltfläche "Hinzufügen" hinzufügen.

Ausstattung



Diese Registerkarte zeigt die genauen Hardware-Optionen der Schließung, welche bei der ersten Programmierung automatisch eingetragen werden.

Konfiguration/Daten



Diese Registerkarte ist in zwei Seiten aufgeteilt:

- Die linke Seite zeigt den Soll-Zustand der Schließung - also der in der LSM Software konfigurierte und gewollte Zustand.
- Auf der rechten Seite wird der Ist-Zustand der Schließung angezeigt - also der Zustand, der zuletzt programmiert wurde.

Folgende Merkmale können **je nach Schließungstyp** aktiviert werden:

■ Zugangskontrolle

Möglichkeit zur Protokollierung der Zutritte. *Diese Funktion funktioniert nur bei Komponenten mit ZK-Funktion.*

Klären Sie, ob der Einsatz dieser Option in Ihrer individuellen Umgebung erlaubt ist; z.B. mit dem Betriebsrat oder dem Datenschutzbeauftragten.

■ Zeitzonesteuerung

Möglichkeit zur zeitlichen Steuerung der Zutritte für Transponder.

■ Unberechtigte Zutrittsversuche protokollieren

Abgewiesene Transponderbuchungen werden in der Schließung festgehalten. Dies gilt nur für Identmedien, die zur gleichen Schließanlage gehören.

■ Gateway

Option für die Nutzung von Gateways. *Nur bei SmartRelais verfügbar.*

❑ Flip Flop

Nach einer Transponderbetätigung kuppelt die Schließung ein und bleibt solange eingekuppelt, bis eine neue Transponderbetätigung folgt.

❑ Keine akustischen Batteriewarnungen

Beim Aktivieren dieser Funktion erfolgen keine akustischen Warnungen zum Status der Batterien in den Komponenten.

❑ Zeitumschaltung

Die Schließung ändert zu festgelegten Zeitpunkten den Zustand automatisch entsprechend den Einstellungen unter "Erweiterte Konfiguration". *Nur bei ZK-Versionen.*

❑ Keine akustischen Programmierquittungen

Beim Programmieren quittiert die Schließung den Ablauf nicht durch Signaltöne.

❑ Karteninterface

Karteninterface mit Schließung verknüpfen.

❑ Erweiterte Konfiguration

Legen Sie erweiterte Konfigurationen, wie z.B. eine zeitgesteuerte Umstellung der Schließung fest.

❑ Software Reset

Schaltfläche zum Zurücksetzen des Ist-Zustands in der LSM Software. Dieser Vorgang wird gezählt und links daneben angezeigt.

DoorMonitoring SmartHandle

Über die Schaltfläche "Monitoring Konfiguration" in der Registerkarte "Konfiguration/Daten" der Schließung können die DoorMonitoring-Funktionen des SmartHandle konfiguriert werden (siehe auch *Inbetriebnahme der DoorMonitoring Schließungen [► 201]*).

Diese Funktion steht nur zur Verfügung, wenn das SmartHandle die DM-Eigenschaft besitzt und dieses in der LSM Software auch direkt als "G2 DoorMonitoring SmartHandle" angelegt wurde!

Door Monitoring Konfiguration

Soll

Tür offen Einstellungen

Abtastintervall für die Door Monitoring Sensoren Sek.

"Tür zu lange offen" Event nach Min.

Escape & Return (zeitgesteuerte Rückkehrfunktion) Sek.

Ereignisse

Protokollierung in der Zutrittsliste

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Türdrücker Sensor Ereignisse

Weiterleitung im Netzwerk

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Türdrücker Sensor Ereignisse

Protokollierung / Weiterleitung der Alarime im Netzwerk

Externe Sensoren

"Tür offen" Eingänge invertieren

Riegel Eingang invertieren

Ist

Tür offen Einstellungen

Abtastintervall für die Door Monitoring Sensoren Sek.

"Tür zu lange offen" Event nach Min.

Escape & Return (zeitgesteuerte Rückkehrfunktion) Sek.

Ereignisse

Protokollierung in der Zutrittsliste

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Türdrücker Sensor Ereignisse

Weiterleitung im Netzwerk

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Türdrücker Sensor Ereignisse

Protokollierung / Weiterleitung der Alarime im Netzwerk

Externe Sensoren

"Tür offen" Eingänge invertieren

Riegel Eingang invertieren

OK Abbrechen

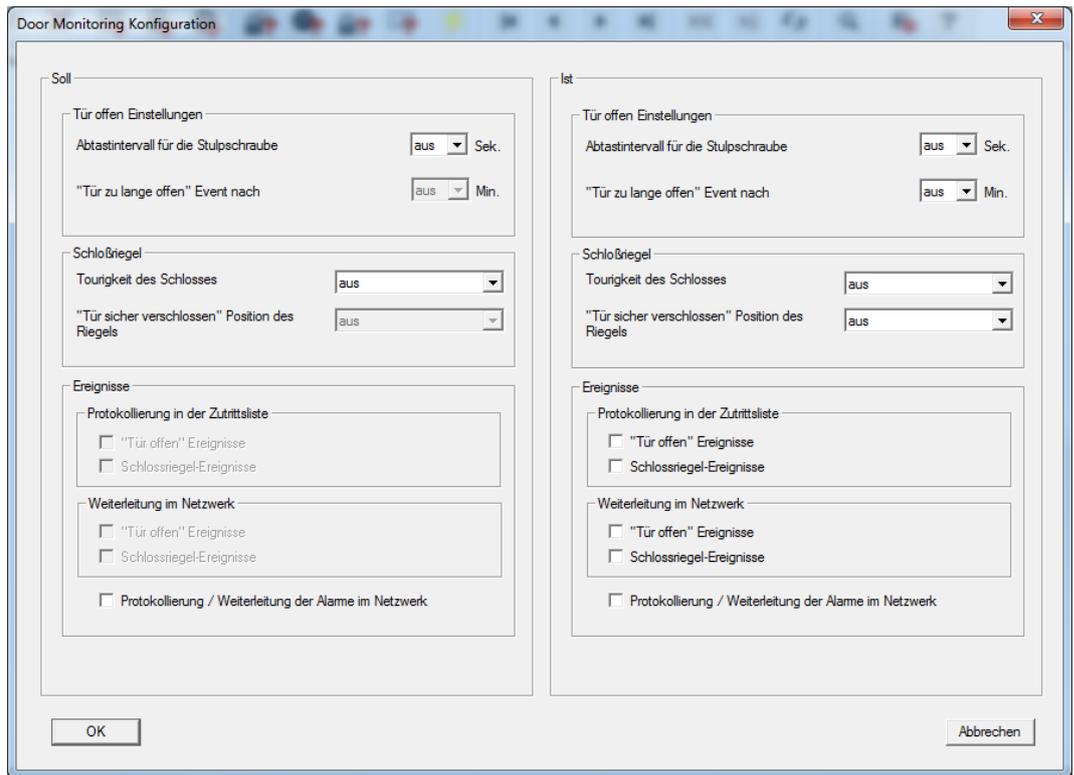
Tätigen Sie die gewünschten Änderungen im linken "Soll-Bereich".

- **Escape & Return:** Verlängert die Einkuppelzeit des SmartHandle, nachdem die Tür wieder als geschlossen detektiert wurde.

DoorMonitoring Schließzylinder

Über die Schaltfläche "Monitoring Konfiguration" in der Registerkarte "Konfiguration/Daten" der Schließung können die DoorMonitoring-Funktionen des Schließzylinders konfiguriert werden (siehe auch *Inbetriebnahme der DoorMonitoring Schließungen* [► 201]).

Diese Funktion steht nur zur Verfügung, wenn der Schließzylinder die DM-Eigenschaft besitzt und dieser in der LSM Software auch direkt als "G2 Door Monitoring Zylinder" angelegt wurde!

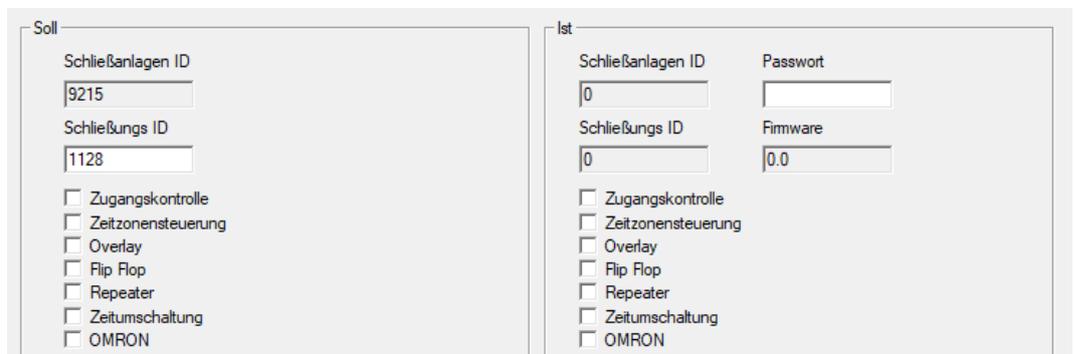


Tätigen Sie die gewünschten Änderungen im linken "Soll-Bereich".

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

Diese Registerkarte ist in zwei Seiten aufgeteilt:

- Die linke Seite zeigt den "Soll"-Zustand der Schließung - also der in der LSM Software konfigurierte und gewollte Zustand.
- Auf der rechten Seite wird der "Ist"-Zustand der Schließung angezeigt - also der Zustand, der zuletzt programmiert wurde.

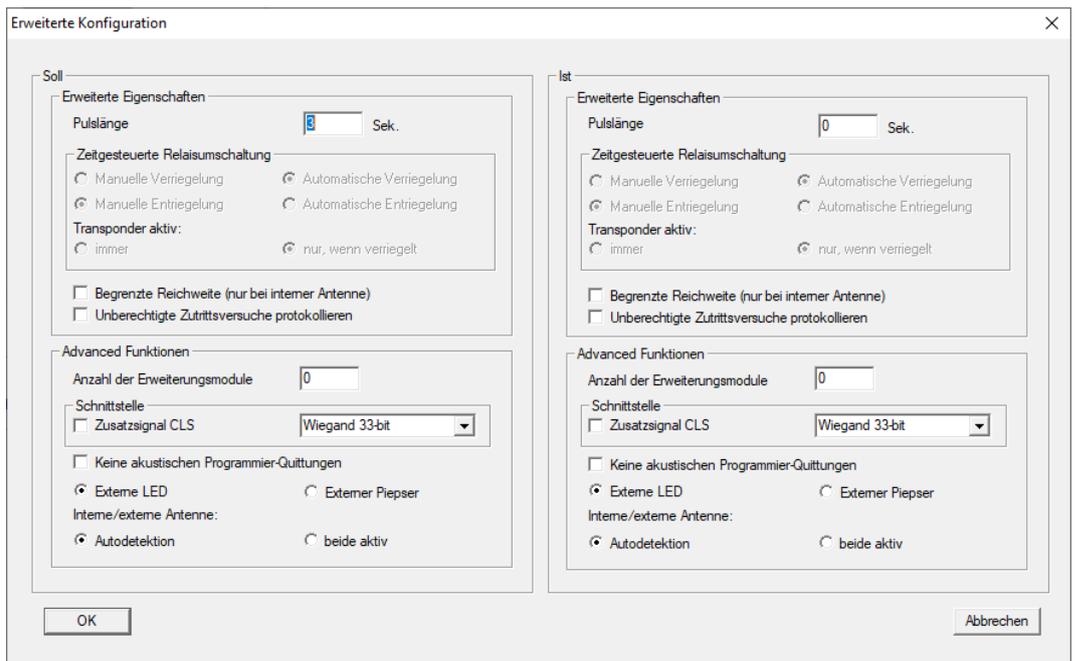


Folgende Merkmale können **je nach Schließungstyp** aktiviert werden:

<input checked="" type="checkbox"/> Zugangskontrolle	Nur bei SREL.ZK und SREL.ADV möglich. Die jeweils letzten 1.024 Transponderbetätigungen werden mit Datum und Uhrzeit gespeichert.
--	---

<input checked="" type="checkbox"/> Zeitzonesteuerung	<p>Nur bei SREL.ZK und SREL.ADV mit LSM Business oder Professional möglich. Ein Zeitzoneplan kann geladen werden und die Transponder werden dann entsprechend ihrer Zeitzonegruppe zugelassen bzw. gesperrt.</p>
<input checked="" type="checkbox"/> Overlay	<p>Ersatztransponder können ihre Ursprungstransponder überschreiben. Nach der erstmaligen Betätigung mit einem Ersatztransponder, ist der Ursprungstransponder gesperrt.</p>
<input checked="" type="checkbox"/> Flip Flop	<p>Der Impulsmodus (Default Einstellung) wird abgeschaltet, die Impulsdauer spielt keine Rolle mehr. Das SmartRelais wechselt bei eingeschaltetem FlipFlop-Modus seinen Zustand bei jeder Transponderbetätigung von AN nach AUS oder umgekehrt. Dieser Modus empfiehlt sich zum Schalten von Licht oder Maschinen etc.</p> <p><i>Bei einer solchen Installation ist gegebenenfalls darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind.</i></p>
<input checked="" type="checkbox"/> Repeater	<p>Das SmartRelais empfängt ein Transpondersignal und sendet dieses verstärkt weiter. In dieser Funktion kann das SmartRelais verwendet werden, um größere Funkstrecken zu überbrücken. Die Entfernung zu einem anderen SmartRelais kann bis zu 2 m betragen.</p>
<input checked="" type="checkbox"/> Zeitumschaltung	<p>Nur bei SREL.ZK und SREL.ADV mit LSM Business oder Professional möglich. Wenn die Zeitumschaltung aktiviert wird, muss ein Zeitzoneplan geladen werden, der eine generelle Freischaltung des SmartRelais während der markierten Zeiten (in Gruppe 5) ermöglicht. Also kann eine Tür tagsüber frei begehbar sein und nachts nur über Transponder geöffnet werden.</p> <p><i>Bei einer solchen Installation ist darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind</i></p>

<input checked="" type="checkbox"/> OMRON	<p>Nur für SREL.ADV. Viele Zutrittskontroll- und Zeiterfassungssysteme besitzen serielle Schnittstellen zum Anschluss von Kartenlesern. Über diese Schnittstellen ist auch der Anschluss eines Smart-Relais möglich. Damit können Sie den SimonsVoss Transponder auch in Fremdsystemen benutzen.</p> <p>Möchten Sie, dass das SmartRelais die Transponderdaten zu einem Fremdsystem überträgt, und bei Freischaltung durch das Fremdsystem vom Smart-Relais ein Fernöffnungsbefehl zu einem Zylinder gesendet wird, dann wählen sie diese Option sowohl am SmartRelais als auch am Zylinder.</p> <p>Der Typ des externen Systems ist unter "Schnittstelle" einzustellen. Klicken Sie hierfür auf die Schaltfläche Erweiterte Konfiguration.</p>
---	--



Über die Schaltfläche **Erweiterte Konfiguration** können einige Einstellungen präzisiert werden:

Pulslänge	<p>Hier geben Sie den Wert für die Impulsdauer des Schaltimpulses in Sekunden an. Der Wert kann 0,1 bis 25,5 Sekunden betragen. Wenn sie zum Beispiel 3 Sekunden eintragen, dann wird ein Türöffner für 3 Sekunden frei geschaltet, bevor er wieder sperrt.</p>
------------------	---

<input checked="" type="checkbox"/> Begrenzte Reichweite	Bei Auswahl dieser Option wird die Lesereichweite Transponder zu SmartRelais von ca. 1,5 m auf ca. 0,4 m begrenzt. Diese Option kann z.B. benutzt werden, wenn sich mehrere SmartRelais in unmittelbarer Nähe zueinander befinden, und einzelne Transponder an mehreren SmartRelais berechtigt sind.
<input checked="" type="checkbox"/> Unberechtigte Zutrittsversuche protokollieren	Nur für SREL.ZK und SREL.ADV: Normalerweise werden nur berechtigte Transponderbetätigungen protokolliert. Wenn gewünscht wird, auch den Versuch der Türöffnung mit einem unberechtigten Transponder zu erfassen, muss diese Option gewählt werden.
Anzahl Erweiterungsmodule	Hier geben Sie die Anzahl der an das SmartRelais angeschlossenen externen Module an. Diese Module werden an die Klemmen RS-485 C OM, RS-485 A und RS-485 B angeschlossen.
"Schnittstelle"	Nur bei SREL.ADV: Für den Betrieb als Serielle Schnittstelle können Sie hier die Art des Kartenlesers einstellen, den das SmartRelais simulieren soll. Als Optionen stehen zur Verfügung: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Wiegand 33 bit <input checked="" type="checkbox"/> Wiegand 26 bit <input checked="" type="checkbox"/> Primion <input checked="" type="checkbox"/> Siemens <input checked="" type="checkbox"/> Kaba Benzing <input checked="" type="checkbox"/> Gantner Legic <input checked="" type="checkbox"/> Isgus
<input checked="" type="checkbox"/> Keine akustischen Programmierquittungen	Nur bei SREL.ADV: Wenn gewünscht wird, dass bei einer Programmierung des SmartRelais keine Programmierquittungen über einen angeschlossenen Buzzer/Piepser gegeben werden sollen, dann ist dieses Feld anzukreuzen.

<p><input type="radio"/> Externe LED/ <input type="radio"/> Externer Piepser</p>	<p>Nur bei SREL.ADV: Hier wird angegeben, welche externe Baugruppe angeschlossen ist. Das SmartRelais erzeugt im FlipFlop-Mode bei einer externen LED ein Dauersignal im geschalteten Zustand, während bei einem angeschlossenen Piepser nur jeder Zustandswechsel kurz mit einem Tonsignal quittiert wird.</p>
<p><input type="radio"/> Autodetektion/ <input type="radio"/> Beide aktiv</p>	<p>Nur bei SREL.ADV</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> <input type="radio"/> Autodetektion <p>Ist eine externe Antenne angeschlossen, wird nur diese benutzt. Das SmartRelais schaltet dann die interne Antenne aus. Wenn keine externe Antenne angeschlossen ist (Standardfall), dann arbeitet das SmartRelais mit der internen Antenne.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> <input type="radio"/> Beide aktiv <p>Das SmartRelais kann Buchungen von Transpondern an beiden Antennen bewerten.</p>

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

Diese Registerkarte ist in zwei Seiten aufgeteilt:

- Die linke Seite zeigt den "Soll"-Zustand der Schließung - also der in der LSM Software konfigurierte und gewollte Zustand.
- Auf der rechten Seite wird der "Ist"-Zustand der Schließung angezeigt - also der Zustand, der zuletzt programmiert wurde.

<p>Schließung: 000023B</p>	<p>Tür: Metro News One Studiolights</p>
<p>Soll</p> <p>Schließanlagen ID <input type="text" value="9215"/></p> <p>Schließungs ID <input type="text" value="197"/></p> <p>Pulslänge <input type="text" value="5"/> Sek.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Zugangskontrolle <input checked="" type="checkbox"/> Zeitzonesteuerung <input type="checkbox"/> Unberechtigte Zutrittsversuche protokollieren <input type="checkbox"/> Gateway <input checked="" type="checkbox"/> Flip Flop <input type="checkbox"/> Interne Antenne immer an <input type="checkbox"/> Nahbereichsmodus (nur bei interner Antenne) <input type="checkbox"/> Zeitschaltung <input type="checkbox"/> Ausnahmen im Zeitonenmanagement zulassen <input checked="" type="checkbox"/> Karteninterface 	<p>Ist</p> <p>Schließanlagen ID <input type="text" value="9215"/></p> <p>Schließungs ID <input type="text" value="197"/> Firmware <input type="text" value="3.0.14"/></p> <p>Pulslänge <input type="text" value="5"/> Sek.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Zugangskontrolle <input checked="" type="checkbox"/> Zeitzonesteuerung <input type="checkbox"/> Unberechtigte Zutrittsversuche protokollieren <input type="checkbox"/> Gateway <input checked="" type="checkbox"/> Flip Flop <input type="checkbox"/> Interne Antenne immer an <input type="checkbox"/> Nahbereichsmodus (nur bei interner Antenne) <input type="checkbox"/> Zeitschaltung <input type="checkbox"/> Ausnahmen im Zeitonenmanagement zulassen <p style="text-align: right;">09.09.2019 10:20:19</p>

Folgende Merkmale können je nach Schließungstyp aktiviert werden:

- Pulslänge

Hier geben Sie den Wert für die Impulsdauer des Schaltimpulses in Sekunden an. Der Wert kann 0,1 bis 25,5 Sekunden betragen. Wenn sie zum Beispiel 3 Sekunden eintragen, dann wird ein Türöffner für 3 Sekunden frei geschaltet, bevor er wieder sperrt.

❑ Zugangskontrolle

ZK und ADV möglich. Die jeweils letzten Transponderbetätigungen werden mit Datum und Uhrzeit gespeichert.

❑ Zeitonensteuerung

Nur bei ZK und ADV möglich. Ein Zeitonenplan kann geladen werden und die Transponder werden dann entsprechend ihrer Zeitonengruppe zugelassen bzw. gesperrt.

❑ Unberechtigte Zutrittsversuche protokollieren

Nur für ZK und ADV: Normalerweise werden nur berechnigte Transponderbetätigungen protokolliert. Wenn gewünscht wird, auch den Versuch der Türöffnung mit einem unberechnigten Transponder zu erfassen, muss diese Option gewählt werden.

❑ Gateway

Das SmartRelais kann als Gateway genutzt werden.

❑ FlipFlop

Der Impulsmodus (Default Einstellung) wird abgeschaltet, die Impulsdauer spielt keine Rolle mehr. Das SmartRelais wechselt bei eingeschaltetem FlipFlop-Modus seinen Zustand bei jeder Transponderbetätigung von AN nach AUS oder umgekehrt. Dieser Modus empfiehlt sich zum Schalten von Licht oder Maschinen etc.

Bei einer solchen Installation ist gegebenenfalls darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind.

❑ Interne Antenne immer an

Auch wenn eine externe Antenne angeschlossen, wird trotzdem die interne Antenne parallel weiter benutzt.

❑ Nahbereichsmodus (nur bei interner Antenne)

Der Nahbereichsmodus wird aktiviert.

❑ Zeitumschaltung

Nur für ZK und ADV. Wenn die Zeitumschaltung aktiviert wird, muss ein Zeitonenplan geladen werden, der eine generelle Freischaltung des SmartRelais während der markierten Zeiten (in Gruppe 5) ermöglicht. Also kann eine Tür tagsüber frei begehbar sein und nachts nur über Transponder geöffnet werden.

Bei einer solchen Installation ist darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind

■ **Ausnahmen im Zeitzonenmanagement zulassen**

Wenn diese Checkbox aktiviert ist, dann sind Ausnahmen im Zeitzonenmanagement zulässig.

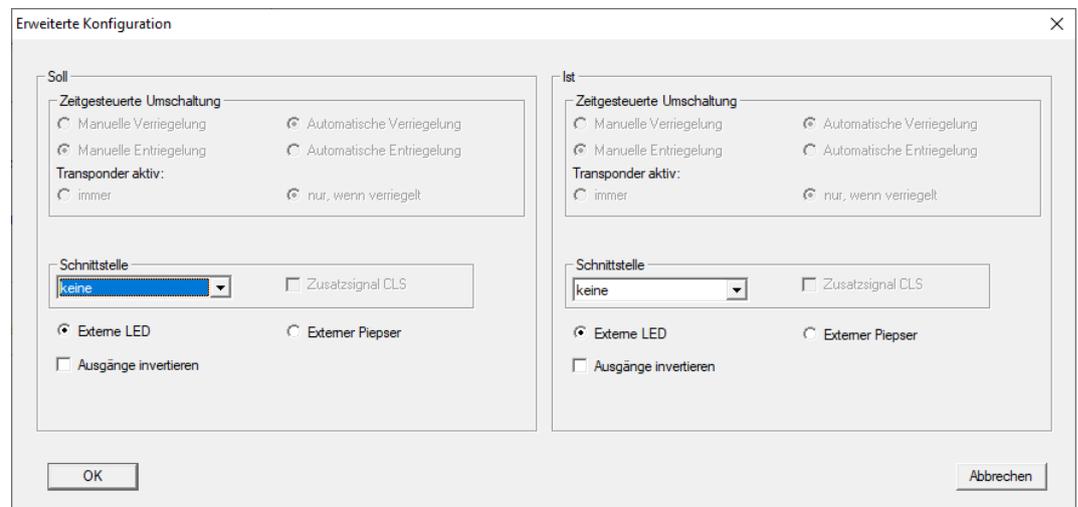
■ **Karteninterface**

Diese Option ist standardmäßig für alle G2 SmartRelais aktiviert. Die LSM legt zuerst einen Datensatz für eine aktive Schließung an und prüft bei der Programmierung, ob die Schließung ein Karteninterface hat. Wenn kein Karteninterface erkannt wird, dann wird die Checkbox von der LSM automatisch deaktiviert. Sie müssen seit der LSM 3.3 nicht mehr angeben, ob sie ein aktives oder ein hybrides SmartRelais G2 haben.



HINWEIS

Wenn Sie die Einstellung Karteninterface manuell verändern, funktioniert die automatische Erkennung nicht mehr und Warnmeldungen werden ausgegeben.



Über die Schalfläche "Erweiterte Konfiguration" können einige Einstellungen präzisiert werden:

■ **Schnittstelle**

Für den Betrieb als Serielle Schnittstelle können Sie hier die Art des Kartenlesers einstellen, den das SmartRelais simulieren soll.

Als Optionen stehen zur Verfügung:

- Wiegand 33 bit
- Wiegand 26 bit
- Primion
- Siemens

- Kaba Benzing
- Gantner Legic
- Isgus

■ Externer Piepser / Externe LED

Nur bei SREL.ADV: Hier wird angegeben, welche externe Baugruppe angeschlossen ist. Das SmartRelais erzeugt im FlipFlop-Mode bei einer externen LED ein Dauersignal im geschalteten Zustand, während bei einem angeschlossenen Piepser nur jeder Zustandswechsel kurz mit einem Tonsignal quittiert wird.

■ Ausgänge invertieren

Über diese Einstellungen können Sie den Relaisausgang invertieren.

SmartRelais 3

Diese Registerkarte ist zweigeteilt.

- Der Bereich "Soll" zeigt den Soll-Zustand der Schließung. Dieser Zustand ist vom Bediener gewollt und in der LSM konfiguriert, aber möglicherweise noch nicht im SREL3-3-ADV-System programmiert.
- Der Bereich "Ist" zeigt den Ist-Zustand der Schließung. Dieser Zustand ist der zuletzt im SREL3-ADV-System programmierte Zustand.

Je nach Schließungstyp können folgende Merkmale aktiviert werden:

■ Pulslänge

Hier geben Sie den Wert für die Impulsdauer des Schaltimpulses in Sekunden an (0 s bis 25 s). Wenn der Wert zum Beispiel drei Sekunden beträgt, dann wird ein Türöffner für drei Sekunden freigeschaltet, bis er wieder sperrt.

■ Zugangskontrolle

Die Zugangskontrolle ist nur in der ZK-Variante verfügbar. Die jeweils letzten Transponderbetätigungen werden mit Datum und Uhrzeit gespeichert.

■ Zeitzonesteuerung

Die Zeitzonesteuerung ist nur in der ZK-Variante verfügbar. Sie können einen Zeitzoneplan laden. Die Transponder werden dann entsprechend ihrer Zeitzonegruppe zugelassen bzw. gesperrt.

■ Unberechtigte Zutrittsversuche protokollieren

Die Protokollierung unberechtigter Zutrittsversuche ist nur in der ZK-Variante verfügbar. Wenn Sie diese Option aktivieren, werden zusätzlich zu den Betätigungen von berechtigten Transpondern auch die Betätigungen unberechtigter Transponder gespeichert.

☒ Gateway

Das SmartRelais kann als Gateway genutzt werden (siehe Gateway-Funktion).

☒ Flip Flop

Das im Controller eingesetzte Relais verhält sich standardmäßig wie ein Monoflop (Impulsöffnung). Wenn Sie diese Option aktivieren, dann wird die eingestellte Pulsdauer ignoriert und das Relais so lange geschaltet, bis erneut ein berechtigtes Identifikationsmedium betätigt wird. Diese Option empfiehlt sich, wenn Licht, Maschinen und ähnliche Geräte angesteuert werden sollen.

ACHTUNG

Beschädigung durch Dauerstrom

Geräte, die auf Impulsöffnung ausgelegt sind, sind möglicherweise nicht für Dauerstrom geeignet. Achten Sie darauf, dass die verwendeten Netzteile und Geräte (z.B. Türöffner) für Dauerstrombetrieb geeignet sind.

☒ Nahbereichsmodus

Der Nahbereichsmodus verringert die Lesereichweite im B-Feld der Leser (siehe Nahfeld-Option).

☒ Zeitumschaltung

Die Zeitumschaltung ist nur in der ZK-Variante verfügbar. Sie können einen Zeitzonenplan laden. Wenn Sie die Zeitumschaltung aktivieren, dann kann das SREL3-ADV-System während der berechtigten oder nicht berechtigten Zeiten (in Gruppe 5) automatisch freigeschaltet oder gesperrt werden. Je nach Einstellung schaltet das SREL3-ADV-System sogar automatisch. Beispielsweise kann eine Tür so tagsüber automatisch offen stehen, nachts dagegen nur mit einem Transponder geöffnet werden (siehe Zeitumschaltung).

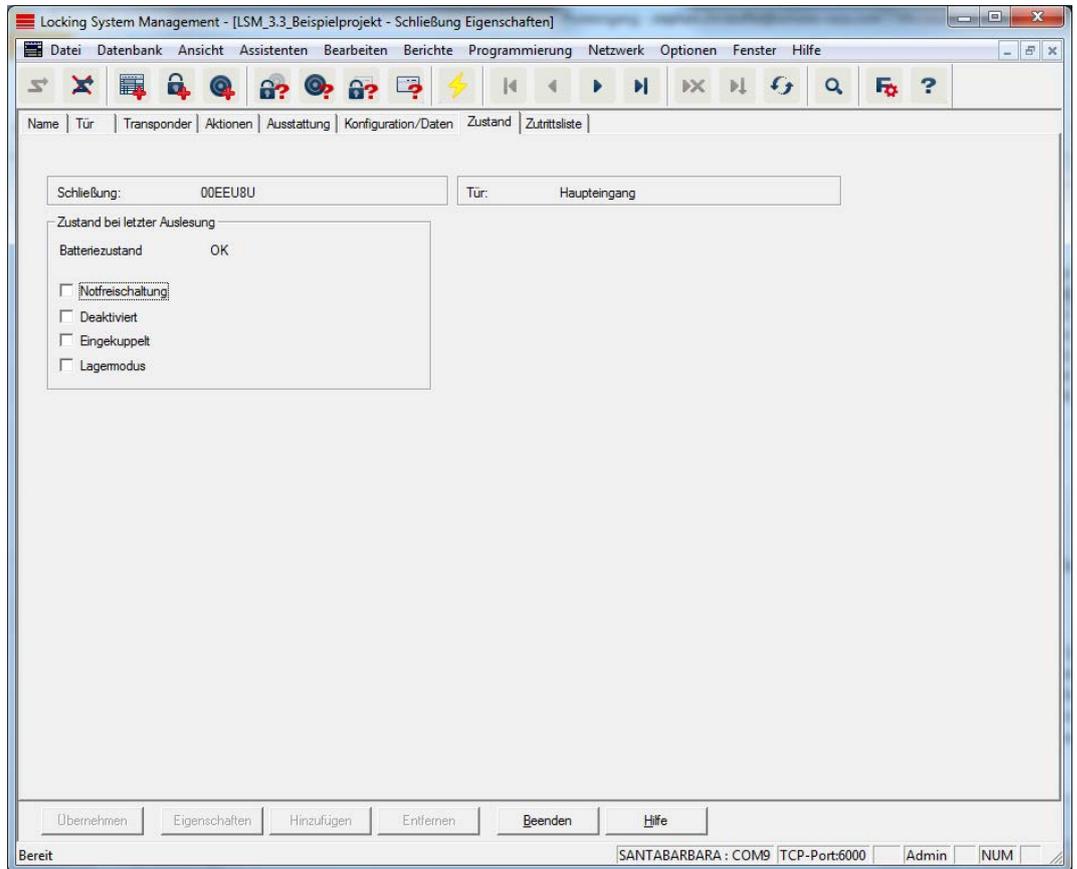
☒ Aktivierungs- bzw. Verfallsdatum ignorieren

Transponder können mit einem Gültigkeitsdatum versehen sein. Wenn Sie die Transponder auch außerhalb dieses Gültigkeitsdatums weiterhin berechtigen wollen, dann können Sie diese Option aktivieren.

☒ Karteninterface

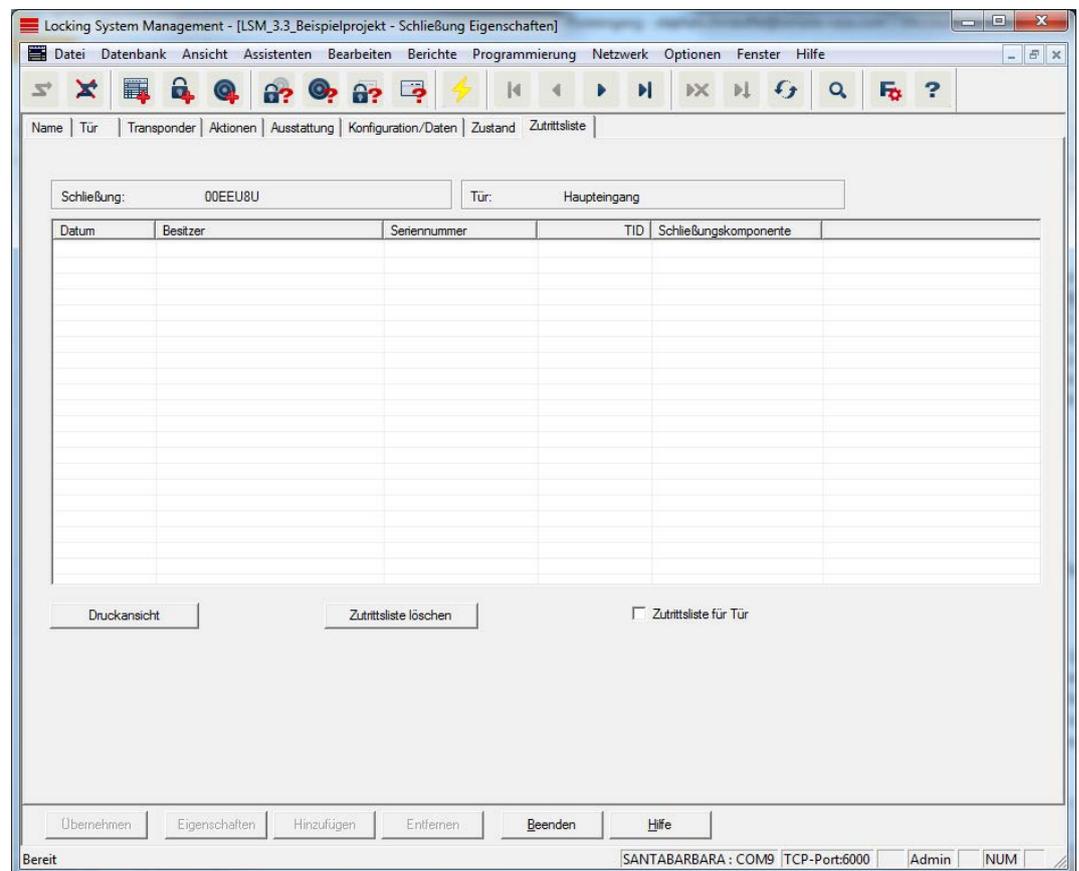
Diese Option sollte nicht verändert werden. Damit kann die LSM bei der Programmierung automatisch erkennen, ob der angeschlossene Leser ein Hybridleser ist. Wenn Sie diese Option manuell verändern, dann funktioniert diese Erkennung nicht mehr.

Zustand



Der zuletzt ausgelesene Zustand der Schließung wird angezeigt und bei jedem Auslesen der Schließung aktualisiert.

Zutrittsliste



Auf dieser Registerkarte kann der letzte Stand der Zutrittsliste angezeigt werden. *Die Funktion "Zutrittskontrolle" muss von der Schließung unterstützt werden und in den Eigenschaften der Schließung aktiviert sein.*

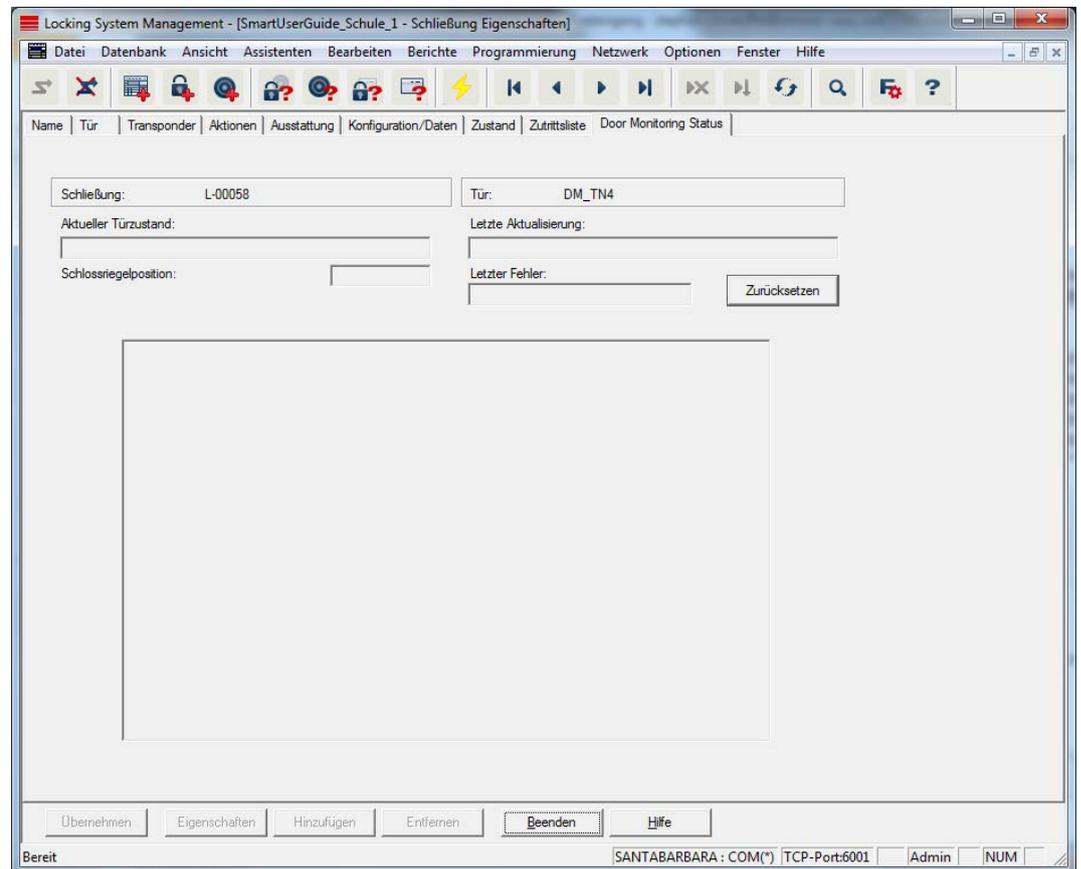
So lesen Sie die Zutrittsliste aus:

1. Schließung über die Menüleiste *Programmierung/Schließung auslesen* auslesen.
2. Auf die Schaltfläche "Zutrittsliste" klicken, um den Auslesevorgang zu starten.
 - ↳ Die Zutrittsliste wird automatisch dargestellt und gespeichert. Sie kann jetzt jederzeit über die Registerkarte Zutrittsliste in den Schließungseigenschaften angezeigt werden.

DoorMonitoring Status

Über die Registerkarte "DoorMonitoring Status" kann der aktuelle Status der Schließung in Echtzeit angezeigt werden (siehe auch *Mögliche (Tür-)zustände [▶ 201]*). Für diese Funktion ist ein konfiguriertes WaveNet notwendig.

Diese Registerkarte steht nur zur Auswahl, wenn die Schließung die DM-Eigenschaft besitzt und diese in der LSM Software auch direkt als "G2 DoorMonitoring Zylinder/SmartHandle" angelegt wurde! Die Abbildung kann variieren.



HINWEIS

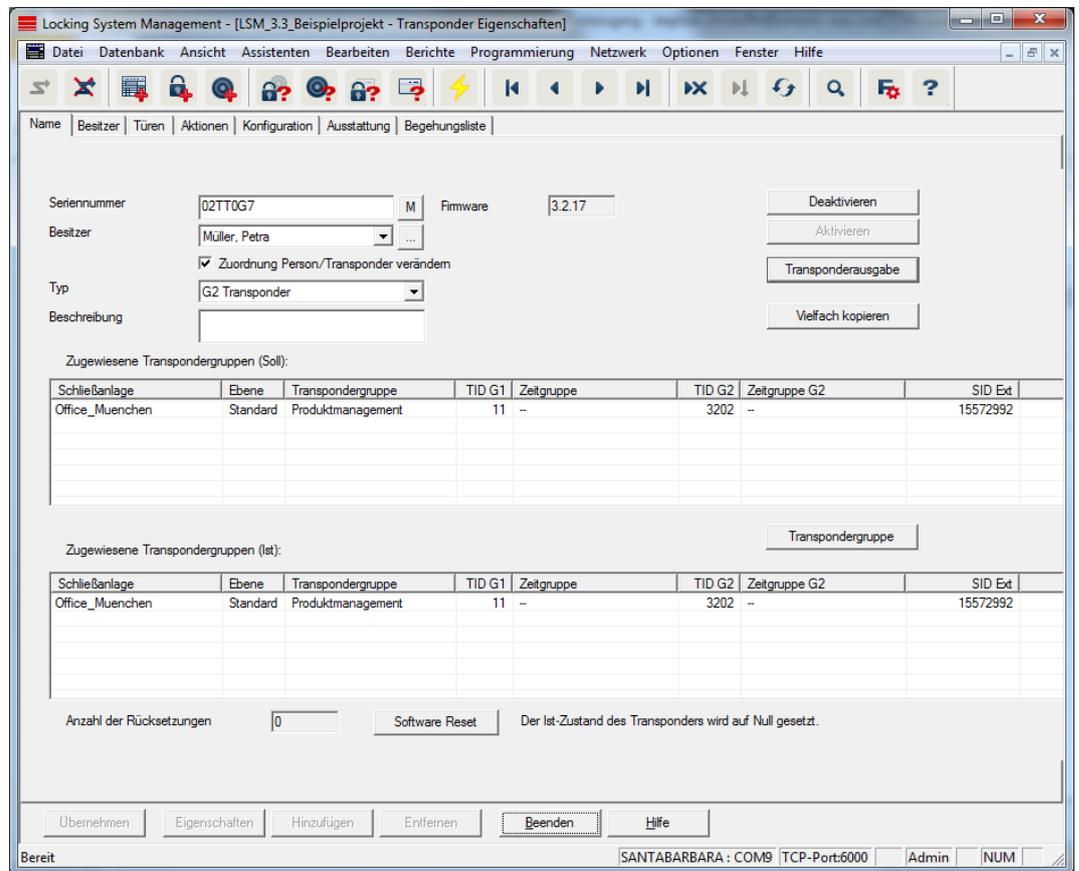
Wenn Sie mehrere Schließungen gleichzeitig überwachen wollen, können Sie mit Smart.Surveil die Schließungen und den jeweiligen Türzustand auch übersichtlich in einer Tabelle anzeigen lassen.

7.1.5.3 Eigenschaften: Transponder

Eigenschaften des aktuell markierten Transponders anzeigen und bearbeiten.

Ein Doppelklick auf einen Transponder öffnet die Eigenschaften des entsprechenden Transponders direkt!

Name



■ **Seriennummer**

Seriennummer des Transponders. Die Schaltfläche "..." zeigt die Eigenschaften der Person an. Bei der Programmierung von G2-Transpondern wird automatisch deren "Interne Seriennummer" (PHI-Nummer (*Physical Hardware Identifier; auf dem Produkt aufgedruckt*)) übernommen.

■ **Besitzer**

Zugewiesene Person des Transponders. Die Schaltfläche "M" zeigt den Transponder in der Matrix an.

■ **Typ**

Art des Transponders.

■ **Beschreibung**

Freies Feld zur Beschreibung des Transponders.

■ **Zugewiesene Transpondergruppen: Soll-Zustand**

Soll-Zustand der Transpondergruppen, in der sich der Transponder befindet.

■ **Transpondergruppe**

Über diese Schaltfläche können Sie den Transponder einer anderen Transpondergruppe zuweisen.

■ **Zugewiesene Transpondergruppen: Ist-Zustand**

Ist-Zustand (letzte Programmierung) der Transpondergruppen, in der sich der Transponder befindet.

■ **Software Reset**

Schaltfläche zum Zurücksetzen des Ist-Zustands in der LSM Software. Dieser Vorgang wird gezählt und links daneben angezeigt.



HINWEIS

Nutzen Sie diese Funktion nur, wenn Sie sich über den Verbleib der programmierten Komponente im Klaren sind! Diese Aktion kann z.B. bei einem physikalisch defekten Transponder durchgeführt werden. Ein korrekt programmierter und funktionsfähiger Transponder, bei dem lediglich ein Software Reset durchgeführt wurde, kann unter Umständen noch an Schließungen berechtigt sein. Das stellt ein hohes Sicherheitsrisiko da!

■ **Deaktivieren**

Schaltfläche zum Deaktivieren eines Transponders.

■ **Aktivieren**

Schaltfläche zum Aktivieren eines Transponders.

■ **Transponderausgabe**

Generierung eines Formulars mit Unterschrift für die Übergabe. Dieses Formular enthält auch eine Liste aller berechtigten Türen.

■ **Vielfach kopieren**

Erzeugt beliebig viele Kopien des Transponders mit denselben Eigenschaften.

Besitzer

Locking System Management - [LSM_3.3_Beispielprojekt - Transponder Eigenschaften]

Transponder: T-00003

Vorname: Petra
Nachname: Müller
Titel: B.Eng.
Adresse:
Telefon: 089-12345
E-Mail: petra.mueller@simons-voss.com
Personalnummer: P-00003
Benutzername: kein
Abteilung: Produktmanagement
Ort/Gebäude:
Eingestellt von: 24.08.2015 nicht relevant
Eingestellt bis: 25.08.2015 nicht relevant
Geburtsdatum: 24.08.1987 nicht relevant
Kostenstelle: 4711
Bemerkung:

Transponder

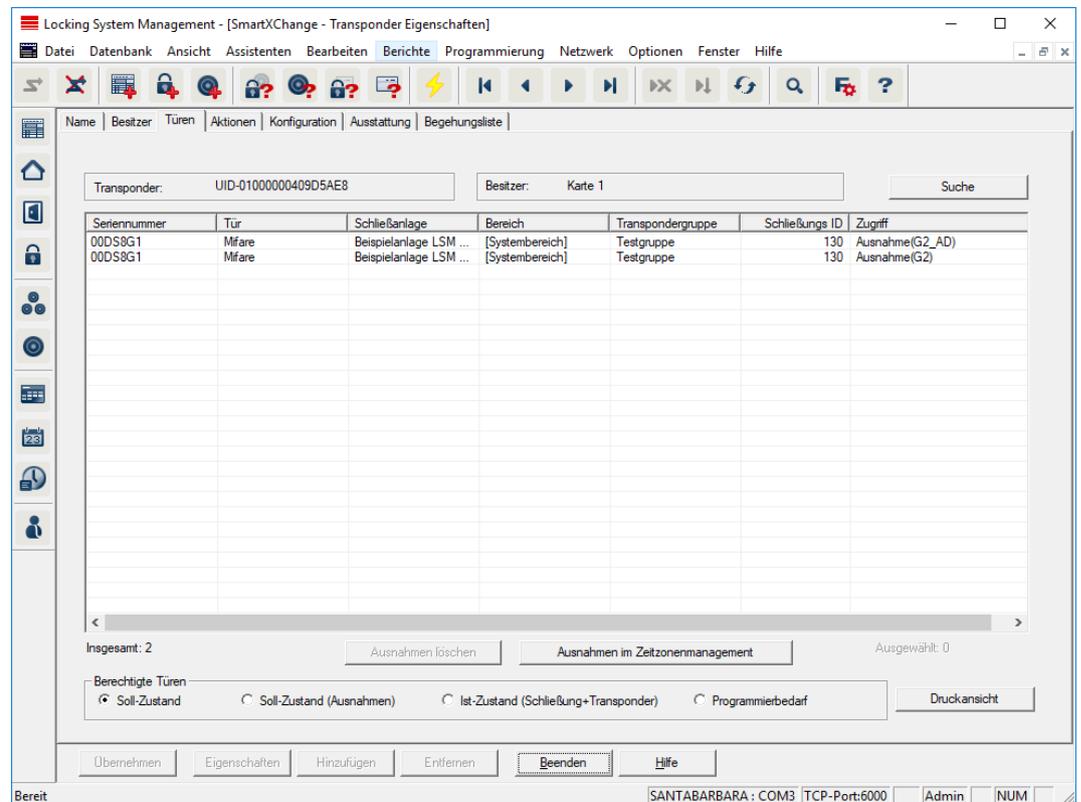
Seriennummer	Typ
T-00003	G2 Transponder

Übernehmen Eigenschaften Hinzufügen Entfernen Beenden Hilfe

Bereit SANTABARBARA : COM9 TCP-Port:6000 Admin NUM

In der Registerkarte "Besitzer" können Sie alle Informationen zum Besitzer des Transponders eintragen. Die Tabelle "Transponder" zeigt, wie viele und welche Transponder dem Benutzer zugeteilt sind. Über die Schaltfläche "..." kann ein Benutzerfoto eingefügt werden. *Es werden Bilder vom Typ JPEG empfohlen, die nicht größer als 500 kB sind.*

Türen



Diese Registerkarte verschafft einen Überblick über die Berechtigungen des ausgewählten Transponders an den Türen. Diese werden alle detailliert in einer Tabelle angezeigt.

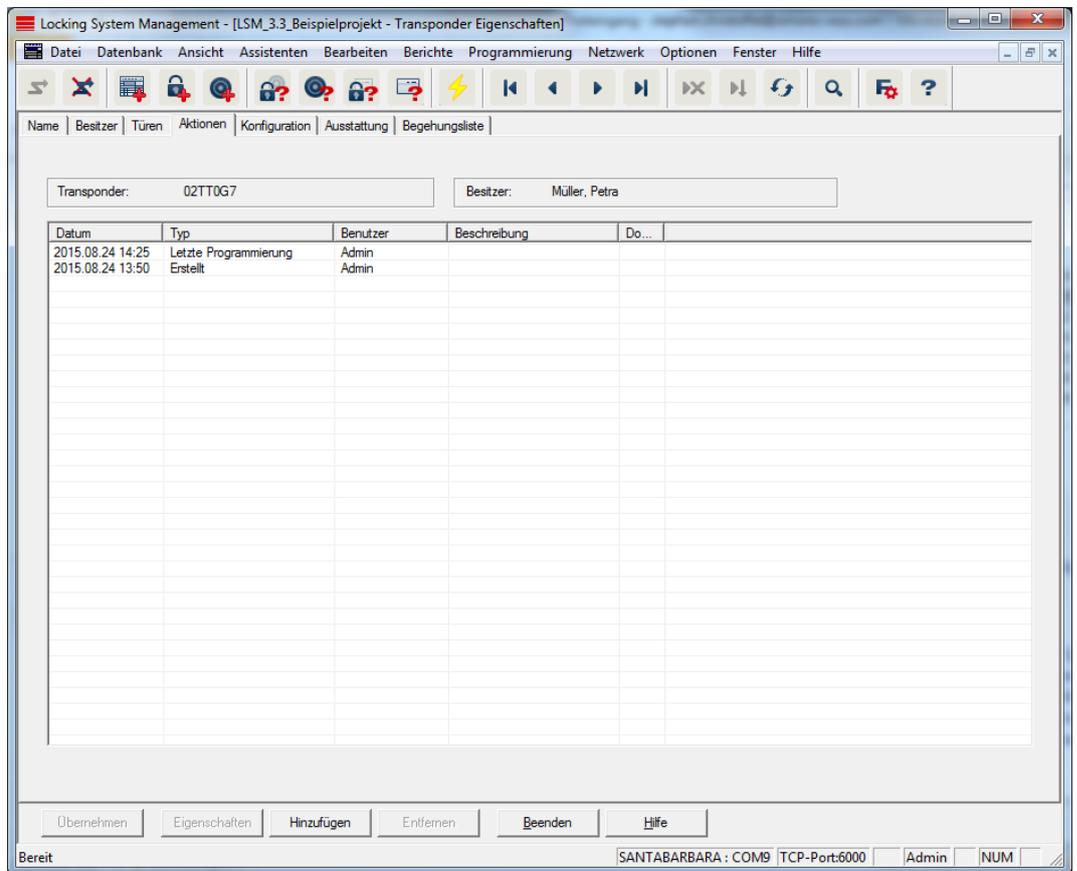
■ Tabelle

Zeigt alle berechtigten Türen des Transponders in einer detaillierten Liste.

■ Berechtigte Türen

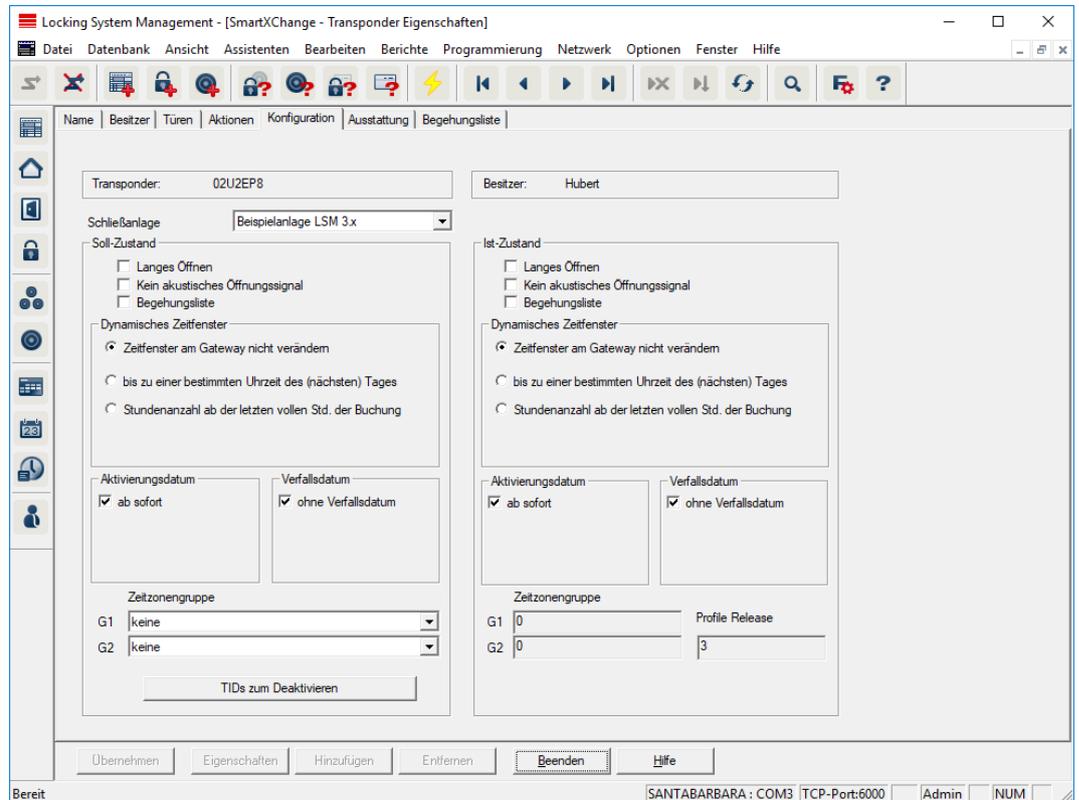
Über die einzelnen Radio-Buttons kann die Tabelle sortiert und gefiltert werden.

Aktionen



Diese Tabelle zeigt, welche Aktionen (z.B. Programmierung, Berechtigungsänderung, etc.) bei dem ausgewählten Transponder durchgeführt wurden. Bestimmte Aktionen, wie z.B. "Geplante Rückgabe" lassen sich manuell über die Schaltfläche "Hinzufügen" hinzufügen.

Konfiguration



Diese Registerkarte ist in zwei Seiten aufgeteilt:

- Die linke Seite zeigt den Soll-Zustand des Transponders, also der in der LSM Software konfigurierte und gewünschte Zustand.
- Auf der rechten Seite wird der Ist-Zustand des Transponders angezeigt, also der Zustand, der zuletzt programmiert wurde.

■ Schließenanlage

Zeigt die aktuell zugewiesene Schließenanlage des Transponders an.

■ Langes Öffnen

Die Schließung bleibt dadurch länger eingekuppelt. Die Pulslänge der Schließung wird verdoppelt. *Anwendungsbeispiel: Personen mit Behinderung benötigen möglicherweise mehr Zeit für das Öffnen der Tür.*

■ Kein akustisches Öffnungssignal

Die Schließung reagiert auf den Transponder ohne Quittierungston. *Anwendungsbeispiel: betreutes Wohnen. Die Nachtschwester gelangt geräuschlos ins Zimmer.*

■ Begehungsliste

Speichert alle Begehungen im Transponder.

■ Zeitfenster am Gateway nicht verändern

Dieser am Gateway buchende G2 Transponder wird in seiner Gültigkeit zeitlich nicht befristet.

❑ **bis zu einer bestimmten Uhrzeit des nächsten Tages**

Dieser am Gateway buchende G2 Transponder wird in seiner Gültigkeit bis zu einer bestimmten Uhrzeit beschränkt. Geben Sie eine Zeit ein.

❑ **Stundenanzahl ab der letzten vollen Stunde der Buchung**

Dieser am Gateway buchende G2 Transponder wird in seiner Gültigkeit um die festgelegte Dauer in Stunden verlängert. Geben Sie eine Stundenanzahl ein.

❑ **Aktivierungsdatum**

Datum und Uhrzeit, ab wann der Transponder gültig sein soll.

❑ **Verfallsdatum**

Datum und Uhrzeit, ab wann der Transponder nicht mehr gültig sein soll.

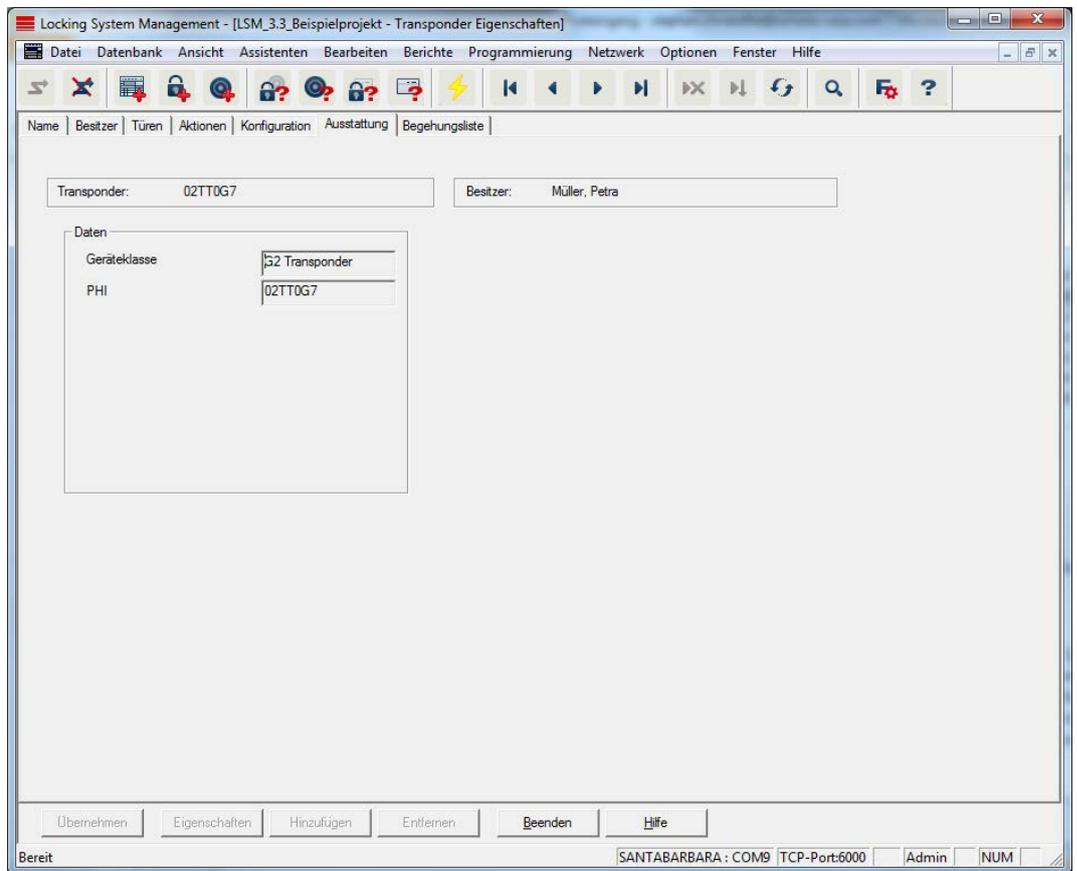
❑ **Zeitzonengruppe**

Sie können dem Transponder eine vorher definierte Zeitzonengruppe zuweisen.

❑ **TIDs zum Deaktivieren**

Sie können auf dem Transponder IDs anderer Transponder speichern, die gesperrt wurden. Sobald sich der Transponder an einer Schließung anmeldet, werden die Sperrungen an der Schließung wirksam.

Ausstattung



Lesen Sie genauere Spezifikationen des Transponders nach.

7.1.5.5 Neue Schließung

Neue Schließung

Schließanlage: Beispielanlage LSM 3.x
 Bereich: [Systembereich]

Schließungstyp: G2 Schließzylinder aktiv/hybrid
 Tür auswählen:
 Türen ohne Schließungen anzeigen
 Seriennummer: L-00003 Auto

Tür einfügen
 Neue Tür: Ausgang
 Raumnummer:
 Etage:
 Standort: kein Gebäude: kein

Zuordnung zu übergreifenden Ebenen

Schließanlage	Bereich	Ebene

Übergreifende Ebene: Grün
 Schließanlage: Übergreifend grün
 Bereich: [Systembereich]

Buttons: Konfiguration, Hinzufügen, Entfernen, Speichern & Weiter, Beenden

Nutzen Sie diese Option, um manuell eine neue Schließung einzufügen.

Wenn bereits mehrere Schließanlagen und übergreifende Schließebenen erstellt wurden, kann die neue Schließung diesen direkt zugeordnet werden. Hierfür werden entsprechende Möglichkeiten in Form von Dropdownleisten angeboten.

- Wählen Sie optional eine Schließanlage und den Bereich aus, um die Schließung gleich korrekt zuzuweisen. Schließanlagen und Bereiche müssen vorher definiert werden. Es ist später jederzeit möglich, diese Einstellungen zu verändern.
- Über die Schaltfläche "Tür einfügen" können Sie eine neue Tür erstellen. Eine Tür kann mehrere Schließungen enthalten.
- Über die Schaltfläche "Speichern & Weiter" legen Sie die neue Schließung im Schließplan an. Wählen Sie "Beenden", um zur Matrix zurückzukehren oder legen Sie gleich eine weitere Tür an.

In der LSM Software können je nach verwendeter Hardware unterschiedliche Schließungen verwaltet werden. Wählen Sie in der Dropdown-Liste bei Schließungstyp, welche Art von Schließung Sie anlegen möchten.

7.1.5.6 Neuer Transponder

Neuer Transponder

Schließanlage: Beispielanlage LSM 3.x

Transpondergruppe: [Systemgruppe]

Typ: G2 Transponder

Besitzer: kein

Seriennummer: T-00003

Auto:

Besitzer ohne zugewiesenen Transponder anzeigen

Neue Person anlegen

Personalnummer: P-00115

Nachname: Geiger

Vorname: Korbinian

Abteilung: Produktmarketing

Adresse:

Telefon:

Schließanlage	Transpondergruppe	Ebene

Schließanlage: SmartXChange Test2

Transpondergruppe: [Systemgruppe]

Speichern & Weiter

Beenden

Legen Sie über diese Option manuell einen neuen Transponder an. Wenn bereits mehrere Schließanlagen und Transpondergruppen erstellt wurden, kann der neue Transponder diesen direkt zugeordnet werden. Hierfür werden entsprechende Möglichkeiten in Form von Dropdownleisten angeboten.

- Wählen Sie optional eine Schließanlage und die Transpondergruppe aus, um den Transponder gleich korrekt zuzuweisen. Schließanlagen und Transpondergruppen müssen vorher definiert werden. Es ist jederzeit möglich, diese Einstellungen zu verändern.
- Über die Schaltfläche "Konfiguration" können erweiterte Einstellungen wie die Gültigkeit des Transponders eingestellt werden.
- Über die Schaltfläche "Speichern & Weiter" legen Sie den Transponder im Schließplan an. Wählen Sie "Beenden", um zur Matrix zurückzukehren oder legen Sie gleich einen weiteren Transponder an.

Beachten Sie, dass in der LSM Software jedes Identmedium grundsätzlich als Transponder bezeichnet wird. In der LSM Software können je nach verwendeter Hardware unterschiedliche Identmedien verwaltet werden:

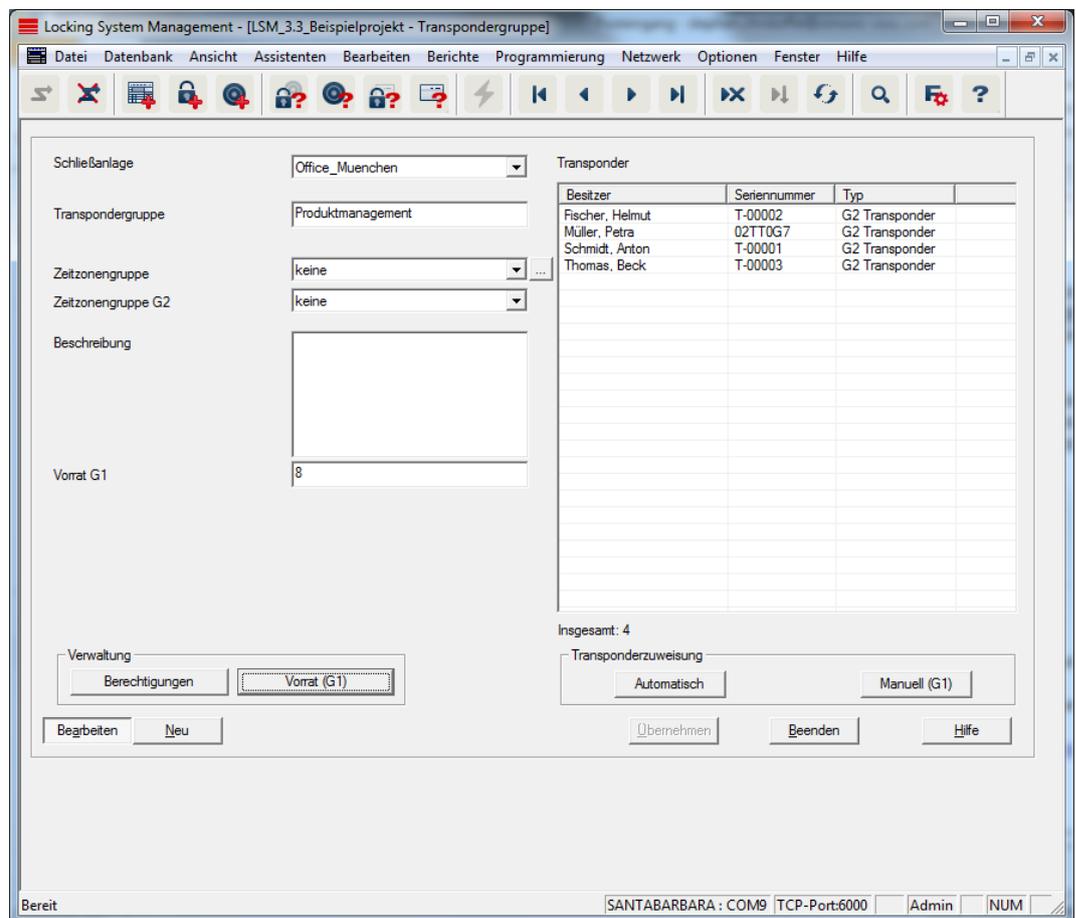
G1 Biometrie	Biometrietransponder
G1 Biometrieleser-Benutzer	Biometrieleser-Benutzer im G1 Standard
G1 Karte	Karte im G1 Standard
G1 SmartClip	SmartClip in G1 Standard
G1 Transponder	Transponder in G1 Standard
G2 Karte	Karte in G2 Standard
G2 PIN-Code Benutzer	Benutzer eines Pin Code Terminals
G2 Transponder	Transponder in G2 Standard
Undefiniert	Noch nicht festgelegter G1 Transponder



HINWEIS

Transponder dürfen niemals gleichzeitig einer Schließanlage und einer übergreifenden Ebene zugeordnet werden!

7.1.5.7 Transpondergruppe



Dieses Menü zeigt die bereits angelegten Transpondergruppen. Über die Schaltflächen "Nächster Datensatz" und "Vorheriger Datensatz" aus dem Menüband können die einzelnen Transpondergruppen durchgewechselt werden. Über die Schaltfläche "Neu" lassen sich weitere Transponder anlegen.

■ Schließanlage

Auswahl der angelegten Schließanlage.

■ Transpondergruppe

Name der Transpondergruppe.

■ Übergeordnete Gruppe

Transpondergruppe, die in der Hierarchie eine Position weiter oben angebunden ist.

■ Zeitzonengruppe

Legt für die Transpondergruppe die Zeitgruppe G1 fest.

■ Zeitzonengruppe G2

Legt für die Transpondergruppe die Zeitgruppe G2 fest.

■ Beschreibung

Freies Feld zur Beschreibung der Transpondergruppe.

■ **Vorrat G1**

Anzahl der insgesamt in der Transpondergruppe vorhandenen TransponderIDs.

■ **Berechtigungen**

Möglichkeit zur Vergabe der Gruppenberechtigungen.

■ **Vorrat (G1)**

Möglichkeit zum Verwalten der G1 TransponderIDs.

■ **Automatisch**

Möglichkeit zur automatischen Zuordnung eines freien Transponders zu der Transpondergruppe.

■ **Manuell (G1)**

Möglichkeit zur manuellen Zuordnung eines bestimmten Transponders zu einer bestimmten TransponderID.

7.1.5.8 Person

Dieses Menü zeigt die bereits angelegten Personen. Über die Schaltflächen "Nächster Datensatz" und "Vorheriger Datensatz" aus dem Menüband können die einzelnen Personen durchgewechselt werden.

Das Menü entspricht der Registerkarte "Besitzer" aus *Bearbeiten/Eigenschaften: Transponder*.

Zusätzlich lassen sich über die Schaltfläche "Neu" neue Personen anlegen.

7.1.5.9 Bereich

Nutzen Sie dieses Menü, um die einzelnen Transponderbereiche anzuzeigen. Über die Schaltflächen "Nächster Datensatz" und "Vorheriger Datensatz" aus dem Menüband können die einzelnen Transpondergruppen durchgewechselt werden.

Zusätzlich lassen sich über die Schaltfläche "Neu" neue Bereiche anlegen.

7.1.5.10 Tür

Dieses Menü zeigt die bereits angelegten Türen. Über die Schaltflächen "Nächster Datensatz" und "Vorheriger Datensatz" aus dem Menüband können die einzelnen Türen durchgewechselt werden.

Das Menü entspricht der Registerkarte "Türen" aus *Bearbeiten/Eigenschaften: Schließung*.

Zusätzlich lassen sich über die Schaltfläche "Neu" neue Türen anlegen.

7.1.5.11 Gebäude

Über dieses Menü kann der Schließanlage ein neues Gebäude hinzugefügt bzw. ein vorhandenes Gebäude bearbeitet werden. Gebäude können nur erstellt werden, wenn bereits ein Standort angelegt wurde.

7.1.5.12 Standort

Über dieses Menü kann der Schließanlage ein neuer Standort hinzugefügt bzw. ein vorhandener Standort bearbeitet werden.

7.1.5.13 Feiertagsliste

Diese Liste gilt global im Projekt. Hier können Feiertage nach Bundesland ausgewählt werden und sogar neue Feiertage erstellt werden.

7.1.5.14 Feiertag

An dieser Stelle können einzelne Feiertage erstellt werden. Hier besteht die Möglichkeit, einen neuen "Feiertag" bzw. einen Urlaubszeitraum festzulegen. *Neu angelegte Feiertage müssen in der Feiertagsverwaltung einer Feiertagsliste zugewiesen werden.*

7.1.5.15 Zeitzonenplan

Locking System Management - [LSM_3.3_Beispielprojekt - Zeitzonesplan]

Druckansicht

Name: Reinigungszeit

Bereich: [Ausnahmen] Außenhülle

Schließanlage: Office_Muenche

Beschreibung: Den Reinigungskräften soll nur MO, MI, DO in der Zeit von 16:00 Uhr bis 20:00 Uhr Zutritt gewährt werden.

Feiertagsliste: Bayern

Namen der Gruppen für die Schließanlage anzeigen: Office_Muenchen

Gruppe	Ale	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag	Sonntag
Gruppe 1	+	+	-	+	-	+	-	-	-
Gruppe 2	-	-	-	-	-	-	-	-	-
Gruppe 3	-	-	-	-	-	-	-	-	-
Gruppe 4	-	-	-	-	-	-	-	-	-
Gruppe 5 - ...	-	-	-	-	-	-	-	-	-
Gruppe 6	-	-	-	-	-	-	-	-	-
Gruppe 7	-	-	-	-	-	-	-	-	-
Gruppe 8	-	-	-	-	-	-	-	-	-
Gruppe 9	-	-	-	-	-	-	-	-	-
Gruppe 10	-	-	-	-	-	-	-	-	-
Gruppe 11	-	-	-	-	-	-	-	-	-

letzte Veränderung: 27.08.15 11:43:07

Gruppe 1

0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00

Montag
Dienstag
Mittwoch
Donnerstag
Freitag
Samstag
Sonntag
Sonntag

Bearbeiten Neu Druckansicht Übernehmen Beenden Hilfe

Bereit SANTABARBARA : COM9 TCP-Port:6000 Admin NUM

In diesem Bereich können Zeitzonenpläne erstellt werden.

❑ **Name**

Passender und eindeutiger Name für den Zeitzonenplan.

❑ **Beschreibung**

Treffende Beschreibung des Zeitzonenplans.

❑ **Feiertagsliste**

Wählen Sie ein entsprechendes Bundesland aus.

❑ **Name der Gruppen für die Schließanlage anzeigen**

Auswahl, von welcher Schließanlage die manuell geänderten Zeitgruppennamen angezeigt werden.

❑ **Tabelle der Zeitgruppen**

Pro Zeitzonenplan können bis zu 100 Zeitgruppen definiert werden. Wählen Sie zuerst eine Gruppe und bearbeiten Sie dann den Wochenplan.



HINWEIS

Die fünfte Gruppe ist für die Zeitzumschaltung vorgesehen (siehe Zeitzumschaltung).

❑ **Kleine Tabellen rechts oben**

Wenn der Zeitzonenplan bereits einem Bereich zugeordnet wurde, wird das in den beiden kleinen Tabellen angezeigt.



HINWEIS

Erstellen Sie zunächst immer erst einen Zeitzonenplan und weisen Sie diesen später einem Bereich *oder einer einzelnen Schließung* zu. Dies geschieht z.B. über *Bearbeiten/Bereich*.

❑ **Wochenplan**

- ❑ Felder, die blau ausgefüllt werden, entsprechen einer Berechtigung zu dieser Zeit.
- ❑ Felder können einzeln angeklickt oder durch eine Auswahl mit gedrückter Maustaste geändert werden.

❑ **Bearbeiten**

Zum Bearbeiten des Zeitzonenplans muss diese Schaltfläche aktiviert sein. Änderungen können über die Schaltfläche "Übernehmen" gespeichert werden.

❑ **Neu**

Die Schaltfläche "Neu" erstellt einen neuen, leeren Zeitzonenplan.

7.1.5.16 Zeitgruppe

In der Zeitgruppe können alle im Zeitzonenplan vergebenen Zeitgruppen angezeigt werden. Diese Ansicht eignet sich speziell für einen Gesamtüberblick über Schließanlage, Zeitgruppe, Transpondergruppe und Transponder.

Über die Schaltfläche "Zugewiesene Transponder" kann eine Übersicht ausgedruckt werden.

7.1.5.17 Lokale Zeitzone

Geben Sie in diesem Fenster Ihre lokale Zeitzone ein, sofern Sie Standorte in verschiedenen Zeitzonen verwalten. Die Schaltfläche "Aus der Registrierung einlesen" bietet eine Auswahl der gängigen weltweiten Zeitzonen.

Ist eine Schließung mit einer lokalen Zeitzone programmiert worden, stellt dieser Beispielsweise Sommer- und Winterzeit automatisch um.

7.1.5.18 Benutzer

Die erste Anmeldung erfolgt in der LSM automatisch als Administrator ("Admin"). Diese Rolle verfügt über alle Berechtigungen.

In der LSM Business können verschiedene Benutzer angelegt werden. Somit können mehrere Benutzer eine Datenbank bzw. eine Schließanlage verwalten.

Unter *Bearbeiten/Benutzer* können neue Benutzer angelegt sowie deren Berechtigungen angezeigt werden (siehe auch *Benutzer verwalten* [[▶ 168](#)]). Über die Schaltflächen "Vorheriger Datensatz" und "Nächster Datensatz" kann zwischen den Benutzern hin und her geschaltet werden.

■ "Benutzerkonto ist gesperrt"

Ist die Checkbox aktiviert, ist der Benutzer aktuell gesperrt.

■ "Benutzer muss Kennwort bei der nächsten Anmeldung ändern"

Ist diese Checkbox aktiviert, muss der Benutzer bei seiner nächsten Anmeldung ein neues Kennwort festlegen. (Das geht grundsätzlich auch zu jederzeit unter *Datei/Benutzerkennwort ändern*.)

■ Schaltfläche "Benutzergruppen"

An dieser Stelle kann der Benutzer einer oder mehreren bereits existierenden Benutzergruppen zugewiesen werden. Die Benutzergruppe legt fest, welche Rechte der Benutzer bekommt.

■ Schaltfläche "Bearbeiten"

Über diese Schaltfläche können die Nutzerdaten geändert werden.

■ Schaltfläche "Neu"

Über diese Schaltfläche kann ein neuer Benutzer angelegt werden.

7.1.5.19 Benutzergruppe

Benutzer werden zu Benutzergruppen hinzugefügt. Auf diese Weise werden die Rechte der Benutzer verteilt. Die erste Anmeldung in der LSM BUSINESS erfolgt als "Admin", welcher der Benutzergruppe "Administrator" mit allen Rechten zugeordnet ist.

Unter *Bearbeiten/Benutzergruppe* können neue Benutzergruppen angelegt sowie deren Berechtigungen eingeschränkt werden. Über die Schaltflächen "Vorheriger Datensatz" und "Nächster "Datensatz" kann zwischen den Benutzergruppen hin und her geschaltet werden.

■ Gruppenname

Name der Gruppe.

■ Beschreibung

Beschreibung der Gruppe.

■ Benutzer

Benutzer, die bereits der Benutzergruppe zugeordnet wurden. Über die Schaltfläche "Bearbeiten" können existierende Benutzer der Benutzergruppe hinzugefügt werden. Dies ist auch über *Bearbeiten/Benutzer* möglich.

■ Schreibzugriff

Bei aktivierter Checkbox lassen sich Daten ändern und Programmierungen durchführen. Bei deaktivierter Checkbox können Daten nur ausgelesen bzw. angezeigt werden.

■ Rolle

An dieser Stelle können die Rechte der Benutzergruppe vergeben werden. *Die Rollenverteilungen werden im nachfolgenden Kapitel [Rollen & Rechte \[▶ 103\]](#) näher beschrieben.*

■ Schaltfläche "Bearbeiten"

Erlaubt es, Änderungen wie "Rechte" oder "Gruppenname" zu bearbeiten.

■ Schaltfläche "Neu"

Erstellt eine neue Benutzergruppe.

Rollen & Rechte

Rolle	Beschreibung
-------	--------------

Schließenanlagenverwaltung	Berechtigungen in der Matrix verwalten.
Transponder programmieren/auslesen	Kommunikation zwischen Transponder und LSM über ein Programmiergerät erlauben.
Schließungen programmieren/auslesen	Kommunikation zwischen Schließung und LSM über ein Programmiergerät erlauben.
Transponder und Gruppen bearbeiten	Bearbeiten von Transpondern und Transpondergruppen.
Schließungen und Bereiche bearbeiten	Bearbeiten von Schließungen und Bereichen.
Netzwerk konfigurieren	Netzwerke erstellen und bearbeiten.
Netzwerk verwalten	Aufgaben wie z.B. Sammelaufträge oder Ereignismanager über konfigurierte Netzwerke durchführen.
Zutrittslisten Administration	Grundsätzliches Recht, einer Benutzergruppe die Berechtigung zum Auslesen von Zutritts- und Begehungslisten zu erteilen.
Zutrittslisten verwalten	Auslesen von Zutritts- und Begehungslisten erlauben.
Personalverwaltung	Bearbeiten von Personen.
LSM Mobile benutzen	Export auf bzw. Import von LSM Mobile erlauben.
Zeitwirtschaft	Feiertagslisten, Zeitzonen und Zeitgruppen erstellen und bearbeiten.
Berichte drucken	Ausdrucken von Berichten und Etiketten erlauben.
Protokoll lesen	Zugriff auf das Menü "Ansicht/Protokoll".
Notöffnung	Durchführung von Notöffnungen erlauben.

7.1.6 Berichte

Um das umfangreiche Berichtswesen nutzen zu können, benötigen Sie mindestens eine LSM Basic Online oder höher.

Jede Berichtsart bietet grundsätzliche folgende Auswahlmöglichkeiten:

Berichte

Transpondergruppe	Transponder	Benutzer			
Verschiedenes	Bereich	Zeitgruppe	Zeitzonepläne		
Schließanlage	Gebäudestruktur	Personalstruktur	Tür	Schließung	Netzwerk

Schließanlage
Beispielanlage LSM 3.x

Schließungen
 Transponder
 Bereiche
 Transpondergruppen
 Statistik
 Programmierbedarf für Schließungen
 Programmierbedarf für Transponder
 Programmierbedarf für Transponder (alle Datensätze)
 Zeitgruppen
 Benutzerdefiniert

Benutzerdefinierte Berichte
Speichern

Anzeigen Abbrechen

1. Art des Berichts, z.B. eine SimonsVoss-Komponente, ein Gebäude oder eine Transpondergruppe, etc.
2. Erste Eingrenzung, worüber berichtet werden soll.
3. Gezielte Eingrenzung, wovon genau berichtet werden soll.
4. Möglichkeit, einen benutzerdefinierten Bericht auszuwählen und dann zu speichern. *Individuelle, benutzerdefinierte Berichte können bei der SimonsVoss Technologies GmbH bestellt werden.*
5. Schaltfläche "Anzeigen" zeigt den Bericht unter den zuvor gesetzten Kriterien an.

Die Kopf- und Fußzeilen der Berichte können unter Optionen/Berichte individuell angepasst werden.

Angezeigte Berichte können direkt ausgedruckt oder in andere Formate exportiert werden.

- 7.1.6.1 Schließanlage
- 7.1.6.2 Bereich
- 7.1.6.3 Transpondergruppe
- 7.1.6.4 Tür
- 7.1.6.5 Schließung
- 7.1.6.6 Transponder
- 7.1.6.7 Zeitgruppe
- 7.1.6.8 Zeitzonenplan
- 7.1.6.9 Netzwerk
- 7.1.6.10 Personalstruktur
- 7.1.6.11 Gebäudestruktur
- 7.1.6.12 Benutzer
- 7.1.6.13 Verschiedenes

Aufenthaltsliste

Ab der LSM 3.4 SP2 können Sie in einem Bericht sehen, wer sich aktuell in einem Bereich aufhält.



WARNUNG

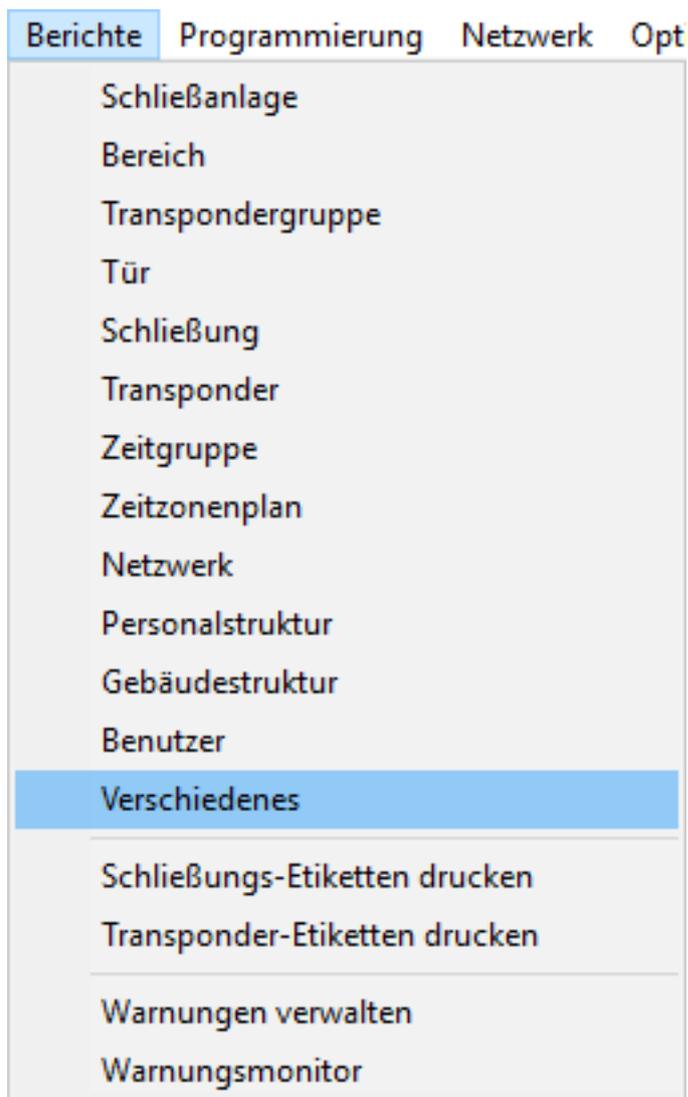
Nichtevakuierung im Gefahrenfall

Der Bericht basiert auf den Daten, die in der LSM-Datenbank gespeichert sind. Diese müssen nicht zwangsläufig dem Istzustand entsprechen, da beispielsweise Personen, die durch eine bereits geöffnete Tür gehen, nicht erfasst werden können. Eine Vereinzelungsanlage an allen Ein- und Ausgängen erhöht zwar die Qualität des Berichts, ist jedoch keine Garantie dafür, dass alle im Gebäude bzw. Bereich befindlichen Personen in dem Bericht erfasst sind.

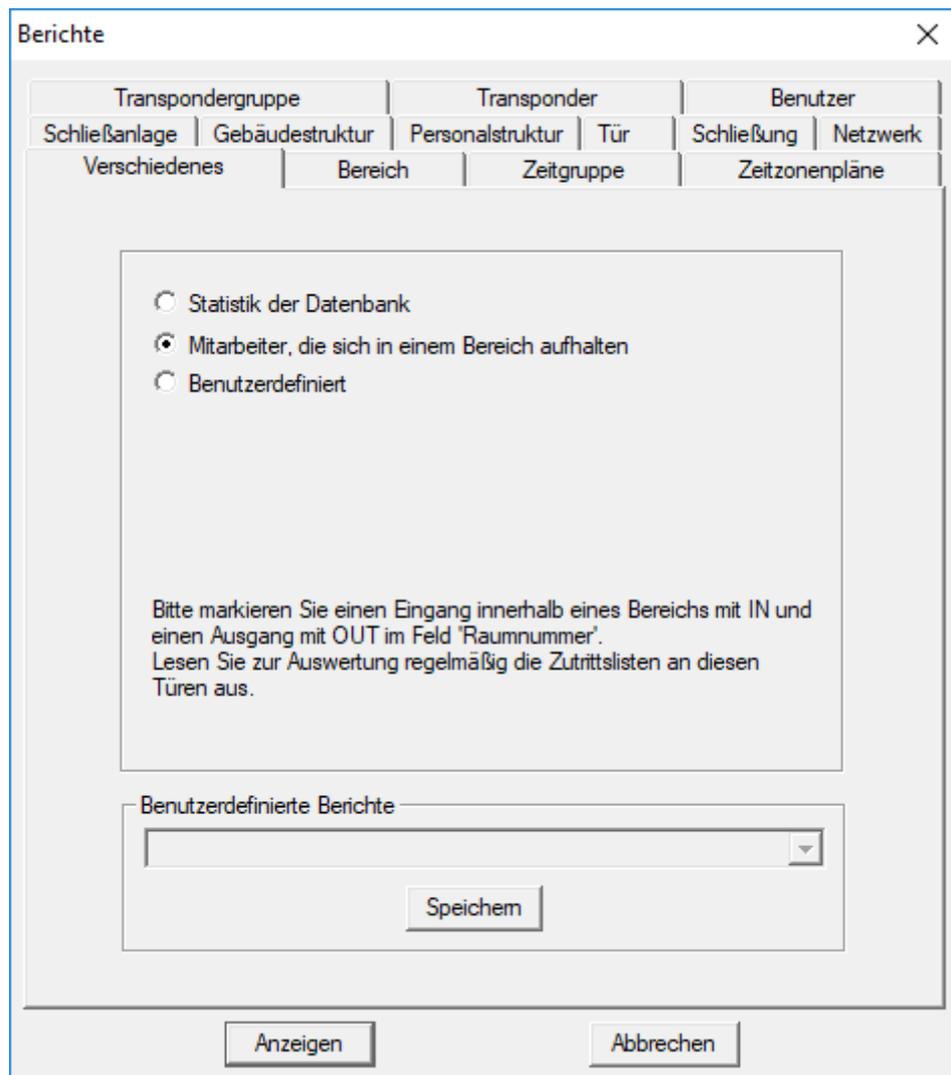
Wenn eine Evakuierung auf Basis dieses Berichts durchgeführt wird, dann werden nicht erfasste Personen möglicherweise nicht evakuiert.

- ❑ Verwenden Sie den Bericht nicht als Ersatz für eine Evakuierungsliste.

- ✓ LSM geöffnet.
 - ✓ Türen und Schließungen nach Bereichen gruppiert.
 - ✓ Namen der Bereiche ohne Angabe der Schließanlage erkennbar.
 - ✓ Eingänge und Ausgänge der Bereiche markiert (siehe *Ein- und Ausgänge von Bereichen markieren* [▶ 109]).
 - ✓ Eingänge und Ausgänge im selben Bereich.
1. Wählen Sie über | Berichte | den Eintrag **Verschiedenes**.



↳ Fenster "Berichte" öffnet sich mit der Registerkarte [Verschiedenes].



2. Wählen Sie die Option Mitarbeiter, die sich in einem Bereich aufhalten aus.

3. Klicken Sie auf die Schaltfläche **Anzeigen**.

↳ Fenster "Druckansicht" öffnet sich.

Der Bericht enthält folgende Informationen:

- Bereich, auf den sich der Abschnitt des Berichts bezieht
 - Besitzer des Identifikationsmediums
 - Personalnummer des Besitzers
 - Zeit, zu der der Bereich betreten wurde (Datum und Uhrzeit)
 - Betretene Tür
 - Standort
 - Gebäude
- Anzahl der Mitarbeiter im Bereich
- Anzahl der Mitarbeiter insgesamt

Ein- und Ausgänge von Bereichen markieren

Sie können Bereiche festlegen. Ab der LSM 3.4 SP2 können Sie eine Anwesenheitsliste für die jeweiligen Bereiche erstellen. Dazu müssen Sie definieren, durch welche Türen ein Bereich betreten und verlassen wird.

Eingänge definieren

Sie definieren einen Eingang mit einer der folgenden Methoden:

- Sie tragen den Ausdruck *IN* anstelle einer Raumnummer in den Eigenschaften der Schließung in der Registerkarte [Tür] ein.
- Sie tragen den Ausdruck *IN* anstelle eines Namens in den Eigenschaften der Schließung in der Registerkarte [Schließungskomponenten] ein.

Ausgänge definieren

Sie definieren einen Ausgang mit einer der folgenden Methoden:

- Sie tragen den Ausdruck *OUT* anstelle einer Raumnummer in den Eigenschaften der Schließung in der Registerkarte [Tür] ein.
- Sie tragen den Ausdruck *OUT* anstelle eines Namens in den Eigenschaften der Schließung in der Registerkarte [Schließungskomponenten] ein.



HINWEIS

Priorität bei der Auswertung der Definitionen

Sie können beliebige Ausdrücke eingeben. Zuerst wertet die LSM den Ausdruck im Namensfeld der Schließung aus (Registerkarte [Schließungskomponenten]). Wenn dort keiner der genannten Ausdrücke (IN oder OUT) verwendet wird, dann wertet die LSM den Ausdruck in der Raumnummer der Tür aus (Registerkarte [Tür]).

7.1.6.14 Schließungs-Etiketten drucken

Zunächst wird eine Liste aller Schließungen angezeigt. Sie können alle Schließungen oder lediglich einzelne Schließungen auswählen.

Über die Schaltfläche "OK" können verschiedene Etikettenarten zum Druck ausgewählt werden.

7.1.6.15 Transponder-Etiketten drucken

Zunächst wird eine Liste aller Transponder angezeigt. Sie können alle Transponder oder lediglich einzelne Transponder auswählen.

Über die Schaltfläche "OK" können verschiedene Etikettenarten zum Druck ausgewählt werden.

Neue Warnung

Name: Austrittsdatum

Typ: Austrittsdatum wird erreicht

Eigenschaften: Austrittsdatum eines Mitarbeiters wird erreicht

Vorlauf: 24 Stunden

Beschreibung: Mitarbeiter, die austreten, müssen bei HR als entfernt gemeldet werden

Transponder am Rückgabetag sperren Aktiviert

Personen

Verwalten

Aldrin, Lily
Enksen, Marshall
Mosby, Ted
Scherbatsky, Robin
Stinson, Barney

OK Abbrechen

■ **Name**

Name der Warnung.

■ **Typ**

Typ der Warnung, wie z.B. Batteriewarnung Schließung.

■ **Eigenschaften**

Ergibt sich aus dem Typ der Warnung.

■ **Vorlauf**

Zeitfenster zwischen Warnung und Eintritt der Warnungsursache.

■ **Beschreibung**

Freies Feld zur Beschreibung der Warnung.

■ **Transponder am Rückgabetag sperren**

Am Rückgabetag werden im Schließplan den Transpondern die Berechtigungen an den Schließungen entzogen -> Programmierbedarf.

■ **Aktiviert**

Wenn gesetzt, wird die Warnung angewendet.

■ **Verwalten**

Auswahl der zu überwachenden Objekte.

■ Tabelle

Anzeige der ausgewählten Komponenten.

Es stehen folgende Warnungen zur Auswahl:

- Austrittsdatum erreicht
- Batteriewarnung Schließung
- Batteriewarnung Transponder
- Export auf Handheld PDA
- Planmäßiger Batteriewechsel
- Transponderrückgabe steht an
- Transponderverfallsdatum

7.1.6.17 Warnungsmonitor

Nur verfügbar in der LSM Business mit aktiviertem Online-Modul.

Im Warnungsmonitor werden Warnungen angezeigt, welche eingetroffen und aktiviert sind. Der Warnungsmonitor startet nach der Anmeldung automatisch und zeigt alle aufgelaufenen Warnungen an. Durch das Auswählen der Statusanzeige können auch bereits akzeptierte oder abgelaufene Warnungen einsehen werden. Mit einem Doppelklick auf den Eintrag öffnen Sie die Eigenschaften des jeweiligen Objektes.

Über *Berichte/Warnungsmonitor* kann der Warnungsmonitor gestartet werden:

The screenshot shows a window titled "Aktuelle Warnungen" with a close button (X) in the top right corner. Below the title bar, the text "Warnungen:" is displayed. A table with four columns is shown: "Name", "Typ", "Datum", and "Betreff". The table is currently empty. To the right of the table is a button labeled "Akzeptieren". Below the table, there is a section titled "Status auswählen" with four radio button options: "aktiviert" (checked), "abgelaufen", "akzeptiert", and "abgearbeitet". To the right of this section is a checkbox labeled "In der laufenden Sitzung nicht mehr erinnern". In the bottom right corner of the window is a button labeled "Beenden".

■ **Tabelle**

Übersicht über aufgelaufenen Warnungen.

■ **Akzeptieren**

Einzelne Warnungen können akzeptiert und dadurch ausgeblendet werden.

■ **Aktiviert**

Nur aktuelle Warnungen werden angezeigt.

■ **abgelaufen**

Bereits abgelaufene Warnungen sind Warnungen, bei denen die eingestellte Zeit bereits verstrichen ist.

■ **akzeptiert**

Bereits akzeptierte Warnungen werden angezeigt.

■ **abgearbeitet**

Bereits abgearbeitete Warnungen sind Warnungen, bei denen eine Folgeaufgabe (z.B. „Sperrern der Transponder“) erledigt wurde.

7.1.7 Programmierung

7.1.7.1 Transponder

Diese Funktion ist nur auswählbar, wenn Sie einen Transponder in der Matrix ausgewählt haben. In der Dropdown-Liste ist direkt der Transponder gewählt, welcher in der Matrix ausgewählt war. Klicken Sie auf die Schaltfläche "Programmieren", um den Programmiervorgang für den in der Dropdown-Liste ausgewählten Transponder zu starten.

Wenn Sie mehrere Transponder hintereinander programmieren möchten, können Sie mit dem ersten Transponder beginnen und die Option "Nach der Programmierung zum nächsten Transponder springen" auswählen.

7.1.7.2 Schließung

Diese Funktion ist nur auswählbar, wenn Sie eine Schließung in der Matrix ausgewählt haben. In der Dropdown-Liste ist direkt die Schließung gewählt, welche in der Matrix ausgewählt war. Klicken Sie auf die Schaltfläche "Programmieren", um den Programmiervorgang für die in der Dropdown-Liste ausgewählte Schließung zu starten.

Wählen Sie im Feld "Programmiergerät" das Programmiergerät aus, welches für die Programmierung verwendet werden soll.

7.1.7.3 Markierte Schließung auslesen/Uhr setzen

Lesen Sie die in der Matrix ausgewählte Schließung aus, um die Uhrzeit einzustellen oder die Zutrittsliste auszulesen.

7.1.7.4 Schließung auslesen

Über diesen Befehl wird direkt eine Schließung über das Standard-Programmiergerät (SMARTCD.G2) ausgelesen.



HINWEIS

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

7.1.7.5 Mifare Schließung auslesen

Über diesen Befehl wird direkt eine passive Mifare-Schließung über das passive Programmiergerät (SMARTCD.MP) ausgelesen.



HINWEIS

Halten Sie die Elektronikseite der Schließung (z.B. beim Schließzylinder erkennbar am schwarzen Ring zwischen PZ-Gehäuse und Knauf) direkt auf das Antennensymbol des Programmiergeräts!

7.1.7.6 Transponder auslesen

Über diesen Befehl wird direkt ein Transponder über das Standard-Programmiergerät (SMARTCD.G2) ausgelesen. Achten Sie auf die Anweisungen der LSM Software.

7.1.7.7 G1 Karte auslesen

Über diesen Befehl wird eine G1 Karte direkt über das CD.MIFARE (*nicht mehr erhältlich*) ausgelesen. Achten Sie auf die Anweisungen der LSM Software.

7.1.7.8 G2 Karte auslesen

Über diesen Befehl wird direkt eine G2 Karte über das SMARTCD.HF Programmiergerät ausgelesen. Achten Sie auf die Anweisungen der LSM Software.

Bei hybriden Komponenten muss zusätzlich zum SMARTCD.HF auch das SMARTCD.G2 mit dem Computer verbunden sein.

7.1.7.9 Sonderfunktionen

Compact Reader auslesen

Liest einen Compact Reader aus.

Aktivierungstransponder

Über diese Funktion kann ein Aktivierungstransponder erstellt werden. Mit einem Aktivierungstransponder können deaktivierte Schließungen wieder aktiviert werden. Zum Öffnen der Schließung wird zusätzlich ein berechtigter Transponder benötigt!

G2 Aktivierungs-Karte

Über diese Funktion kann eine G2 Aktivierungs-Karte erstellt werden. Mit einer G2 Aktivierungs-Karte können deaktivierte Schließungen wieder aktiviert werden. Zum Öffnen der Schließung wird zusätzlich eine berechnigte G2 Karte benötigt!

G2 Batteriewechsel-Transponder

Nachdem die Schließung wegen kritischem Batteriestand in den Freeze-Modus gewechselt ist, kann die Schließung erst wieder mit Hilfe eines Batteriewechsel-Transponders aktiviert werden. Zum Öffnen der Schließung wird zusätzlich ein berechtigter Transponder benötigt!

G2 Batteriewechsel-Karte

Nachdem die Schließung wegen kritischem Batteriestand in den Freeze-Modus gewechselt ist, kann die Schließung erst wieder mit Hilfe einer G2 Batteriewechsel-Karte aktiviert werden. Zum Öffnen der Schließung wird zusätzlich eine berechnigte G2 Karte benötigt!

7.1.7.10 Notöffnung durchführen

Es ist möglich, eine Schließung mithilfe der LSM Software und dem entsprechenden Programmiergerät zu öffnen. Beachten Sie, dass Sie hierfür das Schließanlagenpasswort eingeben müssen.

7.1.7.11 SmartCD.G2 testen

Über diese Funktion wird die Funktionsfähigkeit eines angeschlossenen SMARTCD.G2 getestet.

7.1.7.12 SmartCD.MP testen

Über diese Funktion wird die Funktionsfähigkeit eines angeschlossenen SMARTCD.MP oder SMARTCD.HF getestet. Achten Sie darauf, dass zum Testzeitpunkt nur eines der passiven Programmiergeräte angeschlossen ist.

7.1.7.13 LSM Mobile

Mit einem auf Microsoft Windows basierendem Laptop, Netbook oder PDA ist es möglich, Programmieraufgaben aus der LSM Software zu exportieren. So können Sie beispielsweise mehrere SimonsVoss-Komponenten parallel mit mobilen Geräten programmieren.

Export auf LSM Mobile

Exportiert die Programmierbefehle einer Schließanlage.

Import von LSM Mobile

Importiert die durchgeführten Programmieraufgaben zurück in die LSM Software.

Exportierte Aufgaben

Zeigt die aktuellen Programmierexporte zur LSM Mobile an.

7.1.7.14 Virtuelles Netzwerk

Weitere Informationen siehe auch *Virtuelles Netzwerk (VN) verwalten* [[▶ 228](#)].

Export auf VNetzwerk

Import - Synchronisation

Reset VN Aufgabe

Exportierte VN Aufgaben

7.1.8 Optionen

7.1.8.1 Datenschutzkonformes Arbeiten nach DSGVO

Siehe *Datenschutzkonformes Arbeiten nach DSGVO* [[▶ 145](#)].

7.1.8.2 Matrix drucken

Das Drucken der Matrix ist nur möglich, wenn die Matrixansicht auch aktuell gezeigt wird.

7.1.8.3 Protokollieren

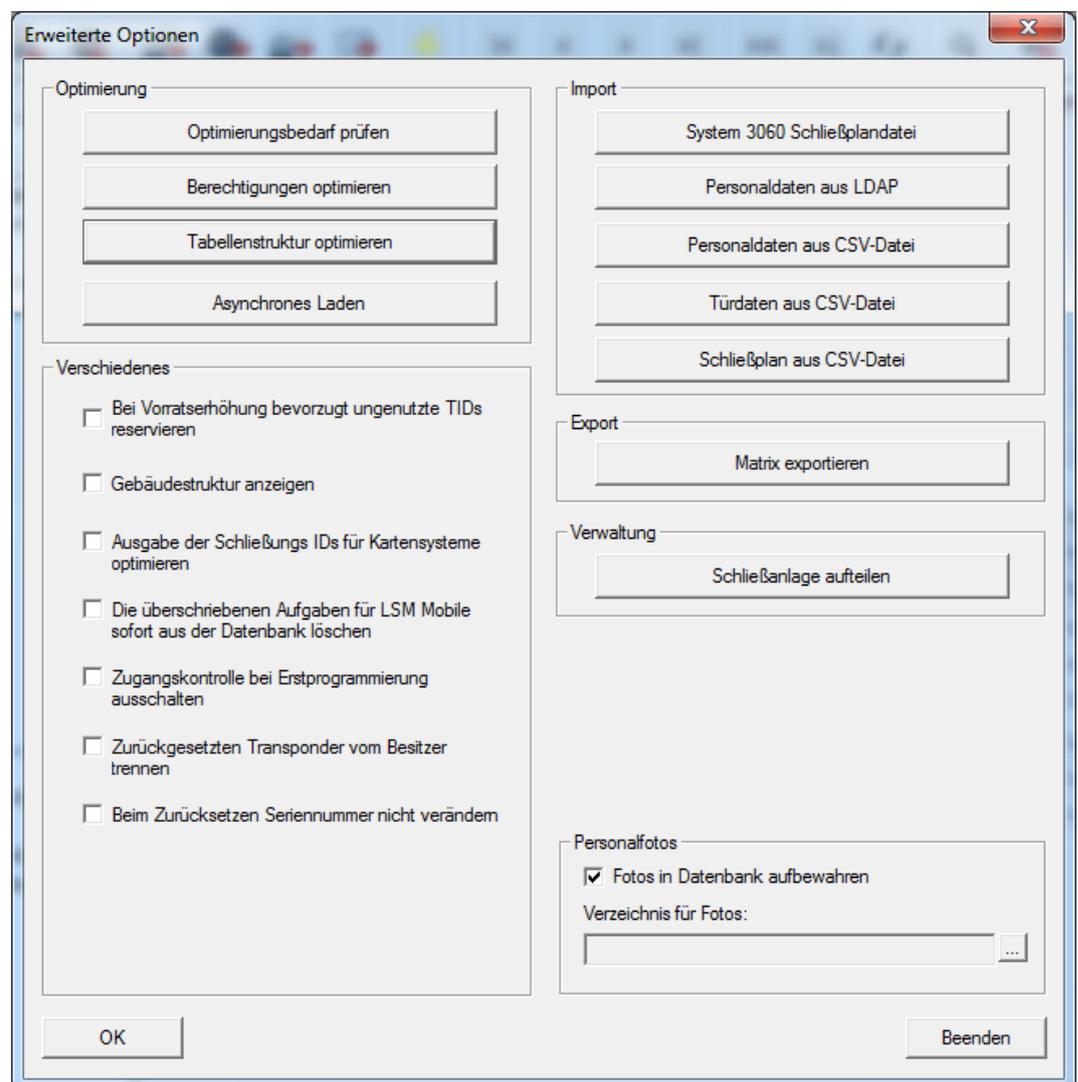
An dieser Stelle kann angegeben werden, welche Protokolleinträge wie lange gespeichert werden. Im Regelfall werden alle Protokollierungen 180 Tage gespeichert. Es können Zeiträume zwischen 7 Tagen und 670 Tagen eingestellt werden.

7.1.8.4 Automatische Nummerierung

Neue Komponenten werden standardmäßig durchnummeriert. In diesem Optionsfeld können Sie die Syntax für verschiedene Komponenten definieren.

7.1.8.5 Erweitert

Stellen Sie sicher, dass vor der Durchführung von Optimierungen der Datenbank immer eine aktuelle und funktionsfähige Datensicherung vorliegt.



Optimierungsbedarf prüfen

Für Nutzer, welche die LSM Software schon länger nutzen, stellt sich gelegentlich die Frage der richtigen Performance der Datenbankanwendung. Gerade durch Umstrukturierungen kann es dazu kommen, dass mehr Daten (Berechtigungskreuze) die Datenbank belasten. So ist es möglich, einer Transpondergruppe eine Berechtigung zu geben und einer Person dieser Gruppe eine explizite Einzelberechtigung. Dies

bedeutet nichts anderes, als das diese Person zwei unabhängig voneinander existierende Berechtigungen für die gleiche Tür haben kann. Dies ist nicht nur verwirrend, sondern auch unnötig.

Klicken Sie auf die Schaltfläche "Optimierungsbedarf prüfen", um einen Optimierungsbedarf der Schließanlage zu prüfen. Folgen Sie anschließend den Anweisungen der LSM Software.

Berechtigungen optimieren

Führen Sie diesen Befehl aus, wenn die Prüfung auf Optimierungsbedarf dazu rät.

Klicken Sie auf die Schaltfläche "Berechtigungen optimieren", um einen Optimierungsbedarf der Berechtigungen zu prüfen. Folgen Sie anschließend den Anweisungen der LSM Software.

Tabellenstruktur optimieren

Bei längerer Verwendung einer Datenbank kann es zu Unregelmäßigkeiten in den einzelnen Tabellen kommen. Durch die Optimierung der Struktur werden die Indizes der Tabellen neu gesetzt und eventuelle Dateninkonsistenzen entfernt.

Asynchrones Laden

Wird derzeit nicht unterstützt.

Verschiedenes

■ Bei Vorraterhöhung bevorzugt ungenutzte TIDs reservieren

Wird der Vorrat einer Transpondergruppe erhöht, so werden TIDs verwendet, die innerhalb der Schließanlage noch nie verwendet wurden (sofern noch TIDs verfügbar). Bei nicht aktivierter Checkbox werden auch TIDs verwendet, die bereits zuvor schon einmal in eine Schließung einprogrammiert waren, jedoch momentan nicht benutzt werden.

■ Gebäudestruktur anzeigen

Bei aktivierter Checkbox werden in der Maske "Wavenet verwalten" in der Spalte "Tür" vor dem Türnamen die Kürzel für Gebäude und Etage der gewählten Tür (sofern vorhanden) angezeigt.

■ Ausgabe der Schließungs-IDs für Kartensysteme optimieren

Bei aktivierter Checkbox und einer im Kartenmanagement G2 gesetzten Konfiguration mit "L" bzw. "L_AV" müssen beim Anlegen neuer G2 Schließungen die LID`s wie folgt vergeben werden:

- Bei Hybrid- und Mifareschließungen wird die nächste freie LID verwendet.

- Bei Schließungen mit Aktivtechnologie wird eine LID vergeben, die oberhalb des LID-Bereichs liegt, der im G2 Kartenmanagement bei "Schließungs-IDs" angegeben ist.

- **Die überschriebenen Aufgaben für LSM Mobile sofort aus der Datenbank löschen**

Bei aktivierter Checkbox wird (bei erneutem Export) in der Maske "Exportierte Aufgaben" der vorherige Exportauftrag für den gleichen GUI-Benutzer gelöscht.



HINWEIS

Exportaufträge für den gleichen Benutzer, die vor dem Setzen dieses Hakens durchgeführt wurden, werden nicht automatisch gelöscht!

- **Zugangskontrolle bei Erstprogrammierung ausschalten**

Aktivieren Sie diese Checkbox, wenn Sie generell keine Zugangskontrolle in der Schließanlage wünschen, jedoch die Zeitonensteuerung nutzen möchten. Beim Anlegen von neuen Schließungen ist diese Funktion dann automatisch deaktiviert.

- **Zurückgesetzten Transponder vom Besitzer trennen**

Aktivieren Sie diese Checkbox, wenn der Transponder nach dem Zurücksetzen vom verknüpften Benutzer getrennt werden soll und gleichzeitig die Seriennummer des Transponders durch das aktuelle Datum + Uhrzeit ersetzt werden soll.

- **Beim Zurücksetzen Seriennummer nicht verändern**

Aktivieren Sie diese Checkbox, wenn die Seriennummer eines Transponders (aus Revisionsgründen) beim Zurücksetzen nicht geändert werden soll.

System 3060 Schließplandatei

Importieren Sie einen beliebigen Schließplan aus einer LDB-Datenbank (*Vorgängersoftware der LSM: Locking Database Software*).

Personaldaten aus LDAP

Werden auf einem Server Personaldaten über LDAP zur Verfügung gestellt, können diese über die Schaltfläche „Personaldaten aus LDAP“ in die LSM Software importiert werden.

Personaldaten aus CSV-Datei

Über diese Schaltfläche lassen sich Personaldaten (Name, Vorname, Abteilung, Personalnummer, etc.) aus einer CSV-Datei in die LSM Software importieren.

Türdaten aus CSV-Datei

Über diese Schaltfläche lassen sich Türdaten (Tür, Raumnummer, Bereich, Innenmaß, etc.) aus einer CSV-Datei in die LSM Software importieren.

Schließplan aus CSV-Datei

Über diese Schaltfläche lassen sich Schließpläne aus einer CSV-Datei in die LSM Software importieren.

Matrix exportieren

Diese Schaltfläche bietet die Möglichkeit, die Matrix bzw. den Schließplan in eine CSV-Datei zu exportieren. Beachten Sie, dass nur die Inhalte der in der Matrix geöffneten Bereiche und Transpondergruppen exportiert werden.

Schließanlage aufteilen

Hier können Sie eine vorhandene Schließanlage in zwei Anlagen aufteilen. Dies ist z.B. sinnvoll, wenn in einem Gebäude ein neuer Mieter einzieht und der einen Teil der bereits vorhandenen Schließanlage nun selbst verwalten möchte.

Ausnahmen im Zeitonenmanagement auswählen

Wurde einer Transpondergruppe eine Zeitgruppe zugewiesen, so ist es über diese Funktion möglich, einzelnen Transpondern dieser Transpondergruppe die Zuweisung zur Zeitgruppe an bestimmten G2-Schließungen zu entziehen.

Zeitgesteuerte Berechtigungen

Über diese Funktion ist es möglich, einzelne Berechtigungskreuze zu einem bestimmten Zeitpunkt zuzulassen oder zu sperren (im Sollzustand!). Dies ist nur bei vernetzten Schließungen sinnvoll, da nach dem Ändern der Berechtigungen die Schließungen auch zeitnah programmiert werden müssen, um die Änderung wirksam zu machen.

Personalfotos

Standardmäßig werden die Personalfotos direkt in der Datenbank gespeichert. Es gibt jedoch auch die Möglichkeit, die Personalfotos in einem beliebigen Verzeichnis zu speichern.

7.1.8.6 Berichte

Geben Sie an dieser zentralen Stelle alle Daten an, die mit dem Bericht ausgegeben werden sollen.

In der LSM BUSINESS können die Daten individuell oder für alle Berichte gleich eingestellt werden.

7.1.8.7 Zutrittslisten

Die Zutrittslisten können eingeschränkt werden. Es ist möglich, nur einen bestimmten Zeitbereich in Tagen oder eine maximale Anzahl an Zutritten in der Schließung zu protokollieren.

Beachten Sie, wie viele Zutritte auf den jeweiligen Schließungen gespeichert werden können.

7.1.8.8 Sicherheit Benutzerkennwort

Diese Option erlaubt es, die gesamte Schließanlage noch besser abzusichern.

■ **Kennwort muss regelmäßig geändert werden**

Aktivieren, um alle Nutzer zur Passwortänderung nach einer vordefinierten Zeit zu zwingen.

■ **Kennwort Historie der letzten 10 Kennwörter verwenden**

Aktivieren, um die letzten 10 Kennwörter zu verbieten.

■ **Dreimalig falsch eingegebenes Kennwort**

Aktivieren, um einen Benutzer nach dreimaliger falscher Passworteingabe zu sperren.

■ **Hohe Passwortsicherheit**

Nur Passwörter mit hoher Sicherheit erlauben.

7.1.9 Netzwerk

Das Arbeiten mit Netzwerken (z.B. WaveNet oder VN) kann sehr komplexe Formen annehmen. Informieren Sie sich im WaveNet-Handbuch über das Arbeiten mit Netzwerken.

7.1.9.1 Aktivierung der Schließung

An dieser Stelle können Sie Schließungen im Netzwerk

■ aktivieren

■ deaktivieren

■ fernöffnen

7.1.9.2 Sammelaufträge

Über den Punkt Sammelaufträge können Sie einen Vorgang wie das Programmieren über eine größere Anzahl von Schließungen gleichzeitig starten.

7.1.9.3 Ereignismanager

- *Eventmanagement (Ereignisse) einrichten [▶ 219]*

- *Reaktion erstellen [▶ 222]*

7.1.9.4 Taskmanager

Nur verfügbar in der LSM Business mit aktiviertem Online-Modul.

- *Eventmanagement (Ereignisse) einrichten [▶ 219]*

- *Schließung auslesen [▶ 254]*

7.1.9.5 E-Mail Benachrichtigungen

Nur verfügbar in der LSM Business mit aktiviertem Online-Modul.

7.1.9.6 VN Dienst

Erweiterte Einstellungen für das virtuelle Netzwerk.

7.1.9.7 Kommunikationsknoten

Über diese Auswahl können Kommunikationsknoten und deren Anschlussgeräte (z.B. Router- oder CentralNodes) festgelegt werden.

7.1.9.8 Lokale Anschlüsse

Verwalten Sie an dieser Stelle die lokalen Anschlüsse des PCs/Servers.

7.1.9.9 WaveNet verwalten

Über "WaveNet verwalten" kann die Topologie des WaveNets angelegt und weitere Einstellungen vorgenommen werden.

7.1.9.10 WaveNet Manager

Diese Aktion startet den WaveNet-Manager. Der WaveNet-Manager muss separat installiert werden.

7.1.9.11 WaveNet-Topologie importieren

Diese Aktion öffnet ein Fenster zum Import von WaveNet-Topologien.

7.1.9.12 LON-Netzwerk verwalten

Ältere LON-Netzwerke können hier zentral verwaltet werden.

7.1.9.13 Terminalserver-Client Einstellungen

7.1.10 Fenster

Wechseln Sie zwischen geöffneten Fenstern.

7.1.11 Hilfe

7.1.11.1 Hilfethemen

Hilfethemen zur LSM Software.

7.1.11.2 SimonsVoss Online Support

SimonsVoss bietet einen Online-Support für eine schnelle Hilfestellung. Über diese Funktion wird ein kostenloser TeamViewer-Anruf über das Internet gestartet. Der Computer muss über eine Internetverbindung verfügen, um diese Funktion nutzen zu können. Ein Support-Mitarbeiter schaltet sich nach Ihrer Freigabe kurzzeitig auf Ihren Computer auf, um Sie bei einem Problem zu unterstützen.



HINWEIS

Setzen Sie sich zuerst mit der SimonsVoss Technologies GmbH in Verbindung, bevor Sie den Online-Support starten (Siehe *Hilfe und weitere Informationen* [[▶ 262](#)]!

7.1.11.3 SimonsVoss im Web

Zeigt die SimonsVoss-Homepage an (siehe *Hilfe und weitere Informationen* [[▶ 262](#)]). Sie benötigen eine Internetverbindung, um diese Funktion nutzen zu können.

7.1.11.4 Info über LockSysMgr...

Zeigt die Software- und Treiberversion der verwendeten LSM Software an.

7.1.11.5 Registrierung

Zeigt die registrierten Module an. An dieser Stelle können Sie auch aktivierte Clients deaktivieren und die LSM registrieren (siehe LSM registrieren).

7.1.11.6 Versionsübersicht

Zeigt die Versionen aller mit der LSM Software verwendeten Installationen.

7.1.11.7 FAQ

Zeigt die SimonsVoss FAQ Datenbank im Browser (siehe *Hilfe und weitere Informationen* [▶ 262]). Sie benötigen eine Internetverbindung, um diese Funktion nutzen zu können.

7.1.11.8 Auf Updates überprüfen

Prüft die aktuell installierte LSM Software auf Updates. Sie benötigen eine Internetverbindung, um diese Funktion nutzen zu können.

7.1.11.9 Datenbankbericht

Exportiert einen Bericht im CSV-Format.

7.2 Menüband

Im Menüband können wichtige und häufig verwendete Funktionen direkt aufgerufen werden.



1. Anmelden
2. Abmelden
3. Neue Schließanlage
4. Neue Schließung
5. Neues Identmedium (z.B. Transponder oder Karte)
6. Schließung auslesen
7. Transponder auslesen
8. MIFARE-Schließung auslesen
9. G2-Karte/Tag auslesen
10. Programmieren
11. Erster Datensatz
12. Vorheriger Datensatz
13. Nächster Datensatz
14. Letzter Datensatz
15. Entfernen
16. Übernehmen
17. Aktualisieren
18. Durchsuchen
19. Filter

20.Hilfe

7.3 Schließanlage

In diesem Bereich kann zwischen verschiedenen Schließanlagen innerhalb eines Projekts ausgewählt werden. Außerdem ist es möglich, die jeweiligen Schließanlageneigenschaften einzusehen und nachträglich zu bearbeiten.

7.4 Gruppen und Bereiche

Diese Bereiche enthalten eine Navigationshilfe, in der die beiden Gruppierungen (Transpondergruppen und Bereiche) in Form von zwei Baumstrukturen abgebildet sind.

Durch Ziehen mit der Maus auf den Trennbalken zwischen Bereichen und Transpondergruppen, sowie zwischen Matrix und Navigationsbereich lässt sich die Fenstergröße variieren.

Um sich in der Baumstruktur möglichst effizient und sicher bewegen zu können, sind in der Baumansicht abhängig vom Anzeigezustandes verschiedene Symbole dargestellt:

	Schließanlage Transpondergruppen
	Transpondergruppe ohne Transponder
	Transpondergruppe, die ausgeblendet ist
	Transpondergruppe, die angezeigt wird

	Schließanlage Bereich
	Bereich ohne Türen
	Bereich, der ausgeblendet ist
	Bereich, der angezeigt wird

Vorgehensweise:

Untergliederte Bereiche und Transpondergruppen mit bis zu 6 Ebenen sind nur in der LSM BUSINESS möglich.

- Klicken Sie auf das Pluszeichen links neben einem roten Symbol und die nächsttiefere Ebene der untergeordneten Gruppierung wird sichtbar.
- Durch weiteres Klicken auf die neuen Pluszeichen können Sie gezielt in weitere, noch tiefere Ebenen vordringen. Dabei beträgt die maximale Hierarchietiefe 6 Ebenen.
- Durch Anklicken auf die Minuszeichen links neben dem blauen Symbol werden die untergeordneten Ebenen geschlossen.

- Durch einen Doppelklick auf das Minuszeichen neben der Schließanlage werden alle geöffneten Gruppierungen geschlossen.
- Durch Doppelklicken auf einen Bereich oder eine Gruppe wechselt diese jeweils ihre Ansicht (Anzeige der Inhalte in der Matrix an oder aus).
- Sie können sich auch schnell einen Gesamtüberblick verschaffen, indem Sie die gesamte Baumstruktur öffnen:
 - Ansicht/Alle untergeordneten Bereiche/Gruppen öffnen
- Um alle geöffneten Bereiche oder Gruppen auch wieder zu schließen, muss in der Baumstruktur die oberste Gruppe geschlossen werden.

Beachten Sie, dass bei einem zunehmenden Umfang der Baumstruktur die Aufbereitung der anzuzeigenden Daten und die Darstellung auf dem Bildschirm entsprechend mehr Zeit benötigen wird. Dies kann sich beim Neuaufbau als auch bei der Aktualisierung der Ansicht bemerkbar machen.

7.5 Matrix

Diese Ansicht bildet eine Matrix, die sowohl die hierarchischen Personal- und Raumstrukturen visualisiert, als auch in der Lage ist, komplette Transpondergruppen gegen komplette Bereiche zu berechtigen. In der Ansicht Bereiche/Transpondergruppen wird dadurch das schnelle und einfache Herstellen der Grundberechtigungen ermöglicht. Sollen davon abweichende Berechtigungen in Form von individuellen Erweiterungen oder Einschränkungen vergeben werden, so ist dies in der Ansicht Türen/ Personen möglich.

Ansicht Türen/Personen

✘	Berechtigung, die gesetzt, aber noch nicht in die Schließung einprogrammiert wurde.
✘	Berechtigung, die in die Schließung einprogrammiert wurde.
✘	Berechtigung, die entfernt wurde und noch nicht in die Schließung übertragen ist.
✘	Noch nicht programmierte Berechtigungen, die zur Gruppenstruktur der Schließanlage konform sind, also aus der Gruppenansicht kommen, sind mit einem kleinen schwarzen Dreieck gekennzeichnet.
✘	Programmierte Berechtigungen, die zur Gruppenstruktur der Schließanlage konform sind, also aus der Gruppenansicht kommen, sind mit einem kleinen schwarzen Dreieck gekennzeichnet.
✘	Entfernte Berechtigungen, die zur Gruppenstruktur der Schließanlage konform sind und noch nicht programmiert wurden.

	Berechtigungen, die nicht zur Gruppenstruktur der Schließanlage konform sind, zeigen nur das Kreuz, aber kein schwarzes Dreieck (Einzelberechtigung).
	Berechtigungen, die entgegen der Gruppenstruktur der Schließanlage nachträglich entzogen wurden, haben das schwarze Dreieck, aber kein Berechtigungskreuz mehr.
	Kariertes (ausgegrautes) Kästchen: Es können keine Berechtigungen gesetzt werden. Sie besitzen keine Schreibrechte oder der Schließplan sperrt dieses Kästchen (z.B. bei deaktiviertem Transponder oder G2-Karte an aktivem Zylinder).

Ansicht Bereiche/Transpondergruppe

	Ein schwarzes Kreuz mit Innenkreis symbolisiert eine Gruppenberechtigung.
	Ein graues Kreuz mit Innenkreis steht für eine „geerbte“ Berechtigung.

Gruppenberechtigung Baumansicht

	manuell gesetzt (schwarz)
	direkte Vererbung (grün)
	Indirekte Vererbung – geerbt über untergeordnete Gruppe (blau)
	Sowohl direkte als auch indirekte Vererbung (blau/grün)

Programmierbedarf

Programmierbedarf kann aus unterschiedlichen Gründen an einem Transponder oder einer Schließung entstehen. Um die unterschiedlichen Gründe für Programmierbedarf darzustellen, sind die Programmierblitze farbig unterschiedlich gekennzeichnet.

	Programmierbedarf an der Komponente (gelb)
	<ul style="list-style-type: none">  Programmierbedarf beim Transponder (rot): <ul style="list-style-type: none">  Gültigkeit abgelaufen  Deaktiviert  Schließung (rot): <ul style="list-style-type: none">  Nur übergreifende Schließebene zugeordnet  Keiner Tür zugeordnet  Keiner Schließanlage zugeordnet  Tür ohne Schließung

	Programmierbedarf an einer Schließung nach Erstellen eines Ersatztransponder im Overlay-Modus einer G1 Anlage
---	---

- Durch einen Doppelklick auf eine Komponente in der Matrix kann direkt in die Eigenschaften des Objekts gewechselt werden.

8. Hintergrundwissen zur LSM

In diesem Kapitel werden theoretische Vorgehensweisen beschrieben, die das Verständnis in der Arbeit mit der LSM Software erleichtern sollen.

8.1 Gruppenberechtigungen

Mit einer Gruppenberechtigung kann man eine komplette Transpondergruppe für einen ganzen Bereich berechtigen. Damit können sehr schnell und übersichtlich die Grundberechtigungen im Schließplan erstellt werden. Hier ist es hilfreich, sich bei der Vergabe der Berechtigungen schon im Vorfeld über die geplante Gebäudenutzung und die Organisationsstruktur des Unternehmens klar zu werden. Eine klar strukturierte Anlage trägt später im Tagesgeschäft maßgeblich dazu bei, schnelle und präzise Aussagen über mögliche Zutritte zu treffen und den Tagesablauf im Unternehmen oder der Organisation zu ermöglichen. Ausnahmen der Gruppenberechtigungen können unter *Ansicht/Türen/Personen* durch das Entfernen oder Hinzufügen eines einzelnen Berechtigungskreuzes jederzeit auch nachträglich angepasst werden.

Bereiche und Transpondergruppen

Ein häufiger Anwendungsfall ist folgender: Ein Unternehmen besteht aus verschiedenen Abteilungen mit Mitarbeitern, die Zutritt zu einer, mehreren oder allen Abteilungen benötigen. Es wäre möglich, jeden einzelnen Transponder eines Mitarbeiters an einzelnen Schließungen - nämlich an denen, zu denen Zutritt benötigt wird - zu berechtigen. Der Verwaltungsaufwand steigt jedoch mit der Anzahl der Transponder.

Viel komfortabler ist es, mit Bereichen und Transpondergruppen zu arbeiten. Damit muss eine Berechtigung, die Gruppenberechtigung, nur einmal vergeben werden. Jeder Transponder, der dieser Gruppe zugewiesen wird, hat automatisch dieselben Rechte wie die Gruppe. Dasselbe gilt für die Schließungen. Wenn eine Schließung einem Bereich zugewiesen wird, dann sind alle Transponder, die an diesem Bereich berechtigt sind, auch an dieser Schließung berechtigt.

Beispiel: Reinigungskräfte sollen auch die Räume des Supports betreten dürfen. Das Unternehmen wird logisch in Abteilungen aufgeteilt:

- Entwicklung
- Marketing
- Vertrieb
- Support
- Hochsicherheitsbereich
- Fertigung

Alle Transponder von Reinigungskräften werden in einer Transpondergruppe Reinigungspersonal zusammengefasst. Ebenfalls werden alle Schließungen, die zu den jeweiligen Abteilungen gehören, schon beim Erstellen einem Bereich zugewiesen, zum Beispiel dem Support. Angenommen, die Supportabteilung hat zehn Schließungen und es arbeiten zehn Reinigungskräfte im Unternehmen. Wenn diese einzeln berechtigt werden, müssten hundert Berechtigungen vergeben und verwaltet werden. Wenn dagegen einfach die Transpondergruppe Reinigungspersonal dem Bereich Support zugewiesen wird, muss nur eine Berechtigung vergeben werden, damit die Reinigungskräfte Zutritt zur Supportabteilung haben.

8.1.1 Gruppenvorräte (nur G1)

Durch das Zuordnen eines Transponders zu einer Gruppe erhält dieser Transponder umgehend alle Berechtigungen, die der Gruppe zugeteilt wurden. Wird ein neuer Transponder einer Gruppe zugeordnet, entsteht an den betroffenen Schließungen Programmierbedarf. Um dies zu vermeiden, können den Gruppen beim Anlegen (und auch später) sogenannte "Vorräte an TransponderIDs" zugeordnet werden. Diese TransponderIDs sind zu diesem Zeitpunkt aber noch keiner Person zugeordnet. Die Vorräte werden in die Schließungen bei der Programmierung hinterlegt und stehen dann zur Nutzung bereit.

Wird nun eine TransponderID aus diesem Vorrat einer Person zugeordnet und der Transponder programmiert, entsteht kein Programmierbedarf an den Schließungen. Transponder können so automatisch berechtigt und in den Schließungen aktiviert werden, ohne dass der Anwender noch weitere Schritte, wie das Programmieren der Schließung, erledigen muss.

8.1.2 Vererbung

Die Vererbung ist eine Möglichkeit, die Hierarchie einer Firma in der Schließanlage abzubilden. Wird die Vererbung richtig umgesetzt, ist sie eine enorme Entlastung für den Anwender. Dadurch ist es möglich, durch das Zuweisen eines Transponders einer bestimmten Transpondergruppe bestimmte Abläufe zu automatisieren. Eingesetzt werden kann die Vererbung beim Einsatz einer Hierarchie bei den Transpondergruppen und bei den Bereichen. Bei der Vererbung werden die Gruppenberechtigungen berücksichtigt; die individuellen Einzelberechtigungen werden nicht vererbt.

8.2 Berechtigungen im G2 Protokoll

Im G2-Protokoll werden die Berechtigungen auf allen Komponenten gespeichert. Dies erlaubt es, einen neuen Transponder an einer berechtigten Schließung zu betätigen, ohne dass diese Schließung neu programmiert werden muss. Auf gleichem Wege lassen sich auch

Sperrungen (sogenannte Sperr-IDs) übertragen. Nachdem ein neuer Ersatztransponder erstmalig an einer Schließung betätigt wurde, wird dessen ursprüngliche Berechtigung in der Schließung gelöscht.

8.3 Zeitzonenpläne

Die LSM Software bietet die Möglichkeit, Transponder nur zu bestimmten Zeiten an Schließungen zu berechtigen.

Beispiel: Eine Reinigungskraft besitzt einen Transponder, welcher grundsätzlich in den zu reinigenden Räumen berechtigt ist. Die Räume sollen aber nur montags, mittwochs und freitags zwischen 16:00 Uhr und 20:00 Uhr gereinigt werden.

An dieser Stelle kommen Zeitzonenpläne ins Spiel. Im Folgenden wird kurz an einem Beispiel erklärt, wie Zeitzonenpläne umgesetzt werden. Außerdem soll vermittelt werden, wie sich Zeitzonenpläne an den verschiedenen SimonsVoss-Komponenten verhalten:

Grundsätzlich sollten Zeitzonenpläne so einfach wie möglich gehalten werden. Im Normalfall werden Zeitzonenpläne für Schließungen erstellt. Im Zeitzonenplan der Schließung werden wiederum einzelne Zeitgruppen erstellt. In diesen Gruppen ist beschrieben, zu welchen Zeiten welcher Transponder berechtigt sein darf.

Um den Zeitzonenplan so einfach und allgemein wie möglich zu halten, werden statt einzelnen Schließungen ganze Bereiche herangezogen. Parallel werden nicht einzelne Transponder, sondern ganze Transpondergruppen bestimmten Zeitgruppen zugewiesen. Für das Beispiel würde das so aussehen:

Zeitzonenplan erstellen

- Neuen Zeitzonenplan für den Bereich *Außenhaut* erstellen. Dieser Bereich umfasst alle Türen, von denen man sich Zutritt zum Gebäude verschaffen kann.
- Im neuen Zeitzonenplan *Außenhaut* wird eine Zeitgruppe (z.B. Gruppe 1) ausgewählt. Diese Gruppe wird beispielsweise *Reinigungszeiten* genannt.
- Für die Gruppe *Reinigungszeiten* wird nun im Zeitzonenplan ein Zeitfenster festgelegt. Die entsprechenden Zeiten können anhand eines Wochenkalenders beliebig ausgewählt werden.

Zeitzonenplan dem Bereich zuordnen

- Der erstellte Zeitzonenplan *Außenhaut* mit der definierten Zeitgruppe *Reinigungszeiten* wird nun dem Bereich *Außenhülle* zugeordnet.

- Der Bereich *Außenhülle* ist dann mit dem Zeitzonenplan verknüpft. Allerdings ist noch nicht definiert worden, welche Transpondergruppen der Zeitgruppe *Reinigungszeiten* zugeordnet sind.

Zeitgruppe einer Transpondergruppe zuordnen

- Die Transpondergruppe *Reinigungskräfte* muss anschließend mit der Zeitzonengruppe verknüpft werden.
- Jetzt wurde ein Zeitzonenplan *Außenhülle* erstellt, dessen Zeitgruppe *Reinigungszeiten* mit der Transpondergruppe *Reinigungskräfte* verknüpft ist.

Nach diesem theoretischen Vorgehen können beliebig viele und komplexe Zeitzonenpläne definiert werden. Abschließend soll noch veranschaulicht werden, was nun im Hintergrund zwischen den Geräten abläuft:

- Der Zeitzonenplan wird in jede Schließung des Bereichs *Außenhülle* programmiert, sofern diese die ZK-Funktion unterstützt.
- Auf den Transpondern der Transpondergruppe *Reinigungskräfte* wird die Zeitzonengruppe *Reinigungszeiten* gespeichert.
- Wird nun der Transponder *Reinigungskraft 1* an der Schließung *Haupteingang* betätigt, sendet der Transponder seine Transponder-ID und die Zeitgruppe an die Schließung.
- Die Schließung *Haupteingang* prüft in erster Instanz, ob der Transponder überhaupt an der Schließung berechtigt ist. In der zweiten Instanz wird geprüft, ob die Zeitgruppe zur aktuellen Zeit (Tag und Uhrzeit) an der Schließung berechtigt ist.
- Werden beide Abfragen positiv durchlaufen, kann die Schließung betätigt werden. Sollte eine Prüfung der Schließung negativ quittiert werden, wird der Zugang verwehrt.
- Bei Schließungen mit ZK-Option können sowohl Zutritte als auch abgewiesene Transponder gespeichert werden.

8.4 Übergreifende Schließebene

In einem Projekt können mehrere Schließanlagen verwaltet werden. Beispielhaft werden übliche Szenarien vorgestellt:

■ Ein Unternehmen mit mehreren Standorten/Gebäuden

Ein Unternehmen hat einzelne Niederlassungen an unterschiedlichen Orten. Normalerweise arbeitet ein Mitarbeiter immer in derselben Niederlassung. Spezielle Personengruppen sollen aber Zutritt zu mehreren Niederlassungen/Gebäuden haben.

In diesem Fall werden die einzelnen Niederlassungen/Gebäude in separate Schließanlagen unterteilt. Ein Mitarbeiter der Hauptniederlassung soll auch an Türen anderer Standorte berechtigt sein. Dieser Mitarbeiter der Hauptniederlassung wird dann in die Schließanlage der anderen Niederlassung verknüpft. Dort können schließlich individuelle Berechtigungen gesetzt werden.

■ Ein Gebäude mit mehreren Parteien

In einem Gebäude sind mehrere Parteien untergebracht. Die einzelnen Parteien benötigen eigene Schließanlagen. Jedoch müssen sich die Parteien verschiedene Schließungen (z.B. Schranke, Drehkreuz, Haupteingang, etc.) teilen.

In diesem Fall werden die einzelnen Parteien in separate Schließanlagen unterteilt. Zusätzlich wird eine übergreifende Schließebene angelegt. In diese übergreifende Schließebene können zum Beispiel alle gemeinsam genutzten Schließungen eingefügt werden. Parallel werden Personen und/oder Bereiche in die übergeordnete Schließanlage eingefügt und die entsprechenden Berechtigungen gesetzt.

■ Feuerwehrtransponder für ausgewählte Schließungen aller Schließanlagen

Spezielle Feuerwehrtransponder für beispielsweise Schlüsselrohre enthalten Berechtigungen für alle Türen eines Gebäudes. Dadurch kann die Feuerwehr im Brandfall alle Schließungen mit einem Transponder öffnen.

In diesem Fall wird eine neue übergreifende Schließebene mit der Farbe "rot" angelegt. In dieser werden über die Bereichseigenschaften alle gewünschten Türen im Projekt hinzugefügt. Zusätzlich wird eine Transpondergruppe "Feuerwehr" erstellt, welche über einen Mausklick an allen Türen in der übergreifenden Schließebene "rot" berechtigt ist.

Allgemeine Hinweise zu übergeordneten Schließebenen:

- Wird eine Schließung oder ein Transponder in einen anderen Schließplan verknüpft, verhält sich diese Verknüpfung wie das ursprünglich erstellte Original. Wird der originale Transponder bzw. die Schließung verändert oder gelöscht, wirkt sich das direkt auf die Verknüpfung in der anderen Schließanlage aus.
- Die rote Ebene weist zusätzlich besondere Merkmale auf (z.B. auch das Öffnen deaktivierter Schließungen), die für die Feuerwehr konzipiert wurde. Nutzen Sie diese Ebene nach Möglichkeit nur für den Einsatz bei Notfallzugriffen.



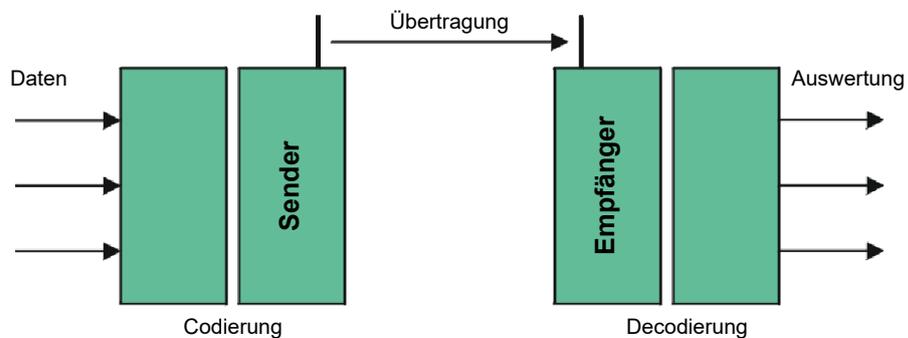
HINWEIS

Wird eine übergreifende Schließebene mit bereits zuvor programmierten Schließungen angelegt, müssen danach alle Schließungen neu programmiert werden. Achten Sie auf den neu erzeugten Programmierbedarf, der durch die Programmierblitze angezeigt wird.

8.5 Verschlüsselung (WaveNet)

Aufwändige Kryptografie schützt die Daten, die in Ihrem WaveNet transportiert werden.

Technische Realisierung



End-to-end-Verschlüsselung

End-to-end bedeutet in diesem Zusammenhang: Zwischen Zentralsoftware und Schließungen. Die Daten werden verschlüsselt und verlassen die Zentralsoftware. Sie werden erst in der Schließung wieder entschlüsselt.

Kommunikation	Verschlüsselung
End-to-end (generell)	3DES (112 bit)
Zutrittslisten (gegen unbefugtes Mitlesen)	Einfach-DES (56 bit)
Broadcast-Signale	AES (128 bit)

Digital signierte Datenpakete

Die 128-Bit-Signierung der Datenpakete schützt gegen Manipulationen auf der Funkstrecke. Wenn die Signatur eines Datenpakets nicht korrekt ist, dann wird das Datenpaket ignoriert.

Schutz gegen Replay-Attacken

Jedes sicherheitsrelevante Datenpaket enthält einen Zähler. Dieser Zähler wird für jedes neue Datenpaket erhöht. Wenn ein Datenpaket mit demselben Zählerstand nochmals ankommt, dann wird das Datenpaket

ignoriert. Wenn ein Angreifer also ein Datenpaket mitschneidet und erneut sendet (Replay-Attacke), dann ist der Zähler des Datenpakets derselbe wie der des Originalpakets und die Kopie des Angreifers wird erkannt und ignoriert.

9. 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.

9.1 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 [▶ 132].*
- 3. Klicken Sie auf die Schaltfläche "Übernehmen".
- 4. Klicken Sie auf die Schaltfläche "Beenden".

9.2 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".

9.3 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".

9.4 Transponder nachträglich einer Transpondergruppe zuweisen

- ✓ Der Transponder wurde bereits erstellt und eine Transpondergruppe ist angelegt.
- 1. Öffnen Sie die Schließenlageneinstellungen, z.B. über die Menüleiste *Bearbeiten/Eigenschaften: Schließenanlage*.
- 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.

9.5 Neuen Bereich anlegen

- ✓ Es ist bereits eine Schließenanlage 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".

9.6 Neue Schließung anlegen

- ✓ Es ist bereits eine Schließenanlage 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".

9.7 Pin Code Tastatur anlegen

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

9.7.1 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.

9.7.2 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

9.7.3 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.

9.8 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.

9.9 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.

9.10 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.

9.11 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!

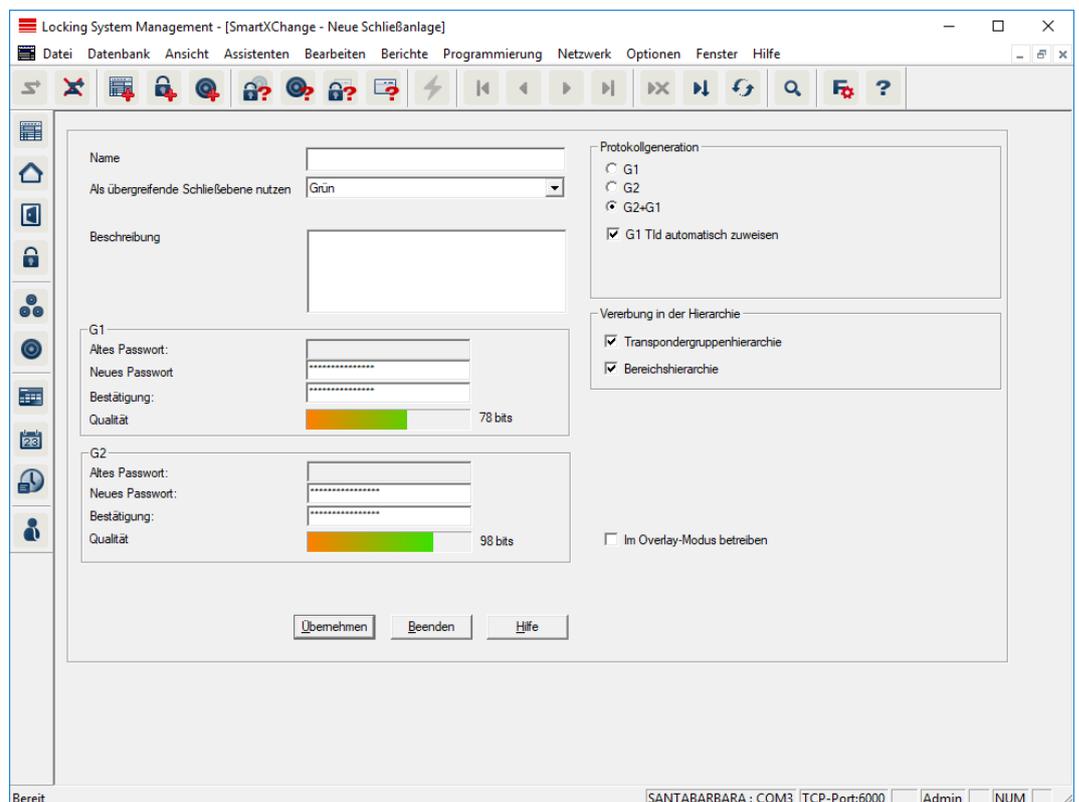
9.11.1 Übergreifende Schließebene anlegen

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.

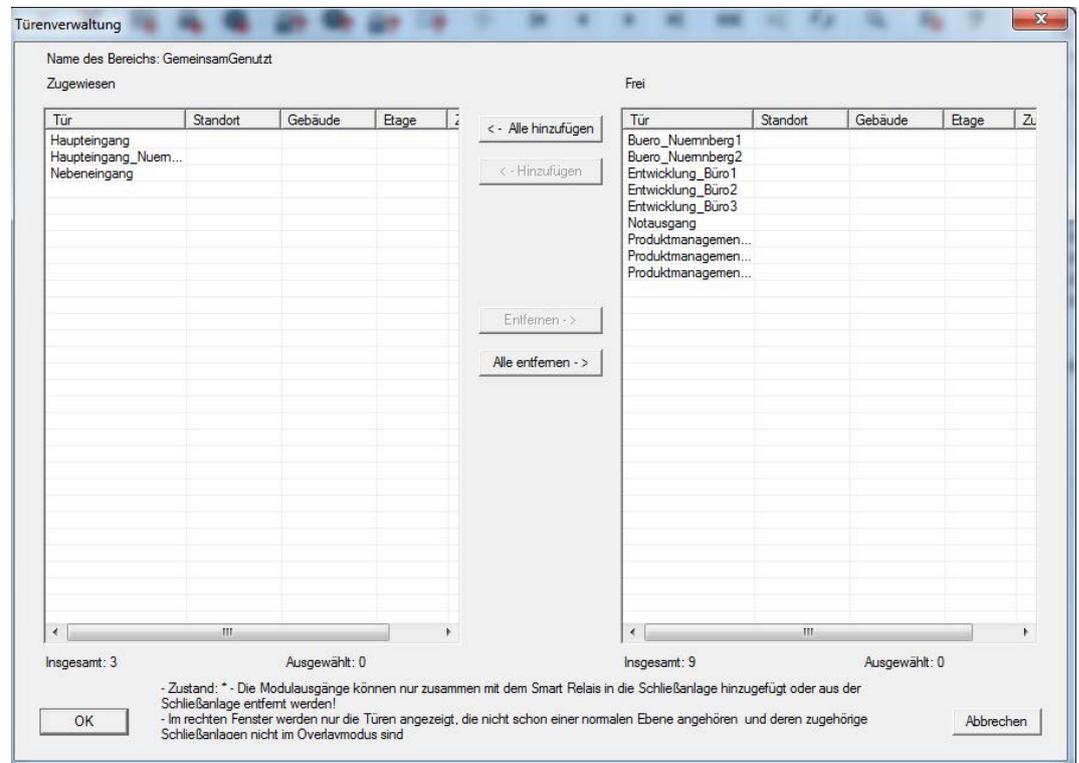


9.11.2 Schließungen verknüpfen

✓ 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.

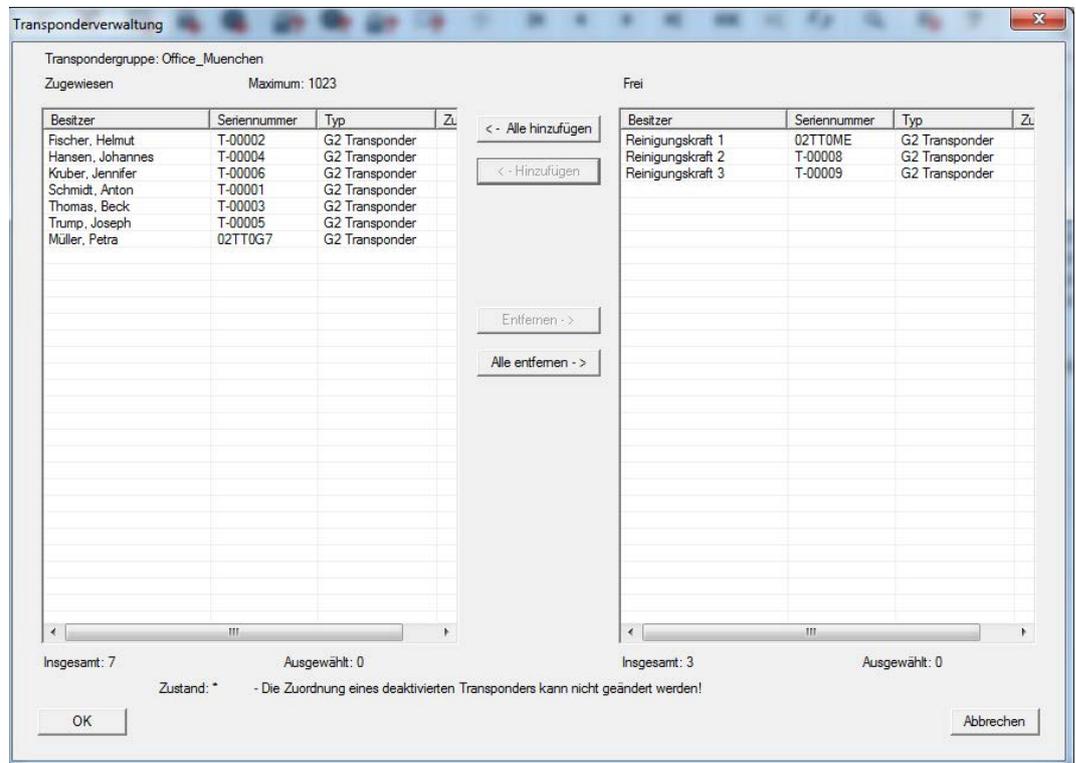


9.11.3 Transponder verknüpfen

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.

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



9.11.4 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.
- Rote übergeordnete Schließanlage öffnen.
 - Transpondergruppe erstellen, die an allen für die Feuerwehr relevanten Bereichen berechtigt sein soll.
 - In den Transpondergruppeneigenschaften auf die Schaltfläche "Berechtigungen" bei Verwaltung klicken.
 - Über die Checkboxen alle gewünschten Bereiche/Schließungen anwählen, um der Transpondergruppe Zugriff an allen Türen zu gewähren.

9.12 Feuerwehrtransponder erstellen

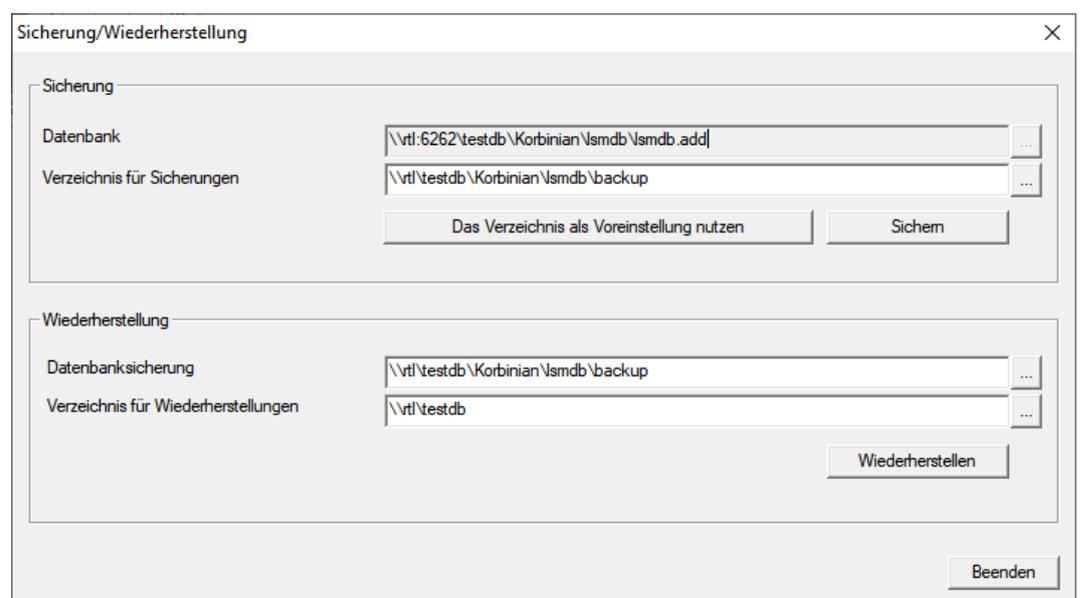
- ✓ Sie haben bereits mindestens eine Schließanlage erstellt.
- Erstellen Sie eine neue, übergreifende Schließebene der Farbe "rot", z.B. über *Bearbeiten/Neue Schließanlage*.

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.

9.13 Datenbank manuell sichern

- ✓ LSM geöffnet.
- 1. Wählen Sie über | Datenbank | den Eintrag **Backup**.
 - ↳ Fenster "Sicherung/Wiederherstellung" öffnet sich.



2. Geben Sie im Bereich "Sicherung" an, welche Datenbank wohin gesichert werden soll.

3. Klicken Sie auf die Schaltfläche **Sichern**.
↳ Backup erstellt.
4. Klicken Sie auf die Schaltfläche **Beenden**.
↳ Fenster "Sicherung/Wiederherstellung" schließt sich.

9.14 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* [▶ 116]).

9.14.1 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.

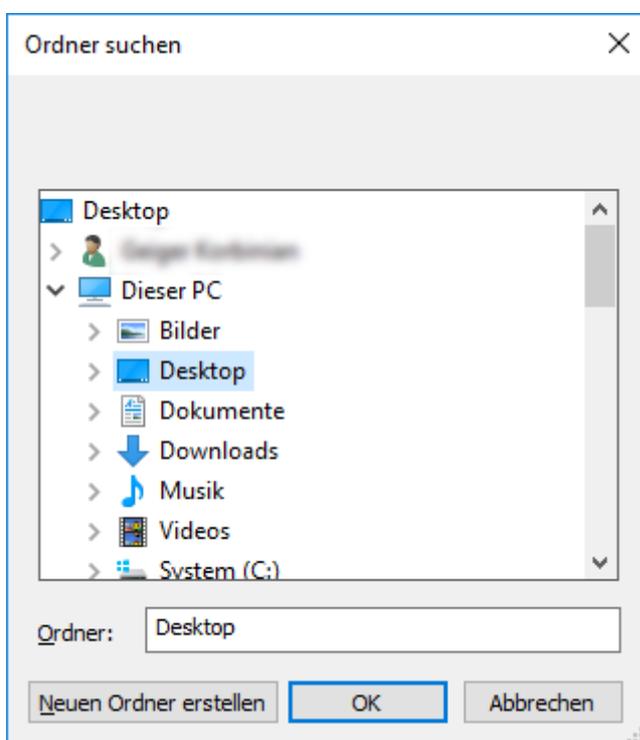
PersonLog	Diese Datei beinhaltet den Verlauf der Bearbeitungen, die an dem Datensatz dieser Person durchgeführt wurden (zum Beispiel Berechtigungsänderungen oder Programmierungen).
-----------	--



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.

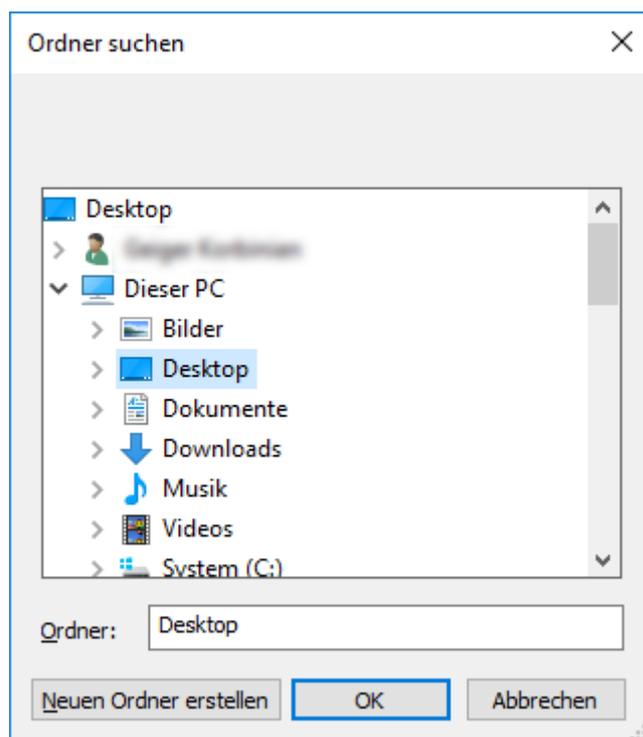
Benutzer

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.

9.14.2 Daten löschen

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

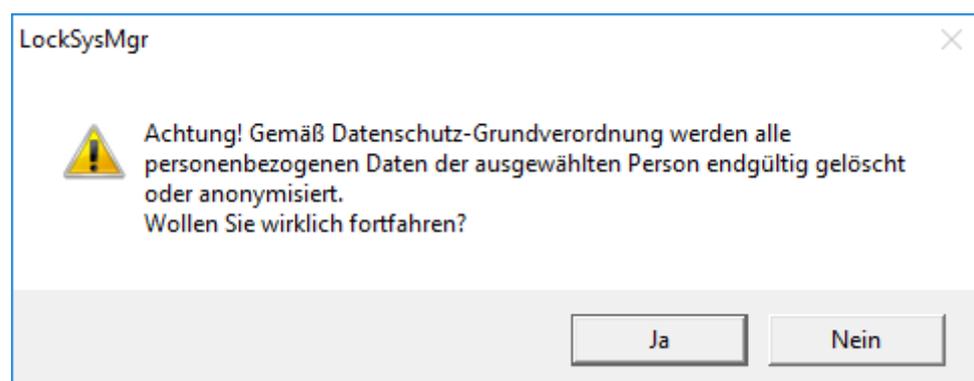
Personen



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

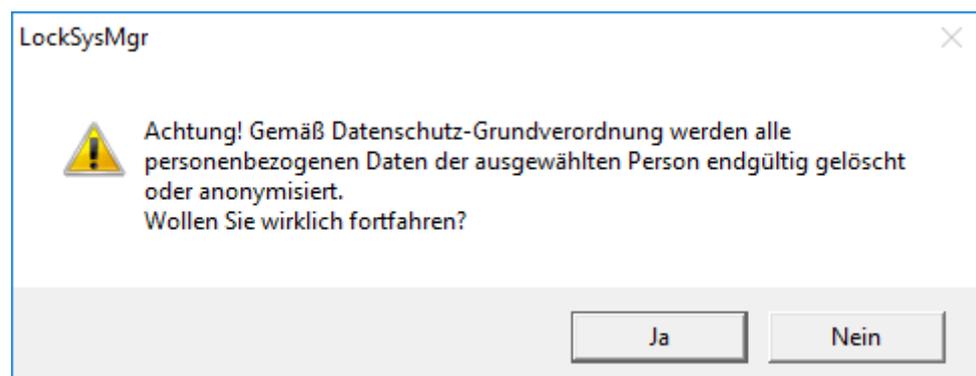
Löschung von Restdaten aus vorherigen Löschungen

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.

9.14.3 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.

9.14.4 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) zuzuordnen zu können.

9.14.5 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.

9.14.6 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.

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

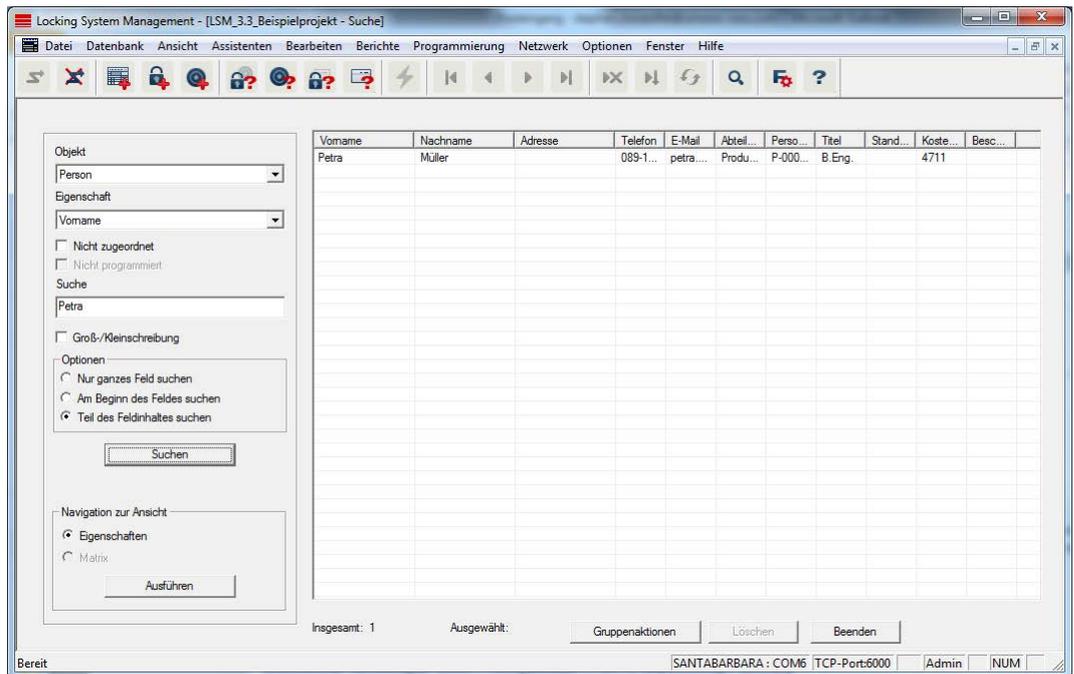
Alle gesammelten Daten zu einer betroffenen Person können (ab Version 3.4), entsprechende Benutzerrechte vorausgesetzt, per Exportfunktion als Kopie durch den Kunden (z.B. im Rahmen eines Audits) zur Verfügung gestellt werden. Dies ermöglicht dem Kunden die Erfüllung des Auskunftsrechts nach Art. 15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

9.14.8 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.

9.15 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.

9.16 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.

9.17 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* [▶ 159]).



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.

9.18 Schließung programmieren

- ✓ Eine Schließung wurde in der Schließenanlage 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.

9.19 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.

9.19.1 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.

9.20 Zeitzonenplan (mit Feiertagen und Betriebsferien) definieren



HINWEIS

Abweichende Zeiten bei G2-Schließungen

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

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

- ✓ Es wurden bereits Schließungen (bzw. Bereiche) und Transponder (bzw. Transpondergruppen) erstellt.
- 1. Klicken Sie in der Menüleiste auf *Bearbeiten/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 Zeitonenplan.
4. Klicken Sie auf die Schaltfläche "Übernehmen".
5. Klicken Sie auf die Schaltfläche "Beenden".

Es wäre auch möglich, den Zeitonenplan 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.

9.21 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.

9.22 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!

9.23 Transponder sperren

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

- *Transponder dauerhaft sperren und Ersatztransponder erstellen* [▶ 159]
- *Transponder temporär sperren* [▶ 163]



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.

9.23.1 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:

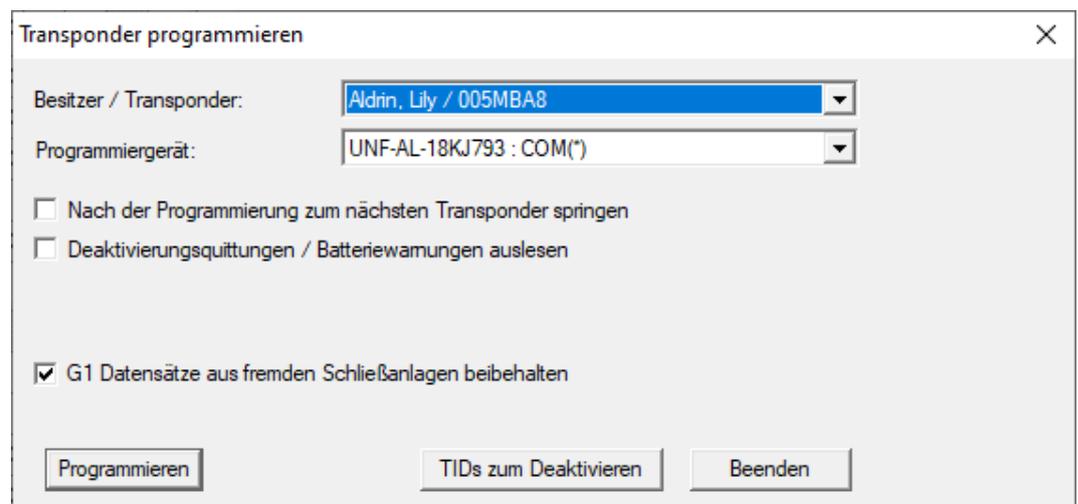
- ✓ Der Ersatztransponder wurde ordnungsgemäß programmiert.
- 1. Betätigen Sie den neuen Ersatztransponder an jeder Schließung.
- 2. Programmieren Sie den neuen Ersatztransponder erneut. Aktivieren Sie im Fenster "Transponder programmieren" die Checkbox "Deaktivierungsquittungen / Batteriewarnungen auslesen".
- 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**.



↳ 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].

Soll-Zustand

- Langes Öffnen
- Kein akustisches Öffnungssignal
- Begehungsliste

Dynamisches Zeitfenster

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

Aktivierungsdatum

- ab sofort

Verfallsdatum

- ohne Verfallsdatum

Zeitzonegruppe

G1

G2

TIDs zum Deaktivieren

- 2. Klicken Sie auf die Schaltfläche **TIDs zum Deaktivieren**.
- ↳ Liste öffnet sich.

TIDs zum Deaktivieren

Schließanlage

G2 TIDs G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

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

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

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

OK Übernehmen Abbrechen

- 3. 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.

9.23.2 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".

Die Begründung

Wollen Sie tatsächlich den Transponder sperren?
Falls "ja", geben Sie bitte den Grund an, z.B. ob der Transponder verlorengegangen oder defekt ist

Temporäre Sperrung

Zusatzinformation:

Ja Nein

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].

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".

9.25 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.

9.26 Freezemode bei G2-Schließungen zurücksetzen

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

- ✓ Batteriewechsel-Identifikationsmedium angelegt (siehe *G2 Batteriewechsel-Transponder* [▶ 115]).
 - ✓ Batteriewechsel-Identifikationsmedium programmiert.
1. Betätigen Sie das Batteriewechsel-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 Batteriewechsel-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 Batteriewechsel-Identifikationsmedium ist ausschließlich für die Aufhebung des Freezemode vor einem Batteriewechsel gedacht. Wenn es missbraucht wird, dann können die Batterien vollständig entleert werden. Die Folge ist ein Totalausfall der Schließung.

9.27 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* [▶ 168].

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.

9.27.1 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* [▶ 254]).

9.28 Benutzer verwalten

Benutzer einer Benutzergruppe zuweisen

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

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

Neuen Benutzer anlegen

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

9.29 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.

9.29.1 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 \[▶ 171\]](#)).

Karte einrichten

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

4. Wählen Sie im Dropdown-Menü ▼ **Kartentyp**: Ihren Kartentyp aus.
5. Wählen Sie im Dropdown-Menü ▼ **Konfiguration**: Ihre Konfiguration aus.
6. Geben Sie ggfs. weitere Parameter wie Sektoren an (Bsp: 2,3,4,5,6,7,8,9,10,11,12,13,14,15).

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.

9.29.2 Übersicht

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

	MIFARE Classic	MIFARE Classic Pre-defined A	MIFARE Classic Pre-defined B	MIFARE Classic + DESFire	MIFARE Plus S/X
MCBasic	✓	✓	✓	✗	✓
MC1200L	✓	✓	✓	✗	✓
MC3800L	✓	✓	✓	✗	✓
MC1000L_AV	✗	✓	✓	✗	✓
MC2400L_AV	✗	✓	✓	✗	✓
MC8000L_AV	✗	✓	✓	✗	✓
MBasic	✗	✗	✗	✓	✗
M1200L	✗	✗	✗	✓	✗
M3800L	✗	✗	✗	✓	✗
M1000L_AV	✗	✗	✗	✓	✗
M4000L_AV	✗	✗	✗	✓	✗
M8000L_AV	✗	✗	✗	✓	✗

	MIFARE Classic	MIFARE Classic Pre-defined A	MIFARE Classic Pre-defined B	MIFARE Classic + DESFire	MIFARE Plus S/X
M10000L_AV	✗	✗	✗	✓	✗

	G1/G2	Lock-IDs	Anzahl der Schließungen	Begehungsliste	Sektoren	Benötigter Speicherplatz	Virtuelles Netzwerk
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗
MC3800L	G2	128-3927	3800	✗	2-15	528	✗
MC1000L_AV	G2	128-1127	1000	19	2-15	528	✓
MC2400L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✗	✗	✗	2-15	48	✗
M1200L	G2	128-1327	1200	✗	2-15	192	✗
M3800L	G2	128-3927	3800	✗	2-15	528	✗
M1000L_AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✗	✗	✗	2-15	48	✗
MD1200L	G2	128-1327	1200	✗	2-15	192	✗
MD3800L	G2	128-3927	3800	✗	n.a. (DESFire)	528	✗

	G1/G2	Lock-IDs	Anzahl der Schließungen	Begehungsliste	Sektoren	Benötigter Speicherplatz	Virtuelles Netzwerk
MD2500 L_AV	G2	128-2627	2500	58	n.a. (DESFire)	1024	✓
MD4000 L_AV	G2	128-4127	4000	100	n.a. (DESFire)	1600	✓
MD1000 L_AV	G2	128-10127	10000	225	n.a. (DESFire)	3048	✓
MD3200 L_AV	G2	128-32127	32000	470	n.a. (DESFire)	7000	✓
MD2400 L_AV	G2	128-2527	2400	34	n.a. (DESFire)	830	✓
MD3650 L_AV	G2	128-3777	3650	2	n.a. (DESFire)	830	✓

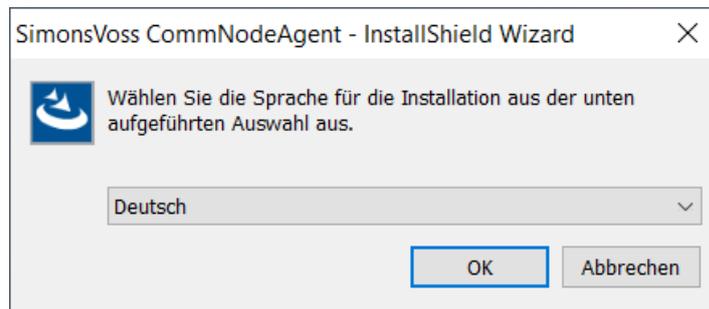
9.30 Weiterleitung von USB-Programmiergeräten zu Terminal-Servern (LSM Professional)

9.30.1 SmartCD.G2 / SmartCD2.G2

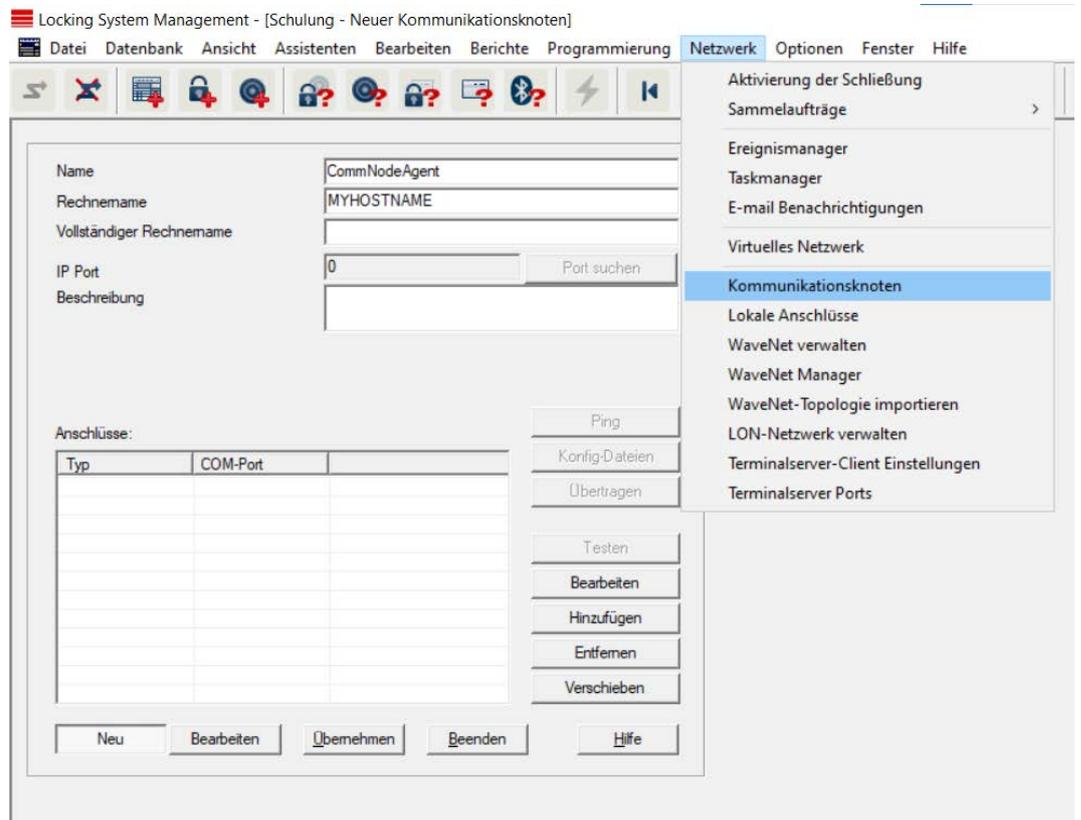
9.30.1.1 CommNodeAgent

Der CommNodeAgent ist eine SimonsVoss-Anwendung (nur vollwertige Windows-Systeme, kein Windows RT) für die Verwendung des aktiven SmartCDs (SmartCD.G2 / SmartCD2.G2) in einer Remotedesktop-Sitzung. Der CommNodeAgent übernimmt die Weiterleitung des USB SmartCDs zu der gewünschten Remotedesktop-Sitzung. Der CommNodeAgent muss am Terminal-Client installiert und in der LSM entsprechend konfiguriert sein.

- ✓ Freier USB-Port am Terminal-Client
 - ✓ Portfreigaben in der Firewall (siehe SimonsVoss-Kommunikationsmatrix)
 - ✓ Bidirektionale DNS-Auflösung Client ↔ Server
 - ✓ CommNodeAgent-Version identisch bzw. kompatibel mit der LSM-Version
1. Installieren Sie den CommNodeAgent und die SmartCD-Treiber auf dem Terminal Client.

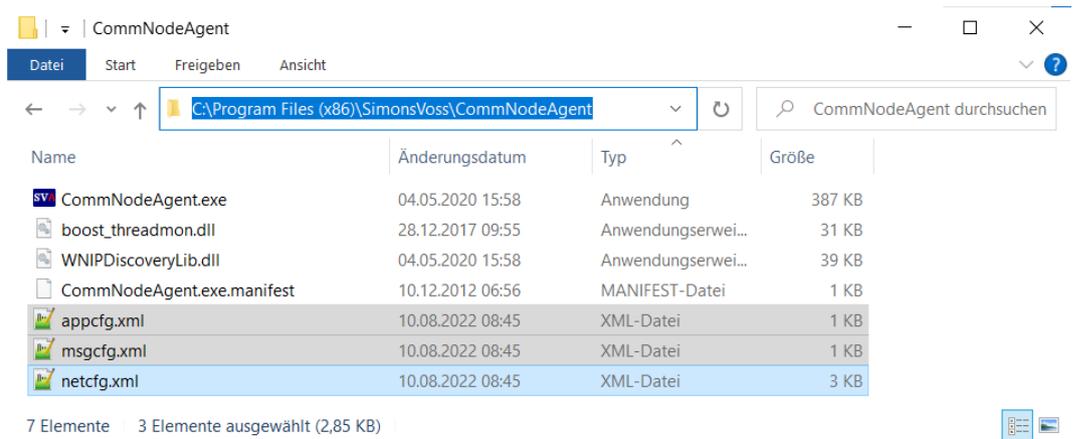


2. Wählen Sie in der oberen Programmleiste über | Netzwerk | den Eintrag **Kommunikationsknoten**.

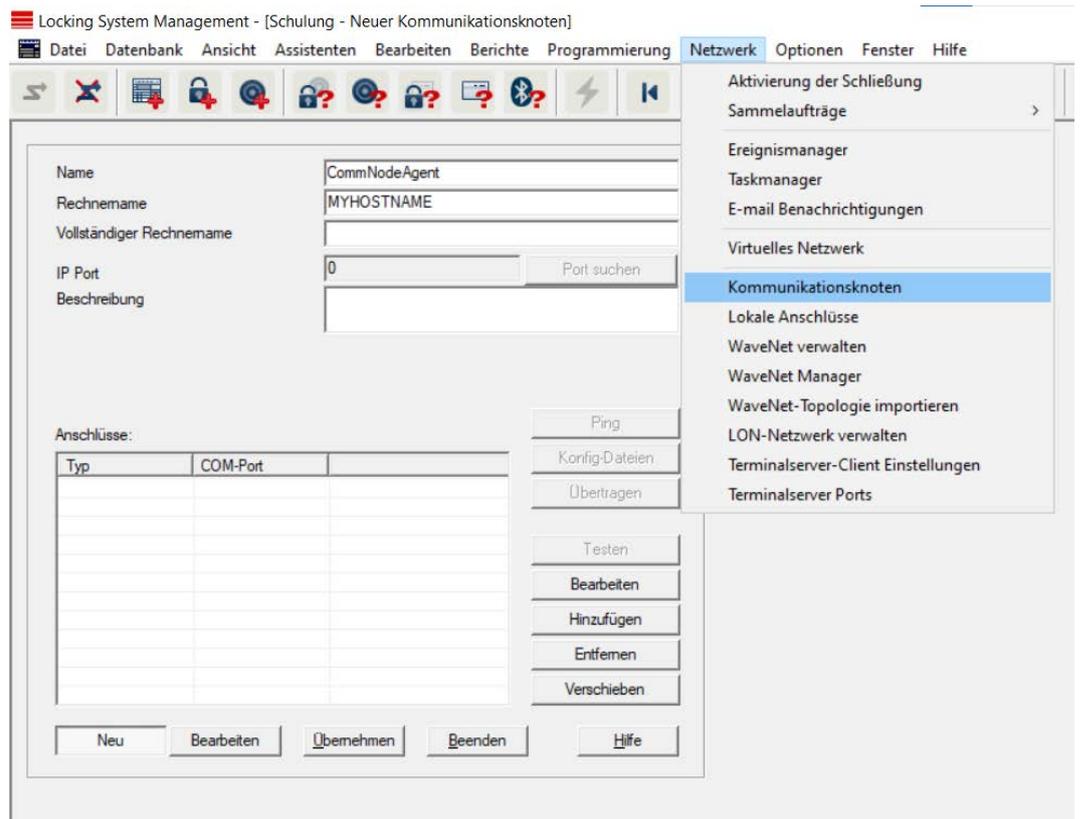


3. Klicken Sie auf die Schaltfläche **Neu**.
4. Geben Sie im Eingabefeld Name einen frei wählbaren Namen für den Kommunikationsknoten ein, z.B. CommNodeAgent.

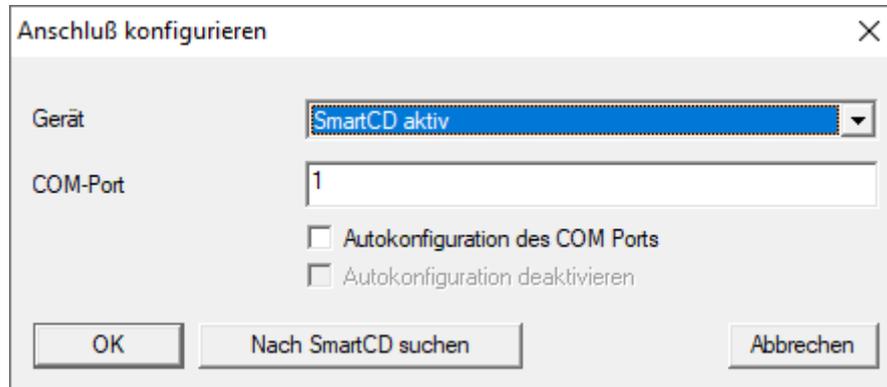
5. Geben Sie den Terminal-Client-Hostnamen im Eingabefeld Rechnername ein.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.
7. Klicken Sie auf die Schaltfläche **Konfig-Dateien**, um Dateien beliebig zu speichern.
8. Um die Konfig-Dateien zu übertragen, kopieren Sie die drei erzeugten XML-Konfig-Dateien aus den obigen Schritten in den Installationsordner des CommNodeAgents.



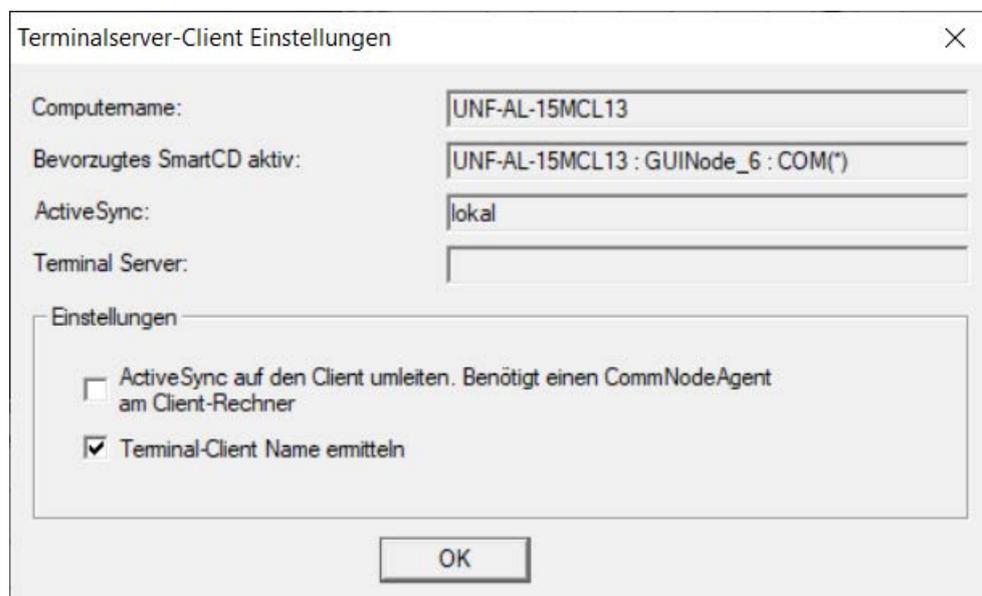
9. Führen Sie CommNodeAgent.exe als Administrator aus.
10. Um das SmartCD zum CommNodeAgent hinzuzufügen, wählen Sie in den oberen Programmleiste über | Netzwerk | den Eintrag **Kommunikationsknoten**.



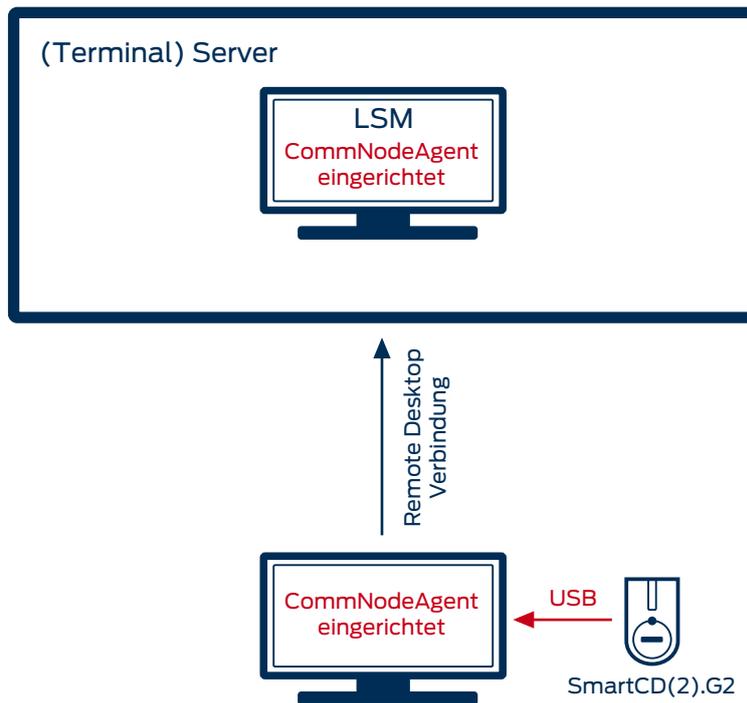
11. Klicken Sie auf die Schaltfläche **Hinzufügen**.
↳ Fenster "Anschluß konfigurieren" öffnet sich.



12. Wählen Sie im folgenden Dialog im Dropdown-Menü ▼ **Gerät** den Eintrag "SmartCD aktiv" aus.
13. Aktivieren Sie die Checkbox **Autokonfiguration des COM Ports**.
14. Klicken Sie auf die Schaltfläche **OK**.
15. Klicken Sie auf die Schaltfläche **Übertragen**.
16. Wählen Sie in der oberen Programmleiste über | Netzwerk | den Eintrag **Terminalserver-Client Einstellungen**.
17. Aktivieren Sie die Checkbox **Terminal-Client Name ermitteln**.



- ↳ Die Terminalserver-Client-Einstellungen werden geprüft.



9.30.1.2 USB / Ethernet Server

USB-Geräte können mittels USB-/Ethernet-Server über das Kundennetzwerk zu einem (Terminal-)Server weitergeleitet werden.

Am Terminal-Client muss keine Installation vorgenommen werden.

- ✓ Die USB-Server-Software muss zentral am Server eingerichtet werden.
- ✓ Der USB-Server selbst benötigt eine entsprechende Netzwerkkonfiguration.

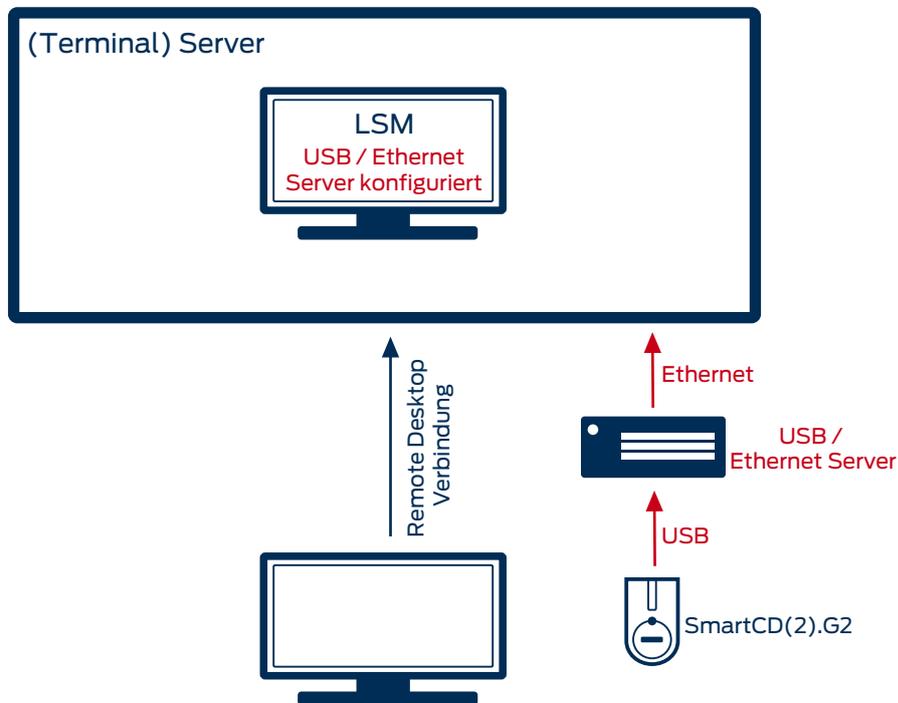
1. Wählen Sie in der oberen Programmleiste über | Netzwerk | den Eintrag **Terminalserver-Client Einstellungen**.
2. Deaktivieren Sie die Checkbox Terminal-Client Name ermitteln.

The screenshot shows a dialog box titled 'Terminalserver-Client Einstellungen'. It contains the following fields and options:

- Computename: UNF-AL-15MCL13
- Bevorzugtes SmartCD aktiv: UNF-AL-15MCL13 : GUINode_6 : COM(*)
- ActiveSync: lokal
- Terminal Server: (empty field)
- Einstellungen section:
 - ActiveSync auf den Client umleiten. Benötigt einen CommNodeAgent am Client-Rechner
 - Terminal-Client Name ermitteln

An 'OK' button is located at the bottom center of the dialog.

Hierbei handelt es sich um keine SimonsVoss-Hardware, daher kann keine Einrichtung / Support seitens SimonsVoss durchgeführt werden. Namhafte Hersteller solcher Geräte sind unter anderem die Firmen Silex und W&T.

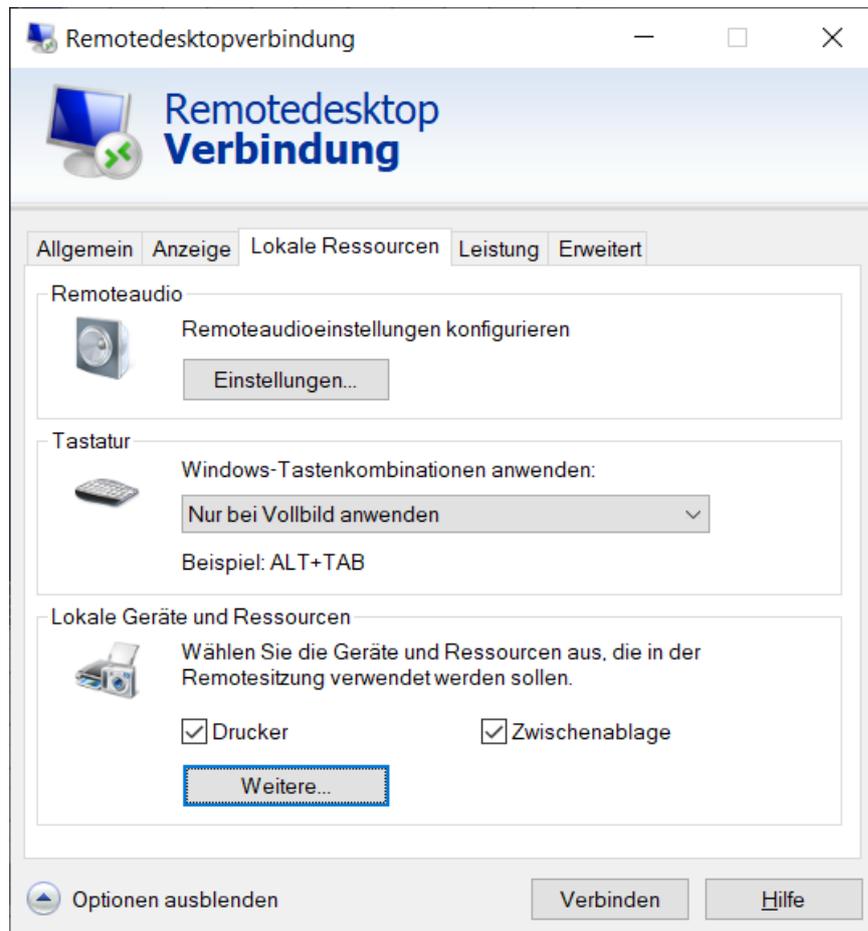


9.30.2 SmartCD MP / HF

9.30.2.1 Remotedesktop-Verbindung (bis LSM 3.5 SP1)

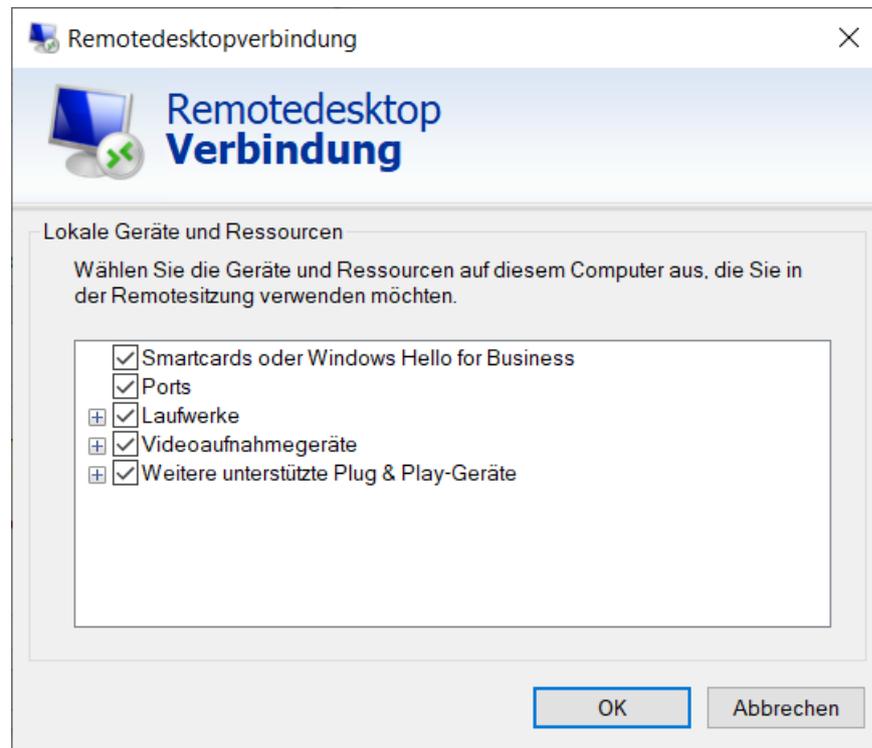
- ✓ SmartCD.MP und SmartCD.HF können nicht über den CommNode-Agent durchgeschliffen werden. Die Weiterleitung erfolgt direkt über die Remotedesktop-Verbindung.
1. Öffnen Sie die Verbindungseinstellungen der Remotedesktop-Sitzung.
 2. Klicken Sie auf die Schaltfläche **Optionen einblenden**, um die Optionen einzublenden.

3. Wechseln Sie zur Registerkarte [Lokale Ressourcen].

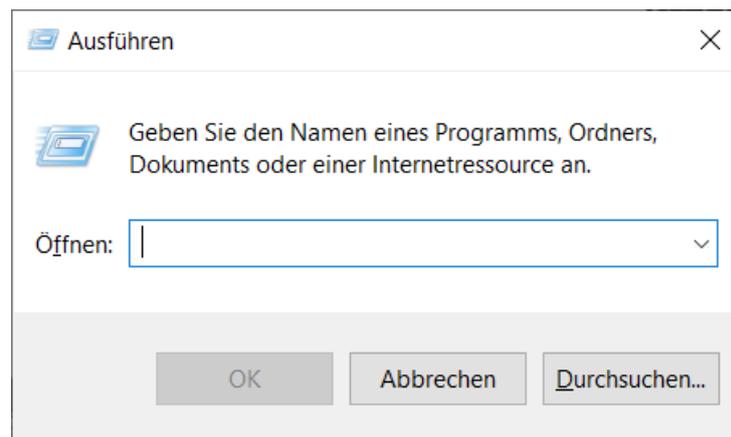


4. Klicken Sie auf die Schaltfläche **Weitere...**.

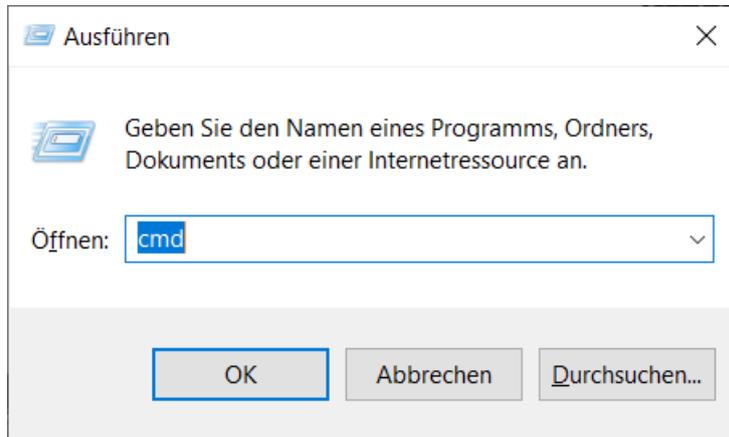
5. Stellen Sie sicher, dass die Checkbox Ports aktiviert ist.



6. Klicken Sie auf die Schaltfläche **OK**.
7. Verbinden Sie sich mit dem Remotedesktop.
8. Tippen Sie auf die Windows-Taste und R gleichzeitig.
↳ Fenster "Ausführen" öffnet sich.



9. Geben Sie im Eingabefeld **CMD** ein.

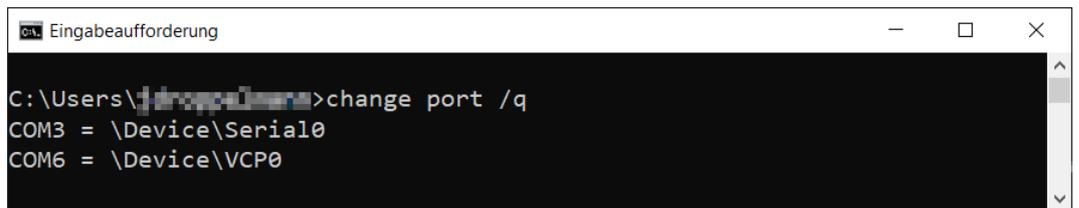


10. Klicken Sie auf die Schaltfläche **OK**.

↳ Das Fenster "Eingabeaufforderung" öffnet sich.

11. Stecken Sie das SmartCD.MP/SmartCD.HF am Terminalclient ab.

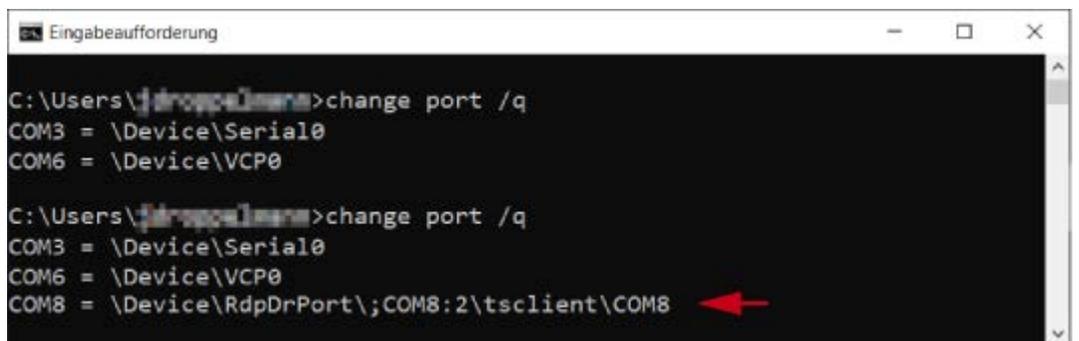
12. Geben Sie *change port /q* ein.



↳ Der Befehl zeigt die Ausgabe ohne angeschlossenes SmartCD.MP/SmartCD.HF.

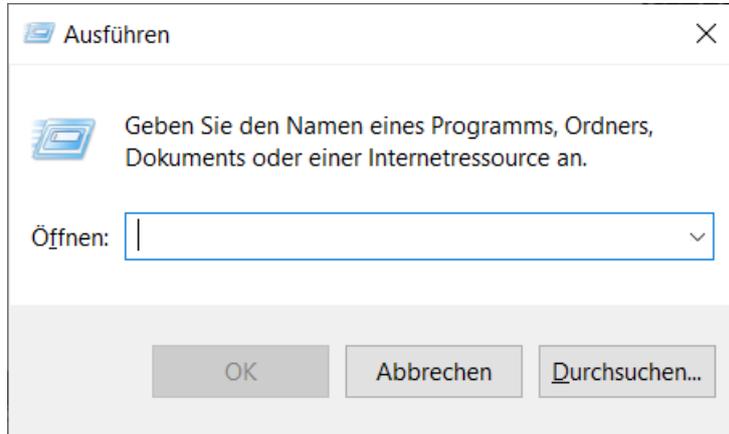
13. Stecken Sie das SmartCD.MP/SmartCD.HF am Terminalclient wieder an.

14. Geben Sie *change port /q* ein.

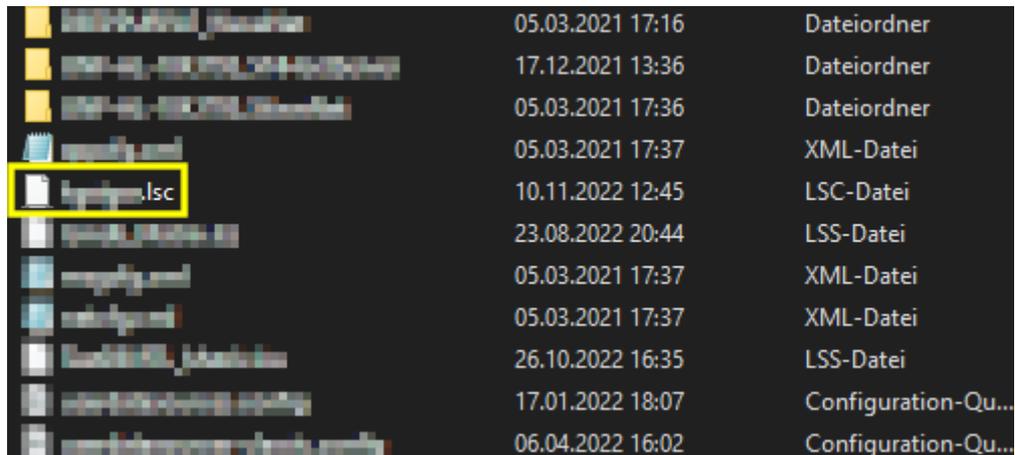


↳ Der zweite Befehl zeigt die Ausgabe mit angeschlossenem SmartCD.MP/SmartCD.HF. Ein neuer Port ist dazugekommen.
→ In diesem Fall ist COM-Port 8 das weitergeleitete SmartCD.MP/SmartCD.HF.

- 15. Tippen Sie auf die Windows-Taste und R gleichzeitig.
↳ Fenster "Ausführen" öffnet sich.



- 16. Geben Sie den Pfad zum Verzeichnis der LSM-User ein:
%localappdata%\SimonsVoss\LockSysMgr\config\
17. Klicken Sie auf die Schaltfläche **OK**.
↳ Explorer zeigt das Verzeichnis der LSM-User an.



HINWEIS

LSC-Datei für LSM-Benutzer

Die LSM legt an dieser Stelle für jeden Benutzer, der sich mindestens einmal angemeldet hat, eine Konfigurationsdatei (.lsc) an.

- Wenn für einen Benutzer noch keine Konfigurationsdatei vorhanden ist, dann bitten Sie den Benutzer, sich an der LSM anzumelden.

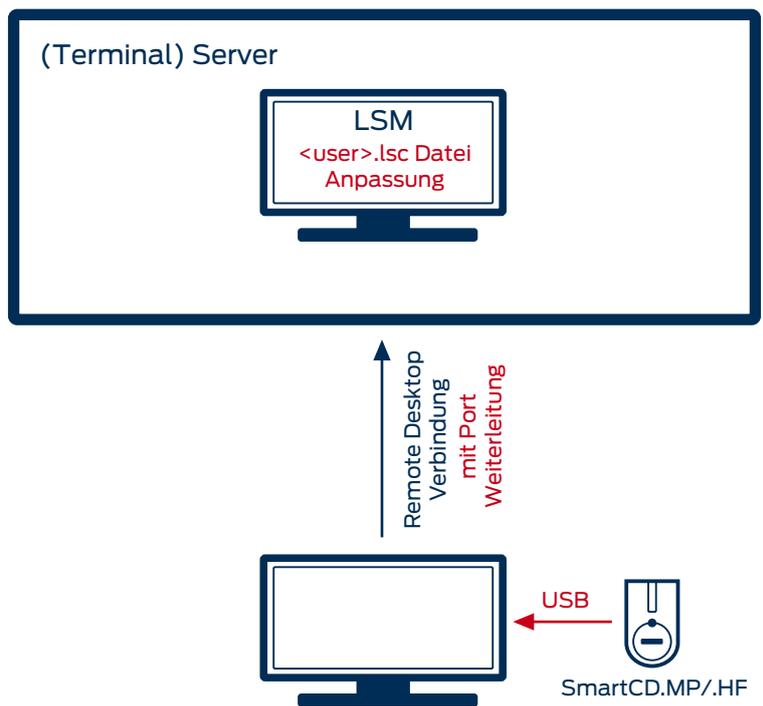
- 18. Öffnen Sie mit einem Doppelklick die Konfigurationsdatei.
- 19. Ergänzen Sie in dieser Datei unter der Zeile [Common] die Zeile:
CardReaderPort=<PORT>

20. Ersetzen Sie <PORT> durch den zuvor mit der "Eingabeaufforderung" ermittelten Wert.

```
MyUser - Notepad
File Edit Format View Help

[SETUP]
AliasDB=TestSystem
DataSource=\\winpc:6262\sv_db$\lsmdb.add
Catalog=lsmdb.add
ServerType=2
LastUsedDB=0
[Login]
UserName=Admin
TestSystem=1
[Common]
CardReaderPort=8
```

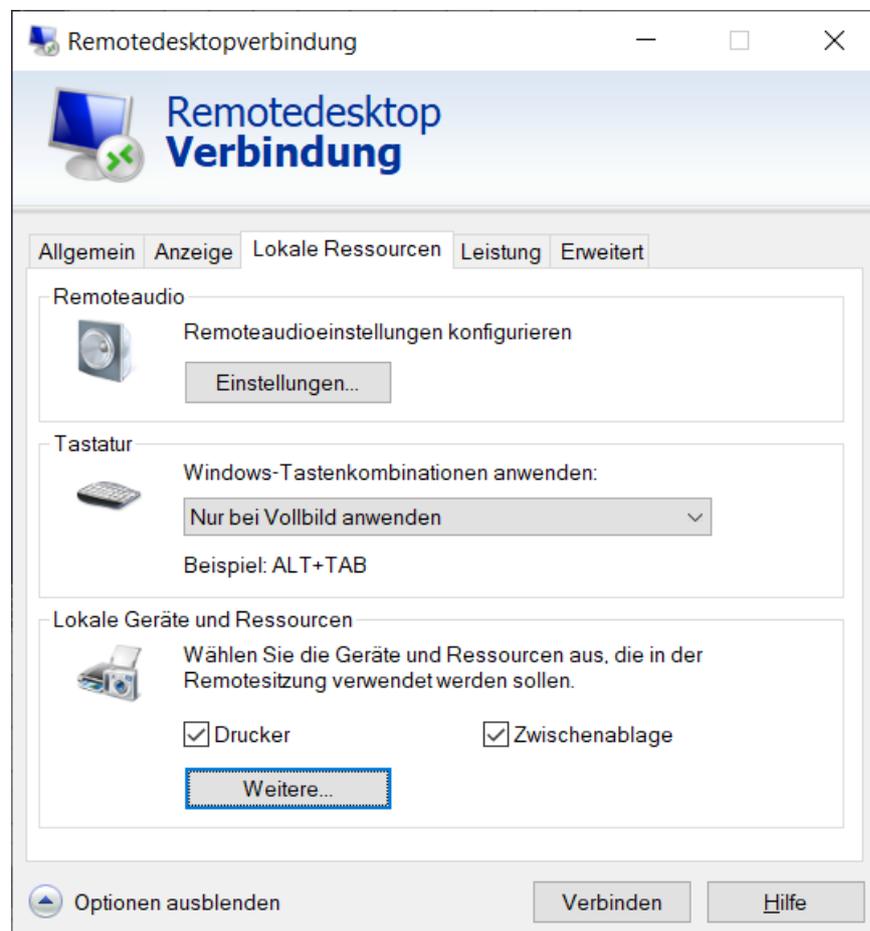
- 21. Speichern Sie die geänderte Konfigurationsdatei.
- 22. Ergänzen Sie die Zeile ggfs. auch für alle anderen Benutzer in deren Konfigurationsdateien.
- 23. Beenden Sie ggfs. die LSM-Sitzung.
- 24. Starten Sie die Remotedesktop-Sitzung neu.



9.30.2.2 Remotedesktop-Verbindung (ab LSM 3.5 SP2)

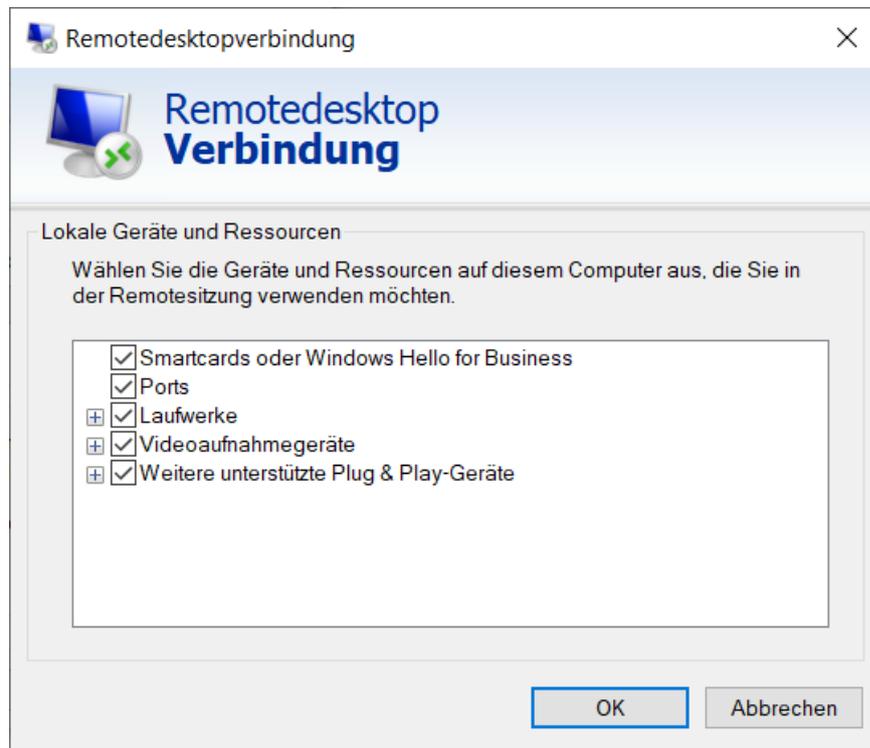
Ab der LSM 3.5 SP2 können Sie die weitergeleiteten Remotedesktop-Ports für jeden Hostnamen direkt in der LSM verwalten.

- ✓ SmartCD.MP und SmartCD.HF können nicht über den CommNode-Agent durchgeschliffen werden. Die Weiterleitung erfolgt direkt über die Remotedesktop-Verbindung.
1. Öffnen Sie die Verbindungseinstellungen der Remotedesktop-Sitzung.
 2. Klicken Sie auf die Schaltfläche **Optionen einblenden**, um die Optionen einzublenden.
 3. Wechseln Sie zur Registerkarte [Lokale Ressourcen].

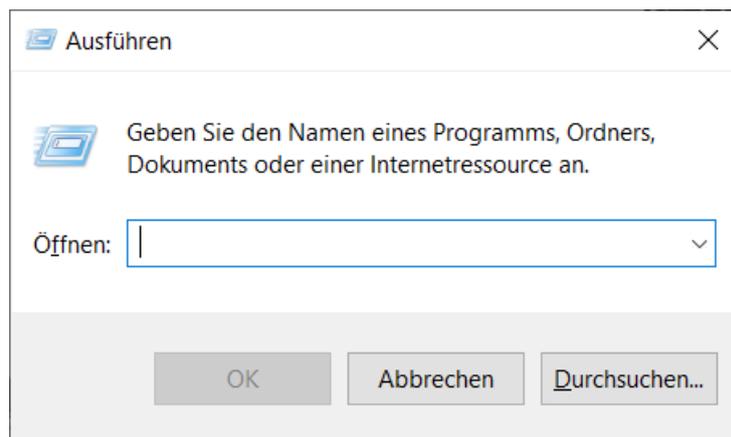


4. Klicken Sie auf die Schaltfläche **Weitere...**.

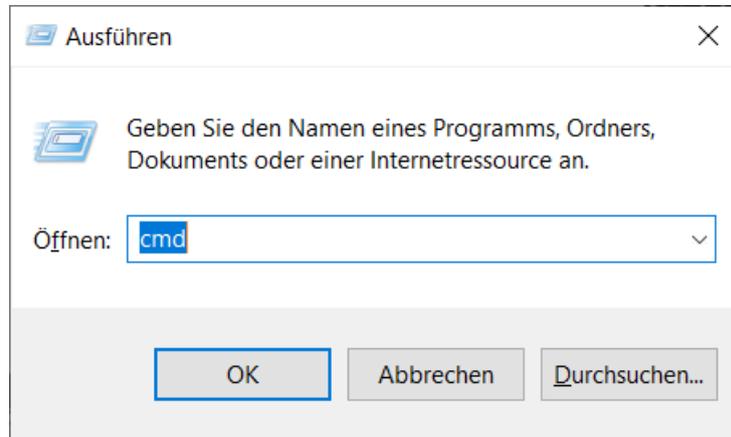
5. Stellen Sie sicher, dass die Checkbox Ports aktiviert ist.



6. Klicken Sie auf die Schaltfläche **OK**.
7. Verbinden Sie sich mit dem Remotedesktop.
8. Tippen Sie auf die Windows-Taste und R gleichzeitig.
↳ Fenster "Ausführen" öffnet sich.



9. Geben Sie im Eingabefeld **CMD** ein.

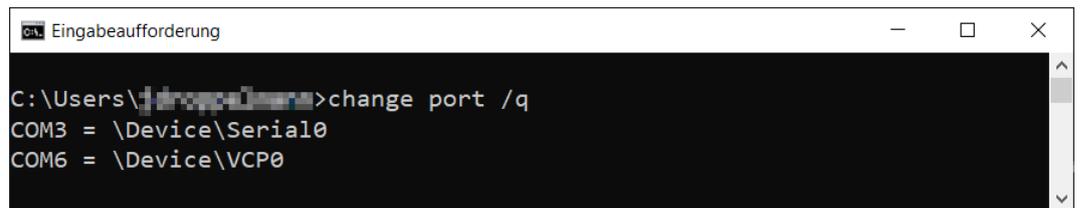


10. Klicken Sie auf die Schaltfläche **OK**.

↳ Das Fenster "Eingabeaufforderung" öffnet sich.

11. Stecken Sie das SmartCD.MP/SmartCD.HF am Terminalclient ab.

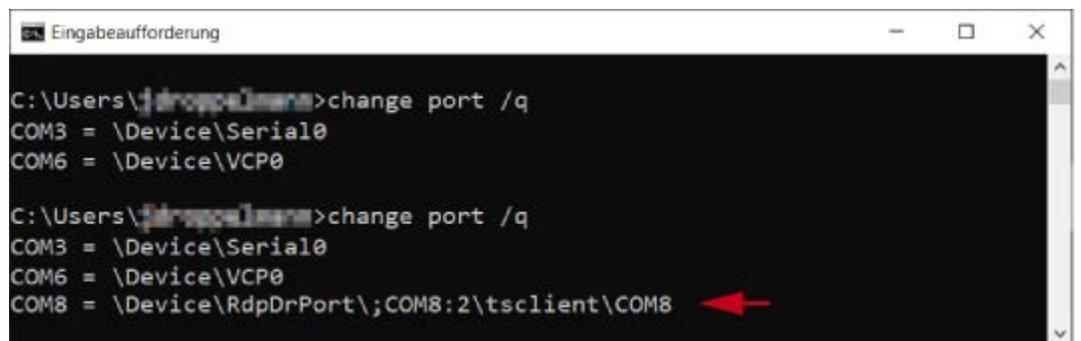
12. Geben Sie *change port /q* ein.



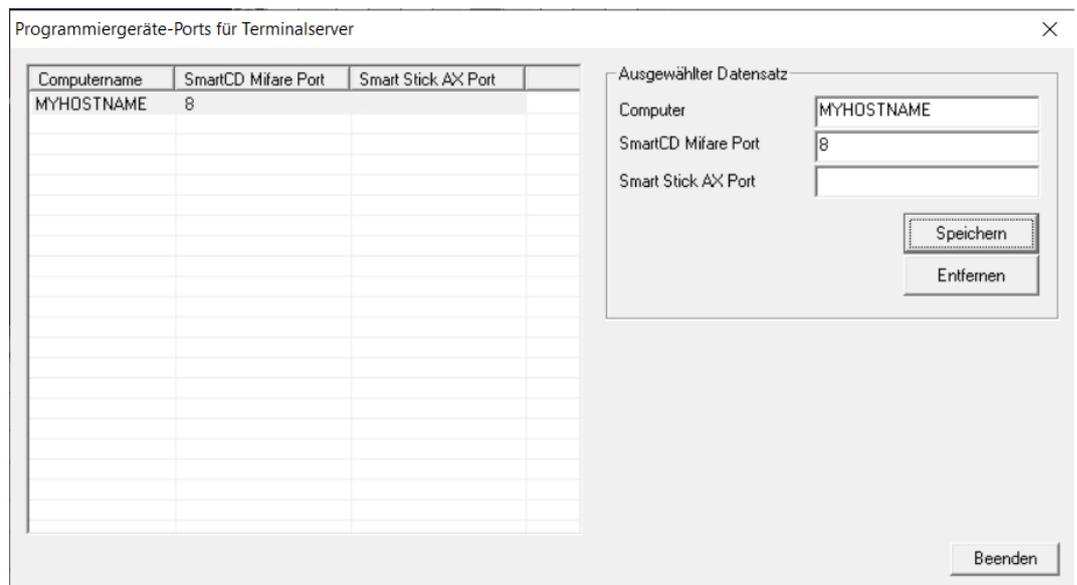
↳ Der Befehl zeigt die Ausgabe ohne angeschlossenes SmartCD.MP/SmartCD.HF.

13. Stecken Sie das SmartCD.MP/SmartCD.HF am Terminalclient wieder an.

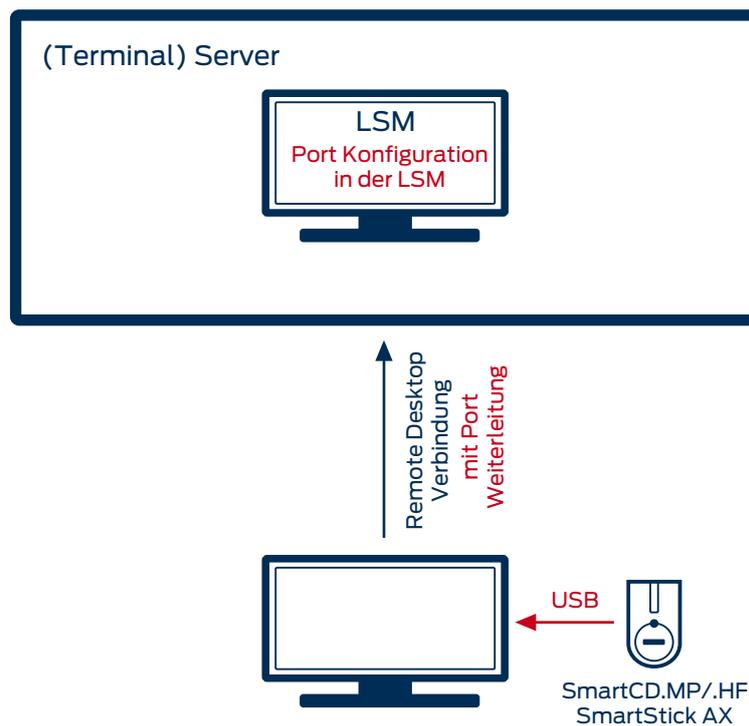
14. Geben Sie *change port /q* ein.



↳ Der zweite Befehl zeigt die Ausgabe mit angeschlossenem SmartCD.MP/SmartCD.HF. Ein neuer Port ist dazugekommen.
→ In diesem Fall ist COM-Port 8 das weitergeleitete SmartCD.MP/SmartCD.HF.



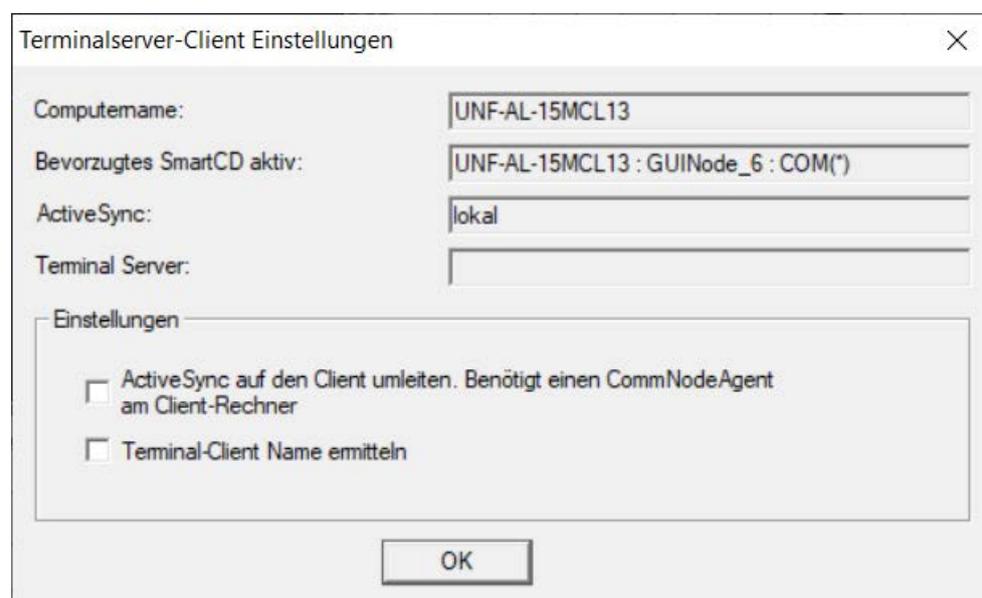
- 19. Beenden Sie ggfs. die LSM-Sitzung.
- 20. Starten Sie die Remotedesktop-Sitzung neu.



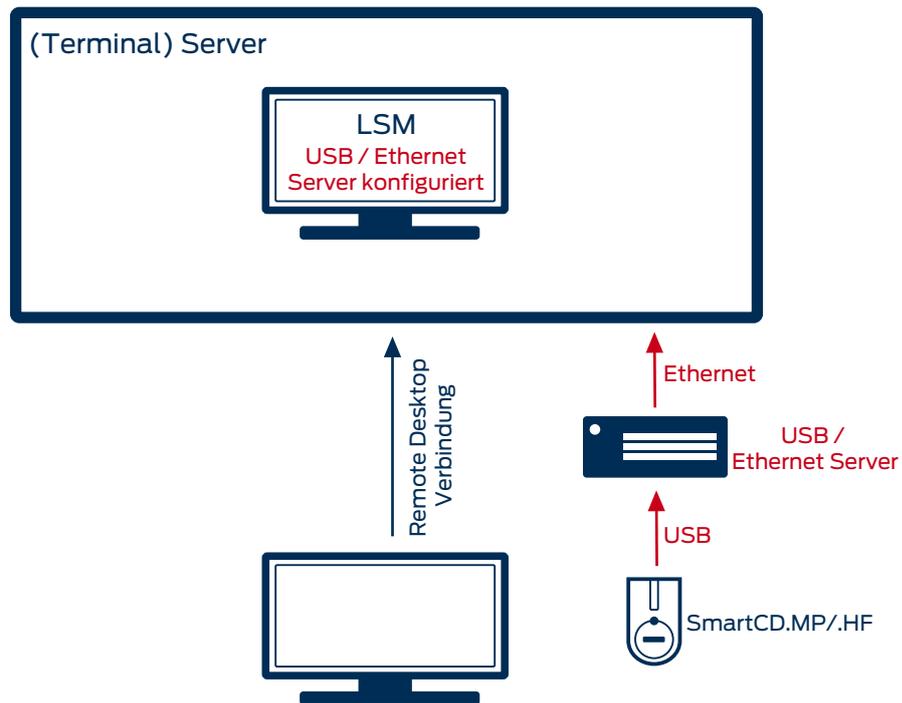
9.30.2.3 USB / Ethernet Server

USB-Geräte können mittels USB-/Ethernet-Server über das Kundennetzwerk zu einem (Terminal-)Server weitergeleitet werden. Am Terminal-Client muss keine Installation vorgenommen werden.

- ✓ Die USB-Server-Software muss zentral am Server eingerichtet werden.
 - ✓ Der USB-Server selbst benötigt eine entsprechende Netzwerkkonfiguration.
1. Wählen Sie in der oberen Programmleiste über | Netzwerk | den Eintrag **Terminalserver-Client Einstellungen**.
 2. Deaktivieren Sie die Checkbox Terminal-Client Name ermitteln.
 - ↳ Eine angepasste Konfigurationsdatei (*.lsc, siehe *Remotedesktop-Verbindung (bis LSM 3.5 SP1)* [▶ 178]) kann zu Störungen führen, ggf. müssen die Einträge dort entfernt werden.



Hierbei handelt es sich um keine SimonsVoss-Hardware, daher kann keine Einrichtung / Support seitens SimonsVoss durchgeführt werden. Namhafte Hersteller solcher Geräte sind unter anderem die Firmen Silex und W&T.



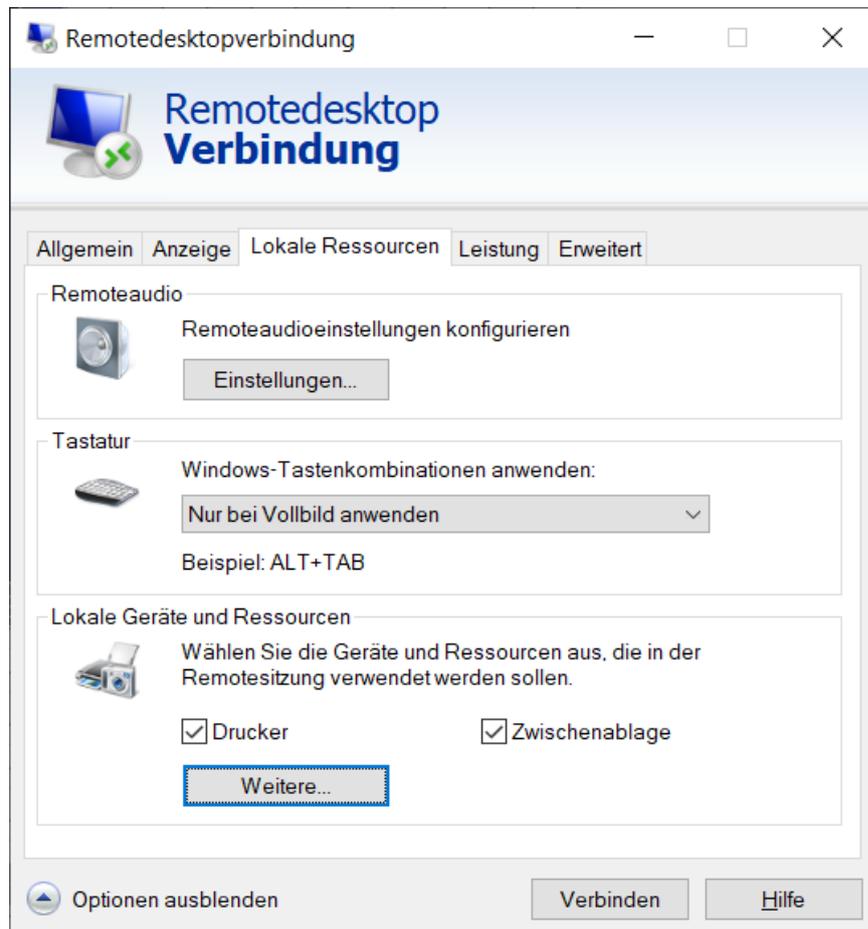
9.30.3 SmartStick AX

9.30.3.1 Remotedesktop-Verbindung (ab LSM 3.5 SP2)

Ab der LSM 3.5 SP2 können Sie die weitergeleiteten Remotedesktop-Ports für jeden Hostnamen direkt in der LSM verwalten.

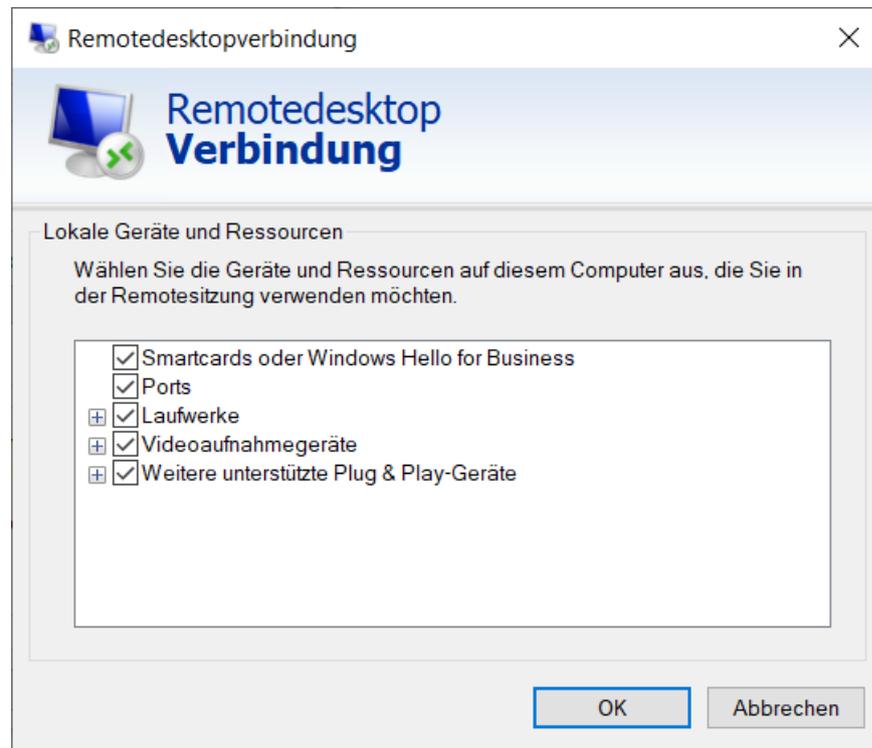
- ✓ Der SmartStick AX kann nicht über den CommNode-Agent durchgeschliffen werden. Die Weiterleitung erfolgt direkt über die Remotedesktop-Verbindung.
1. Öffnen Sie die Verbindungseinstellungen der Remotedesktop-Sitzung.
 2. Klicken Sie auf die Schaltfläche **Optionen einblenden**, um die Optionen einzublenden.

3. Wechseln Sie zur Registerkarte [Lokale Ressourcen].

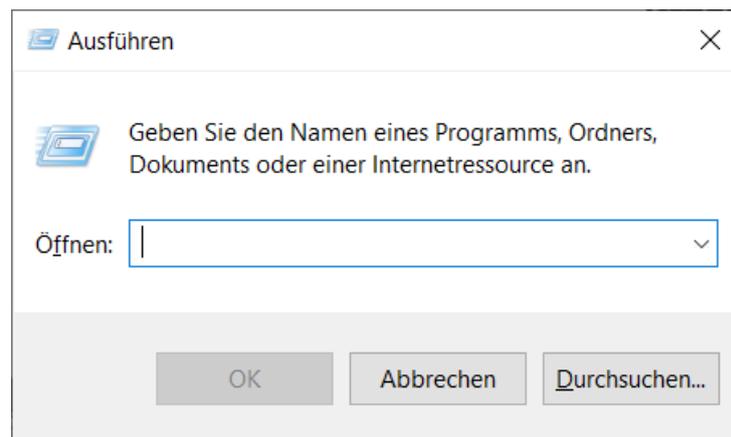


4. Klicken Sie auf die Schaltfläche **Weitere...**.

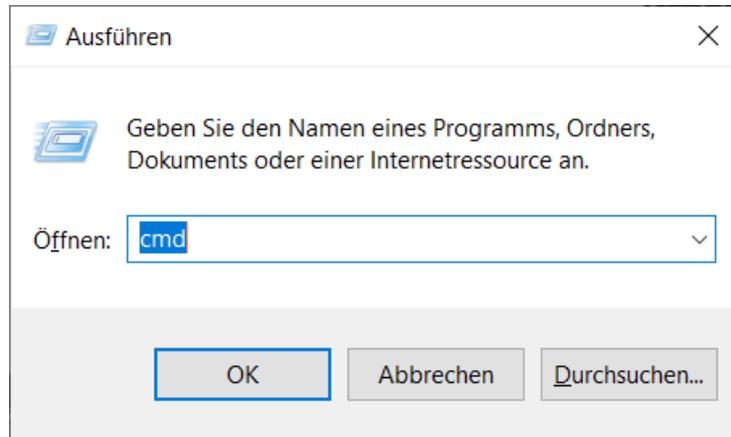
5. Stellen Sie sicher, dass die Checkbox Ports aktiviert ist.



6. Klicken Sie auf die Schaltfläche **OK**.
7. Verbinden Sie sich mit dem Remotedesktop.
8. Tippen Sie auf die Windows-Taste und R gleichzeitig.
↳ Fenster "Ausführen" öffnet sich.



9. Geben Sie im Eingabefeld **CMD** ein.

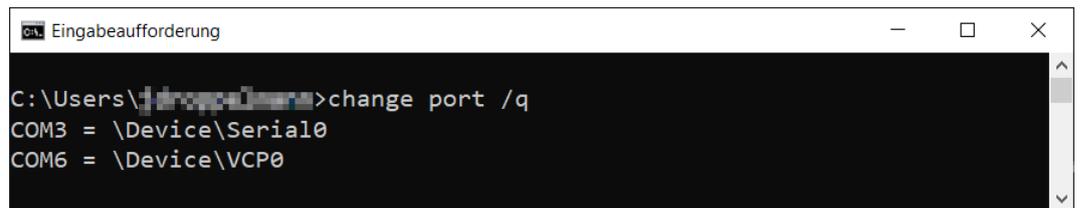


10. Klicken Sie auf die Schaltfläche **OK**.

↳ Das Fenster "Eingabeaufforderung" öffnet sich.

11. Stecken Sie den SmartStick AX am Terminalclient ab.

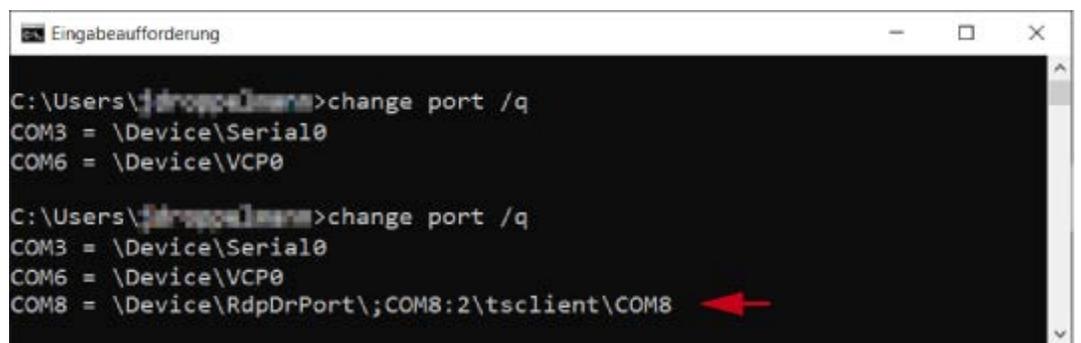
12. Geben Sie *change port /q* ein.



↳ Der Befehl zeigt die Ausgabe ohne angeschlossenen SmartStick AX.

13. Schließen Sie den SmartStick AX am Terminalclient wieder an.

14. Geben Sie *change port /q* ein.



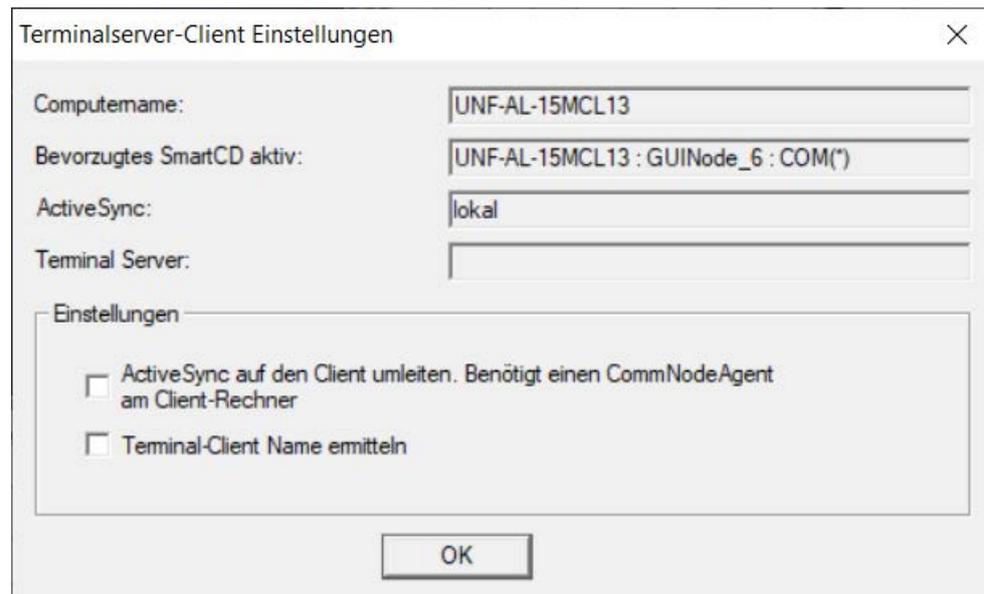
↳ Der zweite Befehl zeigt die Ausgabe mit angeschlossenem SmartStick AX. Ein neuer Port ist dazugekommen.

→ In diesem Fall ist COM-Port 8 der weitergeleitete SmartStick AX.

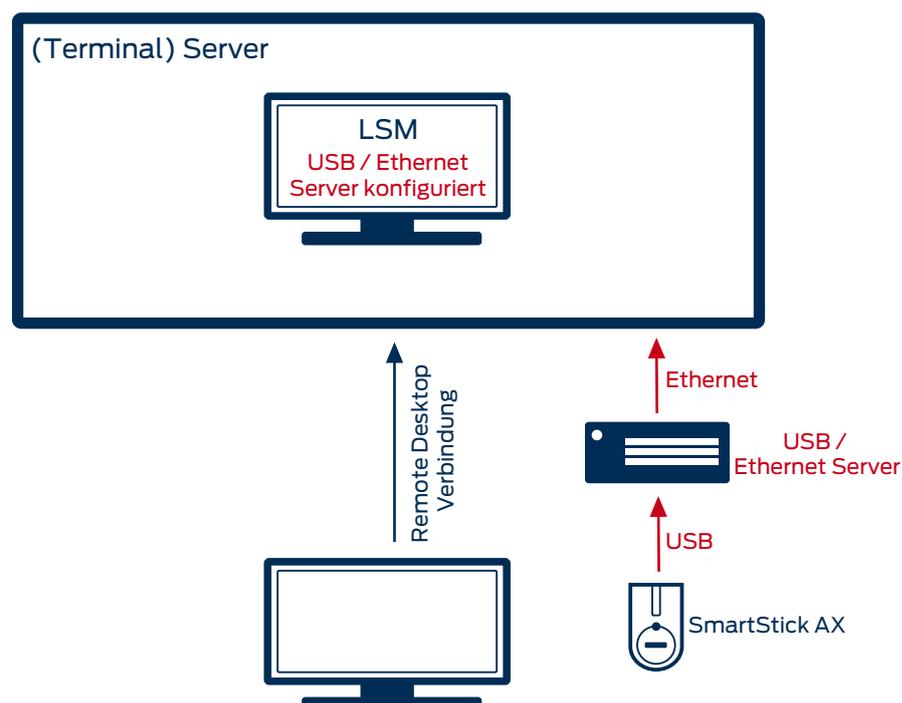
15. Wählen Sie in der LSM in der oberen Programmleiste über | Netzwerk | den Eintrag **Terminalserver Ports**.

↳ Fenster "Programmiergeräte-Ports für Terminalserver" öffnet sich.

- ✓ Die USB-Server-Software muss zentral am Server eingerichtet werden.
 - ✓ Der USB-Server selbst benötigt eine entsprechende Netzwerkkonfiguration.
1. Wählen Sie in der oberen Programmleiste über | Netzwerk | den Eintrag **Terminalserver-Client Einstellungen**.
 2. Deaktivieren Sie die Checkbox Terminal-Client Name ermitteln.



Hierbei handelt es sich um keine SimonsVoss-Hardware, daher kann keine Einrichtung / Support seitens SimonsVoss durchgeführt werden. Namhafte Hersteller solcher Geräte sind unter anderem die Firmen Silex und W&T.



10. 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.

10.1 Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung

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

10.1.1 LSM Software vorbereiten

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

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

10.1.2 Erstprogrammierung der Schließkomponenten

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

10.1.2.1 Neue Schließung anlegen

- ✓ Es ist bereits eine Schließanlage angelegt.
1. Wählen Sie *Bearbeiten/Neue Schließung*.
 2. Füllen Sie alle Attribute aus und setzen Sie ggf. weitere Einstellungen über die Schaltfläche "Konfiguration".

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

10.1.2.2 Schließung programmieren

- ✓ Eine Schließung wurde in der Schließanlage angelegt und ist in der Matrix sichtbar.
1. Rechtsklick auf die gewünschte Schließung.
 2. Programmieren anklicken.
 3. Folgen Sie den Anweisungen der LSM Software.

Achten Sie auf die Auswahl des entsprechenden Programmiergeräts.



HINWEIS

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

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.

10.1.3 Hardware vorbereiten

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



HINWEIS

Standardeinstellungen:

IP-Adresse: 192.168.100.100

Benutzername: SimonsVoss | Passwort: SimonsVoss

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



HINWEIS

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

10.1.4 Kommunikationsknoten erstellen

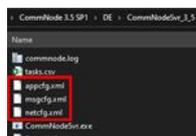
Der Kommunikationsknoten bildet die Schnittstelle zwischen dem CommNode-Server und der LSM-Software. Um die Konfigurations-XMLs anzulegen, muss die LSM-Software als Administrator ausgeführt werden.

1. Öffnen Sie die LSM-Software.
2. Wählen Sie | Netzwerk | **Kommunikationsknoten**.
3. Ergänzen Sie die Informationen "Name", "Rechnername" und "Beschreibung".

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

↳ z.B. UNF-AL-18KJ793; UNF-AL-18KJ793.ALLEGION.COM;
Kommunikationsknoten für das WaveNet-Funknetzwerk 123

4. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.
5. Vergewissern Sie sich, dass der Pfad auf das Installationsverzeichnis des CommNode-Servers verweist und klicken Sie auf die Schaltfläche **OK**.
6. Quittieren Sie die Meldung mit **Nein** und bestätigen Sie die Auswahl mit **OK**. Die drei Konfigurations-XMLs (appcfg, msgcfg und netcfg) müssen direkt im Installationsverzeichnis des CommNode-Servers liegen.



7. Speichern Sie Ihre Einstellungen über die Schaltfläche **Übernehmen**.
8. Quittieren Sie den Hinweis über die Schaltfläche **OK**.
9. Beenden Sie den Dialog über die Schaltfläche **Beenden**.

10.1.5 Netzwerk einrichten und in LSM importieren

10.1.5.1 WaveNet-Konfiguration anlegen

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

- ✓ Die LSM ist ordnungsgemäß installiert und ein Network-Modul ist lizenziert.
- ✓ Der CommNode-Server wurde installiert und der Dienst ist gestartet.
- ✓ Die Konfigurationsdateien des CommNode-Servers wurden erstellt.
- ✓ Der WaveNet-Manager ist in seiner aktuellen Version installiert.
- ✓ In der LSM-Software wurde ein Kommunikationsknoten erstellt.
- ✓ Die Erstprogrammierung der zu vernetzenden Schließung war erfolgreich.
- ✓ Der RouterNode2 ist über das Netzwerk erreichbar und Sie kennen dessen IP-Adresse.
- ✓ Die programmierte Schließung verfügt über einen montierten LockNode, dessen Chip-ID Sie kennen.

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

10.1.5.2 WaveNet-Konfiguration übertragen

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

1. Wählen Sie "Netzwerk/Kommunikationsknoten".
2. Wählen Sie den RouterNode2 auf der Liste der Anschlüsse aus und klicken Sie auf die Schaltfläche "Übertragen".

3. Speichern Sie Ihre Einstellungen über die Schaltfläche "Übernehmen".
4. Beenden Sie den Dialog über die Schaltfläche "Beenden".

10.1.5.3 LockNode einer Schließung zuweisen

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

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

10.1.5.4 WaveNet-Konfiguration testen

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

10.2 Inbetriebnahme der DoorMonitoring Schließungen

In diesem Beispiel wird gezeigt, welche Einstellungen beim Einrichten einer DoorMonitoring-Schließung vorzunehmen sind. Die Voraussetzungen dafür sind im Kapitel "*Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung [▶ 197]*" genannt.

10.2.1 Mögliche (Tür-)zustände

Die angezeigten Zustände sind komponentenabhängig.

10.2.1.1 Mögliche DoorMonitoring-Zustände SmartHandle

- Tür offen/geschlossen
- Tür zu lange offen
- Verriegelt (nur bei selbstverriegelnden Einsteckschlössern)
- Drücker gedrückt/nicht gedrückt

10.2.1.2 Mögliche DoorMonitoring-Zustände Schließzylinder

- Tür offen/geschlossen
- Tür verriegelt

- Tür sicher verriegelt
- Tür zu lange offen
- Stulpschraube manipuliert

10.2.1.3 Mögliche DoorMonitoring-Zustände SmartRelais 3

- Input 1 aktiv/inaktiv
- Input 2 aktiv/inaktiv
- Input 3 aktiv/inaktiv
- *Sabotage-Erkennung* [[▶ 205](#)]

10.2.1.4 Mögliche Zustände RouterNode 2 / GatewayNode 2

- Input aktiv/inaktiv
- Analoge Spannung über/unter Schwellwert

10.2.2 DoorMonitoring-Schließungen im Netzwerk einbinden

So binden Sie DM-Schließungen in das WaveNet-Netzwerk ein:

- ✓ WaveNet-Manager bereits eingerichtet.
 - ✓ RouterNode, welchem die neue Schließung zugewiesen werden soll, ist bereits eingerichtet und "online".
 - ✓ LockNode ist korrekt auf der DM-Schließung montiert.
 - ✓ Chip-ID bekannt.
1. Starten Sie den WaveNet-Manager über | Netzwerk | - **WaveNet-Manager**.
 2. Klicken Sie mit der rechten Maustaste auf den RouterNode.
 - ↳ Fenster "Administration" öffnet sich.
 3. Markieren Sie die Option Suchen nach Chip ID.
 4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 5. Folgen Sie dem Dialog und weisen Sie die Schließung bzw. den dazugehörigen LockNode über dessen Chip-ID dem RouterNode2 zu.
 6. Klicken Sie mit der rechten Maustaste auf den neu hinzugefügten DM-LockNode.
 7. Markieren Sie die Option I/O-Konfiguration.
 8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" öffnet sich.

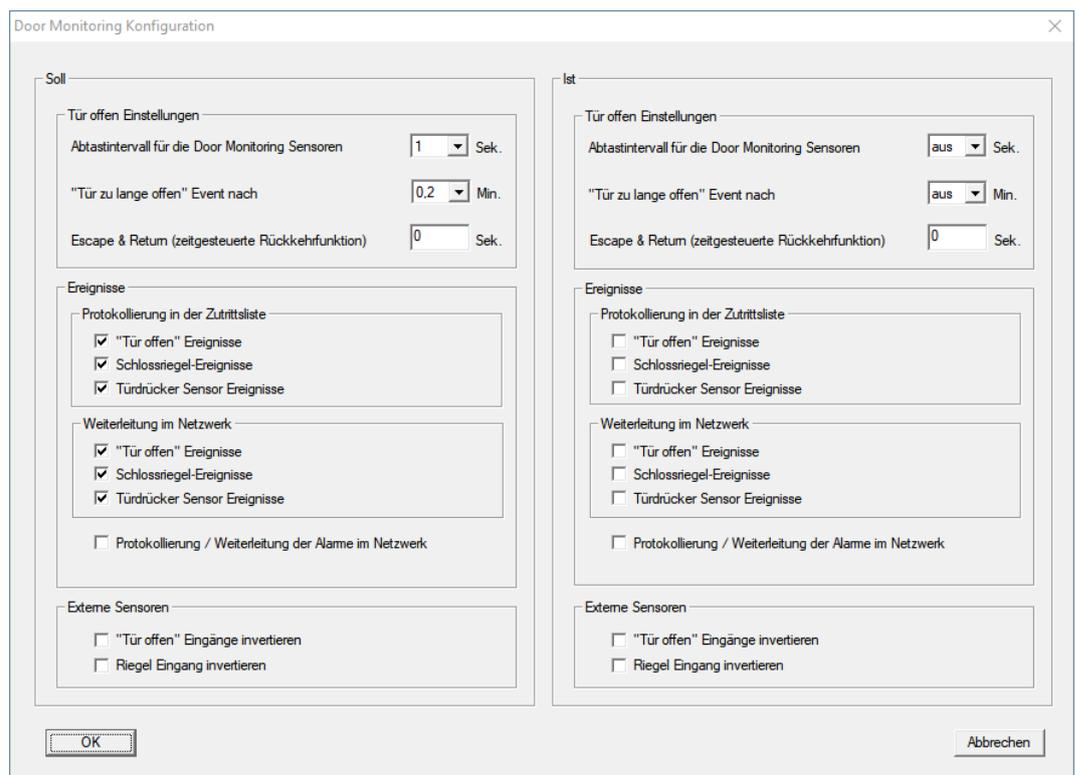


9. Aktivieren Sie die Checkbox Alle Ereignisse zum I/O-Router senden.
10. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
11. Klicken Sie auf die Schaltfläche **Speichern**.
12. Klicken Sie auf die Schaltfläche **Beenden**.
13. Klicken Sie auf die Schaltfläche **Ja**.
 - ↳ WaveNet-Manager schließt sich.
14. Importieren Sie die neuen Einstellungen und weisen Sie diese dem entsprechenden Kommunikationsknoten zu.

10.2.3 DoorMonitoring-SmartHandle

In der LSM und in Smart.Surveil können Sie Ihre DoorMonitoring-SmartHandles überwachen. Dazu müssen Sie jedoch die DoorMonitoring-SmartHandles erst in der LSM konfigurieren:

- ✓ LSM geöffnet.
 - ✓ Matrixansicht geöffnet.
1. Öffnen Sie mit einem Doppelklick auf das DM-SmartHandle die Einstellungen.
 2. Wechseln Sie zur Registerkarte [Konfiguration/Daten].
 3. Klicken Sie auf die Schaltfläche **Monitoring Konfiguration**.
 - ↳ Fenster "Door Monitoring Konfiguration" öffnet sich.



4. Aktivieren Sie im Bereich "Soll"-"Ereignisse" in den Bereichen "Protokollierung in der Zutrittsliste" und "Weiterleitung im Netzwerk" die DoorMonitoring-Ereignisse, die Sie überwachen wollen (z.B. "Tür öffnen" Ereignisse, Schlossriegel-Ereignisse und Türdrücker Sensor Ereignisse).
 5. Nehmen Sie ggfs. weitere DoorMonitoring-Einstellungen vor, z.B. im Bereich "Tür öffnen Einstellungen".
 6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Door Monitoring Konfiguration" schließt sich.
 7. Klicken Sie auf die Schaltfläche **Übernehmen**.
 8. Programmieren Sie das SmartHandle.
- ↳ DoorMonitoring-Events werden in der LSM-Datenbank gespeichert und können von der LSM und von SmartSurveil ausgewertet werden.

10.2.3.1 Sabotage-Erkennung

Ab der LSM 3.4 SP2 können Sie Sabotageversuche am SmartHandle AX und am SmartRelais 3 Advanced erkennen. Wenn das dort verwendete Gehäuse geöffnet wird, dann erkennt die Elektronik das und sendet die Information an die LSM. Wenn Sie die Information auswerten wollen, dann können Sie ein Ereignis dazu einrichten und darauf reagieren (siehe *Eventmanagement (Ereignisse) einrichten [▶ 219]*).

10.2.3.2 DoorMonitoring (SmartHandle) - Türdrücker-Events

Ab der LSM 3.5 SP3 können Sie den Zustand des Drückers am SmartHandle AX erkennen. Wenn der Drücker gedrückt ist, dann erkennt die Elektronik das und sendet die Information an die LSM. Wenn Sie die Information auswerten wollen, dann können Sie ein Ereignis dazu einrichten und darauf reagieren (siehe (*Eventmanagement (Ereignisse) einrichten [▶ 219]*)).

10.2.4 DoorMonitoring-Zylinder

In der LSM und in Smart.Surveil können Sie Ihre DoorMonitoring-Zylinder überwachen. Dazu müssen Sie jedoch die DoorMonitoring-Zylinder erst in der LSM konfigurieren:

- ✓ LSM geöffnet.
 - ✓ Matrixansicht geöffnet.
1. Öffnen Sie mit einem Doppelklick auf den DM-Zylinder die Einstellungen.
 2. Wechseln Sie zur Registerkarte [Konfiguration/Daten].
 3. Klicken Sie auf die Schaltfläche **Monitoring Konfiguration**.
 - ↳ Fenster "Door Monitoring Konfiguration" öffnet sich.

4. Aktivieren Sie im Bereich "Soll"- "Ereignisse" in den Bereichen "Protokollierung in der Zutrittsliste" und "Weiterleitung im Netzwerk" die DoorMonitoring-Ereignisse, die Sie überwachen wollen (z.B. "Tür offen" Ereignisse).
5. Nehmen Sie ggfs. weitere DoorMonitoring-Einstellungen vor, z.B. im Bereich "Tür offen Einstellungen".
6. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Door Monitoring Konfiguration" schließt sich.
7. Klicken Sie auf die Schaltfläche **Übernehmen**.
8. Programmieren Sie den Zylinder.
↳ DoorMonitoring-Events werden in der LSM-Datenbank gespeichert und können von der LSM und von SmartSurveil ausgewertet werden.

10.2.5 Controller-Inputs auswerten

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

Ereignis anlegen

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

- ✓ LSM geöffnet.
 - ✓ SREL3-ADV-System in Matrix angelegt.
1. Wählen Sie über | Netzwerk | den Eintrag Ereignismanager aus.
 - ↳ Fenster "Netzwerkereignis Manager" öffnet sich.
 2. Klicken Sie auf die Schaltfläche Neu .
 - ↳ Fenster "Neues Ereignis" öffnet sich.

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

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

Input Ereignis

Die Inputs eines Lock-Nodes sollen folgendemmaßen berücksichtigt werden:

Input auswählen

Input 1
 Input 2
 Input 3

Input ändert sich

von 0 auf 1
 von 1 auf 0
 beides

OK Abbrechen

9. Wählen Sie im Bereich "Input auswählen" den gewünschten Input aus.
 10. Wählen Sie im Bereich "Input ändert sich" die Zustandsänderung aus, die das Ereignis auslösen soll.
 11. Klicken Sie auf die Schaltfläche **OK**.
 12. Klicken Sie auf die Schaltfläche **Auswählen**, um dem Ereignis eine Schließung zuzuordnen.
 - ↳ Fenster "Verwaltung" öffnet sich.
 13. Markieren Sie eine oder mehrere Schließungen.
 14. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 15. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster schließt sich.
 - ↳ Schließung ist dem Ereignis zugeordnet.
 16. Wenn Sie eine Aktion festlegen wollen, können Sie mit der Schaltfläche **Neu** bzw. **Hinzufügen** eine Aktion zuordnen.
 17. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster schließt sich.
 - ↳ Ereignis wird im Bereich "Ereignisse" angezeigt.
 18. Klicken Sie auf die Schaltfläche **Beenden**.
 - ↳ Fenster schließt sich.
- ↳ Input ist als Ereignis angelegt und löst je nach Einstellung eine Aktion aus..

10.2.6 WaveNet-Konfiguration übertragen

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

1. Wählen Sie "Netzwerk/Kommunikationsknoten".

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

10.2.7 LockNode einer Schließung zuweisen

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

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

10.2.8 Inputereignisse der Schließung aktivieren

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

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

10.3 RingCast einrichten

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

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

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



HINWEIS

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

10.3.1 RouterNode für RingCast vorbereiten



HINWEIS

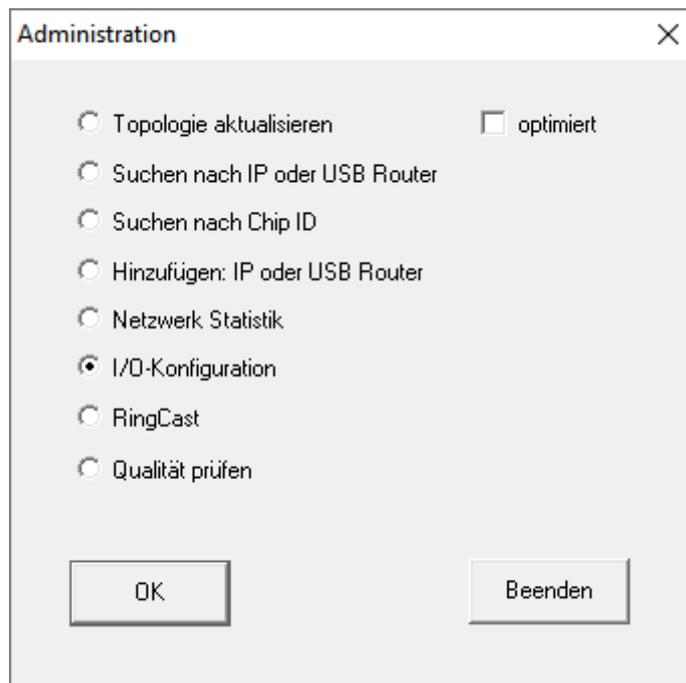
Firmwareabhängige Verfügbarkeit von RingCast für RouterNodes

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

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

Bereiten Sie die RouterNodes für den RingCast vor:

- ✓ Im Wavenet-Funknetzwerk sind mindestens zwei verschiedene ringcastfähige RouterNodes konfiguriert und "online" (siehe Firmware-Informationen).
 - ✓ Jedem RouterNode des geplanten RingCasts ist mindestens eine Schließung zugewiesen. Beide Schließungen sind "online".
1. Öffnen Sie den WaveNet-Manager.
 2. Klicken Sie mit der rechten Maustaste auf den ersten RouterNode 2.
 - ↳ Fenster "Administration" öffnet sich.



3. Wählen Sie die Option I/O-Konfiguration.
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "I/O Konfiguration" öffnet sich.
5. Optional: Wählen Sie beispielsweise für **Ausgang 1** "Input Quittung statisch", um während der Deaktivierung ein Signalgerät ansteuern zu können.
6. Wählen Sie im Dropdown-Menü **Eingang** des gewünschten Eingangs den Eintrag der entsprechenden Reaktion aus (siehe RouterNode: Digitaler Eingang).
7. Wählen Sie im Dropdown-Menü **Verzögerung [s]** den Eintrag "Ring-Cast" aus.
8. Klicken Sie auf die Schaltfläche **LN auswählen**.
9. Prüfen Sie, ob alle gewünschten LockNodes ausgewählt sind. *(Beim erstmaligen Einrichten der I/O-Konfiguration des Routers werden alle LockNodes mit einbezogen.)*
10. Wählen Sie im Dropdown-Menü **Protokollgeneration** Ihre Protokollgeneration.



HINWEIS

Protokollgeneration in der LSM

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

11. Geben Sie das Schließanlagenpasswort ein.

12. Klicken Sie auf die Schaltfläche **OK**.
13. Nehmen Sie die selben Einstellungen auch an den weiteren RouterNodes 2 vor.

10.3.2 RingCast anlegen

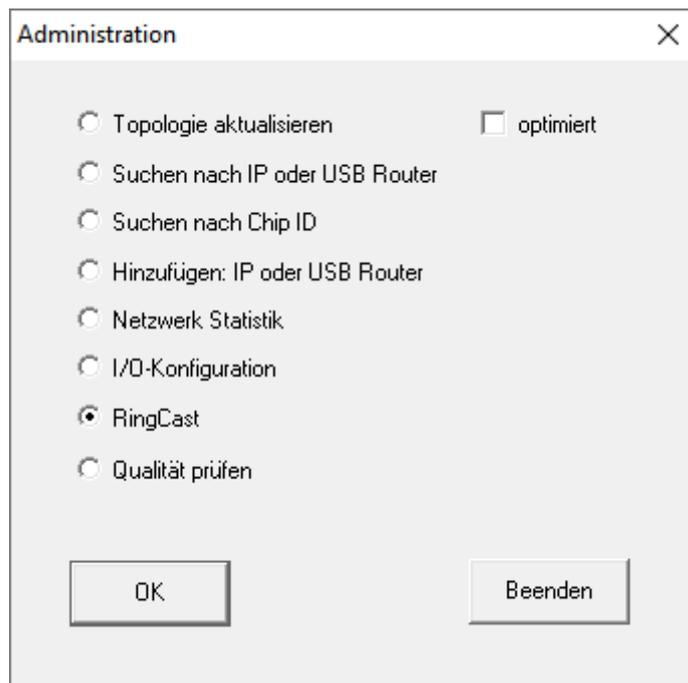


HINWEIS

Neuberechnung des RingCasts

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

- ✓ WaveNet-Manager über LSM geöffnet (siehe Best Practice: Aus der LSM-Software).
 - ✓ RouterNodes und LockNodes an Stromversorgung angeschlossen.
 - ✓ RouterNodes und LockNodes in WaveNet-Topologie importiert (siehe Geräte finden und hinzufügen).
 - ✓ RouterNodes für RingCast vorbereitet (siehe *RouterNode für RingCast vorbereiten* [▶ 210]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet XX_X.
↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option RingCast.
3. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Administration" schließt sich.

↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne : neu [v]

Name : [] [Löschen]

Input : 1 [v]

Output Router : [] [Löschen] [Status]

Aktualisieren

ausgewählte Router : []

freie Router : []

[Speichern] [Beenden]

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

Input1 [v]

Input1

neu

[Löschen]

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

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

Aktualisieren

ausgewählte Router :

- RN_ER (0x0006_0x0021; 89003644)
- RN_ER (0x000E_0x0041; 0002A8B2)

freie Router :

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

WaveNetManager [X]

Es wurden Änderungen vorgenommen. Möchten Sie die Funkdomänen aktualisieren ?

7. Klicken Sie auf die Schaltfläche **Ja**.
 - ↳ Fenster "WaveNetManager" schließt sich.
 - ↳ Änderungen werden aktualisiert.
- ↳ Der RingCast wird angelegt und ist nach kurzer Zeit im WaveNet-Manager sichtbar.

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

Speichern Sie die neuen Einstellungen und beenden Sie den WaveNet-Manager.

10.3.3 RingCast-Funktionstest

Der RingCast hat keine Selbstprüffunktion.



WARNUNG

Beeinträchtigung oder Ausfall von Schutzfunktionen durch geänderte Bedingungen

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

1. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest* [[▶ 215](#)]).
2. Beachten Sie ggfs. auch weitere Richtlinien bzw. Verordnungen, die für Ihre Schließanlage relevant sind (insbesondere für Flucht- und Rettungswege sowie Brandschutz. Sie stellen die Erfüllung dieser Richtlinien und Verordnungen in Eigenverantwortung sicher.).

Veränderung des Ablaufs von Notfallfunktionen durch Fehlfunktionen

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

1. Testen Sie Ihre Geräte mindestens einmal pro Monat (siehe Geräte-Funktionstest. Nach anderen Vorschriften bezüglich Ihres Gesamtsystems können auch kürzere Abstände erforderlich sein).
2. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest* [▶ 215]).

Schalten Sie am Initiator den entsprechenden Eingang und überprüfen Sie:

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

Test mit zentralem Output-Router



HINWEIS

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

Der zentrale Output-Router erhält die Inputquittung der beteiligten RouterNodes ausschließlich über eine Ethernetverbindung. Der zentrale Output-Router ignoriert deshalb den Status von RouterNodes, die keine Ethernet-RouterNodes (.ER) sind. Wenn Sie den zentralen Output-Router verwenden und Ihr RingCast auch RouterNodes ohne Ethernetschnittstelle enthält, dann bedeutet die Inputquittung des zentralen Output-Routers nur, dass alle Schließungen, die einem Ethernet-RouterNode zugewiesen sind, den Befehl empfangen haben.

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

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

- ✓ WaveNet-Manager über LSM geöffnet (siehe Best Practice: Aus der LSM-Software).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RingCasts, den Sie testen wollen.
- 2. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** den Input aus, dessen RingCast Sie testen wollen.
 - ↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne : Input1

Name : Input1 [Löschen]

Input : 1

Output Router : 0xAA48 [Löschen] [Status]

Aktualisieren

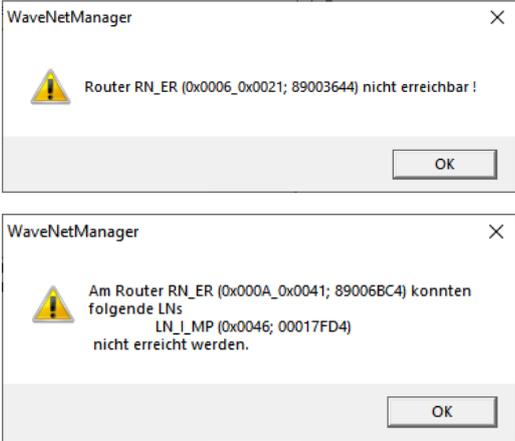
ausgewählte Router :

- RN_ER (0x0006_0x0021; 89003644)
- RN_ER (0x000E_0x0041; 000248B2)

freie Router :

[Speichern] [Beenden]

- 3. Klicken Sie auf die Schaltfläche **Status**.
 - ↳ RingCast wird getestet.

	
<p>Der RingCast konnte alle Schließungen ansprechen.</p>	<p>Der RingCast konnte nicht abgeschlossen werden. Mögliche Ursachen (siehe auch Zentraler Output-Router):</p> <ul style="list-style-type: none">■ Ein oder mehrere RouterNodes haben das Datenpaket nicht empfangen.■ Ein oder mehrere RouterNodes haben einen oder mehrere LockNodes nicht erreicht.■ Ethernetverbindung zu einem oder mehreren RouterNodes ist unterbrochen. Die RouterNodes könnten das Datenpaket zwar kabellos empfangen haben, aber ihre Inputquittungen wegen der unterbrochenen Ethernetverbindung nicht mehr zurückmelden. <ol style="list-style-type: none">1. Prüfen Sie die Erreichbarkeit der genannten RouterNodes (siehe RouterNodes und Erreichbarkeit testen (LSM)).2. Prüfen Sie die Erreichbarkeit der LockNodes (siehe LockNodes und Erreichbarkeit testen (LSM)).3. Prüfen Sie die letzten Reaktionen der LockNodes (siehe IO-Status und LockNode-Reaktionsfähigkeit).

10.4 Eventmanagement (Ereignisse) einrichten

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

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

Für diese Anforderung müssen zunächst folgende Voraussetzungen erfüllt sein:

- Ein WaveNet-Funknetzwerk ist wie im Beispiel *Erstellen eines WaveNet-Funknetzwerks und Einbindung einer Schließung* [▶ 197] eingerichtet.
- Außerdem wurde das Weiterleiten von Ereignissen an der Schließung wie im Schritt *Inputereignisse der Schließung aktivieren* [▶ 209] aktiviert.

10.4.1 E-Mail-Server einrichten

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

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

10.4.2 Taskdienst einstellen

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

10.4.3 Inputereignisse über den RouterNode2 weiterleiten

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

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

- Bestätigen Sie über die Schaltfläche "OK" und beenden Sie den Wave-Net-Manager.

10.4.4 Inputereignisse über das SREL3-ADV-System weiterleiten

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

10.4.4.1 Controller-Inputs auswerten

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

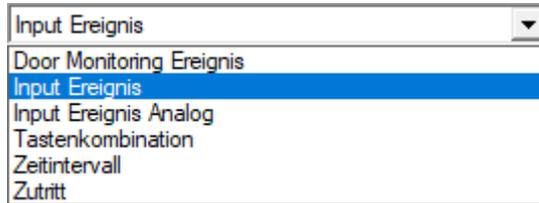
Ereignis anlegen

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

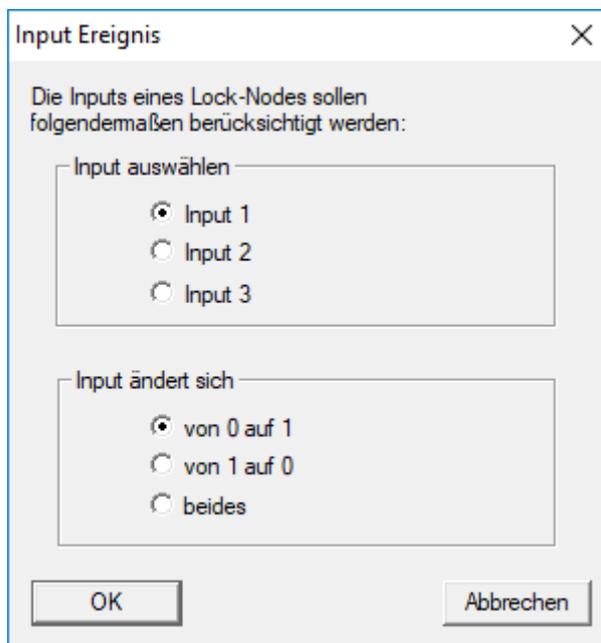
- ✓ LSM geöffnet.
 - ✓ SREL3-ADV-System in Matrix angelegt.
- Wählen Sie über | Netzwerk | den Eintrag **Ereignismanager** aus.
 - ↳ Fenster "Netzwerkereignis Manager" öffnet sich.
 - Klicken Sie auf die Schaltfläche **Neu**.
 - ↳ Fenster "Neues Ereignis" öffnet sich.

- Geben Sie einen Namen für das Ereignis ein.
- Geben Sie optional eine Beschreibung für das Ereignis ein.
- Geben Sie optional eine Meldung ein.

6. Öffnen Sie das Dropdown-Menü ▼ Typ:.
7. Wählen Sie den Eintrag "Input Ereignis" aus.



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



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

17. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster schließt sich.
 - ↳ Ereignis wird im Bereich "Ereignisse" angezeigt.
 18. Klicken Sie auf die Schaltfläche **Beenden**.
 - ↳ Fenster schließt sich.
- ↳ Input ist als Ereignis angelegt und löst je nach Einstellung eine Aktion aus..

10.4.5 Reaktion erstellen

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

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

10.4.6 Ereignis erstellen

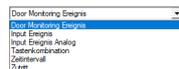
Wenn bereits eine Reaktion erstellt wurde, kann als nächstes ein Ereignis erstellt werden.

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

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

10.4.6.1 Mögliche Ereignisse

Im Fenster "Neues Ereignis" stehen Ihnen im Dropdown-Menü ▼ Typ: verschiedene Ereignisse zur Verfügung.



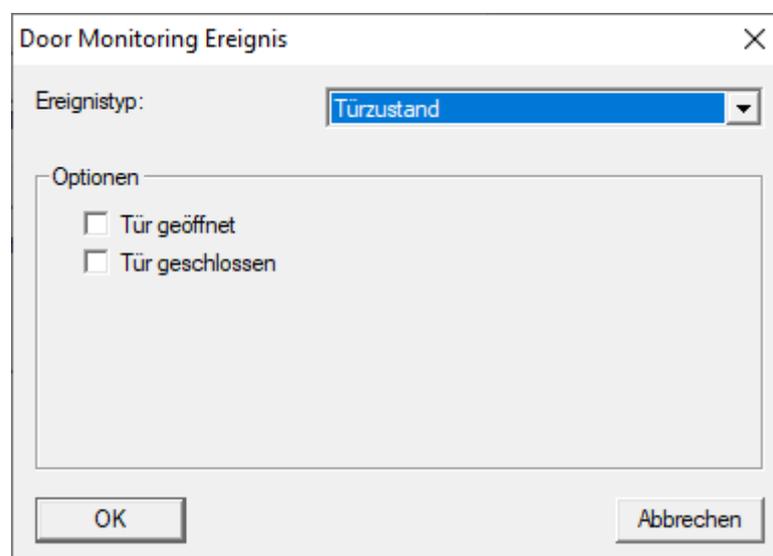
Für DoorMonitoring-Ereignisse benötigen Sie eine DoorMonitoring-fähige Schließung (DM).

DoorMonitoring-Ereignisse

Ihnen stehen folgende DoorMonitoring-Ereignisse zur Verfügung:



Türzustand

A screenshot of the 'Door Monitoring Ereignis' dialog box. The title bar reads 'Door Monitoring Ereignis'. Inside the dialog, there is a dropdown menu labeled 'Ereignistyp:' with 'Türzustand' selected. Below this is a section titled 'Optionen' containing two checkboxes: 'Tür geöffnet' and 'Tür geschlossen', both of which are currently unchecked. At the bottom of the dialog, there are two buttons: 'OK' and 'Abbrechen'.

Folgende Zustände können erkannt werden. Ein Häkchen löst das Ereignis aus, sobald der Zustand eintritt:

- Tür geöffnet
- Tür geschlossen

Schlossriegelbewegung

Door Monitoring Ereignis

Ereignistyp: Schlossriegelbewegung

Optionen

- Tür nicht verschlossen
- Tür verschlossen
- Tür sicher verriegelt

OK Abbrechen

Folgende Zustände können erkannt werden. Ein Häkchen löst das Ereignis aus, sobald der Zustand eintritt:

- Tür nicht verschlossen
- Tür verschlossen
- Tür sicher verriegelt

Tür steht zu lange offen

Door Monitoring Ereignis

Ereignistyp: Tür steht zu lange offen

Optionen

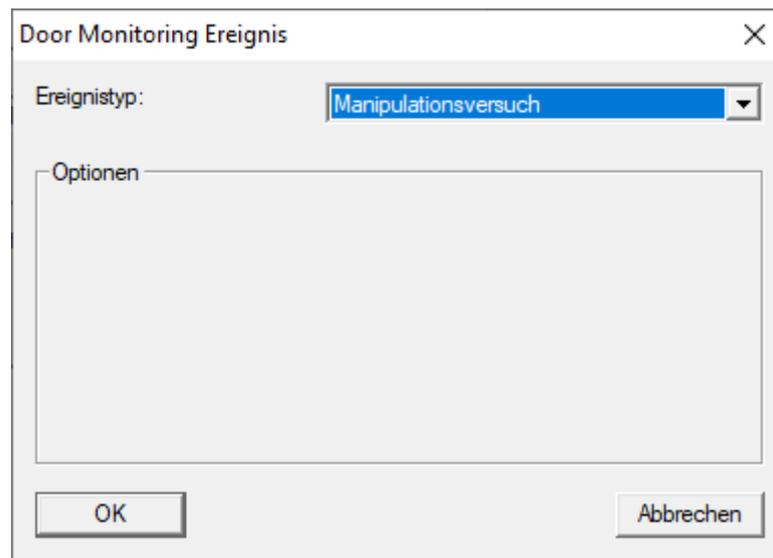
- Tür zu lange offen
- Tür wieder geschlossen

OK Abbrechen

Folgende Zustände können erkannt werden. Ein Häkchen löst das Ereignis aus, sobald der Zustand eintritt:

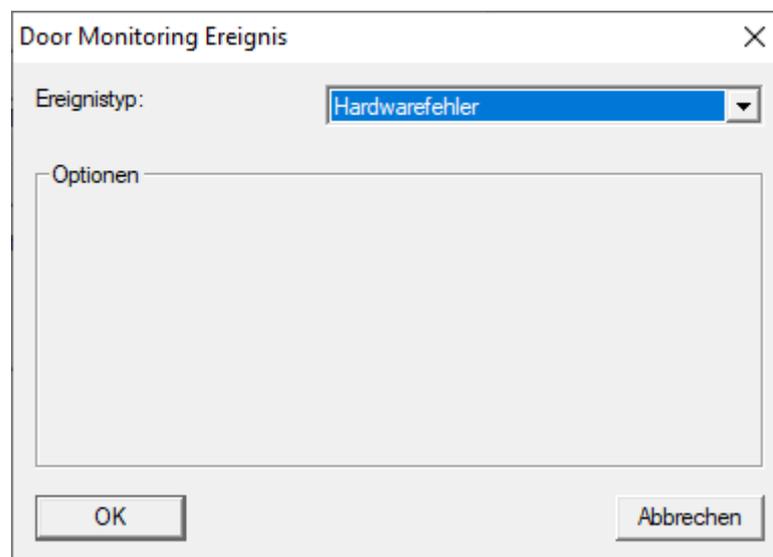
- Tür zu lange offen
- Tür wieder geschlossen

Manipulationsversuch



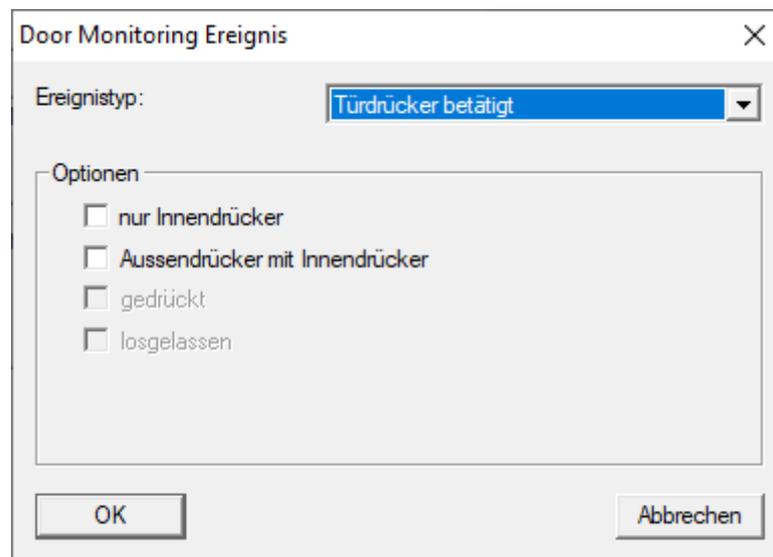
The screenshot shows a dialog box titled "Door Monitoring Ereignis" with a close button (X) in the top right corner. Below the title bar, there is a label "Ereignistyp:" followed by a dropdown menu that has "Manipulationsversuch" selected. Below this is a large, empty rectangular area labeled "Optionen". At the bottom of the dialog, there are two buttons: "OK" on the left and "Abbrechen" on the right.

Hardwarefehler



The screenshot shows a dialog box titled "Door Monitoring Ereignis" with a close button (X) in the top right corner. Below the title bar, there is a label "Ereignistyp:" followed by a dropdown menu that has "Hardwarefehler" selected. Below this is a large, empty rectangular area labeled "Optionen". At the bottom of the dialog, there are two buttons: "OK" on the left and "Abbrechen" on the right.

Türdrücker betätigt

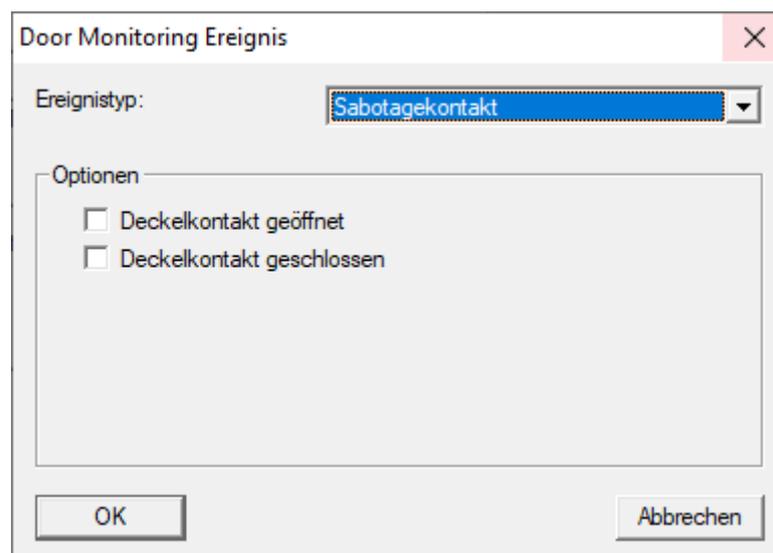


The screenshot shows a dialog box titled 'Door Monitoring Ereignis'. The 'Ereignistyp:' dropdown menu is set to 'Türdrücker betätigt'. Below it, the 'Optionen' section contains four unchecked checkboxes: 'nur Innendrücker', 'Aussendrücker mit Innendrücker', 'gedrückt', and 'losgelassen'. At the bottom, there are 'OK' and 'Abbrechen' buttons.

Folgende Zustände können erkannt werden. Ein Häkchen löst das Ereignis aus, sobald der Zustand eintritt:

- nur Innendrücker
- Aussendrücker mit Innendrücker
- gedrückt
- losgelassen

Sabotagekontakt



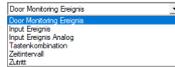
The screenshot shows a dialog box titled 'Door Monitoring Ereignis'. The 'Ereignistyp:' dropdown menu is set to 'Sabotagekontakt'. Below it, the 'Optionen' section contains two unchecked checkboxes: 'Deckelkontakt geöffnet' and 'Deckelkontakt geschlossen'. At the bottom, there are 'OK' and 'Abbrechen' buttons.

Folgende Zustände können erkannt werden. Ein Häkchen löst das Ereignis aus, sobald der Zustand eintritt:

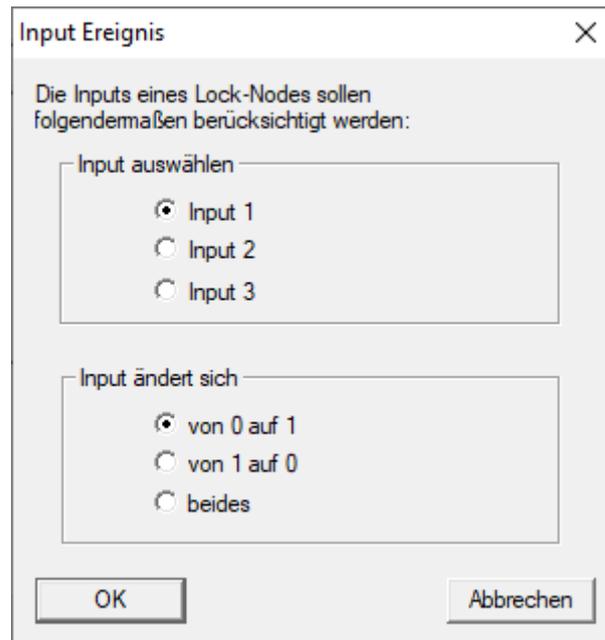
- Deckelkontakt geöffnet
- Deckelkontakt geschlossen

Standard-Ereignisse

Ihnen stehen folgende Standard-Ereignisse zur Verfügung:



Input Ereignis



Input Ereignis

Die Inputs eines Lock-Nodes sollen folgendermaßen berücksichtigt werden:

Input auswählen

- Input 1
- Input 2
- Input 3

Input ändert sich

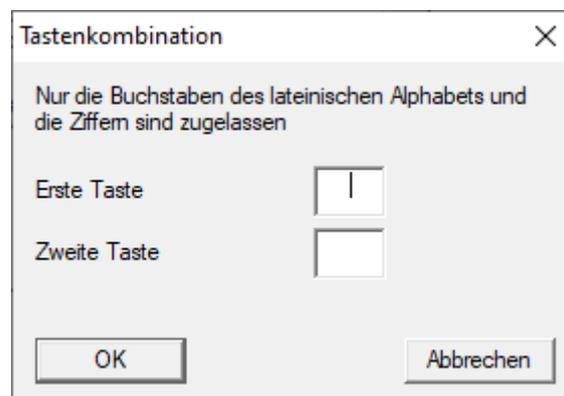
- von 0 auf 1
- von 1 auf 0
- beides

OK Abbrechen

Input Ereignis Analog

Die Einstellungen für analoge Inputereignisse werden direkt am jeweiligen Gerät (z.B. RouterNode 2) vorgenommen.

Tastenkombination



Tastenkombination

Nur die Buchstaben des lateinischen Alphabets und die Ziffern sind zugelassen

Erste Taste

Zweite Taste

OK Abbrechen

Zeitintervall

Zeitintervallereignis

Nach der Überschreitung des folgenden Zeitintervalls wird das Ereignis aktiviert

Zeitintervall Min.

OK Abbrechen

Zutritt

Zutrittseignis

Auf alle Transponder reagieren

Nur auf den folgenden Transponder reagieren:

Schließanlage:

Zeiteinstellung

Realtime Ereignis. Nur mit direktvernetzter G2 Schließung möglich

Alle Begehungen berücksichtigen

Stunde(n)

Begehungen, die mehr als die vorgegebene Zeit zurückliegen, nicht berücksichtigen

OK Abbrechen

10.5 Virtuelles Netzwerk (VN) verwalten

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

In diesem 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).

10.5.1 Virtuelles Netzwerk mit SmartRelais 3 Advanced



HINWEIS

Erhöhte Systemanforderungen für virtuelle Netzwerke mit SmartRelais 3 Advanced

Das virtuelle Netzwerk mit VNHost-Server und SmartRelais 3 Advanced ist sehr leistungsfähig und stellt höhere Anforderungen an die zur Verfügung stehende Leistung.

- Beachten Sie die erhöhten Systemanforderungen (siehe *Systemanforderungen* [▶ 8]).

10.5.1.1 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* [▶ 234]).

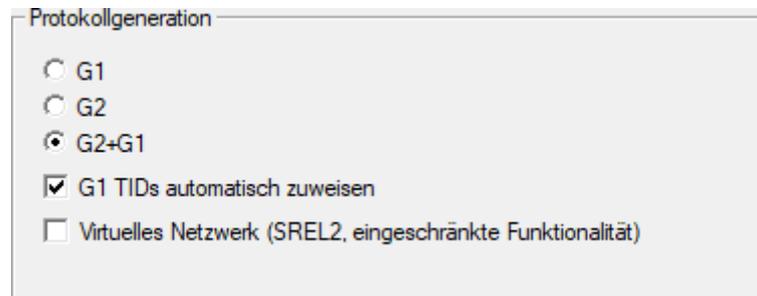
10.5.1.2 Schließenanlage einrichten

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

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

1. Öffnen Sie über | Bearbeiten | - **Eigenschaften: Schließenanlage** die Eigenschaften Ihrer Schließenanlage.
2. Wechseln Sie zur Registerkarte [Name].

3. Stellen Sie sicher, dass die Checkbox Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) nicht aktiviert ist.



Protokollgeneration

G1

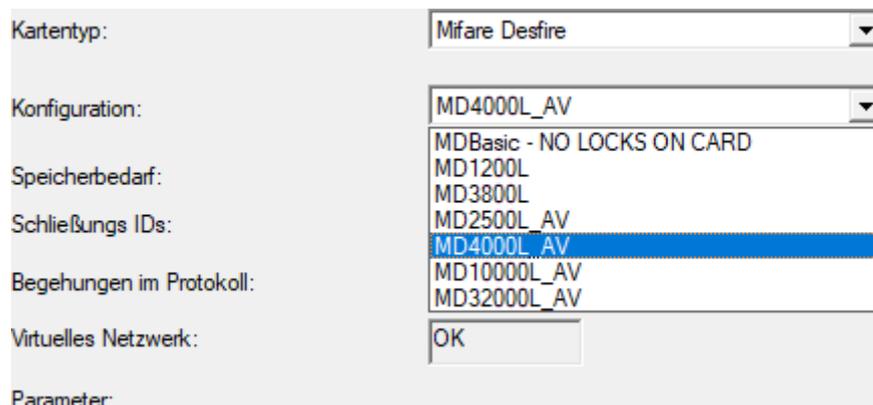
G2

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:

- MDBasic - NO LOCKS ON CARD
- MD1200L
- MD3800L
- MD2500L_AV
- MD4000L_AV
- MD10000L_AV
- MD32000L_AV

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

10.5.1.3 Gateway und VNHost-Server einrichten

- ✓ Schließenanlage erstellt (siehe *Schließenanlage einrichten* [▶ 229]).
- ✓ SmartRelais 3 Advanced konfiguriert und vernetzt (siehe Systemhandbuch zum SmartRelais 3 Advanced).
- ✓ VNHost installiert (siehe *VNHost* [▶ 22]).

1. Öffnen Sie über | Bearbeiten | - **Eigenschaften: Schließung** die Eigenschaften des SmartRelais 3 Advanced (Alternative: Doppelklick).

2. Wechseln Sie zur Registerkarte [Konfiguration/Daten].

Soll

Schließenanlagen ID
9215

Schließungs ID
173

Pulslänge 2 Sek.

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

letzte Veränderung

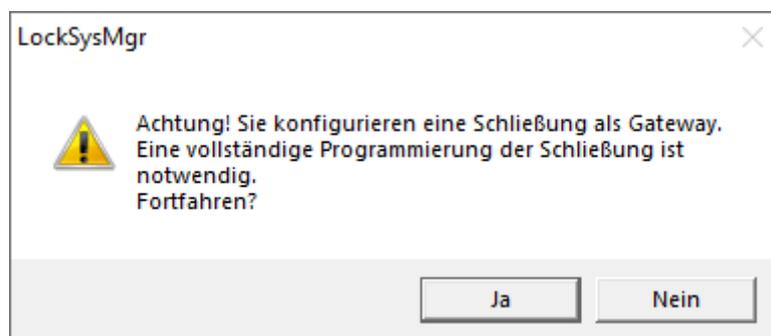
Zeitzone:	21.06.18 17:30:10
Feiertagslisten:	nicht vorhanden

Erweiterte Konfiguration

3. Aktivieren Sie die Checkboxen Zeitzonesteuerung und Zugangskontrolle.

4. Aktivieren Sie die Checkbox Gateway.

↳ Warnung über anstehende Programmierung öffnet sich.



5. Klicken Sie auf die Schaltfläche **OK**.

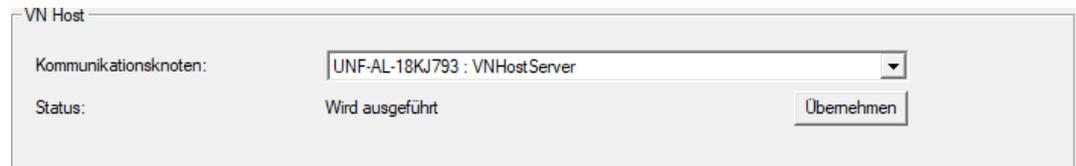
↳ Warnung schließt sich.

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.



VN Host

Kommunikationsknoten: UNF-AL-18KJ793 : VNHostServer

Status: Wird ausgeführt

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**.

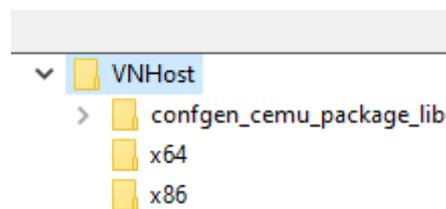
14. Wechseln Sie mit den Schaltflächen ◀ und ▶ zum VNHostServer-Kommunikationsknoten.

Typ	COM-Port

15. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.

↳ Explorer-Fenster öffnet sich.

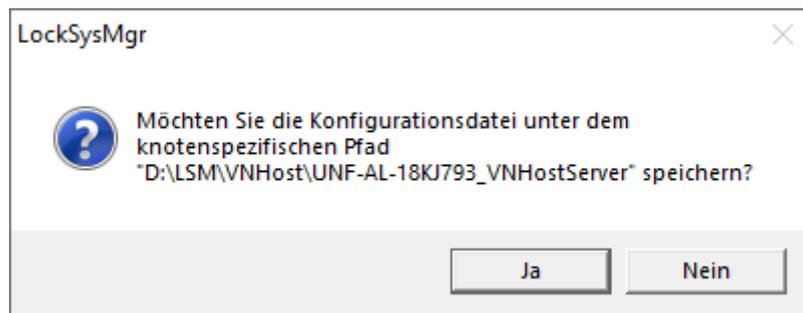
16. Markieren Sie den Installationsordner des VNHost-Servers.



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* [▶ 234]).

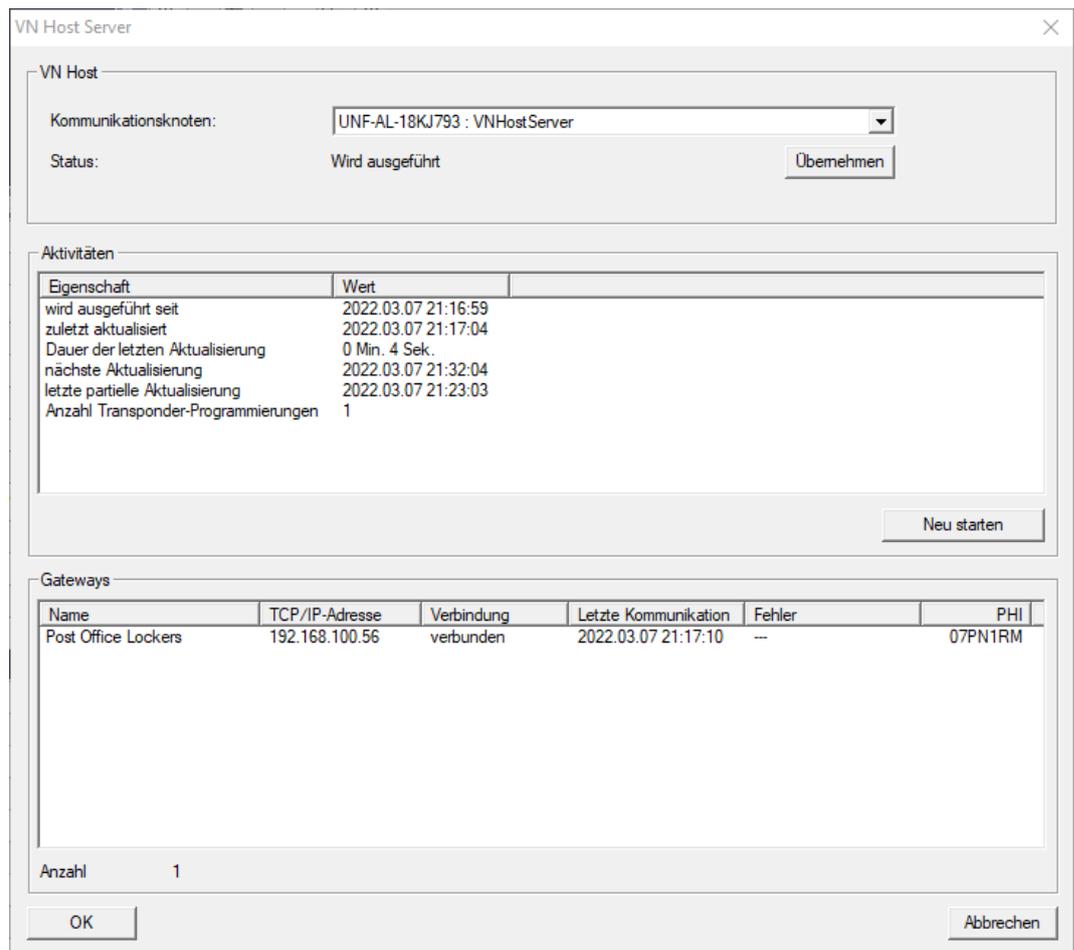
10.5.1.4 Status des virtuellen Netzwerks prüfen

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

✓ Virtuelles Netzwerk eingerichtet (siehe *Schließenanlage einrichten* [▶ 229] und *Gateway und VNHost-Server einrichten* [▶ 230]).

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

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



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.

10.5.2 Virtuelles Netzwerk mit SmartRelais 2 G2

10.5.2.1 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* [▶ 241]).

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.

10.5.2.2 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

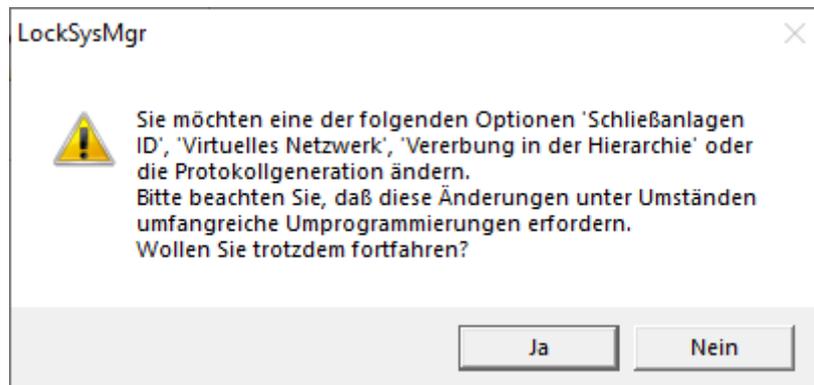
Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität)

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

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



10.5.2.3 VN Dienst einrichten

- ✓ Schließanlage eingerichtet (siehe *Neue Schließanlage anlegen* [▶ 136], *Neuen Transponder anlegen* [▶ 136] und *Neue Schließung anlegen* [▶ 197]).
- ✓ Checkbox Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität) aktiviert.
- ✓ Alle Komponenten programmiert (siehe *Transponder programmieren* [▶ 153] und *Schließung programmieren* [▶ 198]).
- ✓ 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:

TCP/IP Port:

VNServer Installationspfad:

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

OK Abbrechen

2. 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:

TCP/IP Port:

VNServer Installationspfad:

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

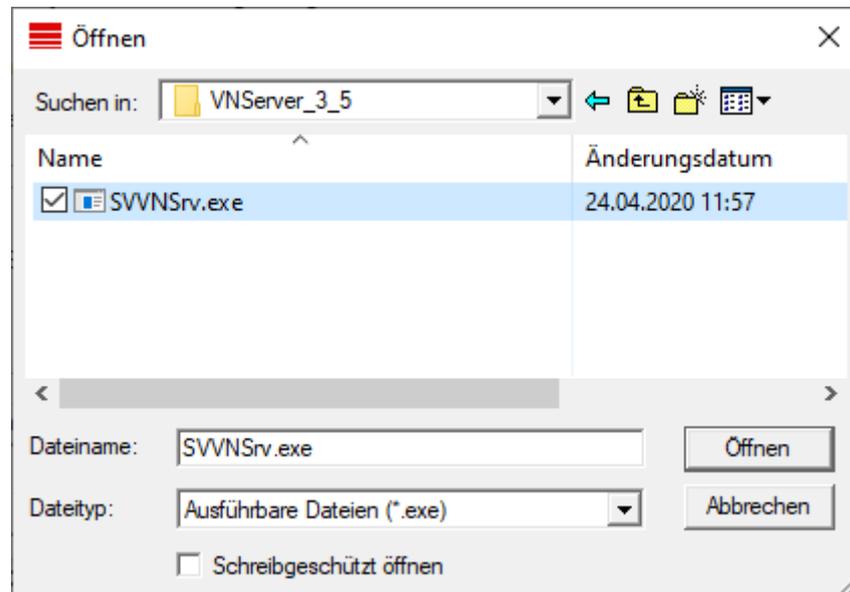
Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

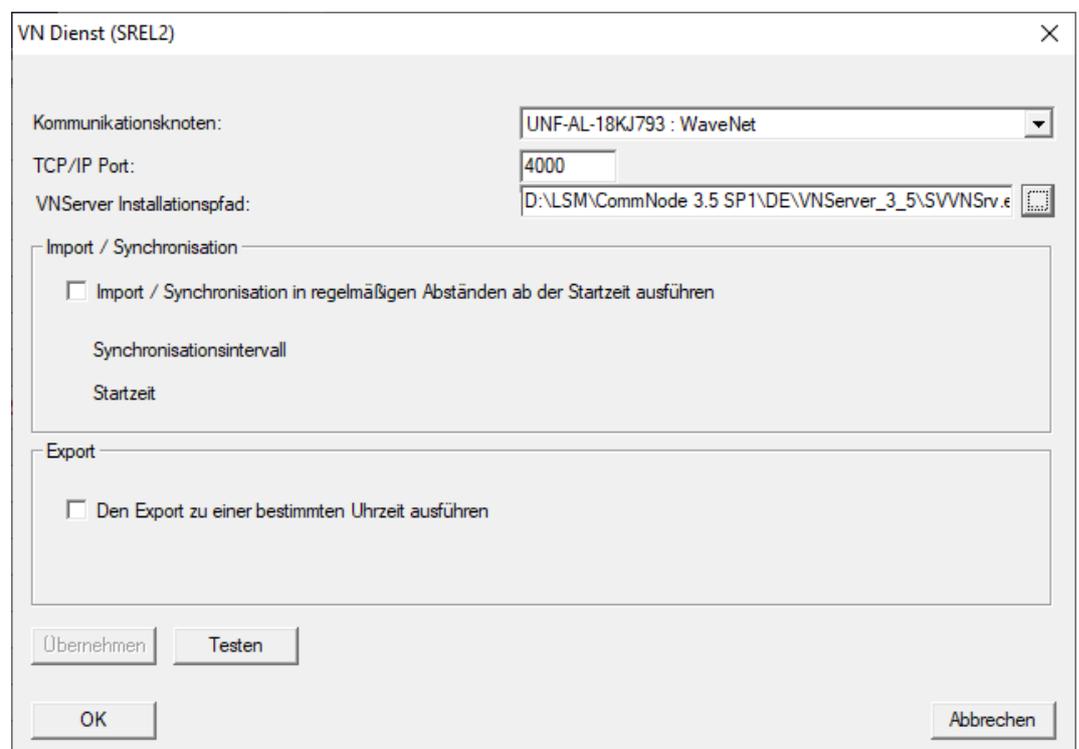
OK Abbrechen

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

5. Wählen Sie die SVVNSvr.exe aus.
*Die SVVNSvr.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.



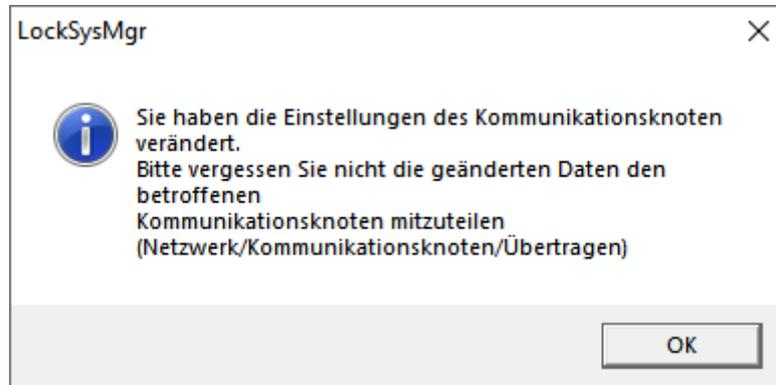
7. Optional: Stellen Sie im Bereich "Import / Synchronisation" ein, wann die Daten vom SmartRelais 2 G2 automatisch wieder in die LSM importiert werden sollen.

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, with the checkbox 'Den Export zu einer bestimmten Uhrzeit ausführen' unchecked. Buttons for 'Übernehmen', 'Testen', 'OK', and 'Abbrechen' are visible at the bottom.

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, with the checkbox 'Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen' unchecked. The 'Synchronisationsintervall' is set to 1 hour, and the 'Startzeit' is set to 20:00. Buttons for 'Übernehmen', 'Testen', 'OK', and 'Abbrechen' are visible at the bottom.

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* [▶ 208]).

10.5.2.4 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* [▶ 197]
- *Hardware vorbereiten* [▶ 198]
- *Kommunikationsknoten erstellen* [▶ 199]
- *Taskdienst einstellen* [▶ 219]

1. Legen Sie verschiedene Identmedien (z.B. *Neuen Transponder anlegen* [▶ 136]) und Schließungen (z.B. *Neue Schließung anlegen* [▶ 197]) an.
2. Führen Sie eine Erstprogrammierung der angelegten Komponenten durch (*Transponder programmieren* [▶ 153] und *Schließung programmieren* [▶ 198]).
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

Schließenanlagen 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 Zeitzonenmanagement 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* [▶ 200]).
12. Weisen Sie diesem das Gateway (bzw. das SmartRelais 2 G2) zu.
↳ Virtuelles Netzwerk ist einsatzbereit.

10.5.2.5 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* [▶ 249]).
2. Wählen Sie über | Programmierung | - **Virtuelles Netzwerk (SREL2)** den Eintrag **Export auf VNetzwerk**.
↳ Fenster "Export auf Virtuelles Netzwerk (SREL2)" öffnet sich.

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 input fields for "VN Befehl:" (value: "VN Export"), "Ausgegeben am:" (value: "2022.03.07 16:32:07"), and "Zustand/Ergebnis:" (value: "wird bearbeitet"). To the right is a "Stoppen" button and a small network diagram icon.
- Middle Section:** Contains input fields for "Gateway", "Letzte Meldung" (value: "2022.03.07 16:32:09"), "Aktuelle Aktion 1" (value: "Gateways aktualisieren"), and "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 input fields for "VN Befehl:", "Ausgegeben am:", "Zustand/Ergebnis:", and "Letzte Meldung am:". To the right is a "Wechseln" button.
- Bottom Right:** A "Beenden" button.

- ↳ Zusammenfassung des Exports wird angezeigt.

VN Ergebnis ✕

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

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

Die exportierten Aufgaben können Sie jetzt in der Übersicht nachverfolgen (*Status der Aufgaben im virtuellen Netzwerk (SREL2.G2)* [▶ 248]).

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 Überehmen 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].

Soll-Zustand

Langes Öffnen
 Kein akustisches Öffnungssignal
 Begehungsliste

Dynamisches Zeitfenster

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

Aktivierungsdatum
 ab sofort

Verfallsdatum
 ohne Verfallsdatum

Zeitzonegruppe

G1:
 G2:

2. Klicken Sie auf die Schaltfläche **TIDs zum Deaktivieren**.

↳ Liste öffnet sich.

TIDs zum Deaktivieren

Schließanlage:

G2 TIDs G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

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

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

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

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.

10.5.2.6 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 [▶ 242]*).

1. Öffnen Sie über | Programmierung | - **Virtuelles Netzwerk (SREL2)** den Eintrag **Exportierte VN Aufgaben**.

↳ Fenster "Exportierte VN Aufgaben" öffnet sich.

The screenshot shows a window titled "Exportierte VN Aufgaben" with a close button (X) in the top right corner. The window contains two tables and a status selection menu.

Table 1: Aufgaben

Benutzer	Exportdatum	Ausführen von	Ausführen bis	Gateway
Admin	2022.03.05 00:32	2022.03.05 00:32	2022.03.05 00:32	Post Office Illumination/00CP17B

Table 2: Task Details

Schließanlage	Schließung	Transponder	G1/G2	Aktion	Status	Beauftragt	Transporttyp

Status auswählen

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

Buttons: **Befehle in Bearbeitung** and **Beenden**

VNServer Meldungen ✕

VN Befehl:	<input type="text" value="Reset VN Aufgaben"/>	<input type="button" value="Stoppen"/>
Ausgegeben am:	<input type="text" value="2022.03.07 16:20:33"/>	
Zustand/Ergebnis:	<input type="text" value="wird bearbeitet"/>	
Gateway	<input type="text"/>	
Letzte Meldung	<input type="text" value="2022.03.07 16:20:41"/>	
Aktuelle Aktion 1	<input type="text" value="Gateways aktualisieren"/>	
	<input type="text"/>	
Aktuelle Aktion 2	<input type="text"/>	

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

Sonstige Aktivitäten

VN Befehl:	<input type="text"/>	<input type="button" value="Wechseln"/>
Ausgegeben am:	<input type="text"/>	
Zustand/Ergebnis:	<input type="text"/>	
Letzte Meldung am:	<input type="text"/>	

↳ Exportierte Aufgaben sind zurückgesetzt.

VNServer Meldungen ✕

VN Befehl: Stoppen

Ausgegeben am:

Zustand/Ergebnis: 

Gateway:

Letzte Meldung:

Aktuelle Aktion 1:

Aktuelle Aktion 2:

Name	Ergebnis
Post Office Illumination / 00CP17B	

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

↳ 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...				
Aufgaben für Transponder vorbereitet	2022.03.07 16:4...	Insgesamt		Ausgeführt	
Vorverarbeitung beendet	2022.03.07 16:4...				
Aktualisierung Gateways abgeschlossen	2022.03.07 16:4...	Insgesamt	1	Fehlerhaft	0
Datenblock erfolgreich übertragen	2022.03.07 16:4...	phi	7859...	phi extension	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)* [▶ 248]).

10.5.2.9 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.

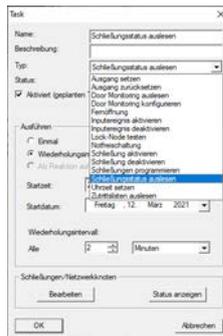
Dynamisches Zeitfenster für Transponder G2

- 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)** .

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:

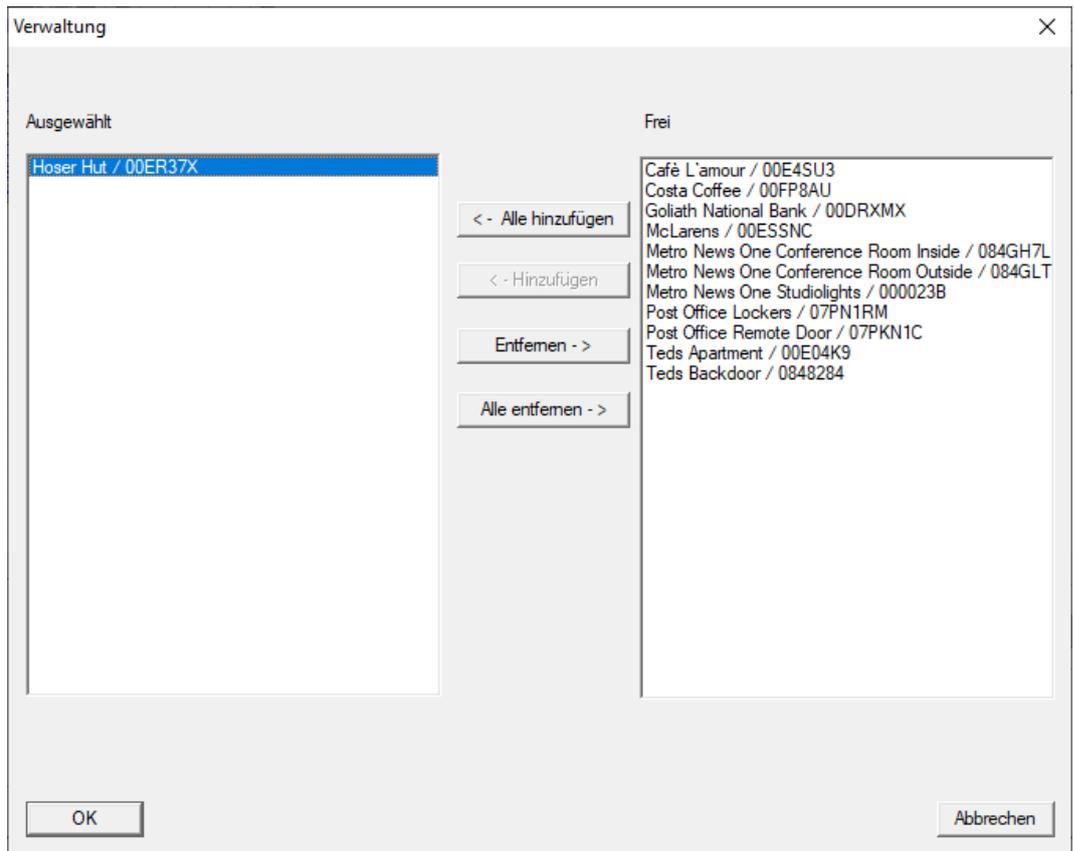
Alle 2 Minuten

Schließungen/Netzwerkknoten

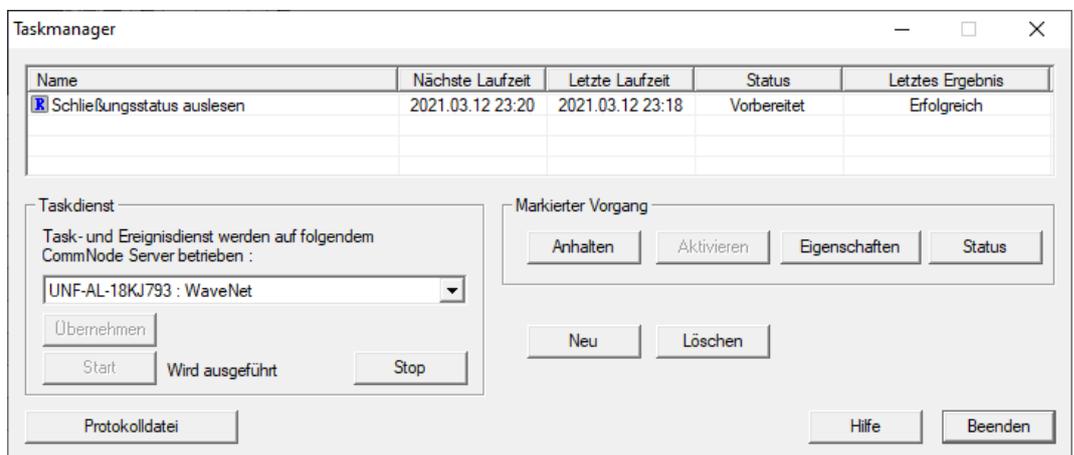
Bearbeiten Status anzeigen

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  .
 - ↳ Fenster "Verwaltung" schließt sich.
11. Klicken Sie auf die Schaltfläche  .
 - ↳ 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.

Task- und Ereignisdienst werden auf folgendem
CommNode Server betrieben :

UNF-AL-18KJ793 : WaveNet ▼

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

Start Wird ausgeführt Stop

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

11. Glossar & Abkürzungen

Im Folgenden werden einzelne Begriffe näher erklärt. Die Erklärungen sind leicht verständlich und spiegeln möglicherweise nicht alle Einzelheiten wieder.

Begriff	Abkürzung	Erklärung
Advantage Database Server	ADS-Server	Essentieller Server-Dienst, der für den Betrieb von LSM BUSINESS und PROFESSIONAL notwendig ist.
CSV-Datei		Gängiges Dateiformat für den Import und Export von Werten, wie beispielsweise Personallisten, Schließanlagen, etc..
DoorMonitoring	DM	Option von Schließkomponenten, welche wichtige Türzustandseigenschaften (z.B. Tür geschlossen und zweifach verriegelt) an die LSM-Software meldet.
Freeze-Modus		Bei kritischem Batteriestand wechseln Schließungen in den Freeze-Modus, um noch eine letzte Türöffnung zu ermöglichen.
Protokollgeneration G1	G1	Erste Protokollgeneration, in der Schließungen und Identmedien kommunizieren.
Protokollgeneration G2	G2	Zweite Protokollgeneration, welche mehrere Komfortfunktionen mit sich bringt.
Lightweight Directory Access Protocol	LDAP	Netzwerkprotokoll zur Abfrage und Änderung von Informationen. In der LSM-Software können beispielsweise Personaldaten direkt über LDAP geladen werden.
Locking Data Base Software	LDB	Die Vorgängerversion der LSM-Software.
Lock-ID	LID	Kennzeichnet die Schließung innerhalb der Schließanlage. (Vergleichbar mit einem Autokennzeichen.)

Begriff	Abkürzung	Erklärung
Local Operating Network	LON-Netzwerk	Local Operating Network (LON) ist ein älterer Standard, der vorwiegend in der Gebäudeautomatisierung eingesetzt wird/wurde.
Locking System Management	LSM	Aktuelle Software, welche eine flexible Verwaltung von SimonsVoss-Schließkomponenten ermöglicht.
Matrix		Die Matrix zeigt übersichtlich, welche Identmedien an welchen Schließungen berechtigt sind.
MIFARE		MIFARE beschreibt einen weltweiten Standard für eines der am meisten genutzten Kartensysteme. (Schließung wird über "passive Karten" betätigt)
Personal Digital Assistant	PDA	Kleiner Computer mit den ungefähren Abmessungen eines Smartphones. Mithilfe eines PDAs können aktive GI-Schließkomponenten mobil programmiert werden.
Physical Hardware Identifier	PHI	Die PHI-Nummer ist auf die SimonsVoss-Komponente aufgedruckt und intern abgespeichert. Die PHI-Nummer ist eindeutig und kann nicht geändert werden.
Profilzylinder	PZ	Ein Profilzylinder ist die gebräuchlichste Form von Sicherheitstürschlössern und eine Form des Schließzylinders.
Router (CentralNode)		Über spezielle Router können entsprechende Schließungen direkt über das Netzwerk angesprochen werden.
SMART.SURVEIL		SMART.SURVEIL ist ein eigenständiges Monitoring-Programm. Es kann auf Rechnern ohne LSM-Software ausgeführt werden und benötigt einen freien User-Client. (Ab LSM 3.4 SP1)

Begriff	Abkürzung	Erklärung
Transponder-ID	TID	Kennzeichnet den Transponder innerhalb der Schließanlage. (Vergleichbar mit einem Autokennzeichen.)
Virtuelles Netzwerk	VN	Über ein "virtuelles Netzwerk" lassen sich verschiedene Netzwerk-Vorteile realisieren, ohne spezielle Router einzusetzen.
Zutrittskontrolle	ZK	SimonsVoss-Komponenten mit ZK-Funktion protokollieren alle Zutritte (bzw. Buchungen") in der Schließanlage.

12. 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.

© 2024, 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

