

LSM 3.5 SP3 Business + Prof. Smart User Guide

Manual

12.12.2023

Contents

1.	General information.....	5
1.1	General safety instructions.....	5
1.2	Product-specific safety instructions.....	6
1.3	Legal notes.....	6
1.4	System requirements.....	7
1.5	Information on the manual.....	8
1.6	Data protection in System 3060.....	8
1.6.1	IT basic protection.....	9
1.6.2	Encryption.....	9
2.	Meaning of the text formatting.....	10
3.	Basic functions.....	11
3.1	Add new locking system.....	11
3.2	Add new transponder group.....	11
3.3	Add new transponder.....	11
3.4	Assign transponder to a transponder group at later point in time.....	12
3.5	Add new area.....	12
3.6	Add new locking device.....	12
3.7	Add PIN code Keypad.....	12
3.7.1	Configure PIN code Keypad.....	13
3.7.2	Add PIN code Keypad to the locking plan.....	13
3.7.3	Programme PIN code Keypad.....	14
3.8	Assign locking device to an area.....	14
3.9	Issue/withdraw authorisation.....	14
3.10	Setting up DoorMonitoring components.....	15
3.11	Common locking level.....	15
3.11.1	Add common locking level.....	15
3.11.2	Link locking devices.....	16
3.11.3	Link transponders.....	17
3.11.4	Authorise transponders.....	18
3.12	Create fire service transponders.....	18
3.13	Backing up the database manually.....	19
3.14	Working in compliance with data protection regulations GDPR.....	20
3.14.1	Export data.....	20
3.14.2	Deleting Data.....	22
3.14.3	What personal data is stored in the software?.....	24
3.14.4	For what purpose is personal data stored in the software?.....	24
3.14.5	How long is personal data stored in the software?.....	25

3.14.6	Is personal data in the software protected against access by third parties?	25
3.14.7	Can the stored data be made available as a copy?	25
3.14.8	Can personal data be deleted from the software?	25
3.15	Search matrix	25
3.16	Execute group actions	26
3.17	Programme transponder	27
3.18	Programme locking device	27
3.19	Programme using LSM Mobile	28
3.19.1	With laptop, netbook or tablet PC	28
3.20	Define time zone plan (with public holidays and company holidays)	29
3.21	Resetting components	30
3.22	Replace defective locking device	31
3.23	Block transponders	31
3.23.1	Block transponder permanently and create replacement transponder	32
3.23.2	Block transponder temporarily	35
3.24	Check and evaluate the battery level in the locking devices	36
3.25	Reset storage mode in G1 locking devices	38
3.26	Reset freeze mode in G2 locking devices	38
3.27	Access administration	39
3.27.1	Access lists	40
3.28	Administer users	40
3.29	Card management	41
3.29.1	Change configuration	41
3.29.2	Overview	42
4.	Performing standard WaveNet-based tasks in LSM	46
4.1	Creating a WaveNet radio network and incorporating a locking device	46
4.1.1	Preparing the LSM software	46
4.1.2	Initial programming of the locking components	46
4.1.3	Preparing hardware	47
4.1.4	Creating communication nodes	48
4.1.5	Setting up the network and importing into LSM	48
4.2	Putting DoorMonitoring locks into operation	50
4.2.1	Possible (door) states	50
4.2.2	Incorporating a DoorMonitoring lock into the network	51
4.2.3	DoorMonitoring SmartHandle	52
4.2.4	DoorMonitoring cylinder	54
4.2.5	Evaluating controller inputs	55
4.2.6	Transmitting the WaveNet configuration	57

4.2.7	Assigning a locking device's LockNode	57
4.2.8	Activating the locking device's input events	57
4.3	Setting up a RingCast	57
4.3.1	Preparing RouterNode for RingCast	58
4.3.2	Adding a RingCast	60
4.3.3	RingCast function test	63
4.4	Setting up event management	66
4.4.1	Setting up an email server	67
4.4.2	Setting up Task services	67
4.4.3	Forwarding input events via the RouterNode2	67
4.4.4	Forward input events via the SREL3 ADV system	67
4.4.5	Creating a response	69
4.4.6	Creating an event	70
4.5	Managing the virtual network (VN)	76
4.5.1	Virtual network with SmartRelay 3 Advanced	77
4.5.2	Virtual network with SmartRelay 2 G2	83
4.6	Read locking device	102
5.	Help and other information	107

1. General information

This manual describes the functions in the 3.5 SP3 Locking System Management software. The Locking System Management software, LSM software for short, was developed to manage complex locking systems with SimonsVoss locking components.

Other documents are available to supplement this manual:

■ *WaveNet manual*

Describes how to use the WaveNet radio network.

■ *SimonsVoss Smart User Guide*

Implement basic functions with the LSM software.

■ *LSM update manual*

Describes the update process for previous versions.

1.1 General safety instructions

Signal word: Possible immediate effects of non-compliance

WARNING: Death or serious injury (possible, but unlikely)

CAUTION: Minor injury

IMPORTANT: Property damage or malfunction

NOTE: Low or none



WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.



NOTE

Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SimonsVoss products for any other purposes.

Qualifications required

The installation and commissioning requires specialized knowledge.

- ❑ Only trained personnel may install and commission the product.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

1.2 Product-specific safety instructions

CAUTION

Loss of locking system password

The locking system password is a central component of the security concept. The loss of the locking system password restricts the operation of the locking system and is a security risk.

1. Keep the locking system password safe (e.g. in a safe)!
2. Make the locking system password visible to authorised persons at all times!

1.3 Legal notes

The purchaser is expressly informed that use of the locking system (e.g. with access event logging and DoorMonitoring functions) may be subject to statutory permit requirements and employee rights to co-determination, especially with regard to data protection legislation. The purchaser or customer and the end user are responsible for ensuring that the product is used in compliance with the law.

Malfunctions may arise if the product is not used as agreed or is used in a non-standard way. They may also occur if the product undergoes repairs or modifications not expressly approved by SimonsVoss Technologies GmbH, or assistance with the product is obtained from a non-specialist service provider; do not use the product or have it repaired or serviced in this way. Any modifications not expressly permitted by SimonsVoss Technologies GmbH will result in the loss of the right to make liability or warranty claims or any specially agreed rights to make guarantee claims.

1.4 System requirements

SimonsVoss recommends using up-to-date, high-performance hardware which exceeds the minimum system requirements at all times to ensure that LSM functions smoothly.

SimonsVoss recommends a high-resolution 21" wide-screen monitor or larger to ensure that even large locking systems with many components can be clearly displayed.

General information

- Local administrator rights for installation
- TCP/IP
(Using the EventAgent requires NetBios.)
- LAN (min. 100 Mbit/s)
- Windows domain (not required for single-user installations)
- Name resolution (not required for single-user installations)
- .NET Framework 4.0 or higher
- USB port(s)
- No support for ARM processors under System 3060

Client PC

- Monitor: min. 48 cm (19")
- Monitor resolution: min. 1024x768; recommended 1280x1024 or higher
- CPU: min. 2.66 GHz with 2 or more cores (Intel/AMD)
- Main memory: min. 4 GB
- Hard disk size: depending on the system size, min. 500 MB
(approx. 1 GB during installation)
- Windows operating system:
 - Windows 11 Professional, 64-bit
 - Windows 10 Professional, 64-bit

Server

- CPU: min. 2.66 GHz with 2 or more cores (Intel/AMD)
(Virtual network with SmartRelais 3 Advanced and VN host: min. 4 cores; cycle depends on number of gateways)
- Main memory: min. 4 GB
- Hard disk size: around 500 MB used
(approx. 1 GB during installation)

Database depends on the volume of the processed data

- Windows server:
 - Windows Server 2022
 - Windows Server 2019
- Virtual environments:
 - VMware ESXi (version 7.0 U2) with Windows Server 2022 and 2019
 - VMware ESXi (version 6.5.0) with Windows Server 2019
- If CommNode server is used: .NET Framework 4.0 or higher
- If application is used based on a server. Sharing on the Advantage Database server for a database directory



NOTE

Read the LSM software release notes to see which version of LSM Mobile is to be used.

1.5 Information on the manual

This manual describes the functions in the LSM software. This allows the user to programme SimonsVoss locking components and manage the locking system.



NOTE

This manual does not describe individual SimonsVoss locking components. You must consult the quick guides and manuals for the individual components to understand individual components.

Transponder

As a basic rule, the LSM software regards all ID media, such as transponders, tags and cards, as transponders. In this manual, the term 'transponder' therefore also refers to all other ID media such as tags and cards.

1.6 Data protection in System 3060

See *Working in compliance with data protection regulations GDPR* [► 20].

1.6.1 IT basic protection

1.6.1.1 What protection requirements do the data processed in the system have?

In general, only non-critical data with so-called normal protection requirements are processed and stored in the software. This means data whose hypothetical loss neither damages the reputation of a person nor the image of a company. A high financial loss is also not to be expected.

1.6.1.2 What IT infrastructure requirements are recommended?

According to the German Federal Office for Information Security (BSI), basic IT security is therefore sufficient as a security concept for a SimonsVoss locking system and is regarded as a recommended minimum requirement for your IT infrastructure.

1.6.2 Encryption

1.6.2.1 Is the data in System 3060 encrypted?

Yes. Data packets are encrypted end-to-end within the system's own communication network. The latest versions of our products offer you a higher level of security since they are always state-of-the-art. Multi-level encryption methods are used (AES, 3DES).

1.6.2.2 What data is encrypted?

Within the system's own communication network, no personal data is processed. It is pseudonymised instead using the identification numbers. They cannot be associated with a real person even without encryption.

1.6.2.3 Are the transmission paths via radio, for example, also encrypted?

No. Due to the end-to-end encryption type used, there is no need to also encrypt the transmission paths.

2. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

Example	button
<input checked="" type="checkbox"/> Example <input type="checkbox"/> Example	checkbox
<input checked="" type="radio"/> Example	Option
[Example]	Tab
"Example"	Name of a displayed window
Example	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
Example	Field
<i>Example</i>	Name of a (Windows) service
<i>Example</i>	Commands (e.g. Windows CMD commands)
Example	Database entry
[Example]	MobileKey type selection

3. Basic functions

This section describes the basic processes in the LSM software. LSM software frequently offers a number of ways to access the function that you require. These basic functions mostly show you the quickest and easiest way.

The SimonsVoss Smart User Guide uses an understandable example to describe in detail how a locking system is created and managed.

3.1 Add new locking system

- ✓ Installation has been completed correctly and a backup has been created.
- 1. Select *Edit/New locking system* in the menu bar.
- 2. Define the required locking system options.
 - ➔ Select a colour from "Use as common locking level" for the common locking levels. *Common locking levels act as additional levels to existing standard locking systems. See Common locking level.*
- 3. Click on the "Apply" button.
- 4. Click on the "Finish" button.

3.2 Add new transponder group

- ✓ A locking system has already been added.
- 1. Right-click on transponder groups in the "Groups area" in the LSM software.
- 2. Click on "New".
- 3. Give the new transponder group a name and make other settings if necessary.
- 4. Click on the "Apply" button.
- 5. Click on the "Finish" button.

3.3 Add new transponder

- ✓ A locking system has already been added.
- 1. Select *Edit/New transponder*.
- 2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
- 3. Click on the "Save & next" button.
- 4. Click on the "Finish" button.

3.4 Assign transponder to a transponder group at later point in time

- ✓ The transponder has already been created and a transponder group has been added.
- 1. Open the locking system settings, using the *Edit/Properties* menu bar, for example: *Locking system*.
- 2. Select the "Transponder" tab.
- 3. Select the transponder from the table with which you wish to correlate a transponder group.
- 4. Select the required transponder group which is to be correlated with the transponder from the drop-down list in "Change assignment to transponder groups".
- 5. Click on the "Execute" button.
- 6. Click on the "Apply" button.
- 7. Click on the "Finish" button.

If a transponder is being newly added, it can be immediately assigned to an existing transponder group.

3.5 Add new area

- ✓ A locking system has already been added.
- 1. Right-click on areas in "Areas-area" in the LSM software.
- 2. Click on "New".
- 3. Give the new area a name and make other settings if necessary.
- 4. Click on the "Apply" button.
- 5. Click on the "Finish" button.

3.6 Add new locking device

- ✓ A locking system has already been added.
- 1. Select *Edit/New locking device*.
- 2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
- 3. Click on the "Save & next" button.
- 4. Click on the "Finish" button.

3.7 Add PIN code Keypad

A PIN code keypad cannot be operated in pure G2 locking systems. The three user PINs act in the same way as G1 transponders.

3.7.1 Configure PIN code Keypad

Changing the master PIN

You only need to carry out this step if no new master PIN has been programmed yet.

1. Enter 0 0 0 0
2. Enter old master PIN: 1 2 3 4 5 6 7 8
3. Enter new master PIN
 - ↳ The new master PIN must consist of 8 characters which must not be consecutive or identical and must not begin with 0.
4. Re-entering the new master PIN



NOTE

The master PIN is essential for using the PIN code Keypad and cannot be imported, read or regenerated. Make a note of the master PIN and keep it in a safe, secret place. *Anyone who knows the master PIN can open or block PIN code Keypad locking devices by creating new user PINs themselves.*

Programming a user PIN

You can issue up to three user PINs for a PIN code Keypad. The user PIN can consist of between 4 and 8 digits, which must not be consecutive or identical.

An aid to better understanding: Each user PIN behaves as a separate transponder. As a result, these individual user PINs must be programmed in the respective (internal) transponders (1, 2 & 3).

1. Enter 0
2. Enter master PIN
3. Enter user PIN – e.g. 1 for User PIN 1
4. Enter the user PIN length – e.g. 4 for a 4-digit user PIN
5. Enter User PIN

Repeat the process to programme other user PINs into the PIN code Keypad.

3.7.2 Add PIN code Keypad to the locking plan

You **must** make a new entry for each user PIN.

1. Select *Edit / New transponder* from the menu bar.
2. Select the "G1 PinCode" entry in Type from the drop-down list and complete the other information.
 - ↳ The entry can be edited in detail in the same way as a transponder at a later point in time.

3. Select *Save & continue*
4. Select *End*

3.7.3 Programme PIN code Keypad

1. LSM: right-click on the transponder/PIN code in the locking plan and select *Programme*.
↳ The 'Programme transponder' window opens.
2. PIN code Keypad: Enter 0 0 + master PIN
3. LSM: Select *Programme*.
↳ The programming process starts.
4. PIN code Keypad: Press user PIN, e.g. 1 for User PIN 1/ Internal Transponder 1, as soon as LSM displays the instruction 'Press the transponder button briefly once now'.
↳ The programming process is now complete.

Repeat the process to programme other user PINs into the locking plan.

3.8 Assign locking device to an area

- ✓ The locking device has already been created and an area has been added.
1. Open the locking system settings, using the *Edit/Properties* menu bar, for example: *Locking system*.
 2. Select the "Doors" tab.
 3. Select the door from the table with which you wish to correlate an area.
 4. Select the required area which is to be correlated with the door from the drop-down list in "Change assignment to area".
 5. Click on the "Execute" button.
 6. Click on the "Apply" button.
 7. Click on the "Finish" button.

If a locking device is being newly added, it can be immediately assigned to an existing transponder area.

3.9 Issue/withdraw authorisation

You can use the matrix to issue and withdraw authorisations. You only need to click on an authorisation field to change the authorisation in the default setting.

You can only issue or withdraw authorisations between a locking device and a transponder.

Observe the two views:

- View/Doors and persons

In this view, the authorisations are changed for the transponder concerned.

■ **View/Areas and transponder groups**

In this view, the authorisations are changed for entire groups.

3.10 Setting up DoorMonitoring components

The DoorMonitoring function is an add-on feature to display door statuses in the LSM software. SmartHandles and locking cylinders with the DoorMonitoring function are installed in the LSM software in exactly the same way as regular locking components.

- Add new DoorMonitoring locking cylinder: Select "G2 DoorMonitoring cylinder" as the locking device type from the drop-down list.
- Add new DoorMonitoring SmartHandle: Select "G2 DoorMonitoring SmartHandle" as the locking device type from the drop-down list.

Tab: Configuration/Data

Use the "Monitoring configuration" button to make further settings.

Tab: DoorMonitoring status

This tab shows the door's current status. The status is shown real time.

A direct connection is required between the LSM software and locking components (e.g. via WaveNet) to ensure that this status display is always up to date. You will find more detailed information on setting up a WaveNet wireless network in the WaveNet manual.

3.11 Common locking level

Common locking levels can only be operated with active components. You cannot use passive card technology or smart tags for common locking levels.

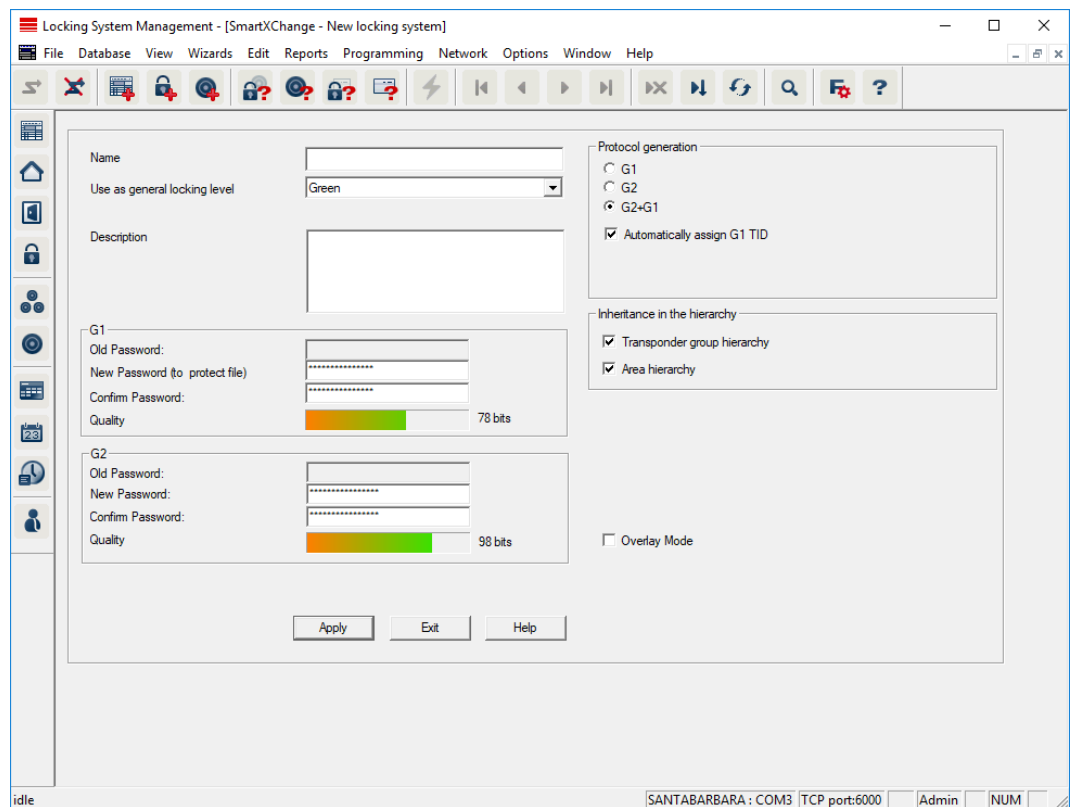
3.11.1 Add common locking level

You must take the following into account for common locking levels:

- Common locking levels must use the same protocol generations.
- The red locking level should only be used for the fire service or other emergency services since it has been specifically optimised for this particular use.

In principle, a common locking level is used in the same way as any other locking system, e.g. using the "New locking system" button in the icon bar:

- Select any colour in "Use as common locking level".



3.11.2 Link locking devices

✓ A common locking level has already been created.

1. Right-click on an area in the common locking level and select "Properties".
2. Select "Door management" button.

3. The right-hand table shows all locking devices in all locking systems in the project. Use the "Add" button to select the locking devices required.

The screenshot shows the 'Door administration' window with a close button (X) in the top right corner. The window is divided into two main sections: 'Assigned' on the left and 'Free' on the right. Both sections have a table with columns: Door, Location, Building, Floor, and Status (St). In the 'Assigned' section, the 'Main entrance' and 'Side entrance' are listed. In the 'Free' section, several items are listed, including 'development_office1', 'development_office2', 'development_office3', 'DM_TN4', 'Emergency exit', and three instances of 'product_manageme...'. Between the tables are buttons: '< - Add all' and '< - Add' at the top, and 'Remove - >' and 'Remove all - >' at the bottom. Below each table, there is a status bar showing 'Total' and 'Selected' counts. For 'Assigned', Total: 2, Selected: 0. For 'Free', Total: 8, Selected: 0. At the bottom of the window, there is a note: '- State: * - The module outputs can only be added to or removed from the locking system along with the Smart Relay!'. There are 'OK' and 'Cancel' buttons at the bottom corners.

3.11.3 Link transponders

Transponders should only be linked to non-common locking levels.

- ✓ Transponders or transponder groups have already been added.
1. Right-click on the transponder group and select "Properties".
 2. Select the "Automatic" button in transponder allocation.

- The right-hand table shows all transponders in all other locking systems in the project. Use the "Add" button to select the transponders required.

The screenshot shows the 'Transponder administration' window. It has a title bar with a close button. Inside, it says 'Transponder group: Office_Munich' and 'Assigned G1 Maximum: 8'. There are two main tables: 'Assigned' on the left and 'Free' on the right. Both tables have columns: Owner, Serial number, Type, and St. The 'Assigned' table has three rows: Hansen, Daniel (T-00003, G2 Transponder), Miller, James (000017N, G2 Transponder), and Peterman, Jennifer (040L922, G2 Transponder). The 'Free' table has three rows: cleaning, 3 (T-00001, G2 Transponder), cleaning, 2 (T-00006, G2 Transponder), and cleaning, 1 (T-00007, G2 Transponder). Between the tables are buttons: '< - Add all', '< - Add', 'Remove - >', and 'Remove all - >'. At the bottom, there are status bars for each table: 'Total: 3 (G1: 3)' and 'Selected: 0' for Assigned; 'Total: 3' and 'Selected: 0' for Free. A message says 'State: * - The assignment of a deactivated transponder cannot be changed!'. There are 'OK' and 'Cancel' buttons at the bottom.

Owner	Serial number	Type	St.
Hansen, Daniel	T-00003	G2 Transponder	
Miller, James	000017N	G2 Transponder	
Peterman, Jennifer	040L922	G2 Transponder	

Owner	Serial number	Type	St.
cleaning, 3	T-00001	G2 Transponder	
cleaning, 2	T-00006	G2 Transponder	
cleaning, 1	T-00007	G2 Transponder	

3.11.4 Authorise transponders

As in each common locking level, selected transponder groups can also be authorised for all locking devices in the "red level" with just a few mouse clicks. This function is particularly suitable for fire service transponders.

- ✓ You have now already added a red common locking level.
- Open red common locking system.
 - Create transponder group which should be authorised for all areas relevant for the fire service.
 - Click on the "Authorisations" button in the transponder group properties in Administration.
 - Use the checkboxes to select all the areas/locking devices required to grant access through all doors to the transponder group.

3.12 Create fire service transponders

- ✓ You have already created at least one locking system.
- Create a new "red" common locking level, using *Edit/New locking system*, for example.
 - Add a new area, such as "All locking devices", and use "Door administration" to assign all the locking devices required to this area.

3. Add a new "Fire service" transponder group to the common locking level.
4. Click on the "Authorisations" button in the properties for the "Fire service" transponder group.
5. Enable the "All systems" checkbox to authorise this transponder group for all locking devices in general.
6. Click on the "OK" button to save the settings.
7. Add a new transponder – "Fire service transponder 1", for example – to the transponder group and programme it. *All locking devices also need to be reprogrammed. Note the new programming requirement which has now appeared.*

The "Fire service transponder 1" fire service transponder created in this step is authorised for all locking devices. Even deactivated locking devices can be opened in the red level, making it markedly different from "green" and "blue" levels.

3.13 Backing up the database manually

- ✓ LSM opened.
1. Select via | Database | the entry **Backup**.
 - ➞ Window "Backup / restore" opens.

The screenshot shows the "Backup / restore" dialog box. It is divided into two main sections: "Backup" and "Recovery".

Backup Section:

- Database:** \\vtl.6262\\testdb\\Korbinian\\smdb\\smdb.add
- Directory for backups:** \\vtl\\testdb\\Korbinian\\smdb\\backup
- Buttons: "Use repository as default", "Backup"

Recovery Section:

- Database backup:** \\vtl\\testdb\\Korbinian\\smdb\\backup
- Directory for restored data:** \\vtl\\testdb
- Button: "Restore"

At the bottom right, there is an "Exit" button.

2. Specify the folder to save the database to in the area "Backup".
3. Click the button **Backup**.
 - ➞ Backup is created.
4. Click on the **Exit** button.
 - ➞ Window "Backup / restore" closes.

3.14 Working in compliance with data protection regulations GDPR

Since 25 May 2018, the General Data Protection Regulation has been valid throughout Europe. It regulates the handling of personal data in order to ensure their protection and at the same time their free movement within the European internal market. First of all, access to the database via the graphical user interface is only possible with a password and corresponding user rights. Additional "Exceptions in time zone management": In addition, no "special categories" of personal data pursuant to Art. 9 GDPR are stored within the LSM software. The mandatory fields used for a person are used exclusively for the unique assignment of identification media within the locking plan. The obligatory data are only required by the system for the duration of the occupation of an identification medium (e.g. company affiliation). The duration of data storage in logs can be changed at will by the locking system administrator himself (see Logging).

3.14.1 Export data



NOTE

Other language texts

The same language as in the LSM software is used for texts in the exported files.

Persons

You can export the saved personal data of people in the locking system as CSV files. Three files are generated during this process:

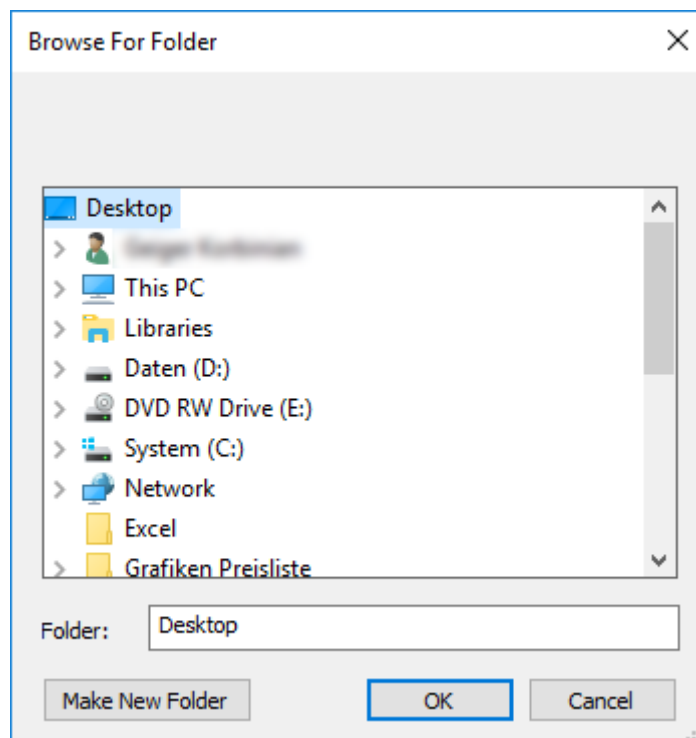
Person	This file contains personal data which can be used to identify the person (for example, sur-name, address or photo).
PersonHistory	This file contains the dates that the data record was created and erased.
PersonLog	This file contains different processing steps which have been performed on the person in question's data record, such as changes to authorisations and programming processes.



NOTE

The GDPR functions access HR Management for this purpose. As a result, the functions need to be assigned to a user group which is authorised to access HR Management.

- ✓ LSM open.
- 1. Use | Options | to select the **GDPR functions** item.
 - ↳ The "GDPR functions" window will open.
- 2. Highlight the entry for the person whose data needs to be exported in the "People" section.
- 3. Click on the **Export personal data** button in the "People" section.
 - ↳ The "Search Folder" window will open.



- 4. Indicate the folder where the files are to be exported.
- 5. Click on the **OK** button.
 - ↳ Data is exported.

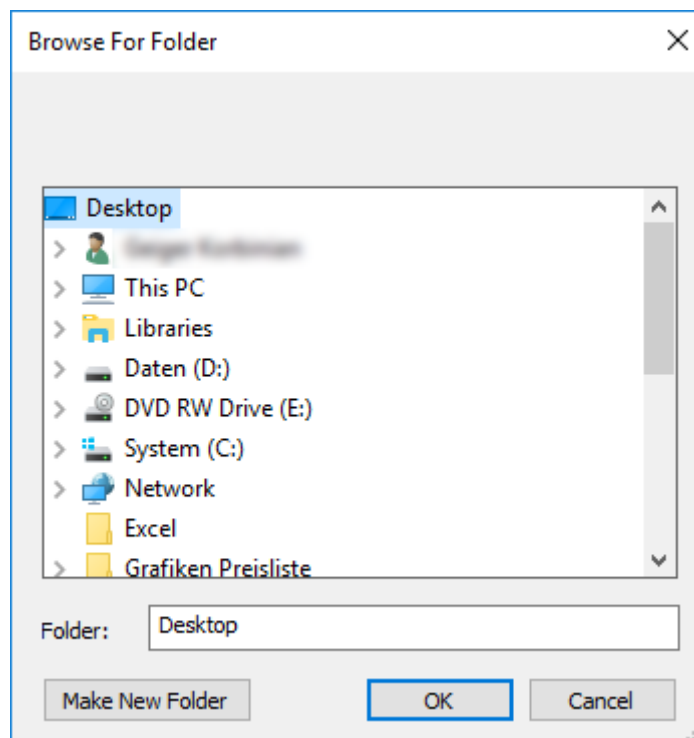
Users

You can export the users' saved personal data as CSV files in the LSM software. Two files are generated during this process:

User	This file contains the data which refers to the user, such as user name and user group.
UserLog	This file contains different processing steps which the user has carried out, such as creating a new locking device.

The GDPR functions access administration functions for this purpose. As a result, they need to be assigned to a user group which is authorised to access Administration.

- ✓ LSM open.
- 1. Use | Options | to select the **GDPR functions** item.
 - ↳ The "GDPR functions" window will open.
- 2. Highlight the entry for the user whose data needs to be exported in the "Users" section.
- 3. Click on the **Export personal data** button in the "Users" section.
 - ↳ The "Search Folder" window will open.



- 4. Indicate the folder where the files are to be exported.
- 5. Click on the **OK** button.
 - ↳ Data is exported.

3.14.2 Deleting Data

You can also use the GDPR module to easily erase personal data.

Persons

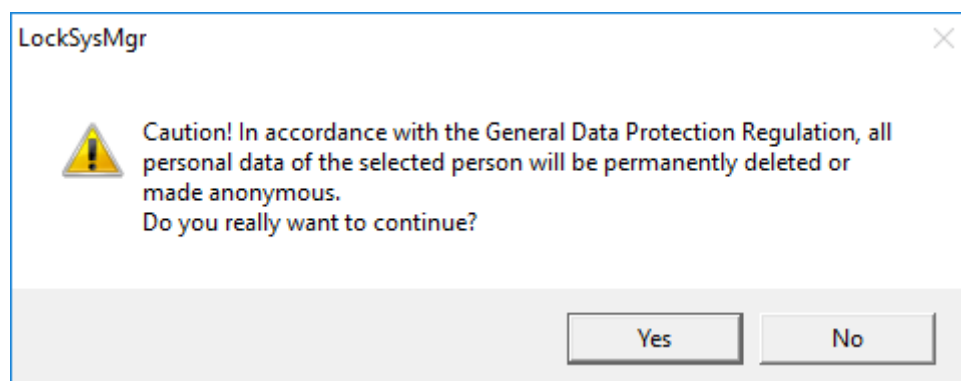


NOTE

The GDPR functions access HR Management for this purpose. As a result, the functions need to be assigned to a user group which is authorised to access HR Management.

- ✓ LSM open.
- 1. Use | Options | to select the **GDPR functions** item.
 - ↳ The "GDPR functions" window will open.

2. Highlight the entry for the person whose data needs to be erased in the "People" section.
3. Click on the **Permanently delete personal data** button in the "People" section.
 - ↳ The "LockSysMgr" window will open.



4. Click on the **Yes** button.
 - ↳ The highlighted person's personal data is erased or anonymised.



NOTE

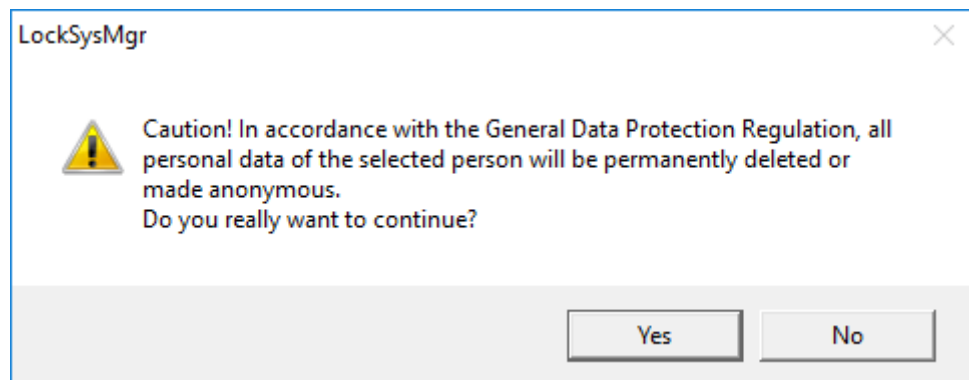
Erasure of remaining data from previous deletions

You can also use the **✕** button in the [Name] tab in the assigned identification media to erase personal data. Unlike erasure using the GDPR module, this button does not delete logs, which will remain in the system. This means that only a part of personal data is erased. People who are deleted in this way are no longer displayed in the GDPR module. Please use the **Delete** button in the "Database" section to meet GDPR requirements and also remove such files.

Users

The GDPR functions access administration functions for this purpose. As a result, they need to be assigned to a user group which is authorised to access Administration.

- ✓ LSM open.
- 1. Use | Options | to select the **GDPR functions** item.
 - ↳ The "GDPR functions" window will open.
- 2. Highlight the entry for the user whose data needs to be erased in the "Users" section.
- 3. Click on the **Permanently delete personal data** button in the "Users" section.
 - ↳ The "LockSysMgr" window will open.



4. Click on the **Yes** button.

↳ The highlighted user's personal data is erased or anonymised.

3.14.3 What personal data is stored in the software?

It is possible to store the following data of a person in the software:

- First name
- Last name*
- Title
- Address
- Phone
- E-Mail
- Personnel number*
- User name
- Department
- City/Building
- Set From/To
- Date of birth
- Cost center
- Photo

Only the last name and personnel number (*mandatory fields) are required when using the software. Special categories of personal data according to Art. 9 GDPR are not stored.

3.14.4 For what purpose is personal data stored in the software?

In order to be able to make full use of the functions of an electronic locking system, it is necessary to be able to assign the identification media used (e.g. transponder) to a specific user (e.g. employee).

3.14.5 How long is personal data stored in the software?

The data is stored within the locking system for at least the duration of the occupation of an identification medium (e.g. company affiliation).

The duration of data storage, e.g. in logs and access lists, can be changed at will by the locking system administrator.

3.14.6 Is personal data in the software protected against access by third parties?

In principle, the user (end customer) of the locking system and the software is responsible for managing and securing access rights.

In the locking system itself, all data is secured using a multi-level encryption process. Opening the graphical user interface to access the data is not possible without a password and appropriate user rights.

There shall be no automatic transmission to third parties, use or processing by SimonsVoss.

3.14.7 Can the stored data be made available as a copy?

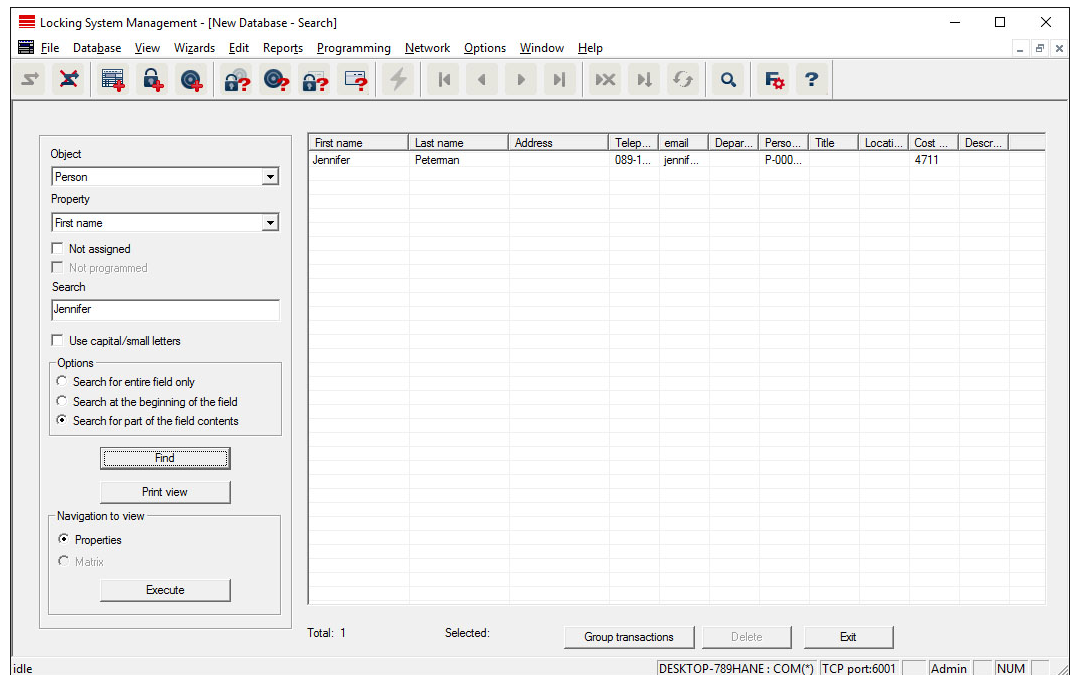
All collected data on a data subject can be made available as a copy by means of an export function (Art. 15 GDPR).

3.14.8 Can personal data be deleted from the software?

Personal data can be validly deleted from the software (from version 3.4 SP1) and the associated database at the request of a data subject in accordance with Art. 17 GDPR.

3.15 Search matrix

The search enables you to search easily for different items, such as a specific door or a specific transponder.



✓ Elements have already been added to the locking system, which you can search for.

1. Click on the magnifier icon in the icon bar.
2. Select the object that you wish to look for, such as persons, transponders, doors or locking devices.
3. Select a characteristic of the object that you are looking for, such as a last name or first name.
4. Enter a search term into the search field.
5. Click on the "Search" button to start the search process.

3.16 Execute group actions

Settings for a number of components can be made in just one single step. In this example, the properties of several G2 locking devices (*e.g. enable access control*) are to be changed all at once.

1. Click on the magnifier icon in the icon bar.
2. Search for all "Locking device"-type objects, for example.
 - ↳ No details need to be added in the "Search" field when searching for all locking devices.
3. Select a number of locking devices by filtering by type or area.
4. Click on the "Group actions" button.
 - ↳ If only G2 locking devices were selected in the preceding step, the correct parameters ("*Configuration changes to G2 locking devices*" and "*G2 locking cylinders active/hybrid*") have already been selected.

5. Press on "Execute" button to start the changes to the selected locking devices.
6. Make the changes as you wish.
7. Click on the "Finish" button to save the new settings.



NOTE

This process allows you to change many settings quickly and easily. Take into account that each changed component must be reprogrammed.

3.17 Programme transponder

- ✓ A transponder has been added to the locking system and is visible in the matrix.

1. Right-click on the transponder concerned.
2. Click on Programme.
3. Follow the instructions in the LSM software.

Ensure that you select the right programming device.

You can use the "TIDs to deactivate" button to open a list from which you can select one or two transponder IDs which are to be deactivated (see [Block transponder permanently and create replacement transponder \[▶ 32\]](#)).



NOTE

Automatically recognise G2 cards

It is not always possible to distinguish between cards as ID media. If there are a number of cards, the card which is to be programmed now needs to be read first to select the right card to be programmed in LSM. This step is omitted if the "Automatically recognise G2 card" box is checked. If LSM already knows the card, its data record is selected and programmed automatically.

3.18 Programme locking device

- ✓ A locking device has been added to the locking system and is visible in the matrix.

1. Right-click on the locking device concerned.
2. Click on Programme.
3. Follow the instructions in the LSM software.

Ensure that you select the right programming device.



NOTE

Only one locking device may be near the programming device at any time.

First transponder activation rejected after initial programming of AX products

If a transponder is the first identification medium to be activated after initial programming, the transponder is rejected once and synchronised with the locking device in the background. Transponders will then function as normal.

3.19 Programme using LSM Mobile

You can use LSM Mobile to carry out programming tasks directly on a locking device using mobile devices. This programming takes place as follows:

1. A list with components which indicate a programming requirement is exported to the LSM Mobile device from the LSM software, *either directly on the pocket PC or as a file for a notebook, netbook or tablet units*
2. LSM Mobile is launched on the mobile device. You can start the programming of components with the export from the LSM software.
3. The LSM software must then be informed which components have been programmed using LSM Mobile. This achieved using an import or synchronisation from LSM Mobile to the LSM software.

3.19.1 With laptop, netbook or tablet PC

This how you programme with the help of LSM Mobile:

- ✓ There are components in the LSM software which require programming.
 - ✓ Initial programming has already been completed on the components requiring programming.
 - ✓ LSM Mobile has been correctly installed on the mobile device. The version numbers are identical.
 - ✓ The drivers have been correctly installed in the SMARTCD.G2 and SMARTCD.MP programming devices (depending on requirements).
1. Select *Programming/LSM Mobile/Export to LSM Mobile/LSM Mobile PC*.
 2. Follow the instructions in the LSM software and export the programming tasks in a file.
 3. Launch LSM Mobile on the mobile PC and import the file with the programming tasks into LSM Mobile.
 4. Follow the instructions in LSM Mobile.

5. Use the programming device to carry out the programming processes on the components concerned.
6. Export the status of the programming tasks.
7. Select *Programming/LSM Mobile/Import from LSM Mobile/LSM Mobile PC*.
8. Follow the instructions in the LSM software and import the file from LSM Mobile.

The programming tasks have been completed using the external device. The import in the last step ensures that the programming flash icons indicating a programming requirement disappear from the LSM software.

3.20 Define time zone plan (with public holidays and company holidays)

It is recommended to apply time zone plans to entire areas and transponder groups. However, it is also possible to link time zone plans directly with locking devices and transponders.

- ✓ Locking devices (or areas) and transponders (or transponder groups) have already been created.
1. Click on *Edit/Time zone plan* in the menu bar.
 - ↳ An "empty time zone plan" will open up. If an existing time zone plan is displayed, click on the "New" button to create a new, empty time zone plan.
 2. Fill out the "Name" and "Description" fields.
 3. Select a public holiday list for your region if required. This is how to proceed if you wish to define one-time company holidays:
 - ↳ Click on the "... field" next to the holiday day drop-down selection.
 - ↳ Click on the "New holiday day" button.
 - ↳ Assign a name: e.g. "Company holiday 2017"
 - ↳ Newly defined holidays may contain a time period. The "Leave" field must be activated for this purpose. You can then enter a time period (From - To).
 - ↳ Select how the new holiday day should be treated: e.g. as "Sunday".
 - ↳ Click on the "Apply" button and then on the "Finish" button.
 - ↳ Click on the "Holiday administration" button.
 - ↳ Use the "Add" button in the holidays list (*in the right-hand column*) to add the newly created holiday (*in the left-hand column*).
 - ↳ Click on the "OK" button and then on the "Finish" button to return to the main time zone plan menu.
 4. Select a group in the table and edit the weekly schedule for the group.
 - ↳ A blue bar indicates an authorisation for this time period.
 - ↳ You can click on fields individually or select them together.
 - ↳ Each time that you click on a field or area, you reverse the authorisation status.



5. Click on the "Apply" button.
6. Click on the "Finish" button.

Assign the time zone plan to an area:

1. Right-click on the area to which you wish to assign the time plan.
2. Select "Properties".
3. Select the corresponding time zone plan from the drop-down list in "Time zone".
4. Click on the "Apply" button.
5. Click on the "Finish" button.

It is also possible to assign the time zone plan to a locking device directly.

Assign a transponder group to the time group:

1. Right-click on the transponder group which is to be assigned to the time group.
2. Select "Properties".
3. Select the corresponding time group from the drop-down list in "Time zone group".
4. Click on the "Apply" button.
5. Click on the "Finish" button.

It is also possible to assign the time group directly to a transponder.

3.21 Resetting components

All SimonsVoss components can be reset at any time. You can even reset SimonsVoss components which do not belong to the locking system. In such a case, you need the corresponding locking system password.

Resetting components is an effective solution in many scenarios. It is advisable to reset and reprogramme the components in question particularly if they may not be functioning correctly.

1. Use *Programming/Read components* to read the components concerned.
2. Select the "Reset" button to start the reset process.
3. Follow the instructions in the LSM software.

➡ If necessary, you will be requested to enter the locking system password or select the dataset to be deleted.

3.22 Replace defective locking device

Locking devices may become damaged or contain a defect.

Proceed as follows to replace a defective locking device with a new one:

1. Remove the defective locking device from the door.
 - ↳ It may be difficult to remove a cylinder from a closed door. If necessary, ask the specialist who installed the SimonsVoss products for advice.
2. Acquire a replacement locking device.
 - ↳ Double-click on the defective locking device in the LSM software to find all details on the locking device in the "Features" tab.
3. Carry out a software reset on the locking device in the LSM software.
 - ↳ Double-click on the defective locking device to open the "Configuration/Data" button, where you will see the "Software reset" button.
 - ↳ Once the software reset is complete, the software indicates a programming requirement for the defective locking device.
4. Carry out a programming process on the replacement locking device.
5. Fit the replacement locking device into the door and check that it functions correctly.



NOTE

If a fault or error occurs, first try to reset the locking device itself by implementing a readout. After resetting the locking device, you can then possibly reprogramme it.



NOTE

You must reset defective locking devices if at all possible before sending them to a retailer or SimonsVoss Technologies GmbH.

3.23 Block transponders

Transponders may get lost, stolen or damaged at some point.

- *Block transponder permanently and create replacement transponder [▶ 32]*
- *Block transponder temporarily [▶ 35]*



NOTE

Transfer of the lock IDs with cards to double-sided locks

Cards can only transfer individual lock IDs, not a complete programming protocol.

- Always hold the card that transmits the lock IDs to both readers.

3.23.1 Block transponder permanently and create replacement transponder



NOTE

For security reasons, the deleted transponder's authorisations must be removed from all locking devices.

- You can do this by reprogramming all locking devices.

Proceed as follows to replace an "old" transponder with a new, non-programmed transponder.

1. Acquire a replacement transponder.
 - ↳ Double-click on the defective transponder in the LSM software to find all details on the transponder in the "Features" tab.
2. Right-click on the defective, lost or stolen transponder and select "Lost transponder".
 - ↳ The transponder concerned is prepared for blocking.
 - ↳ Indicate the reason why blocking is necessary. *When you select "Transponder lost/stolen", you can then programme a new transponder with the same authorisations directly afterwards. With the G2 protocol, this transponder blocks the lost transponder each time an authorised locking device is activated. However, all locking devices concerned still need to be reprogrammed.*
3. Implement all the newly appeared programming requirements on all components.

Avoiding the need to reprogramme locking devices

Creating a new replacement transponder also entails a programming requirement for all locking devices. However, these special programming tasks can also be implemented directly with the new replacement transponder:

- ✓ The replacement transponder has been programmed correctly.
1. Activate the new replacement transponder on each locking device.
 2. Programme the new replacement transponder again. Activate the checkbox "Read deactivation acknowledgement/Battery warnings" in the "Programme transponder" window.

- Update the matrix. The programming requirement has now disappeared.

With LSM 3.5 SP3 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

Programme the TIDs to be disabled directly

The IDs to be disabled are saved on the transponder during the programming process.

- ✓ The transponder is physically available.
- ✓ The transponder's programming window is open.

- Click on the **TIDs to deactivate** button.

- The list will open.

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

- Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.

3. Click on the **OK** button to confirm your input.
 4. Continue with the programming.
- The checked TIDs will be saved to the transponder as TIDs to delete.
When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

Add the TIDs to be blocked to the properties

The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

- ✓ The transponder's properties window is open.

1. Change to the "[Configuration]" tab.

2. Click on the **TIDs to deactivate** button.
- The list will open.

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

3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
 4. Click on the **OK** button to confirm your input.
- The checked TIDs are saved on the transponder either during the next programming process or the next booking on a gateway.

3.23.2 Block transponder temporarily

Permanent blocking of an identification medium leads to the loss of a TID. Therefore LSM 3.5 brings a new function, which enables the temporary blocking of transponders and cards: "Temporary blocking".

The reason

Do you really want to block the transponder?
If 'yes', please specify the reason, e.g. whether the transponder has been lost or is defect

Temporary blocking

Note:

Yes No

The TID isn't actually blocked. Instead the function revokes every authorization of the comprehensive person. Affected doors have to be programmed afterwards. If the transponder is found, returned or passed on to a new person, it's possible to restore the authorizations like before the blocking.

You find temporarily blocked transponders in the locking system's properties in the register [Special TIDs].

[illegible]

3.24 Check and evaluate the battery level in the locking devices

There are different ways to query a locking device's battery level. In regular offline locking systems (and VN), the battery levels must first be transmitted to the LSM software before they can be evaluated in different ways.

Transmitting battery levels to the LSM software

Fast & efficient: "collect" battery levels using a transponder

1. Take a transponder which is authorised for use on all locking devices. Activate this transponder on each locking device.
2. Re-programme the transponder. Activate the checkbox "Read deactivation acknowledgement/Battery warnings" in the "Programme transponder" window.

Importing battery levels by reading the locking device

Select "Programme/read locking device" to read the required locking devices separately.

Transmitting battery levels to the LSM software using LSM Mobile

You can use LSM Mobile to read battery levels directly or transmit them to the LSM software. Follow the instructions in the LSM Mobile manual. You will find it under Documents in the Support section on the SimonsVoss website (www.simons-voss.com/en).

Displaying battery levels

Basic procedure for all LSM versions:

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Double-click on a locking device to display the locking device properties.
- 2. Select the "Status" tab.
- 3. The battery level will be displayed in the "Status at last readout".

Displaying battery warnings collectively in LSM BASIC Online and LSM BUSINESS:

Generate a list which displays all locking devices with battery warnings.

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Select from the "Reports/Building structure" menu bar.
- 2. Select the "Locking devices with battery warnings".
- 3. Click on the "Display" button.

Displaying battery warnings automatically in LSM Business

Create a warning which displays battery warnings directly.

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Selecting from the "Reports/Warnings" menu bar
- 2. Create a new warning using the "New" button.
- 3. Create the warning as you wish. Select "Locking device battery warning" as the type.

4. Do not forget to assign the locking devices concerned to this warning.
The "Locking devices" field should not be empty.
5. Click on the "OK" button to confirm the new warning.
6. Click on the "Exit" button to close the dialogue.

3.25 Reset storage mode in G1 locking devices

If battery warnings are ignored in G1 locking devices, the locking devices concerned switch to storage mode. This prevents the batteries from being fully discharged. Storage mode can be terminated by reprogramming the locking device. The locking device must then be opened with an authorised transponder and the batteries replaced immediately.

3.26 Reset freeze mode in G2 locking devices

Emergency opening of a locking device and elimination of emergency retention mode (freeze mode) has been made easier in G2 than in G1 generation systems.

- ✓ Battery replacement identification medium added (see Special functions/G2 battery replacement transponder).
 - ✓ Battery replacement identification medium programmed.
1. Activate the Battery replacement identification medium on the locking device.
 - ↳ Freeze mode is deactivated.
 2. Activate any authorised identification medium.
 - ↳ Locking device opens.
 3. Change the battery.
 4. Activate the Battery replacement identification medium on the locking device.
 - ↳ Freeze mode is deactivated.
 5. Use any authorised identification medium to verify whether the locking device functions correctly.
 - ↳ Freeze mode is reset.

IMPORTANT

Locking device failure due to misuse

The battery change identification medium is intended exclusively for cancelling the freeze mode before a battery change. If it is misused, the batteries can be completely discharged. The result is a total failure of the locking device.

3.27 Access administration

The reading of access and physical access lists can be greatly restricted to protect privacy. In LSM Basic, the "AdminAL" (Admin Access List) user is added as standard for this purpose. In LSM BUSINESS, you can add a suitable user manually; see *Administer users* [► 40].

The following scenario is described in this section: Only an authorised person (e.g. Works Council logged on as the AdminAL) should be able to read access lists and physical access lists. The general locking system administrator is not given this right.

Configure AdminAL and permit reading of access lists

1. Use the "Admin" user name and your password to log on to your project.
2. Select "Edit/User group" to open user group administration.
3. Use the navigation arrow to scroll to the "Access lists administration" user group (or to any previously added user group in LSM Business).
4. Ensure that the "Access lists administration" and "Manage access lists" rights are activated in the "Role" section.
5. Click on the "Edit" field beneath "Role" section.
6. Activate the required locking systems in transponder groups and areas. If you have added areas or transponder groups, you must activate all required areas and transponder groups separately.
7. Click on the "OK" button to close the mask.
8. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.
9. Select "Database/Log off" to log off from your current project.

Remove rights to read access lists from Admin



NOTE

The "Access lists administration" right must always be assigned to a user/user group and must not be withdrawn from both.

1. Use the "AdminAL" user name to log on to the project.
 - ↳ The default password in LSM BASIC is "system3060".
 - ↳ Change this password immediately.
2. Select "Edit/User group" to open user group administration.
3. Use the navigation arrow to scroll to the "Admin" user group.
4. Deactivate the "Access lists administration" and "Administer access lists" roles.

5. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.

↳ Configuration is now complete. Only the "AdminAL" user account may read or view access lists and physical access lists from now on.

3.27.1 Access lists

Locking devices with ZK function log the accesses in an access list:

- Date
- Time
- ID of the identification medium
- Name of the user

You can read and display the access list with the LSM software. The number of entries in the access list depends on the locking device and the configuration.

	Standard	Gateway
Cylinder	Up to 3000	
SmartHandle	Up to 3000	
SmartRelay	Up to 3600	Up to 200

You can also automate the read-out in a networked locking system (see [Read locking device \[▶ 102\]](#)).

3.28 Administer users

Assign user to a user group

1. Click on "Edit/User group".
2. Use the navigation arrow to scroll to a user group (or use the "New" button to create a new user group).
3. Click on the "Edit" button.
4. Highlight the user that you require and use the "Add" button to assign them to the user group.
5. Click on the "OK" button to confirm the settings that you have made.
6. *Correct the roles if necessary.*
 - ↳ Click on the "Edit" field beneath "Role" section.
 - ↳ Activate the required locking systems in transponder groups and areas. If you have added areas or transponder groups, you must activate all required areas and transponder groups separately.
 - ↳ Click on the "OK" button to close the mask.
7. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.

Creating a new user

1. Click on "Edit/User".
2. Click on the "New" button to add a new user.
3. Issue a new user name and enter a password.
4. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.

3.29 Card management

Below you can see the different card types and the distribution of memory in connection with the SimonsVoss locking system.

IMPORTANT

MIFARE DESFire recommended

Compared to MIFARE Classic, MIFARE DESFire uses microcontroller-based encryption based on AES-128, which has been further developed to meet increased security requirements.

- SimonsVoss recommends the use of transponders or MIFARE DESFire products.



NOTE

Different templates for AX products

If you want to use MIFARE products for SimonsVoss AX products, the templates used for writing and reading must be identical.

3.29.1 Change configuration


You have two options for using cards.

- You can use cards that have already been used.
- You can use new cards.

In both cases, enter the card type, the configuration and, if necessary, the sectors to be described (see [Overview \[▶ 42\]](#)).

Configuring the card

- ✓ LSM open.

1. Switch to the locking system whose card management you want to change.
2. Click on the button to open the properties of the locking system .

3. Change to the tab [G2 card management].

NameLocksDoorsTransponderTransponder groupsAreasPasswordSpecial TIDSPIN-Code TerminalCard management G1G2 card management

Locking system: HIMYMLevel: Standard

Card type: Mifare ClassicConfiguration: MC1000L_AVMemory space needed: 528 BytesLock IDs: 128-1127 in card profileAccess instances in the log: 19Virtual network: OKParameter:

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

Print view

- 4. In the dropdown menu ▼ Card type select your card type.
- 5. In the dropdown menu ▼ Configuration select your configuration.
- 6. If necessary, enter further parameters such as sectors (e.g: 2,3,4,5,6,7,8,9,10,11,12,13,14,15).

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

- 7. Click on the Apply button.
→ You have changed the configuration.

3.29.2 Overview

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

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

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MC3800 L	G2	128-3927	3800	✗	2-15	528	✗
MC1000 L_AV	G2	128-1127	1000	19	2-15	528	✓
MC2400 L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000 L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✗	✗	✗	2-15	48	✗
M1200L	G2	128-1327	1200	✗	2-15	192	✗
M3800L	G2	128-3927	3800	✗	2-15	528	✗
M1000L_AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000 L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✗	✗	✗	2-15	48	✗
MD1200L	G2	128-1327	1200	✗	2-15	192	✗
MD3800 L	G2	128-3927	3800	✗	n.a. (DES-Fire)	528	✗
MD2500 L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	✓
MD4000 L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	✓
MD1000 L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	✓

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MD3200 L_AV	G2	128-3212 7	32000	470	n.a. (DES- Fire)	7000	✓
MD2400 L_AV	G2	128-2527	2400	34	n.a. (DES- Fire)	830	✓
MD3650 L_AV	G2	128-3777	3650	2	n.a. (DES- Fire)	830	✓

4. Performing standard WaveNet-based tasks in LSM

This example shows the key steps in setting up and administrating a WaveNet radio network in LSM Business. The examples are based on specific installations and are meant to help you become familiar with topics related to WaveNet.

4.1 Creating a WaveNet radio network and incorporating a locking device

This example describes how you can create a WaveNet radio network from scratch. The aim is to address a locking device via a RouterNode2.

4.1.1 Preparing the LSM software

Note that the LSM software required to network SimonsVoss locking components must be properly installed and a corresponding network module licensed.

1. Install the CommNode server and ensure that the service has been started.
2. Install the current version of WaveNet Manager. (See Unpacking)
3. Open the LSM software and select "Network/WaveNet Manager".
 - ↳ Enter the WaveNet Manager installation directory and select a directory for the output file.
 - ↳ Use the "Launch" button to open WaveNet Manager.
4. Provide a password to increase your network's security.
 - ↳ WaveNet Manager launches and the settings are saved for the future. Exit WaveNet Manager to make further settings.

4.1.2 Initial programming of the locking components

Before locking devices can be incorporated into the network, they first need to be programmed.

4.1.2.1 Add new locking device

- ✓ A locking system has already been added.
1. Select *Edit/New locking device*.
 2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
 3. Click on the "Save & next" button.
 4. Click on the "Finish" button.

4.1.2.2 Programme locking device

- ✓ A locking device has been added to the locking system and is visible in the matrix.

1. Right-click on the locking device concerned.
2. Click on Programme.
3. Follow the instructions in the LSM software.

Ensure that you select the right programming device.



NOTE

Only one locking device may be near the programming device at any time.

First transponder activation rejected after initial programming of AX products

If a transponder is the first identification medium to be activated after initial programming, the transponder is rejected once and synchronised with the locking device in the background. Transponders will then function as normal.

4.1.3 Preparing hardware

The current RouterNode2 is put into operation quickly and easily. Connect the RouterNode2 as described in the supplied quick guide. The RouterNode2 is pre-configured in the factory, so that it obtains its IP address from a DHCP server. You can quickly identify this IP address using the OAM tool (*available free of charge under Informative Material/ Software Downloads/Drivers in the Support section*).



NOTE

Standard settings:

IP address: 192,168,100,100

User name: SimonsVoss | Password: SimonsVoss

If the locking device has not been equipped with a LockNode (LN.I) in the factory, you need to retrofit one with appropriate accessories.



NOTE

Note down the RouterNode2's IP address and the locking device's chip ID after you have correctly prepared the hardware.

4.1.4 Creating communication nodes

The communication node forms the interface between the CommNode server and the LSM software. You must launch the LSM software using an administrator account to add the configuration XMLs.

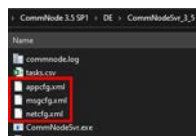
1. Open the LSM software.
2. Select | Network | / **Communication nodes**.
3. Add "Name", "Computer name" and "Description",

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

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

↳ e.g. UNF-AL-18KJ793; UNF-AL-18KJ793.ALLEGION.COM;
communication node for the WaveNet radio network 123

4. Click on the **Config files** button.
5. Ensure that the path links to the CommNode server's installation directory and click on the **OK** button.
6. Press **No** to deny the prompt and confirm your selection by clicking on **OK**. The three configuration XMLs (*appcfg*, *msgcfg* and *netcfg*) must be located directly in the CommNode server's installation directory.



7. Click on the **Apply** button to save your settings.
8. Click on the **OK** button to close the prompt.
9. Click on the **Exit** button to close the dialogue.

4.1.5 Setting up the network and importing into LSM

4.1.5.1 Adding the WaveNet configuration

If all requisites have been met, you can start to configure the network:

- ✓ LSM has been installed correctly and a network module is licensed.
 - ✓ The CommNode server has been installed and the service launched.
 - ✓ The CommNode server's configuration files have been created.
 - ✓ The current version of WaveNet Manager has been installed.
 - ✓ A communication node has been created in the LSM software.
 - ✓ Initial programming of the locking device to be networked has been successfully completed.
 - ✓ RouterNode2 can be reached via the network and you know its IP address.
 - ✓ The programmed locking device features an installed LockNode and you know its chip ID.
1. Select "Network/WaveNet network" and press the "Launch" button to open WaveNet Manager.
 2. Enter the password.
 3. Right-click on "WaveNet_xx_x".
 4. Initialize the RouterNode2 first, e.g. using the option "Add: IP or USB router".
 - ↳ Follow the dialogue instructions and incorporate the RouterNode2 into your WaveNet radio network using its IP address.
 5. Initialize the locking device's LockNode by right-clicking on the newly added RouterNode2 and select the "Search by chip ID" option.
 - ↳ Follow the dialogue instructions and use the associated chip ID to assign the locking device or its LockNode to the RouterNode2.
 6. Click on the "Save", "Exit" and "Yes" buttons one after another to close WaveNet Manager.
 7. Import the new settings and assign them to the corresponding communication node.

4.1.5.2 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transmit" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "Exit" button to close the dialogue.

4.1.5.3 Assigning a locking device's LockNode

The initialized LockNode needs to be linked to a locking device. This is easiest to do using a collective command, particularly if there is more than one LockNode:

1. Select "Network/Collective commands/WaveNet nodes".
2. Select all LockNodes (*WNNode_xxxx*) which have not been assigned yet. *Non-assigned LockNodes have no entry in the "Door" column.*
3. Click on the "Configure automatically" button.
↳ The automatic configuration will start immediately.
4. Click on the "Exit" button to close the dialogue.

4.1.5.4 Testing the WaveNet configuration

You can select "Right-click/Programme" to re-programme the locking device via the network at any time to test networking quickly. The network is working properly if programming is successful.

4.2 Putting DoorMonitoring locks into operation

This example shows what settings need to be made to set up DoorMonitoring locks. You will find the prerequisites for this process in "*Creating a WaveNet radio network and incorporating a locking device [▶ 46]*".

4.2.1 Possible (door) states

States may differ for different components.

4.2.1.1 Possible DoorMonitoring states of SmartHandles

- Door open/closed
- Door open for too long
- Locked (only for self-locking mortise locks)
- Handle in use/not in use

4.2.1.2 Possible DoorMonitoring states of locking cylinders

- Door open/closed
- Door locked
- Door securely locked
- Door open for too long
- Forend screw manipulated

4.2.1.3 Possible DoorMonitoring states of SmartRelais 3

- Input 1 active/inactive
- Input 2 active/inactive
- Input 3 active/inactive

▣ Sabotage detection [▶ 53]

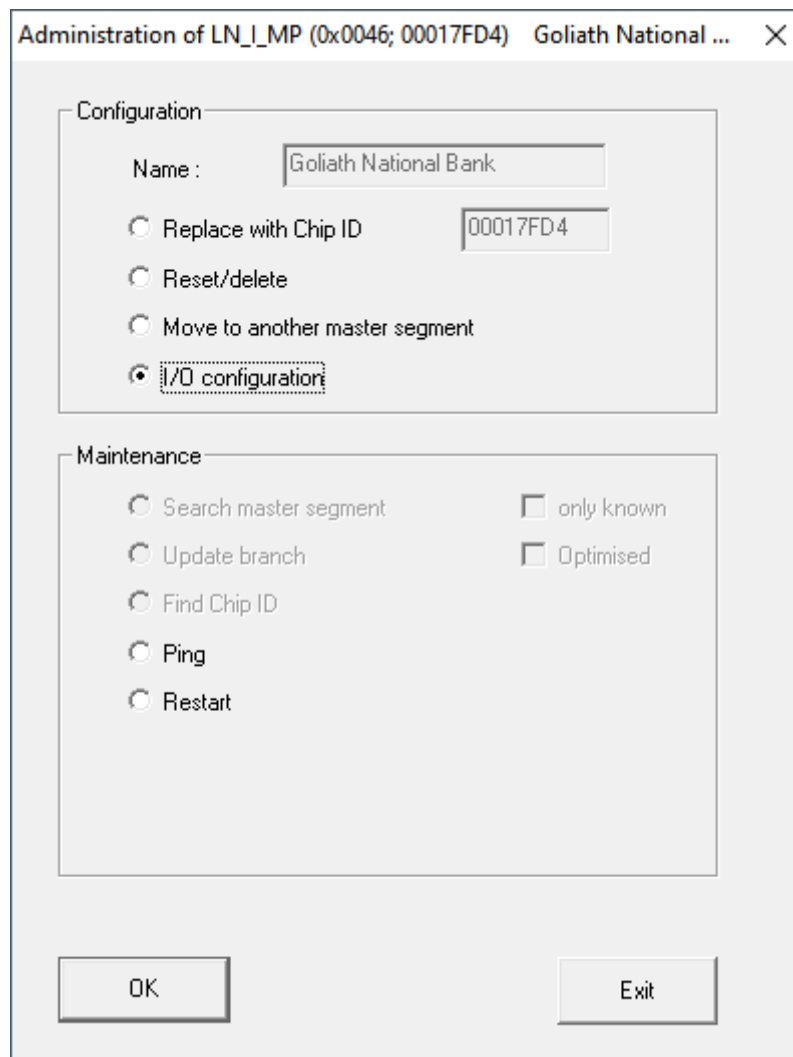
4.2.1.4 Possible states RouterNode 2 / GatewayNode 2

- ▣ Input active/inactive
- ▣ Analogue voltage input above/below threshold

4.2.2 Incorporating a DoorMonitoring lock into the network

This is how you incorporate a DM lock into the WaveNet network:

- ✓ WaveNet-Manager has already been set up.
 - ✓ RouterNode, to which the new lock shall be assigned to, is already set up and "online".
 - ✓ LockNode is correctly mounted on the DM lock.
 - ✓ Chip-ID is known.
1. Start WaveNet-Manager (LSM - | Network | - **WaveNet Manager**).
 2. Right-click the RouterNode.
 - ↳ Window "Administration" opens.
 3. Markieren Sie die Option ☒ Find Chip ID.
 4. Click on the **OK** button.
 - ↳ Window "Administration" closes.
 5. Follow the shown dialogue and assign the lock respectively the corresponding LockNode with its Chip-ID to the RouterNode 2.
 6. Right-click the DM-LockNode which you just added.
 7. Select the Option ☒ I/O configuration.
 8. Click on the **OK** button.
 - ↳ Window "Administration" opens.



9. Mark the check box ☒ Send all events to I/O router.
10. Click on the **OK** button.
 - ➔ Window "Administration" closes.
11. Click on the button **SAVE**.
12. Click on the **Exit** button.
13. Click on the **Yes** button.
 - ➔ WaveNet manager closes.
14. Import the new settings and assign them to the corresponding communication node.

4.2.3 DoorMonitoring SmartHandle

In the LSM or in Smart.Surveil you can monitor your DoorMonitoring SmartHandles. To do this, however, you first have to configure the DoorMonitoring SmartHandles in LSM:

- ✓ LSM open.
 - ✓ Matrix screen open
1. Double-click on the DM-SmartHandle to open the settings.

2. Change to tab [Configuration/Data].
3. Click on the button **Monitoring configuration**.
 ↳ The window "Door Monitoring Configuration" opens.

4. Activate in the area "Target"-"Events" in the areas "Logging in the access list" and "Transmission in the network" the DoorMonitoring events that you would like to monitor (e.g. ☒ "Door open" events, ☒ Lock bolt events and ☒ Door handel sensor events).
5. If necessary, make further DoorMonitoring settings, e.g. in the area "Door open settings".
6. Click on the **OK** button.
 ↳ The window "Door Monitoring Configuration" closes.
7. Click on the **Apply** button.
8. Programme the SmartHandle.
 ↳ DoorMonitoring events are stored in the LSM database and can be evaluated by LSM and SmartSurveil.

4.2.3.1 Sabotage detection

From LSM 3.4 SP2 you can recognise sabotage attempts on the SmartHandle AX and on the SmartRelais 3 Advanced. When the enclosure used there is opened, the electronics detect this and send the information to LSM. If you want to evaluate the information, you can set up an event for it and respond to it (see *Setting up event management* [▶ 66]).

4.2.3.2 DoorMonitoring (SmartHandle) - Door handle events

From LSM 3.5 SP3 onwards, you can see the state of the handle on the SmartHandle AX. When the trigger is pressed, the electronics detect this and send the information to LSM. If you want to evaluate the information, you can set up an event for it and then respond to it (see ([Setting up event management \[► 66\]](#))).

4.2.4 DoorMonitoring cylinder

In the LSM or in Smart.Surveil, you can monitor your DoorMonitoring cylinders. To do this, however, you first have to configure the DoorMonitoring cylinders in LSM:

- ✓ LSM open.
 - ✓ Matrix screen open
1. Double-click on the DM-cylinder to open the settings.
 2. Change to tab [Configuration/Data].
 3. Click on the button **Monitoring configuration**.
 - ➔ The window "Door Monitoring Configuration" opens.

4. Activate in the area "Target"- "Events" in the areas "Logging in the access list" and "Transmission in the network" the DoorMonitoring events that you would like to monitor (e.g. ☒ "Door open" events).
5. If necessary, make further DoorMonitoring settings, e.g. in the area "Door open settings".

6. Click on the **OK** button.
 - ↳ The window "Door Monitoring Configuration" closes.
7. Click on the **Apply** button.
8. Programme the cylinder
 - ↳ DoorMonitoring events are stored in the LSM database and can be evaluated by LSM and SmartSurveil.

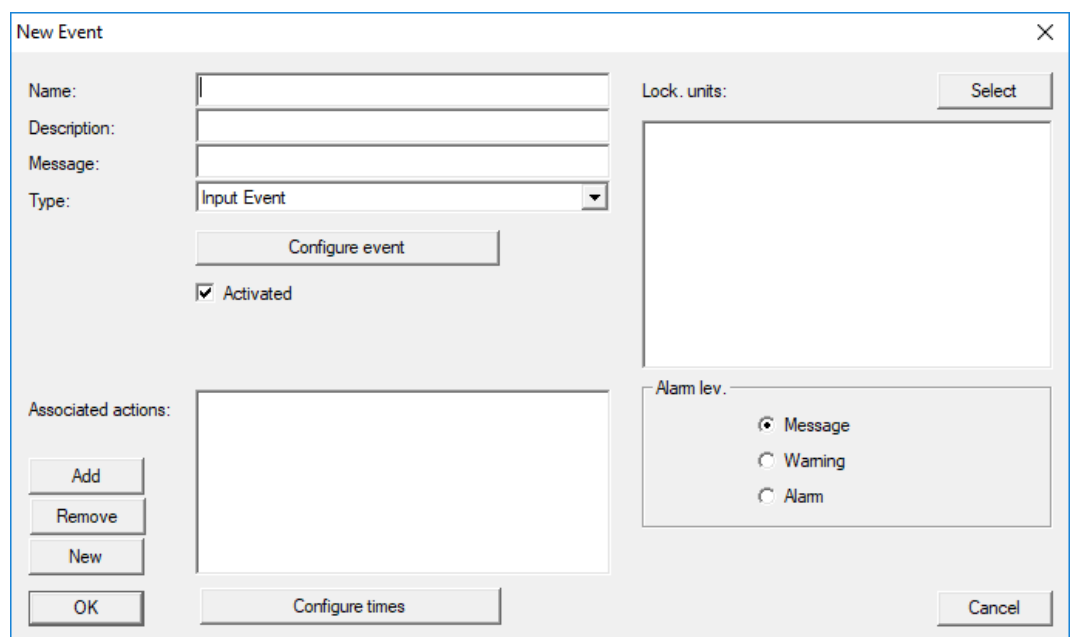
4.2.5 Evaluating controller inputs

The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

Adding an event

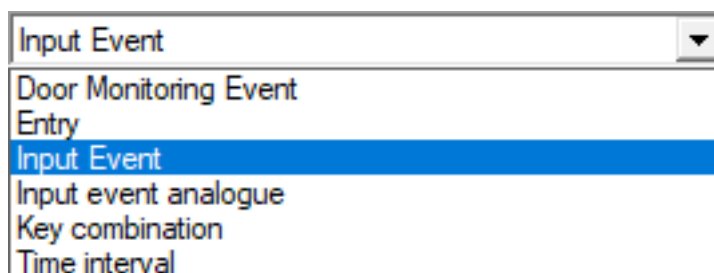
If you wish to use LSM or SmartSurveil (see SmartSurveil) to evaluate an input, you first need to create the corresponding input as an event in LSM. Only then will changes to the input also be saved in the LSM database.

- ✓ LSM open.
 - ✓ SREL3 ADV System added to the matrix.
1. Use | Network | to select the **Event manager** item.
 - ↳ The "Network event manager" window will open.
 2. Click on the **New** button.
 - ↳ The "New Event" window will open.

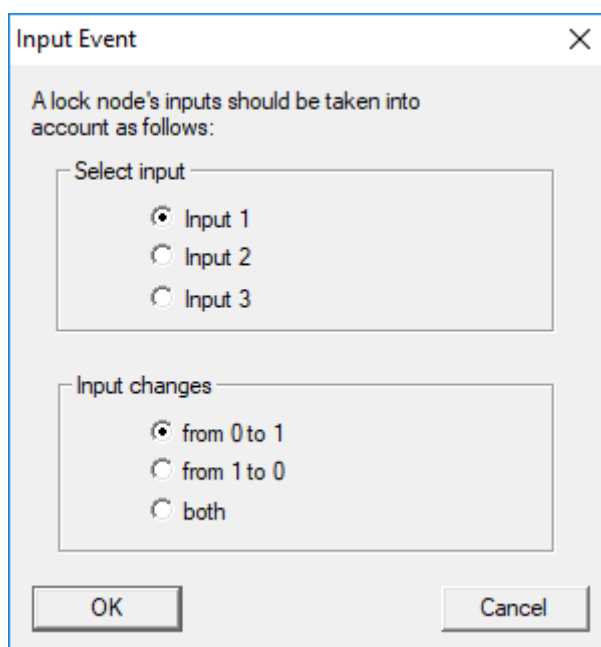


3. Enter a suitable name for the event.
4. Enter an optional description for the event.
5. Enter an optional message.
6. Open the ▼ **Type** drop-down menu.

7. Select the "Input Event" item.



8. Click on the **Configure event** button.
→ The "Input Event" window will open.



9. Select the required input in the "Select input" section.
10. Select the status change that the event should trigger in the "Input changes" section.
11. Click on the **OK** button.
12. Click on the **Select** button to assign a locking device to the event.
→ The "Administration" window will open.
13. Highlight one or more locking devices.
14. Click on the **Add** button.
15. Click on the **OK** button.
→ Window closes.
→ Locking device is assigned to the event.
16. You can use the **New** or **Add** button to assign an action if you wish to configure an action.
17. Click on the **OK** button.
→ Window closes.

- ↳ Event is displayed in the "Events" section.
- 18. Click on the **Exit** button.
 - ↳ Window closes.
- ↳ Input is added as an event and triggers an action.

4.2.6 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transmit" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "Exit" button to close the dialogue.

4.2.7 Assigning a locking device's LockNode

The initialized LockNode needs to be linked to a locking device. This is easiest to do using a collective command, particularly if there is more than one LockNode:

1. Select "Network/Collective commands/WaveNet nodes".
2. Select all LockNodes (*WNNode_xxxx*) which have not been assigned yet. *Non-assigned LockNodes have no entry in the "Door" column.*
3. Click on the "Configure automatically" button.
 - ↳ The automatic configuration will start immediately.
4. Click on the "Exit" button to close the dialogue.

4.2.8 Activating the locking device's input events

You need to make additional settings to ensure that door statuses are displayed correctly in the LSM software:

1. Selecting "Network/Collective commands/WaveNet nodes"
2. Select the DoorMonitoring cylinder (*or any locking cylinder which is to relay events*).
3. Click on the "Activate input events" button.
 - ↳ Programming is started immediately.
4. Click on the "Exit" button as soon as all locking devices have been programmed.

4.3 Setting up a RingCast

The description below tells you how to configure a RingCast. A RingCast allows a RouterNode2 input event to be relayed to other RouterNode2s in the same WaveNet radio network at the same time. In this example, an emergency release is to be implemented on locking devices. All connected

locking devices should open as soon as a fire alarm system triggers Input 1 on a RouterNode2. Each locking device will then remain open until they receive an explicit remote opening command.

Obviously, a RingCast can also be used to perform other tasks such a block lock function, remote opening and gunman attack function.

This example requires a configured WaveNet radio network with two RouterNode2s. A locking device is connected to each RouterNode2. All locking devices should be opened immediately as soon as Input 1 on a RouterNode2 is actuated briefly. This gives people access to all rooms, so that they can seek protection from fire or smoke.



NOTE

If RouterNode2s are networked using Ethernet, RingCast is only supported by models which were supplied from about 2017. A RouterNode2 tries to establish an Ethernet connection to another RouterNode2 but fails. It then tries to establish the new connection wirelessly. The radio communication range is up to 30 m. This depends on the surroundings, so it cannot be guaranteed.

4.3.1 Preparing RouterNode for RingCast



NOTE

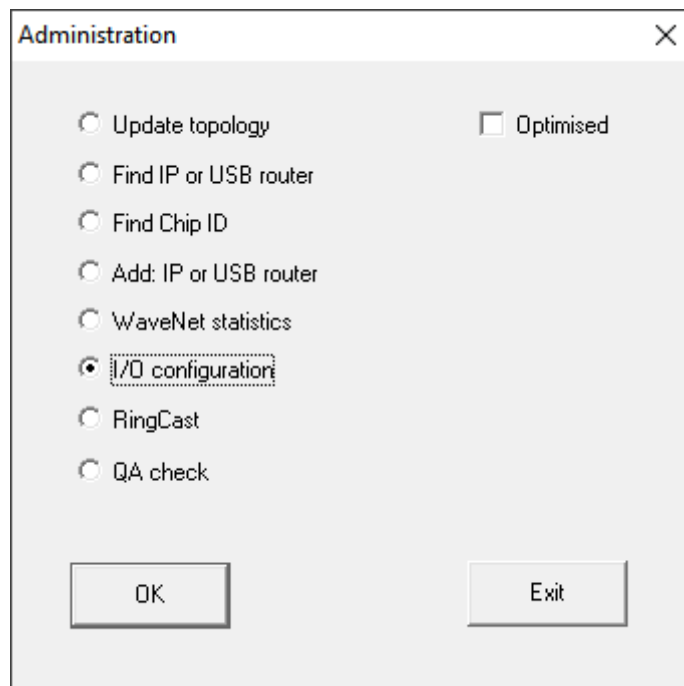
Firmware dependent availability of RingCast for RouterNodes

RingCast support is firmware dependent (see Firmware information).

- If necessary, update the firmware (see Updating firmware).

Prepare the RouterNodes for the RingCast:

- ✓ In the Wavenet radio network, at least two different RingCast-capable RouterNodes are configured and "online" (see Firmware information).
 - ✓ At least one locking device is assigned to each RouterNode of the planned RingCast. Both locking devices are "online".
1. Open the WaveNet Manager.
 2. Right-click on the first RouterNode 2.
 - ➔ Window "Administration" opens.



3. Select the option ☒ I/O configuration.
4. Click on the button **OK**.
 - ➔ Window "Administration" closes.
 - ➔ Window "I/O configuration" opens.
5. Optional: For example, for ▼ **Output** 1 "Input receipt static", to be able to control a signal device during deactivation.
6. In the drop-down menu ▼ **Input** select the desired entry of the corresponding response (see RouterNode: Digital input).
7. In the drop-down menu ▼ **Delay [s]** select the entry "RingCast".
8. Click on the button **Select LN**.
9. Check whether all required LockNodes are selected. (*When the I/O configuration of the router is set up for the first time, all LockNodes are included.*)
10. Select your protocol generation from the drop-down menu ▼ **Protocol generation**



NOTE

Protocol generation in the LSM

The log generation is displayed in the LSM in the locking system properties on the tab page [Name] in the area "Protocol generation".

11. Enter the locking system password.
12. Click on the **OK** button.
13. Make the same settings on the other RouterNodes 2 as well.

4.3.2 Adding a RingCast

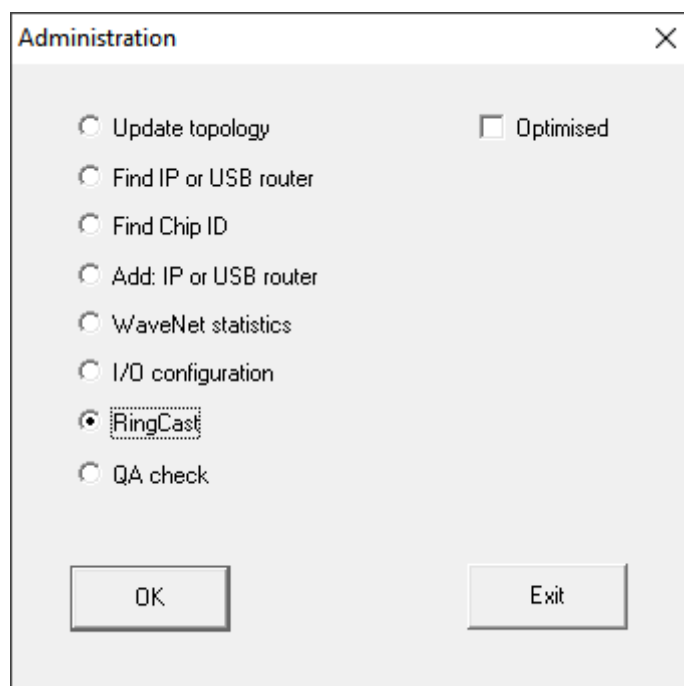


NOTE

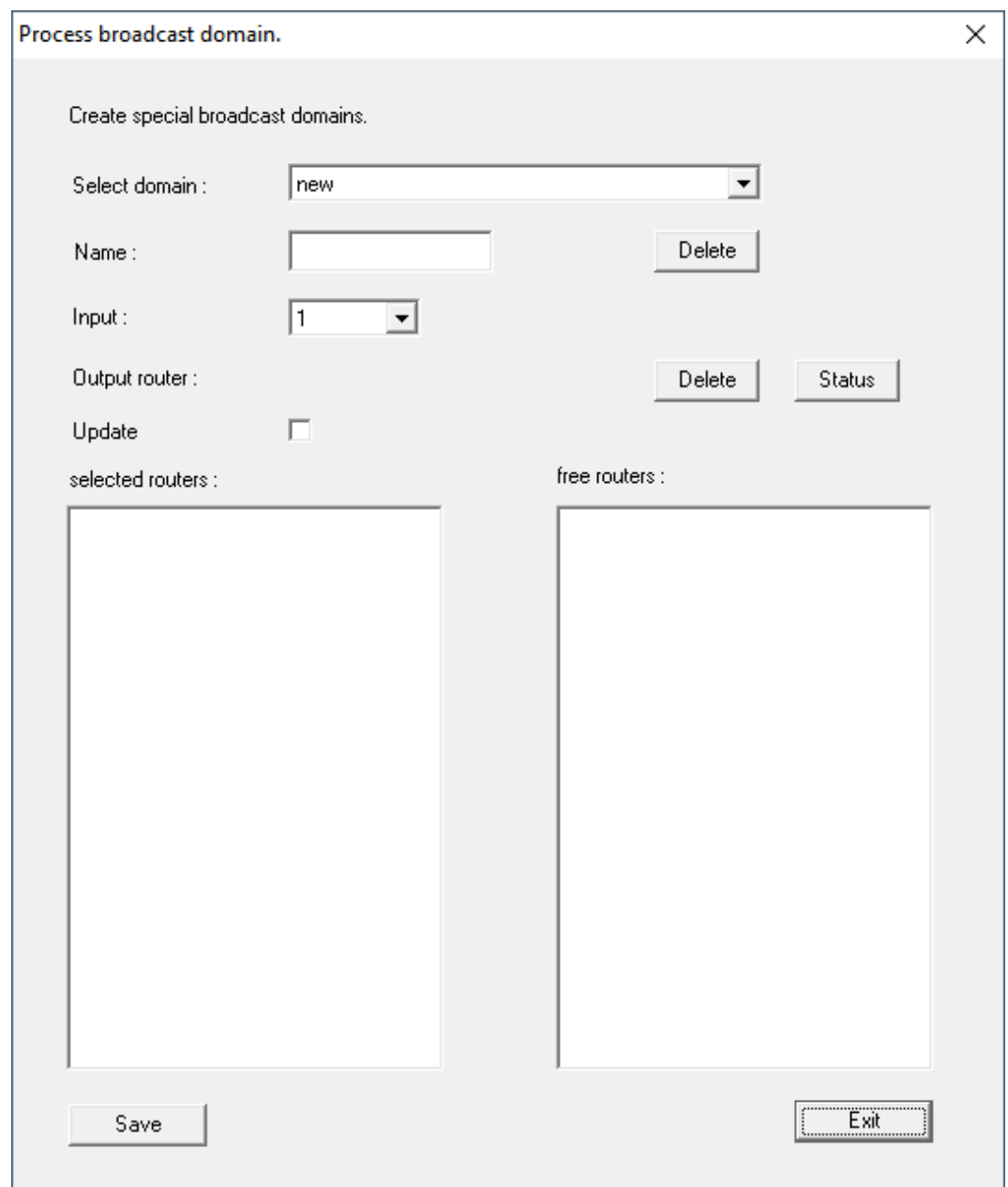
Recalculating the RingCast

If you replace or delete a RouterNode in the RingCast or change its RingCast-relevant IO configuration, the RingCast is automatically recalculated after saving the changes and confirming the request.

- ✓ WaveNet Manager opened via LSM (see Best Practice: From the LSM software)
 - ✓ RouterNodes and LockNodes connected to power.
 - ✓ RouterNodes and LockNodes imported into WaveNet topology (see Finding and adding devices).
 - ✓ RouterNodes for RingCast prepared (see *Preparing RouterNode for RingCast* [▶ 58]).
1. Right-click on the WaveNet XX_X entry.
 - ↳ The window "Administration" opens.



2. Select the option ☒ RingCast.
3. Click on the button **OK**.
 - ↳ The "Administration" window closes.
 - ↳ The window "Edit radio domains" opens.



4. In the dropdown menu ▼ **Select domain** select an input for which in ▼ **Delay [s]** you have selected "RingCast".



- In the field "selected routers" all RouterNode2 appear for which at the beginning at ▼ **Delay [s]** you have selected the input "RingCast" (=Domain).

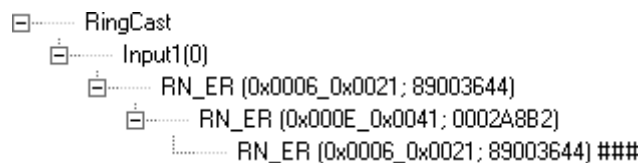
The dialog box titled "Process broadcast domain." contains the following elements:

- Create special broadcast domains.**
- Select domain :** A dropdown menu with "Input1" selected.
- Name :** A text field containing "Input1" and a "Delete" button.
- Input :** A dropdown menu with "1" selected.
- Output router :** A text field containing "0x5530" and "Delete" and "Status" buttons.
- Update** checkbox, which is checked.
- selected routers :** A list box containing two entries: "RN_ER (0x0006_0x0021; 89003644)" and "RN_ER (0x000A_0x0041; 890068C4)".
- free routers :** An empty list box.
- Save** and **Exit** buttons at the bottom.

5. Click the button **Save**.
6. Click the button **Exit**.
 - ↳ The "Edit radio domains" window closes.
 - ↳ The window "WaveNetManager" opens.

The dialog box titled "WaveNetManager" displays a question mark icon and the text: "Changes have been made. Do you want to update the broadcast domain?". At the bottom, there are two buttons: "Ja" (Yes) and "Nein" (No).

7. Click on the button **Yes**.
 - ↳ The "WaveNetManager" window closes.
 - ↳ Changes will be updated.
- ↳ The RingCast is created and will be visible in the WaveNet Manager after a short time.



Save the new settings and exit the WaveNet Manager.

4.3.3 RingCast function test

The RingCast has no self-test function.



WARNING

Impairment or failure of protective functions due to changed conditions

The activation of the protection functions in RingCast is based on wireless connections and Ethernet connections. Wireless connections in particular can be affected by changing environmental conditions (see Radio network und Challenges in wireless networks). This also influences the activation of the protective functions in the RingCast and can jeopardise the safety of persons and property that are additionally protected by the protective functions in the RingCast, for example.

1. Test the protective functions at least once a month (see [RingCast function test \[▶ 63\]](#)).
2. If necessary, also observe other guidelines or regulations that are relevant for your locking system (especially for escape and rescue routes and fire protection. You are solely responsible for ensuring compliance with these guidelines and regulations).

Change in the sequence of emergency functions due to malfunctions

SimonsVoss and "Made in Germany" stand for maximum safety and reliability. In individual cases, however, malfunctions of your devices cannot be ruled out. This may pose a risk to the safety of persons and property, which are additionally protected by the protective functions in the RingCast.

1. You should test your devices at least once a month (see Device function test Shorter intervals may also be required according to other regulations concerning your overall system).
2. Test the protective functions at least once a month (see [RingCast function test \[▶ 63\]](#)).

Switch the corresponding input on the initiator and check:

- whether the locks react as desired (see also RouterNode: Digital input).

- whether the output set on the RouterNode shows the acknowledgement by switching as desired (see also RouterNode: Digital output).

Test with central output router



NOTE

Central output router in RingCast with R/CR router nodes

The central output router receives the input acknowledgement of the participating router nodes exclusively via an Ethernet connection. The central output router therefore ignores the status of router nodes that are not Ethernet router nodes (.ER). If you are using the central output router and your RingCast also contains router nodes without an Ethernet interface, the central output router's input acknowledgement only means that all locking devices assigned to an Ethernet router node have received the command.

- Check the status of other router nodes (R/CR) independently of the central output router manually (see Test reachability (LSM) and RouterNodes or IO Status and LockNode responsiveness).

The use of a central output router (see Central output router) simplifies the test of the RingCast considerably. Switch the corresponding input at the initiator and check whether the central output router sends an input acknowledgement or switches the corresponding output. If the output does not switch, then check which RouterNodes have caused problems:

- ✓ WaveNet Manager opened via LSM (see Best Practice: From the LSM software)
1. Click with the right mouse button on the RingCast entry you want to test.
 2. In the drop-down menu ▼ **Select domain** select the input whose RingCast you want to test.
 - ↳ The window "Edit radio domains" opens.

Process broadcast domain. ✕

Create special broadcast domains.

Select domain :

Name : Delete

Input :

Output router : Delete Status

Update ☒

selected routers :

RN_ER (0x0006_0x0021; 89003644)
RN_ER (0x000A_0x0041; 89006BC4)


free routers :

Save Exit

3. Click on the button **Status**.


→ RingCast is tested.

WaveNetManager ✕

 **The test was successful.**


OK

WaveNetManager ✕

 Router RN_ER (0x0006_0x0021; 89003644) not available !

OK

WaveNetManager ✕

 Am Router RN_ER (0x000A_0x0041; 89006BC4) konnten folgende LNs
LN_I_MP (0x0046; 00017FD4)
nicht erreicht werden.

OK

<p>The RingCast was able to address all locking devices.</p>	<p>The RingCast could not be closed. Possible causes (see also Central output router):</p> <ul style="list-style-type: none"> ■ One or more RouterNodes have not received the data packet. ■ One or more RouterNodes have not reached one or more LockNodes. ■ Ethernet connection to one or more RouterNodes is interrupted. The RouterNodes could have received the data packet wirelessly, but could no longer return their input acknowledgements due to the interrupted Ethernet connection. <ol style="list-style-type: none"> 1. Check the reachability of the RouterNodes mentioned (see RouterNodes und Test reachability (LSM)). 2. Check the reachability of the LockNodes (see LockNodes und Test reachability (LSM)). 3. Check the last responses of the LockNodes (see IO Status and LockNode responsiveness).
--	--

4.4 Setting up event management

Networking locking devices via a RouterNode2 brings many advantages. One decisive advantage is the permanent communication between the RouterNode2 and the locking device.

In this example, a pre-defined email is to be sent from the LSM software as soon as a transponder is activated on a specified locking device at night.

The following prerequisites need to be fulfilled for this requirement:

- A WaveNet radio network is set up as in the example *Creating a WaveNet radio network and incorporating a locking device* [► 46].
- Forwarding of locking device events has also been activated as in *Activating the locking device's input events* [► 57].

4.4.1 Setting up an email server

A rudimentary email client is set up to send emails in the LSM software. An own email account which supports SMTP format is required to forward emails.

1. Select "Network/Email notifications"
2. Click on the "Email" button.
3. Enter all SMTP settings for your email provider.
4. Click on the "OK" button.
5. Click on the "OK" button.

4.4.2 Setting up Task services

1. Select "Network/Task manager".
2. Select your communication node under Task services.
3. Click on the "Apply" button.
4. Click on the "Finish" button.

4.4.3 Forwarding input events via the RouterNode2

If events (*e.g. a transponder makes a booking on a networked locking device*) are to be forwarded to the CommNode server via the RouterNode2, this function needs to be activated in the router's I/O configuration.

1. Open WaveNet Manager.
2. Right-click the router and select "I/O configuration".
3. Select the "All LN events" option in the "Report events to management system" drop-down list.
4. Press OK to confirm and exit WaveNet Manager.

4.4.4 Forward input events via the SREL3 ADV system

The SREL3 ADV system allows input entries to be forwarded to LSM.

4.4.4.1 Evaluating controller inputs

The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

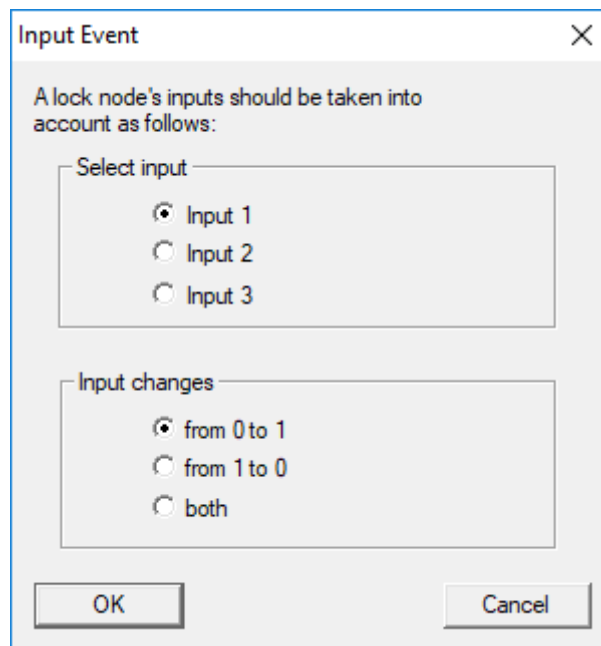
Adding an event

If you wish to use LSM or SmartSurveil (see SmartSurveil) to evaluate an input, you first need to create the corresponding input as an event in LSM. Only then will changes to the input also be saved in the LSM database.

- ✓ LSM open.
- ✓ SREL3 ADV System added to the matrix.
- 1. Use | Network | to select the **Event manager** item.
 - ↳ The "Network event manager" window will open.
- 2. Click on the **New** button.
 - ↳ The "New Event" window will open.

- 3. Enter a suitable name for the event.
- 4. Enter an optional description for the event.
- 5. Enter an optional message.
- 6. Open the ▼ **Type** drop-down menu.
- 7. Select the "Input Event" item.

- 8. Click on the **Configure event** button.
 - ↳ The "Input Event" window will open.



9. Select the required input in the "Select input" section.
10. Select the status change that the event should trigger in the "Input changes" section.
11. Click on the **OK** button.
12. Click on the **Select** button to assign a locking device to the event.
 - ↳ The "Administration" window will open.
13. Highlight one or more locking devices.
14. Click on the **Add** button.
15. Click on the **OK** button.
 - ↳ Window closes.
 - ↳ Locking device is assigned to the event.
16. You can use the **New** or **Add** button to assign an action if you wish to configure an action.
17. Click on the **OK** button.
 - ↳ Window closes.
 - ↳ Event is displayed in the "Events" section.
18. Click on the **Exit** button.
 - ↳ Window closes.
- ↳ Input is added as an event and triggers an action.

4.4.5 Creating a response

First create a response. This response can be selected at a later stage if a specific scenario arises.

1. Select "Network/Event manager".
2. Click on the "New" button under "Responses" on the right-hand side.
3. Add a name and description for the response.

4. Select "Email" as the type.
5. Click on the "Configure response" button.
6. Click on the "New" button.
7. Enter the recipient's email address, a subject and a message body. *You can use the "Test" button to test the email configuration immediately.*
8. Exit the dialogue by pressing the "OK" button three times. Press the "Exit" to return to the matrix.

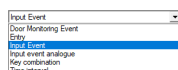
4.4.6 Creating an event

Once a response has been created, you can then go on to create an event.

1. Select "Network/Event manager".
2. Click on the "New" button under "Events" on the left-hand side.
3. Add a name and description for the response.
4. Select "Access" as the type.
5. Click on the "Configure event" button.
6. Activate the "Respond to all transponders" check box. *The event is to occur every time that a transponder is activated. Alternatively, you can restrict the event to a single transponder.*
7. You can adjust the action further in the "Time setting" section.
8. Click on the "OK" button.
9. Click on the "Select" button in the "Locking devices" section.
10. Add all locking devices which are to trigger the event when the transponder is activated and press OK to confirm your selection.
11. Click on the "Add" button in the "Associated actions" section.
12. Add the previously created response.
13. Click on the "Configure time" button.
14. Enter the night hour times. The event only becomes active within the pre-determined time frame here.
15. Exit the dialogue by pressing the "OK" button three times. Press the "Exit" to return to the matrix.

4.4.6.1 Possible door events

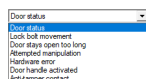
In the window "New Event" can be found in the drop-down menu ▼ Type different events available.



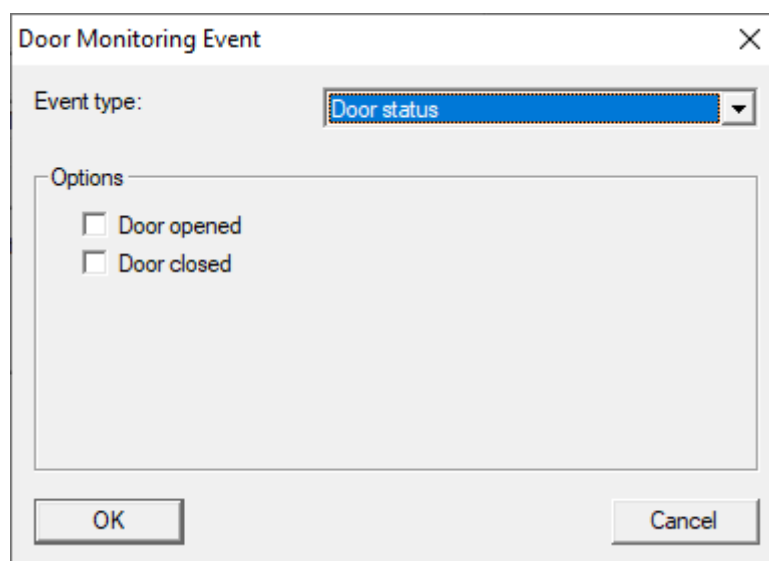
You need a DoorMonitoring-capable locking device (DM) for DoorMonitoring events.

Door monitoring event type

The following DoorMonitoring events are available to you:



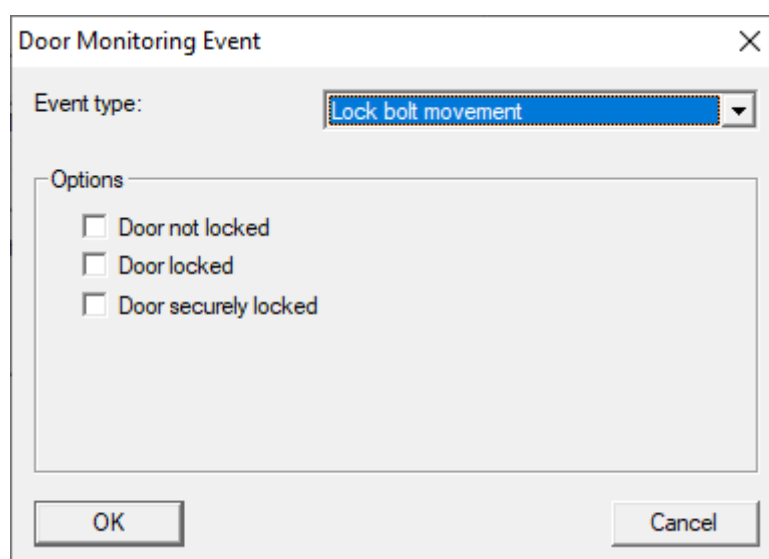
Door status

A screenshot of a dialog box titled 'Door Monitoring Event'. It has a close button (X) in the top right corner. Below the title bar, there is a label 'Event type:' followed by a dropdown menu. The dropdown menu is open, and 'Door status' is selected and highlighted in blue. Below this, there is a section titled 'Options' which contains two checkboxes: 'Door opened' and 'Door closed'. Both checkboxes are currently unchecked. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

The following states can be detected. A check mark triggers the event as soon as the condition occurs:

- ☒ Door open
- ☒ Door closed

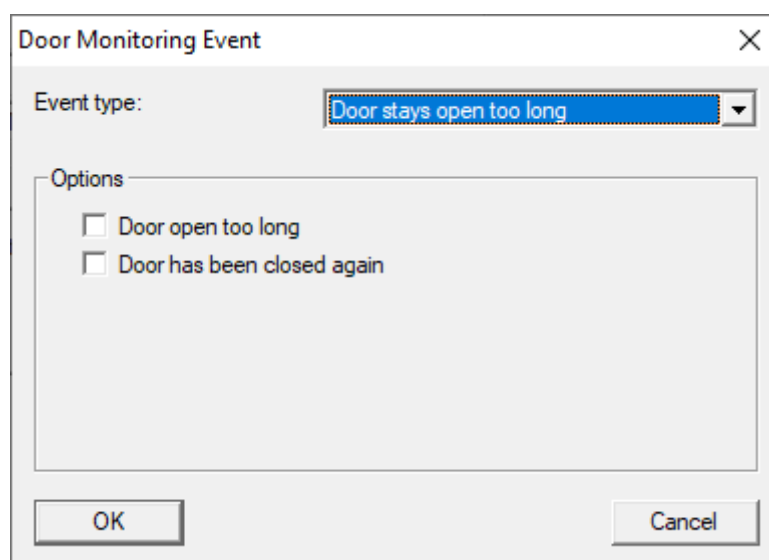
Lock bolt movement

A screenshot of a dialog box titled 'Door Monitoring Event'. It has a close button (X) in the top right corner. Below the title bar, there is a label 'Event type:' followed by a dropdown menu. The dropdown menu is open, and 'Lock bolt movement' is selected and highlighted in blue. Below this, there is a section titled 'Options' which contains three checkboxes: 'Door not locked', 'Door locked', and 'Door securely locked'. All three checkboxes are currently unchecked. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

The following states can be detected. A check mark triggers the event as soon as the condition occurs:

- ☒ Door not locked
- ☒ Door locked
- ☒ Door securely locked

Door stays open too long

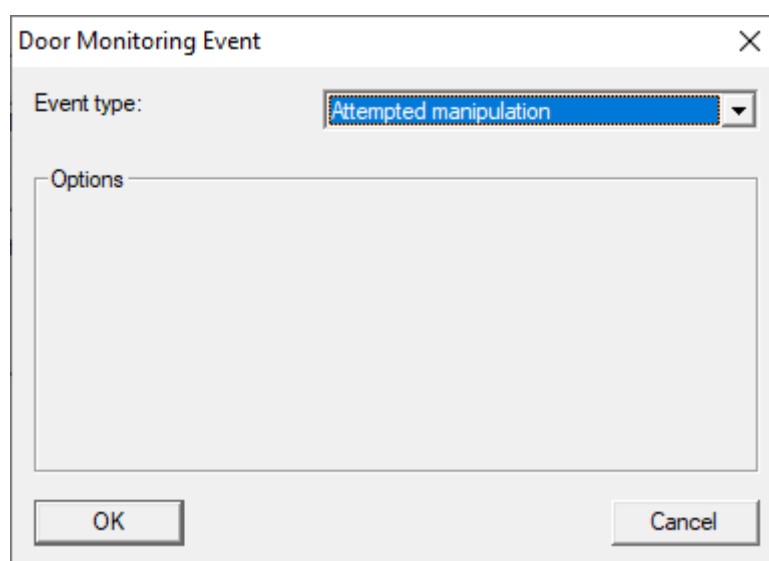


The dialog box is titled "Door Monitoring Event" and has a close button (X) in the top right corner. It contains a label "Event type:" followed by a dropdown menu showing "Door stays open too long". Below this is a section labeled "Options" containing two checkboxes: "Door open too long" and "Door has been closed again", both of which are unchecked. At the bottom are "OK" and "Cancel" buttons.

The following states can be detected. A check mark triggers the event as soon as the condition occurs:

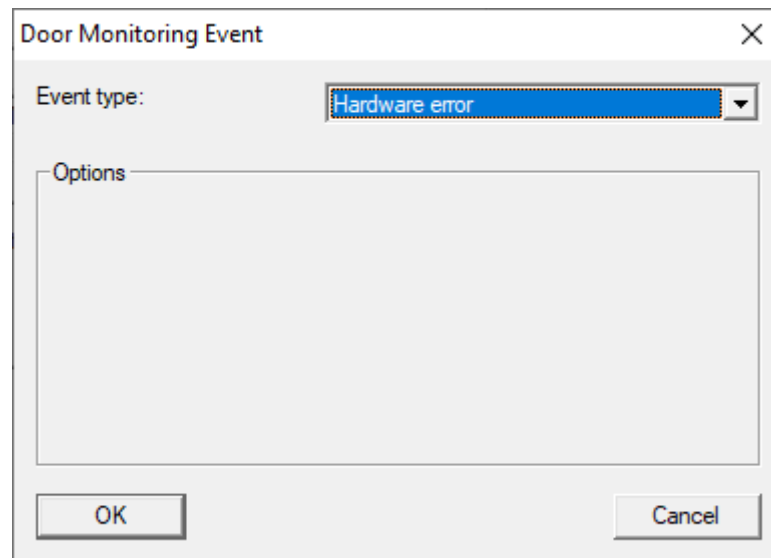
- ☒ Door open too long
- ☒ Door closed again

Attempted manipulation



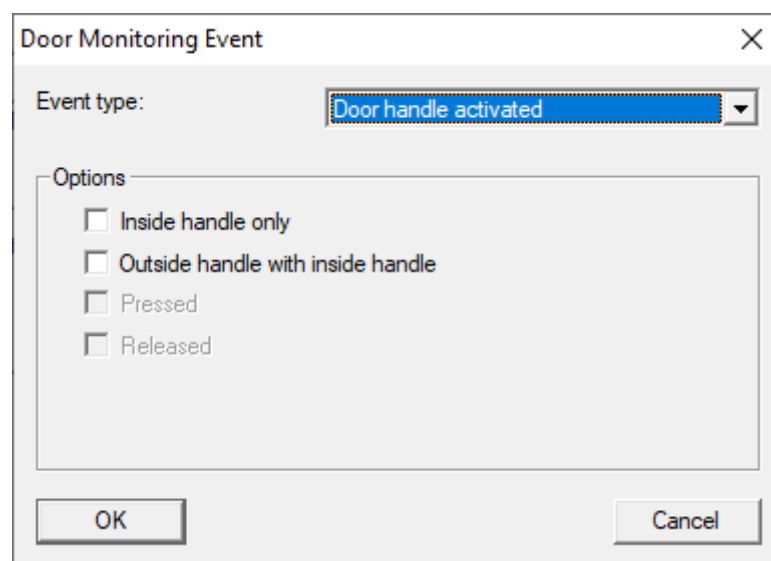
The dialog box is titled "Door Monitoring Event" and has a close button (X) in the top right corner. It contains a label "Event type:" followed by a dropdown menu showing "Attempted manipulation". Below this is a section labeled "Options" which is currently empty. At the bottom are "OK" and "Cancel" buttons.

Hardware error



The dialog box is titled "Door Monitoring Event" and has a close button (X) in the top right corner. It contains a label "Event type:" followed by a dropdown menu showing "Hardware error". Below this is a large empty rectangular area labeled "Options". At the bottom are "OK" and "Cancel" buttons.

Door handle activated

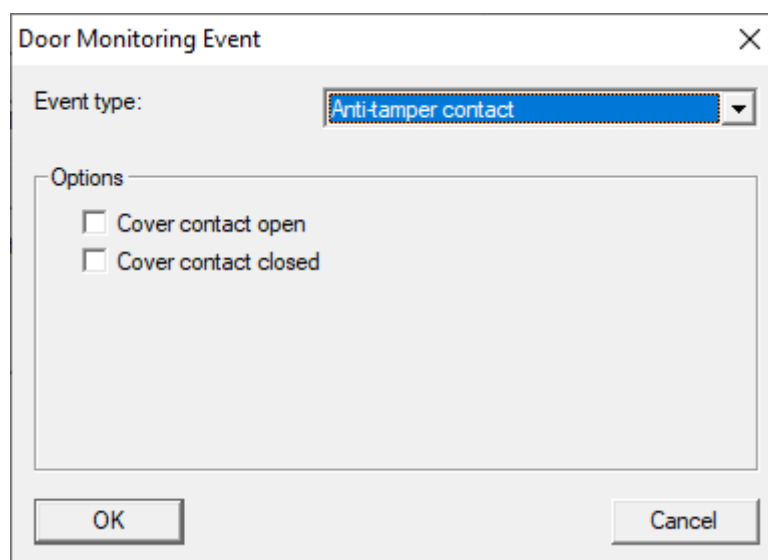


The dialog box is titled "Door Monitoring Event" and has a close button (X) in the top right corner. It contains a label "Event type:" followed by a dropdown menu showing "Door handle activated". Below this is a rectangular area labeled "Options" containing four checkboxes: "Inside handle only", "Outside handle with inside handle", "Pressed", and "Released". At the bottom are "OK" and "Cancel" buttons.

The following states can be detected. A check mark triggers the event as soon as the condition occurs:

- ☒ Inside handle only
- ☒ Outside handle with inside handle
- ☒ Pressed
- ☒ Released

Anti-tamper contact



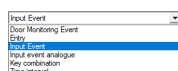
The 'Door Monitoring Event' dialog box features a title bar with a close button. It contains an 'Event type:' label followed by a dropdown menu currently showing 'Anti-tamper contact'. Below this is an 'Options' section with two unchecked checkboxes: 'Cover contact open' and 'Cover contact closed'. At the bottom are 'OK' and 'Cancel' buttons.

The following states can be detected. A check mark triggers the event as soon as the condition occurs:

- ☒ Cover contact open
- ☒ Cover contact closed

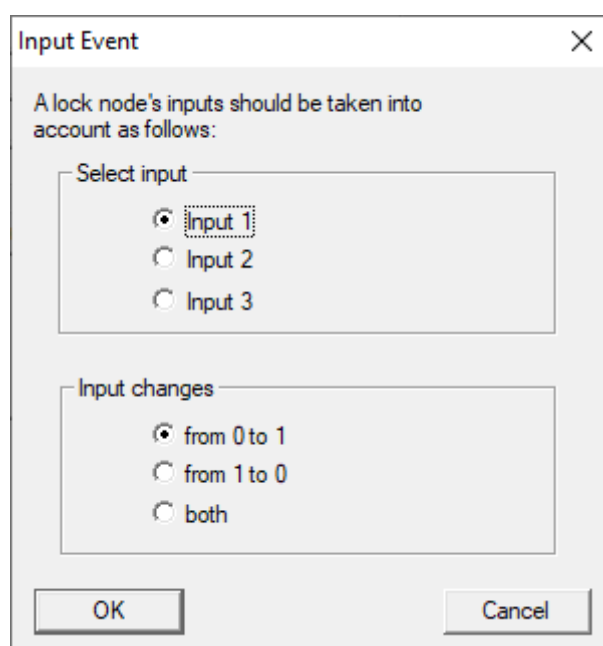
Default Events

The following standard events are available:



A small dropdown menu with the title 'Input Event'. The list of options includes 'Door Monitoring Event', 'Entry', 'Input Event' (which is highlighted), 'Input event analogue', 'Key combination', and 'Time interval'.

Input Event

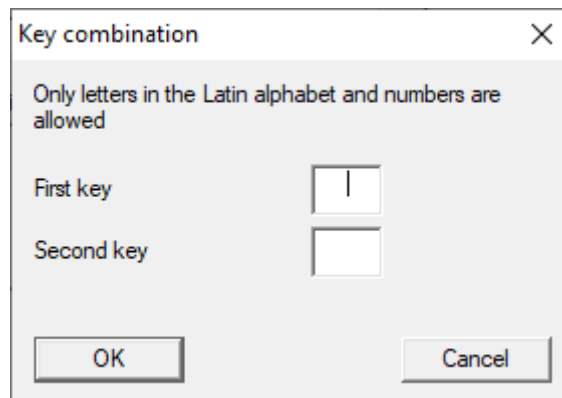


The 'Input Event' dialog box has a title bar with a close button. It begins with the text 'A lock node's inputs should be taken into account as follows:'. Below this is a 'Select input' section with three radio buttons: 'Input 1' (selected), 'Input 2', and 'Input 3'. The next section is 'Input changes' with three radio buttons: 'from 0 to 1' (selected), 'from 1 to 0', and 'both'. At the bottom are 'OK' and 'Cancel' buttons.

Analog input event

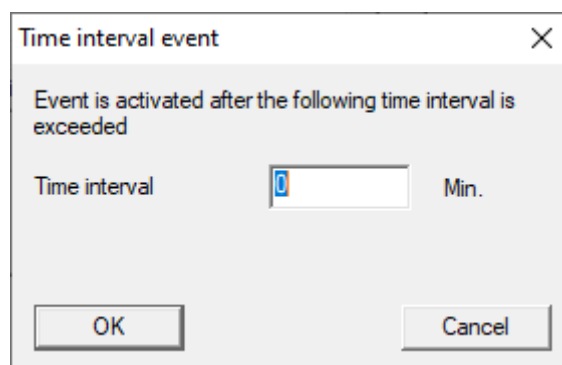
The settings for analog input events are made directly on the respective device (e.g. RouterNode 2).

Key shortcut



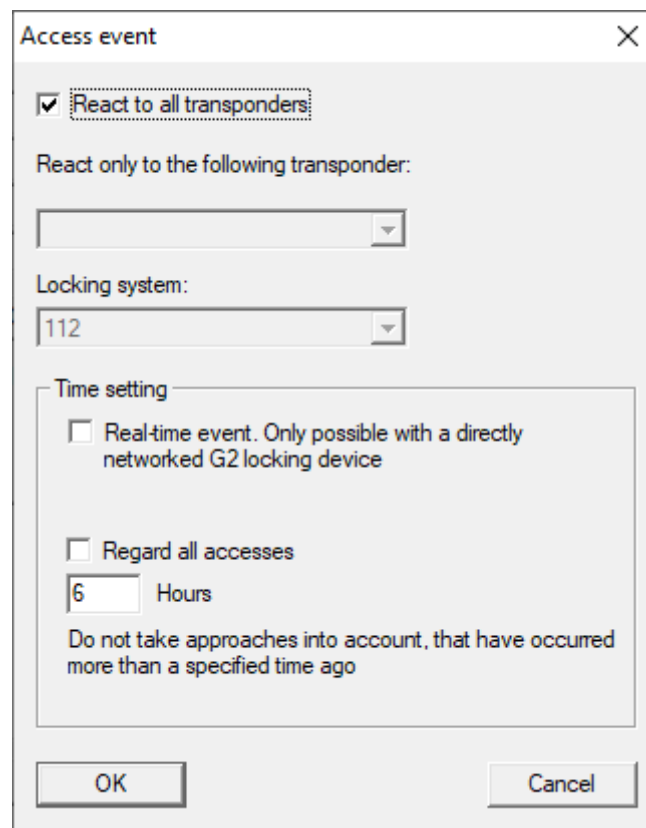
A dialog box titled "Key combination" with a close button (X) in the top right corner. The text inside reads: "Only letters in the Latin alphabet and numbers are allowed". Below this text are two input fields. The first field is labeled "First key" and contains the letter "I". The second field is labeled "Second key" and is currently empty. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Time interval



A dialog box titled "Time interval event" with a close button (X) in the top right corner. The text inside reads: "Event is activated after the following time interval is exceeded". Below this text is a label "Time interval" followed by a text input field containing the number "0". To the right of the input field is the label "Min.". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Access



The 'Access event' dialog box contains the following elements:

- ☒ **React to all transponders:**
- React only to the following transponder:
- Locking system:
- Time setting**
 - ☐ Real-time event. Only possible with a directly networked G2 locking device
 - ☐ Regard all accesses
 - Hours
 - Do not take approaches into account, that have occurred more than a specified time ago
-

4.5 Managing the virtual network (VN)

Authorisations can be networked and quickly changed and adjusted via a virtual network (VN network), even without full networking. Authorisation for locks (and block IDs of blocked identification media) is stored directly in the identification medium and forwarded to a locking device when actuated. It is therefore important to book all identification media at a gateway at regular intervals in virtual networks.

This example shows the basic set-up of a virtual network.

All types of virtual networks require an AV card template when using cards (AV = **A**udit trail / **V**irtual network).

4.5.1 Virtual network with SmartRelay 3 Advanced



NOTE

Increased system requirements for virtual networks with SmartRelais 3 Advanced

The virtual network with VN host server and SmartRelais 3 Advanced is very powerful and places higher demands on the available capacity.

- Note the increased system requirements (see *System requirements* [▶ 7]).

4.5.1.1 Functional principle

It is possible to use the system as a gateway in the virtual network. The controller establishes a connection to the VN host server to do so. The VN host server forwards changed authorisations (programming requirement) and data from the LSM database to the controller. This means that complete, time-consuming loading of the database is no longer required; instead, the controller collects the provided data when an identification medium is detected (pull principle). The entire system is programmed via a single interface – the controller.

The VN host server regularly checks whether there are changes to the LSM database that are to be distributed via the gateway. It also does the reverse and checks whether there is information at the gateway that should be written to the database (see *Check virtual network status* [▶ 82]).

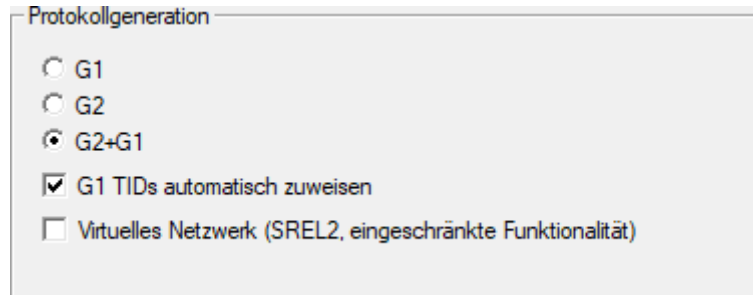
4.5.1.2 Setting up a locking system

No special preparation is required for a virtual network with SmartRelay 3 Advanced.

The ☐ Virtual network (SREL2, limited functions) checkbox must not be activated in the locking system properties.

1. Open the properties of your locking system using | Edit | - **Locking system properties**.
2. Change to the "[Name]" tab.

3. Make sure that the ☐ Virtual network (SREL2, limited functions) check-box is not activated.

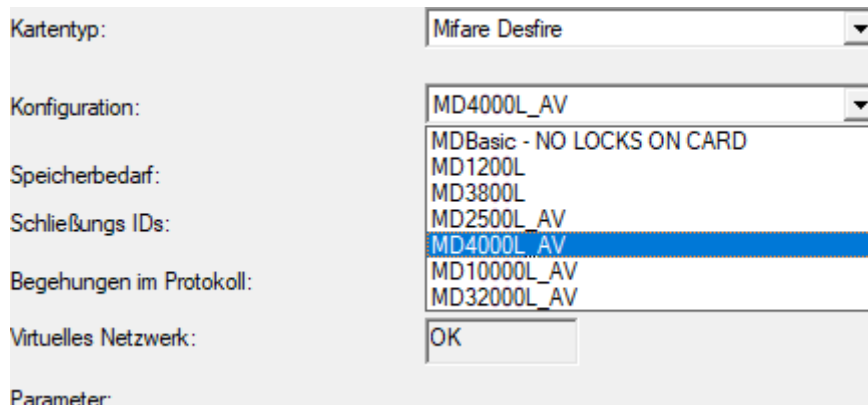


Protokollgeneration

☐ G1
☐ G2
☒ G2+G1

☒ G1 TIDs automatisch zuweisen
☐ Viruelles Netzwerk (SREL2, eingeschränkte Funktionalität)

4. Click on the **Apply** button.
5. If you use cards: select an AV card template from the [G2 card management] tab.



Kartentyp: Mifare Desfire

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

Speicherbedarf:

Schließungs IDs:

Begehungen im Protokoll:

Viruelles Netzwerk: OK

Parameter:

6. Click on the **Apply** button.

4.5.1.3 Setting up the gateway and VN host server

- ✓ Locking system created (see [Setting up a locking system \[► 77\]](#)).
- ✓ SmartRelais 3 Advanced configured and networked (see system manual for SmartRelais 3 Advanced).
- ✓ VN host installed (see VN host).

1. Use | Edit | - **Lock properties** to open the SmartRelais 3 Advanced's properties (alternatively, double click).

2. Change to the "[Configuration/Data]" tab.

Soll

Schließanlagen ID
9215

Schließungs ID
173

Pulslänge 2 Sek.

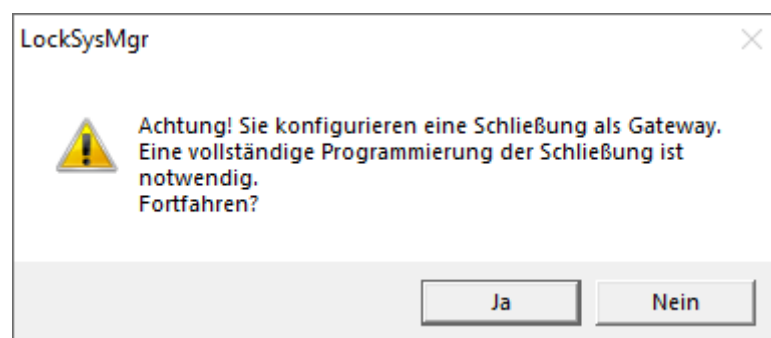
☒ Zugangskontrolle
☐ Zeitzonesteuerung
☒ Unberechtigte Zutrittsversuche protokollieren
☐ Gateway
☐ Flip Flop
☐ Keine Batteriewarnungen
☒ Nahbereichsmodus
☐ Zeitumschaltung
☐ Aktivierungs- bzw. Verfallsdatum ignorieren
☒ Karteninterface

letzte Veränderung

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

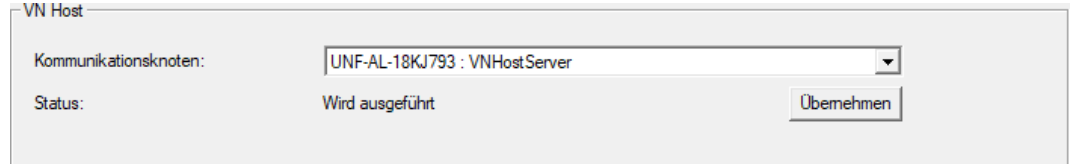
Erweiterte Konfiguration

3. Activate the ☒ Time zone management and ☒ Audit trail checkboxes.
4. Activate the ☒ Gateway check box.
↳ Warning about pending programming will open.



5. Click on the **OK** button.
↳ Warning closes.
6. Click on the **Yes** button.
↳ Programming requirement (flash) is displayed.
7. Authorise all identification media which are to receive new authorisations at the gateway at a later point.
8. Programme the SmartRelais 3 Advanced.
↳ Programming requirement disappears.

9. Use | Network | to select the **Virtual network** input.
↳ The "VN host server" window will open.



10. Make sure that the "VN host server" entry is selected from the ▼ **Communication nodes** drop-down menu in the "VNHost" section.



NOTE

Different communication nodes on the SmartRelais 3 Advanced

The VN host server is always used for the virtual network on the SmartRelais 3 Advanced. However, another communication node can also be used for programming, remote opening and similar.

- ❏ Select the "VN host server" entry for the virtual network even if your SmartRelais 3 Advanced is using another communication node.

11. Click on the **Apply** button.
12. Click on the **OK** button.
↳ "VN host server" window closes.
13. Use | Network | to select the **Communication nodes** input.

14. Switch to the VN host server communication node using the ► and ◀ buttons.

Name: VNHostServer

Rechnername: [empty]

Vollständiger Rechnername: [empty]

IP Port: 6001 [Port suchen]

Beschreibung: [empty]

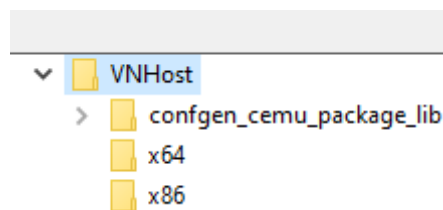
Anschlüsse:

Typ	COM-Port	

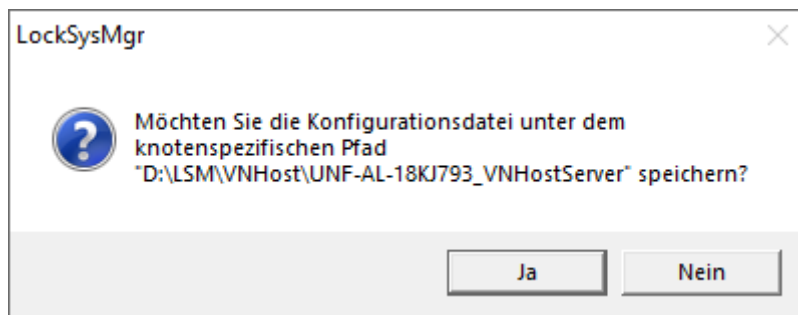
[Ping] [Konfig-Dateien] [Übertragen] [Testen] [Bearbeiten] [Hinzufügen] [Entfernen] [Verschieben]

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

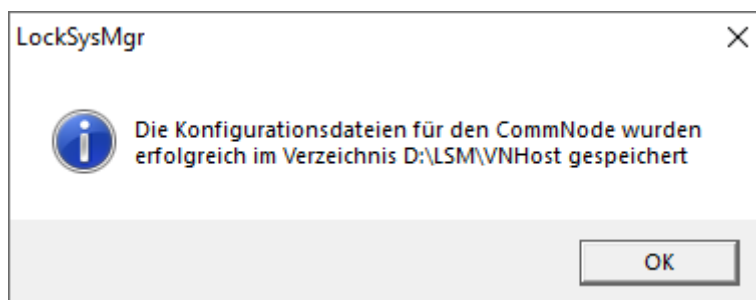
15. Click on the **Config files** button.
- The Explorer window will open.
16. Select the VN host server's installation folder.



17. Click on the **OK** button.
- Explorer window closes.
- The "LockSysMgr" window will open.



18. Click on the **No** button.
↳ Config files are saved.



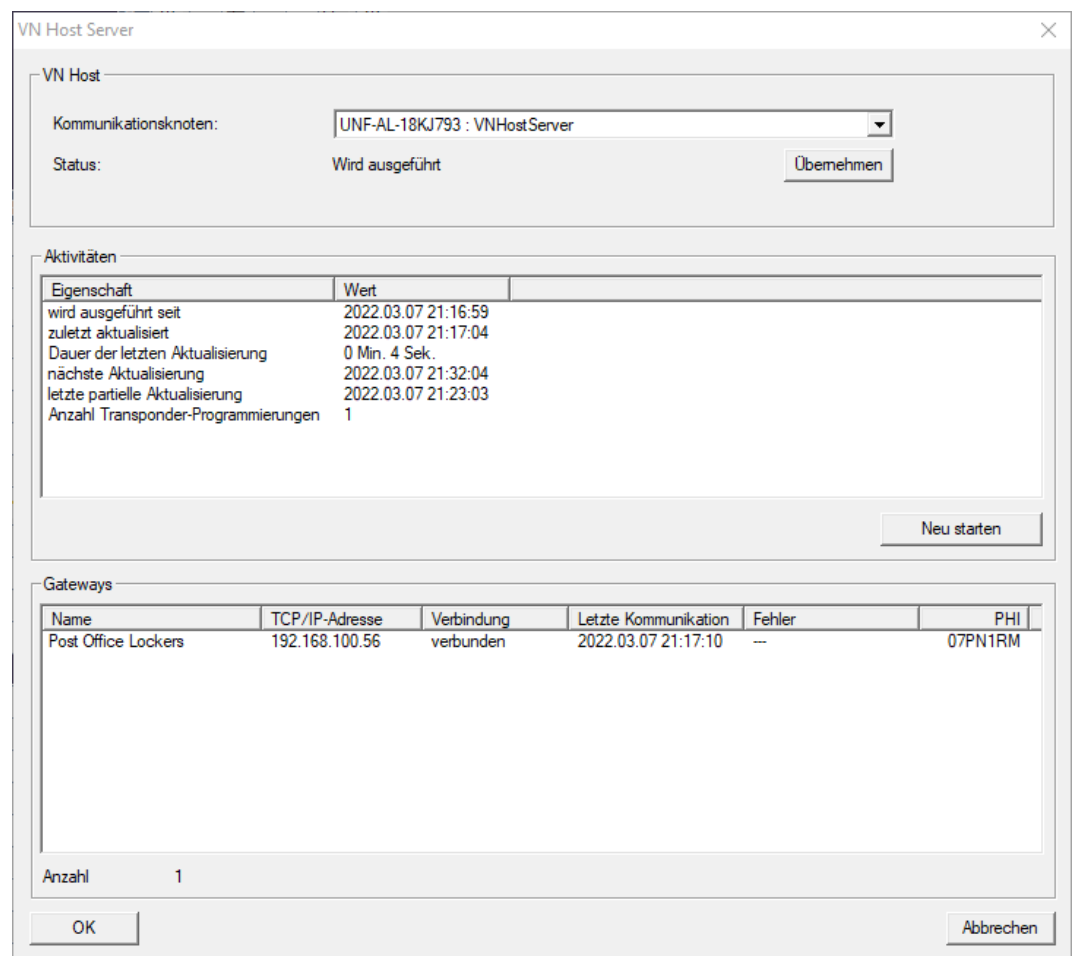
19. Click on the **Transmit** button.
↳ Config files are forwarded to the VN host server communication node.
20. If your SmartRelais 3 Advanced is connected via another communication node: Also save and transfer the config files for this communication node.
↳ Virtual network ready for use.

You can now monitor the status of your virtual network (see [Check virtual network status \[▶ 82\]](#)).

4.5.1.4 Check virtual network status

Once you have set up your virtual network, you can monitor its status.

- ✓ Virtual network configured (see [Setting up a locking system \[▶ 77\]](#) and [Setting up the gateway and VN host server \[▶ 78\]](#)).
- Use | Network | to select the **Virtual network** input.
- ↳ "VN host server" window shows the current status.



You can see the communication node currently being used (for virtual network in the "VNHost"section: "VN host server").

In the "Activities" section, you will see:

- Launch of the VN host server
- Time of the last update
- Time of the next scheduled update
- Number of pending programmings

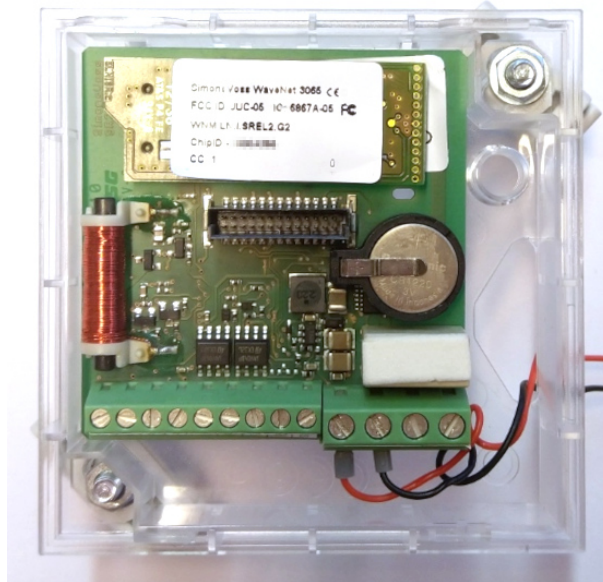
You will find a list of all SmartRelais 3 Advanced configured as ☒ Gateway and their statuses in the section.

4.5.2 Virtual network with SmartRelay 2 G2

4.5.2.1 Functional principle

Unlike SmartRelay 3, SmartRelay 2 G2 (SREL2.G2) is not connected via a network cable, but via WaveNet instead. This is why an integrated LockNode and a RouterNode are required to operate a virtual network with SmartRelay 2 G2, ideally a RouterNode 2 (see [Creating components and setting up LSM \[▶ 89\]](#)).

LSM then forwards the data to be distributed in the virtual network to RouterNode 2 via a network cable and then to SmartRelay 2 G2 via WaveNet. This then acts as a gateway.

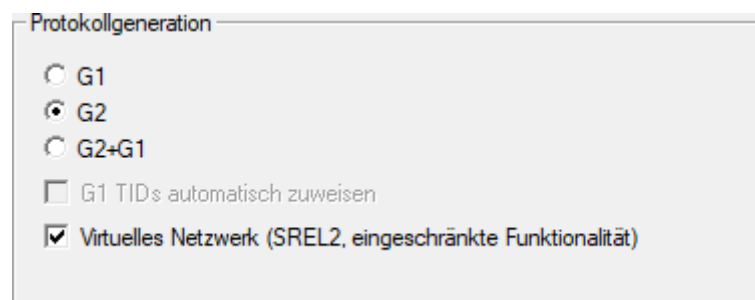


Identification media which are actuated on the gateway then distribute the data to the locking devices.

4.5.2.2 Setting up a locking system

The ☒ Virtual network (SREL2, limited functions) checkbox must be activated in the (exclusively) G2 locking system.

1. Open the properties of your locking system using | Edit | - [Locking system properties](#).
2. Change to the "[Name]" tab.
3. Activate the checkbox in "Protocol generation" the area ☒ Virtual network (SREL2, limited functions).

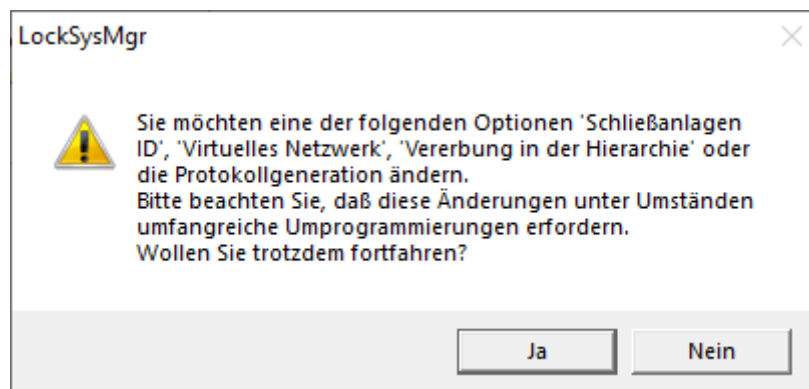


4. If you use cards: select an AV card template from the [G2 card management] tab.

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

- ↳ Locking system is designed for use with a virtual network with SmartRelay 2 G2.

If this setting is applied to an existing locking system, considerable programming may be required.



4.5.2.3 Setting up a VN service

- ✓ Locking system configured (see *Add new locking system* [▶ 11], *Add new transponder* [▶ 11] and *Add new locking device* [▶ 46]).
 - ✓ ☒ Virtual network (SREL2, limited functions) checkbox activated.
 - ✓ All components programmed (see *Programme transponder* [▶ 27] and *Programme locking device* [▶ 47]).
 - ✓ SmartRelay 2 G2 networked (see WaveNet manual).
1. Use | Network | to select the **VN service (SREL2)** input.
 - ↳ The "VN service (SREL2)" window will open.

VN Dienst (SREL2)

Kommunikationsknoten: kein

TCP/IP Port: 4000

VNServer Installationspfad: ...

Import / Synchronisation

☐ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

☐ Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

OK Abbrechen

2. Select from the ▼ **Communication nodes** drop-down menu the communication node to which WaveNet with RouterNode 2 and SmartRelay 2 G2 is connected.

VN Dienst (SREL2)

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: ...

Import / Synchronisation

☐ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

☐ Den Export zu einer bestimmten Uhrzeit ausführen

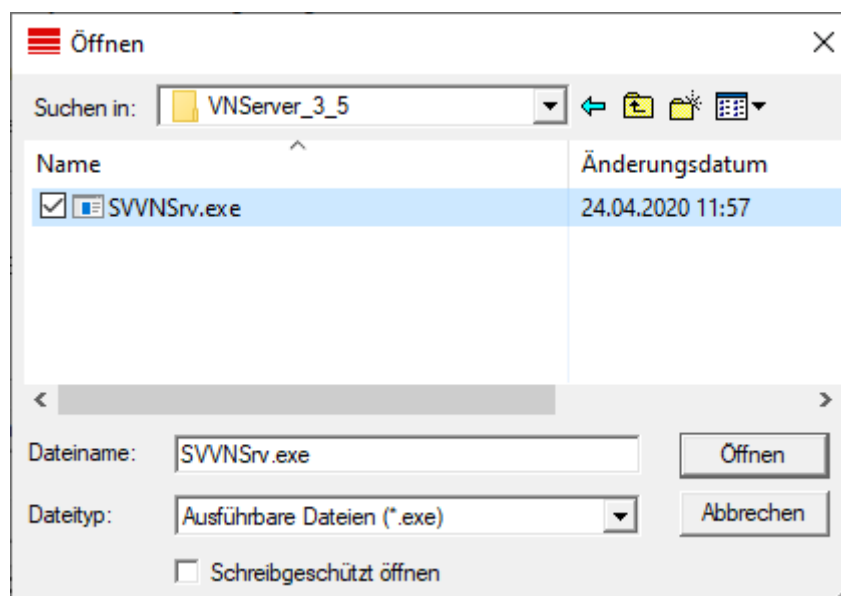
Übernehmen Testen

OK Abbrechen

3. Ensure that the TCP/IP port is set to 4000.
4. Click on the ... button to open Explorer.

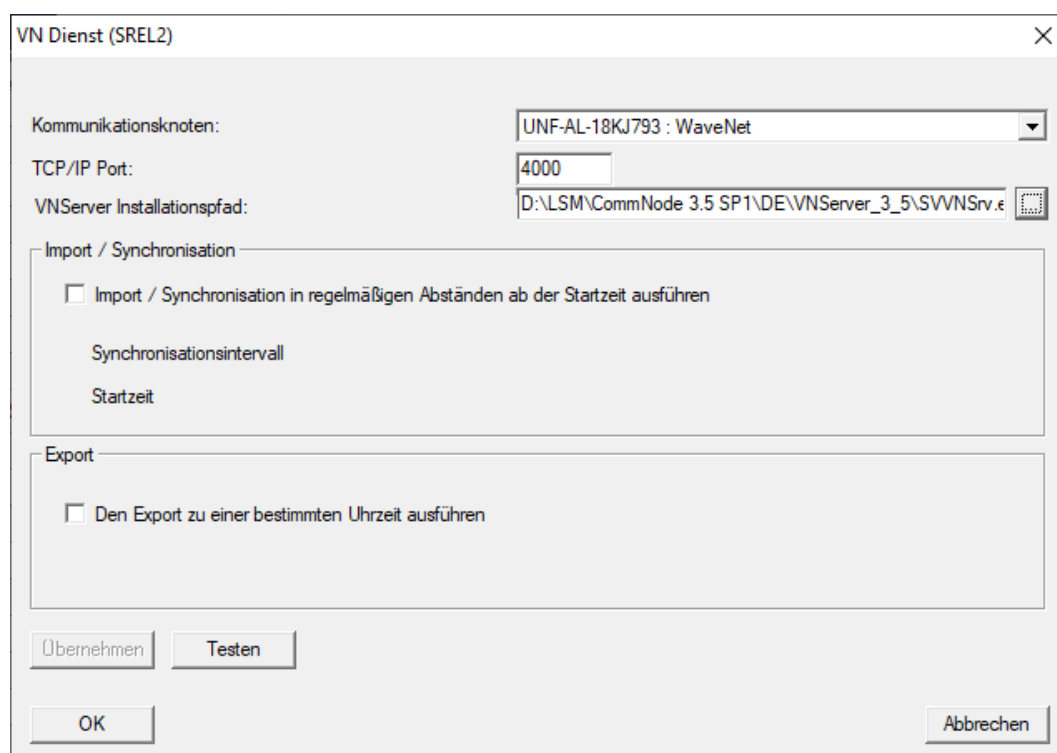
5. Select SVVNSrv.exe.

SVVNSrv.exe is installed together with the CommNode server. Default directory: (C:\Programs(x86)\SimonsVoss\VNServer_x_x)



6. Click on the **Open** button.

→ Explorer window closes.



7. Optional: Go to the "Import/synchronisation" section and configure when the data from SmartRelay 2 G2 should be automatically imported back into LSM.

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

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: D:\LSM\CommNode 3.5 SP1\DE\VNServer_3_5\SVVNSrv.ε ...

Import / Synchronisation

☒ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall: 1 Stunden

Startzeit: 20:00

Export

☐ Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen OK Abbrechen

8. Optional: Go to the "Export" section and configure when the data should be automatically transferred from LSM to SmartRelay 2 G2.

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

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: D:\LSM\CommNode 3.5 SP1\DE\VNServer_3_5\SVVNSrv.ε ...

Import / Synchronisation

☐ Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall: 1 Stunden

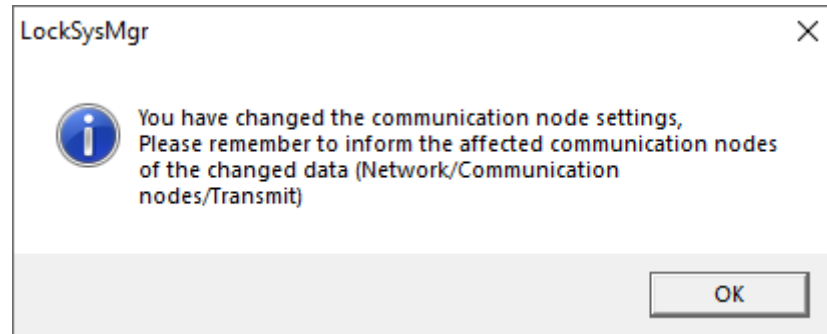
Startzeit: 20:00

Export

☒ Den Export zu einer bestimmten Uhrzeit ausführen 07:00

Übernehmen Testen OK Abbrechen

9. Click on the **OK** button.
 - ↳ The "LockSysMgr" window will open.



10. Click on the **OK** button.
 - ↳ "LockSysMgr" window closes.
 - ↳ "VN service (SREL2)" window closes.
11. Transfer the settings to the CommNode (see *Transmitting the WaveNet configuration* [▶ 57]).

4.5.2.4 Creating components and setting up LSM

Before you start setting up LSM, the most important settings for operating a network must be configured in the LSM software and the RouterNode 2 must be ready for use.

- *Preparing the LSM software* [▶ 46]
- *Preparing hardware* [▶ 47]
- *Creating communication nodes* [▶ 48]
- *Setting up Task services* [▶ 67]

1. Create different identification media (e.g. *Add new transponder* [▶ 11]) and locking devices (e.g. *Add new locking device* [▶ 46]).
2. Perform initial programming of the components created (*Programme transponder* [▶ 27] and *Programme locking device* [▶ 47]).
3. Create a SmartRelay 2 G2 (▼ **Type** "G2_SmartRelay active/hybrid").
4. Open the locking device properties.
5. Change to the "[Configuration/Data]" tab.

6. Activate the ☒ Gateway check box.

Soll

Schließanlagen ID
9215

Schließungs ID
172

Pulslänge 5 Sek.

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

letzte Veränderung

Zeitzone:	nicht vorhanden
Feiertagslisten:	nicht vorhanden

Erweiterte Konfiguration



7. Switch back to the matrix view.
8. Authorise all identification media on SmartRelay 2 G2 which are to receive new authorisations there at a later point in time.
9. Carry out initial programming of the SmartRelay 2 G2.
10. Ensure that a LockNode is installed in the SmartRelay 2 G2.
11. Set up RouterNode 2 using WaveNet Manager (see [Setting up the network and importing into LSM \[► 48\]](#)).
12. Assign the gateway (or SmartRelay 2 G2) to it.
- ↳ The virtual network is now ready for use.

4.5.2.5 Exporting authorisation changes

Exporting authorisation changes only works if there is at least one change. To perform the test, remove authorisation for locking cylinder 1 from transponder 1, for example.

1. Perform a reset before the first export (see [Resetting tasks in the virtual network \[► 97\]](#)).
2. Use | Programming | - **Virtual Network** to select the **Export to VNetwork** entry.
↳ The "Export to virtual network (SREL2)" window will open.

3. Select all SmartRelay 2 G2s to which you need to send/export the changes.


4. Check whether you have selected the correct locking system in the  **Locking system** drop-down menu.
5. Click on the **Prepare** button.
 All exportable changes are listed in the "Persons" section.
6. Select all changes that you wish to export to the previously selected SmartRelay 2 G2.

- Click on the **Export** button.
→ The export process will start. The changes are sent to the gateway.

VNServer Meldungen ✕

VN Befehl: VN Export Stoppen

Ausgegeben am: 2022.03.07 16:32:07

Zustand/Ergebnis: wird bearbeitet 

Gateway

Letzte Meldung: 2022.03.07 16:32:09

Aktuelle Aktion 1: Gateways aktualisieren

Aktuelle Aktion 2:

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

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

→ A summary of the export is displayed.

VN Ergebnis

VN Befehl: VN Export

Ausgegeben am: 2022.03.07 16:32:07

Zustand/Ergebnis: erfolgreich durchgeführt

Zusammenfassungen:

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

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

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

Beenden

You can now track the exported tasks in the overview (*Status of the tasks in the virtual network (SREL2.G2)* [▶ 96]).

The authorisation change is now available at the gateway. There are now two scenarios:

- ❑ Transponder 1 books at the gateway. Locking device 1 will later recognise that transponder 1 is no longer authorised and refuse access.
- ❑ Another transponder (not transponder 1) first makes a booking at the gateway and authorises locking device 1. Transponder 1's locking ID is communicated to locking cylinder 1.

With LSM 3.5 SP3 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

Programme the TIDs to be disabled directly

The IDs to be disabled are saved on the transponder during the programming process.

- ✓ The transponder is physically available.
- ✓ The transponder's programming window is open.

1. Click on the **TIDs to deactivate** button.

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

→ The list will open.

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. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
 3. Click on the **OK** button to confirm your input.
 4. Continue with the programming.
- The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

Add the TIDs to be blocked to the properties

The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

✓ The transponder's properties window is open.

1. Change to the "[Configuration]" tab.

2. Click on the **TIDs to deactivate** button.

➞ The list will open.

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

3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.

- #### 4.5.2.6 Status of the tasks in the virtual network (SREL2.G2)

- ✓ Tasks exported to the virtual network (see *Exporting authorisation changes* [► 90]).

1. Select | Programming | - Virtual Network to open the Exported VN tasks entry.
↳ The "Exported VN tasks" window will open.

[illegible]

[illegible]

LockSysGUI

Alle VN Aufgaben und Befehle werden zurückgesetzt! Führen Sie bitte anschließend den VN Export erneut aus.
Fortfahren?

Ja Nein

- ↳ Gateways are programmed to reset the exported tasks.

VNServer Meldungen

VN Befehl:

Reset VN Aufgaben


Ausgegeben am:

2022.03.07 16:20:33

Zustand/Ergebnis:

wird bearbeitet

Stoppen



Gateway

Letzte Meldung

2022.03.07 16:20:41

Aktuelle Aktion 1

Gateways aktualisieren

Aktuelle Aktion 2

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

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

→ Exported tasks are reset.

VN Ergebnis

VN Befehl:

Reset VN Aufgaben

Ausgegeben am:

2022.03.07 16:20:33

Zustand/Ergebnis:

erfolgreich durchgeführt

Zusammenfassungen:

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

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

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

Beenden

You can export the required tasks to the virtual network again (see *Exporting authorisation changes* [▶ 90]).

4.5.2.8 Importing authorisation changes

Once the changes have been exported to the gateway, you will not be able to see which changes have already been retrieved from the gateway in the LSM software. To do this, you will first need to import the changes again:

1. Use | Programming | - **Virtual Network** to select the **Import / synchronisation** entry.
 ↳ The import process will start immediately.

VNServer Meldungen

VN Befehl: VN Import

Ausgegeben am: 2022.03.07 16:41:16

Zustand/Ergebnis: wird bearbeitet

Gateway

Letzte Meldung: 2022.03.07 16:41:17

Aktuelle Aktion 1: Gateways auslesen

Aktuelle Aktion 2: Übertragung der Datenpakete

Name	Ergebnis
Post Office Illumination / 00CP17B	

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

→ Import report is now displayed.

You can automate the import and export of changes to a gateway here: | Network | - VN service (SREL2) .

IMPORTANT

WaveNet capacity utilisation due to import and export

If many changes are imported and exported at the same time, full use is made of the WaveNet's capacity. This may affect other functions which also use the WaveNet.

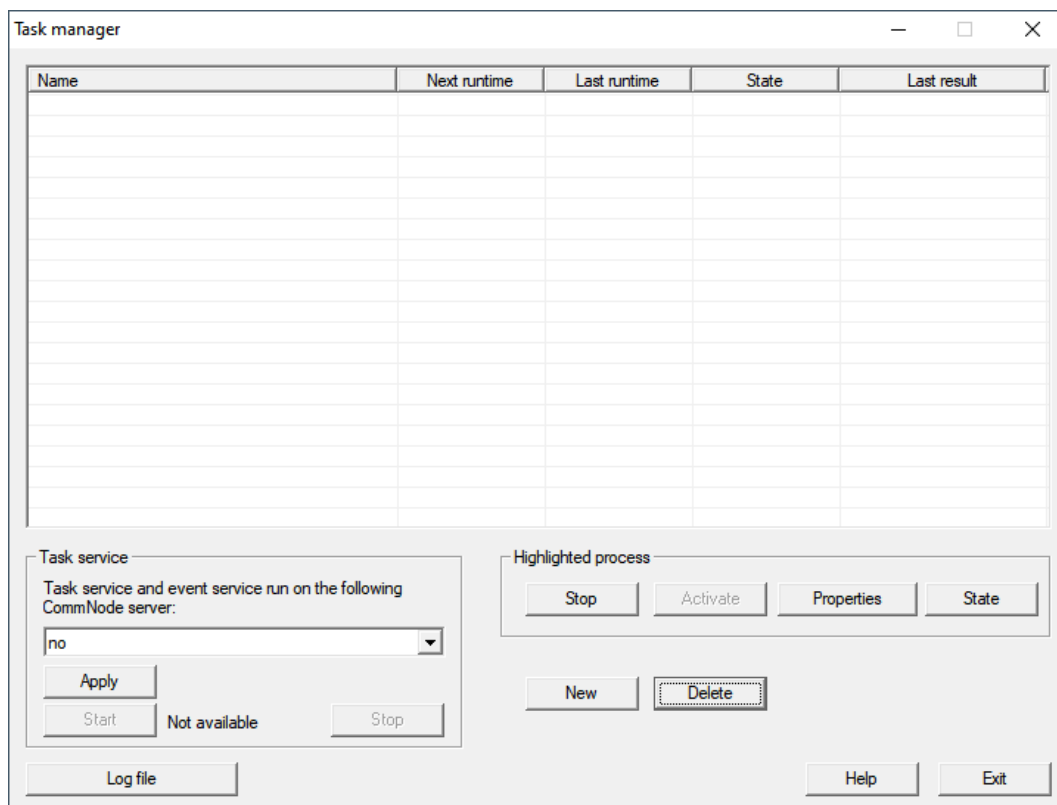
4.6 Read locking device

One of the great advantages of networked locking devices is that you can conveniently check the status from your workstation.

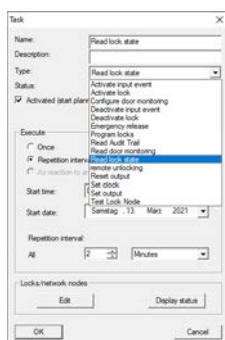
You can even automate this with the Task Manager.

You can then further process the information in LSM, for example by means of warnings and messages (see Warning monitor and Manage warnings).

- ✓ LSM open.
 - ✓ Locking devices to be read out programmed and networked (see *Creating a WaveNet radio network and incorporating a locking device* [▶ 46]).
1. Select via | Network | the entry **Task manager**.
➔ Windows "Task manager" launches.



2. Click on the button **New** to create a new task.
↳ Windows "Task" launches.
3. Enter a name for the task.
4. From the drop-down menu, select ▼ **Type** the entry "Read lock state" off.



5. Select in the area "Execute" the option ☒ Repeat interval off.
6. Set the desired interval.



NOTE

Effect of the repeat interval on the battery run time

The more often you read the locking device, the more often the locking device is woken up from the energy-saving standby mode. Battery life may therefore be shorter.

Task

Name: Read lock state

Description:

Type: Read lock state

Status:

☒ Activated (start planned task as stated)

Execute

☐ Once

☒ Repetition interval

☐ As reaction to an event

Start time: 00:28

Start date: Samstag, 13. März 2021

Repetition interval:

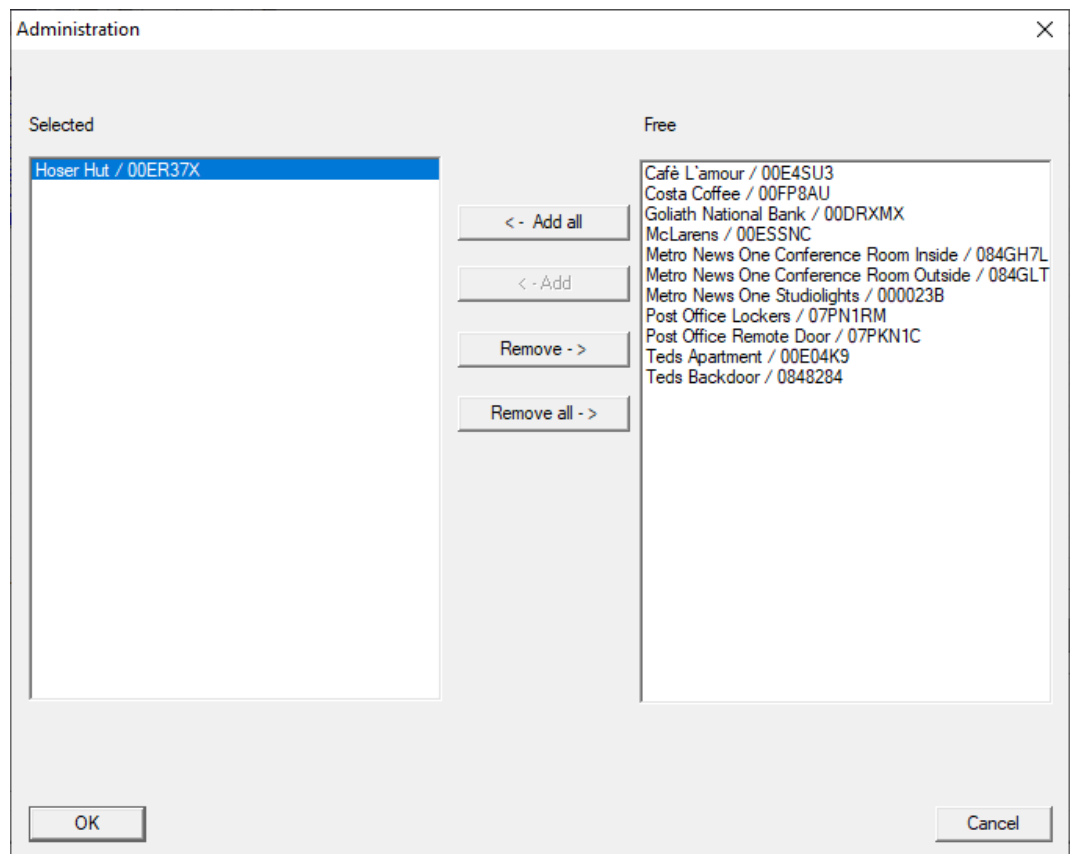
All 2 Minutes

Locks/network nodes

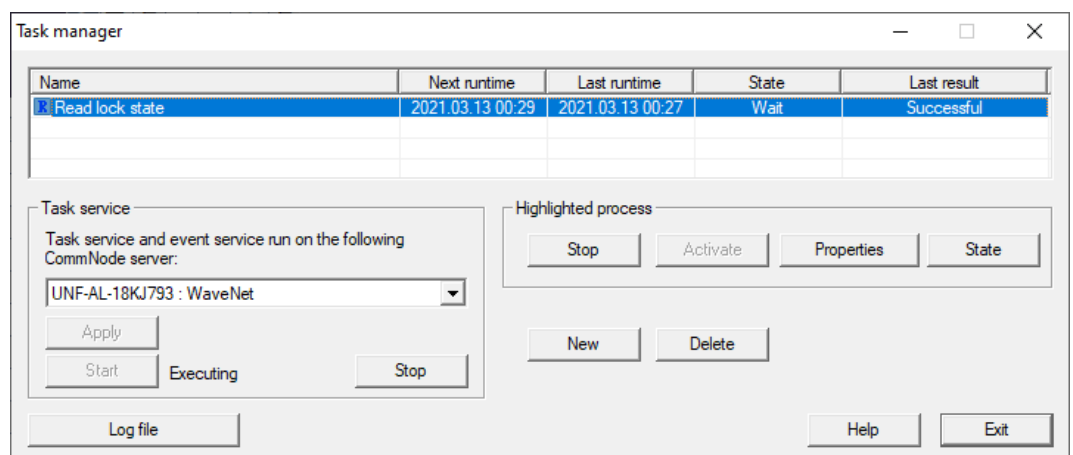
Edit Display status

OK Cancel

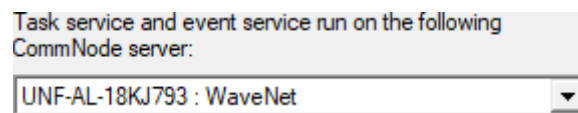
- Click in the area "Locks/network nodes" on the button **Edit**.
→ Windows "Administration" launches.



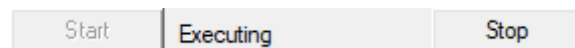
8. Select the locking devices you want to read.
9. Then move the locking devices using the button **Add** into the left column.
10. Click on the **OK** button.
 - ↳ Windows "Administration" closes.
11. Click on the **OK** button.
 - ↳ Windows "Task" closes.
 - ↳ Task is listed in the Task Manager.



12. Ensure that in the field: "Task service" in the drop down menu ▼ **Task service and event service run on the following CommNode server** of the appropriate CommNode is selected.



13. Make sure that the task service is also running.



14. Click on the **Exit** button.

- ↳ Windows "Task manager" closes.
- ↳ Locking status of the set locking devices is queried automatically.

5. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

Software and drivers

Software and drivers can be found on the website:

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

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

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

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany



This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2023, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF

