LSM 3.5 SP3 Business + Prof.

Manual

24.01.2024

SimonsVoss technologies

Contents

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.

Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to ± 15 minutes per year.

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 [▸ 142]*.

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 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. Intended use

LSM 3.5 SP3 stands for Locking System Management and is database-supported software. It allows you to create, manage and control locking plans.

3. 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
☑ Example ☐ Example	checkbox
◉ 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
Example	Name of a (Windows) service
Example	Commands (e.g. Windows CMD commands)
`Example`	Database entry
[Example]	MobileKey type selection

4. Installation

This section describes initial LSM software installation on a system which does not have a previous version of LSM installed. It is possible to update to the current LSM version 3.5 SP3 from an earlier version, but you must ensure that LSM 3.5 SP3 is not installed in parallel to older versions of LSM.

LSM Business and LSM Professional also require the Advantage Database Server in its 12.x version.

The LSM update manual documents LSM software updates.

4.1 Software

4.1.1 LSM Business/Professional

Installing LSM Professional is similar.

4.1.1.1 Install and configure ADS server

The Advantage Database Server is an essential tool for operating LSM Business. Using the ADS server is the only way to ensure that a number of people can access the locking plans in the database at the same time and that data are successfully exchanged in the process.

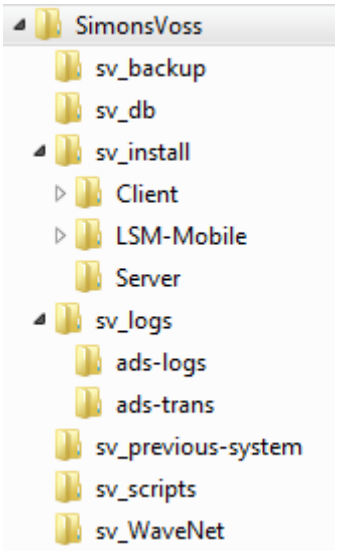
This section shows all the necessary steps which you need to take on the server.

NOTE

You need a valid licence key to install the ADS server *(validation code and replication code)*. Contact your vendor, keeping your SimonsVoss delivery note for LSM Business software at hand if you do not have a licence key yet. The SimonsVoss delivery note contains a certificate with a serial number and validation code which is used to register the ADS licence.

Create folder structure

During installation, create the following folder hierarchy in the main directory (e.g. `C:\SimonsVoss`):



Ordner	Inhalt
sv_backup	Local backup files for restoring an earlier state of the locking system
sv_db	Locking plan
sv_install	Installation files (if necessary)
sv_logs	Log files of the Advantage Database Server
sv_previous_system	Files from older LSM versions
sv_scripts	Contains objects such as the backup script, which is added to the Windows task scheduler
sv_WaveNet	Files generated by the WaveNet manager

Install ADS server

Install the ADS server on the server:

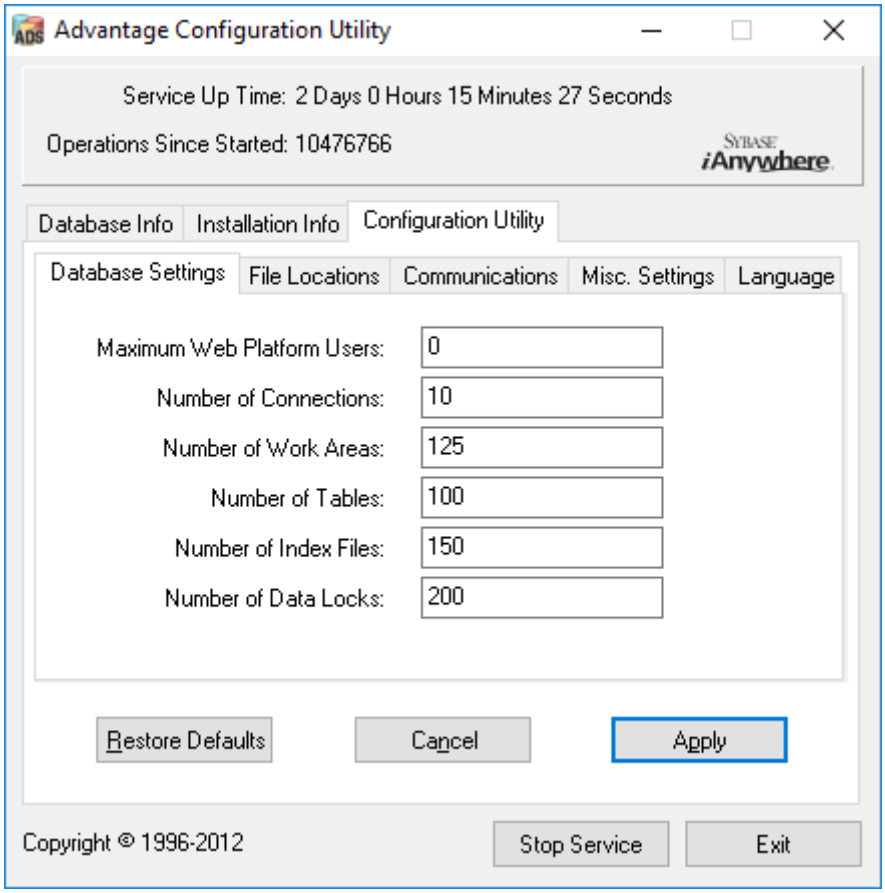
1. Launch the set-up file as an administrator.
2. Follow the installation instructions.
   ↳ You need to accept the licence conditions to carry out installation.
   ↳ Enter the required codes to register the ADS server correctly when prompted.

Configure ADS server

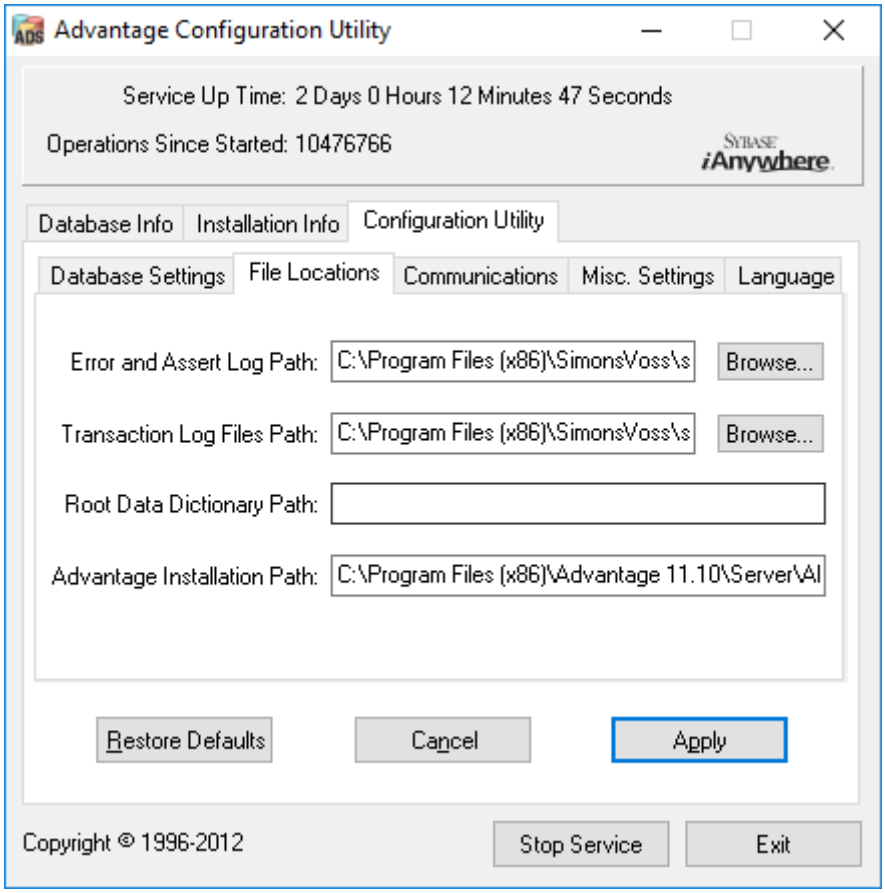
Configure the ADS server with the help of the Advantage Configuration Utility:

1. Launch the Advantage Configuration Utility, e.g. at *Start/Programme/Advantage Database Server/Advantage Configuration Utility*. (The Configuration Utility may have already been launched)
2. Select the "Configuration Utility" tab.

3. Change the following properties in the "Database Settings" tab and press the "Apply" button to save:

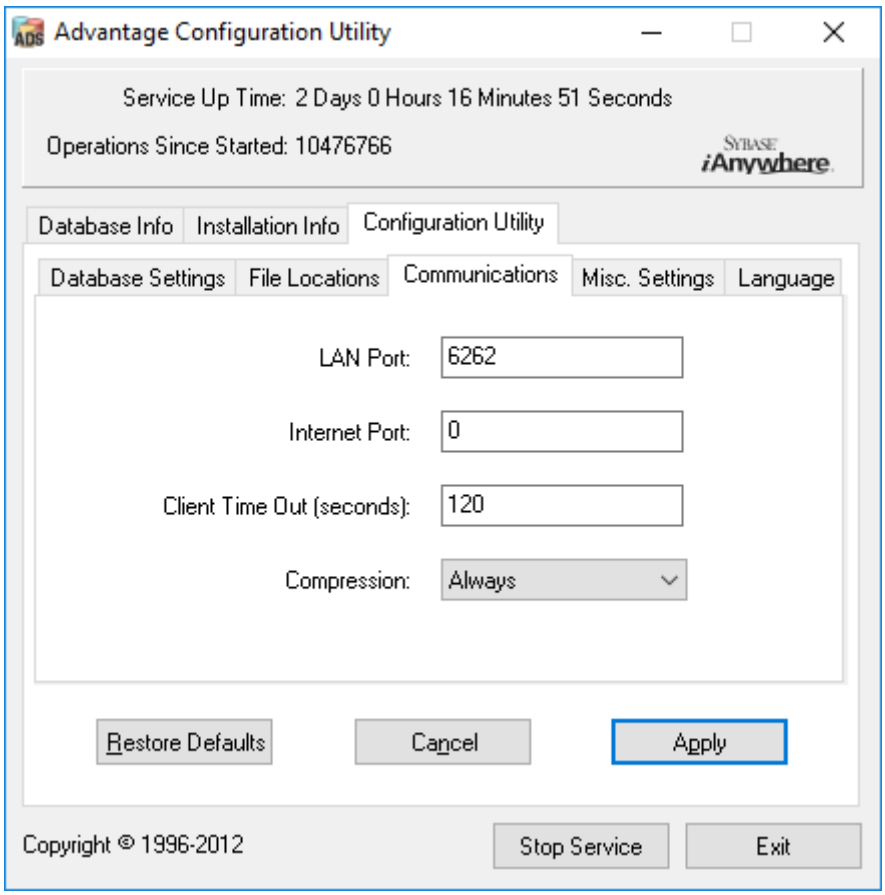


4. Change the following properties in the "File Locations" tab and press the "Apply" button to save:

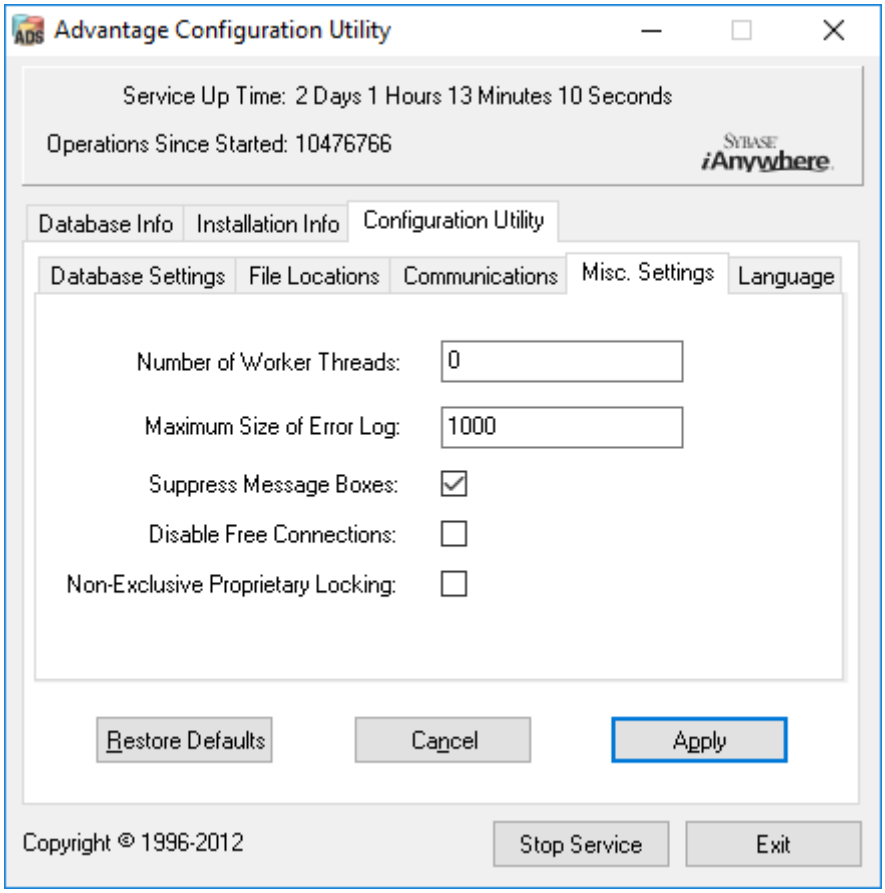


↳ Note that the drive path may differ from the one on the server (here C:).

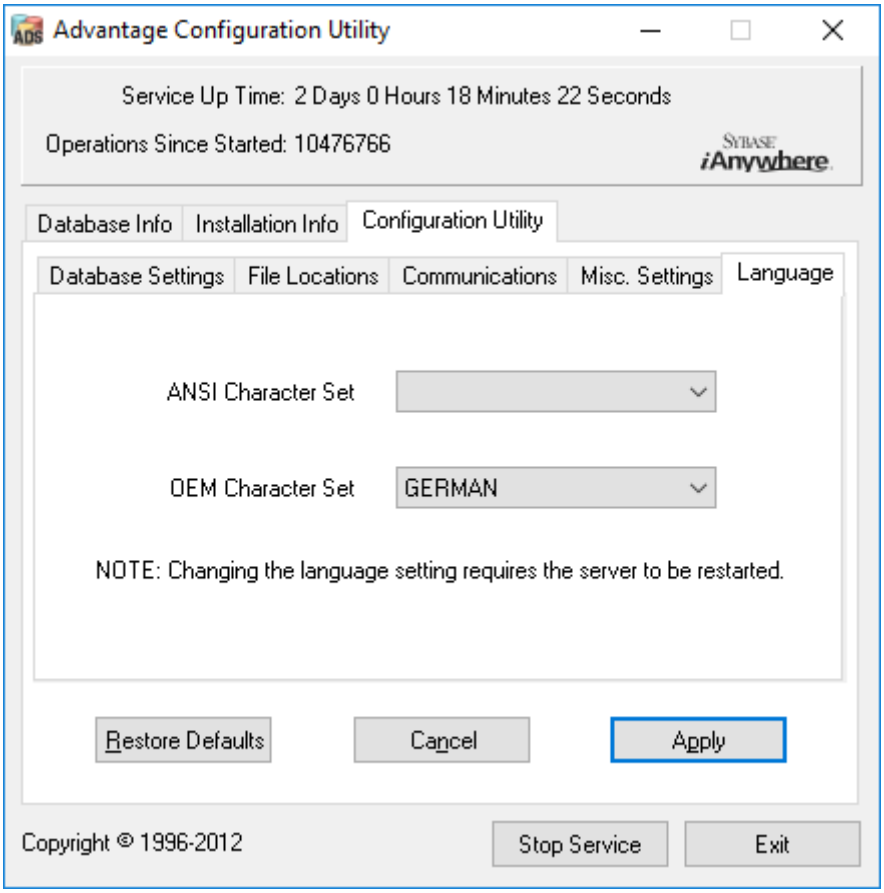
5. Change the following properties in the "Communications" tab and press the "Apply" button to save:



6. Change the following properties in the "Misc. Settings" tab and press the "Apply" button to save:



7. Change the following properties in the "Language" tab and press the "Apply" button to save:



Check ADS server service

Check whether the ADS server service is automatically run as a system service:

1. Open the control panel, e.g. using *Start/Control panel*.
2. Open the "Administration" folder.
3. Open the "Services" folder
4. Check whether the "Advantage Database Server" service status is "Launched" and the launch type is set to "Automatic".
   ↳ Double-click on the ADS service to change any values if necessary.

Share database on the network

The "sv_db" database directory on the server must be shared on the network. Configure a share with read rights. We recommend configuring a "hidden share". *You can shared resources by inserting the $ character at the end of the share path.*

4.1.1.2 Install and configure LSM Business

CAUTION

Install VN host after LSM

The VN host cannot access the database if LSM has not been installed yet and a locking system has been set up. If the VN host does not find a database it can access during installation, problems may arise.

1. Install LSM before the VN host.
2. Add a locking system.
3. Install VN host

Install LSM Business

LSM Business is installed on the client computers as required. These computers access the ADS server on the network which manages the locking plans.

NOTE

We strongly recommend installing the LSM software directly into a local administrator account. *Log on using an Administrator account; do not merely select "Run as administrator" when logged on as an ordinary user.*

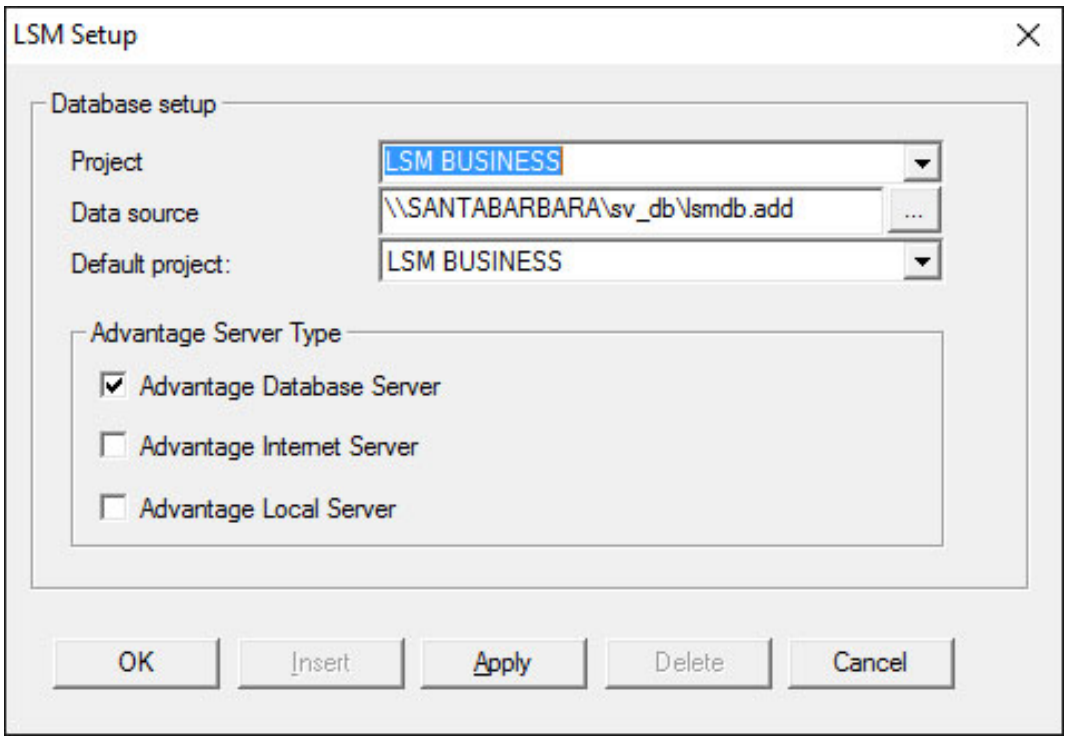
1. Launch the set-up file as an administrator.
2. Follow the installation instructions.
   ↳ You need to accept the licence conditions to carry out installation.
3. Launch LSM Business *(desktop icon or Start/Programme/SimonsVoss/LSM BUSINESS)*

Configure LSM Business

LSM Business needs to be configured once. In this step, we copy an empty locking plan onto the server and configure LSM Business, so that it can access this locking plan.

1. Extract the locking plan, which is stored in the LSM Business installation directory (e.g. C:\Programs (x86)\SimonsVoss\LockSysMgr_3_5\db), and transfer it to the "sv_db" server directory.
2. Launch LSM Business (e.g. using *Start/Programs/SimonsVoss/LSM Business*).
3. Select "Setup".

4. If it is being run for the first time, a window will open, where the database path is to be set.



   ↳ Enter a project name.
   ↳ Use the "..." button to select the path to the server and link directly to the lsmdb.add file. In the case of hidden releases, the path to lsmdb.add must be entered directly with the $ character, e.g.: \ \<SERVER>\sv_db$\lsmdb.add
   ↳ *You cannot select a local directory in LSM Business.*
5. Apply the settings.

4.1.1.3 Install Crystal Reports hotfix

Crystal Reports is used as a reporting tool in the background. The tool is automatically installed when LSM Basic Online, Business and Professional are installed. A current hotfix needs to be installed to ensure correct operation.

1. Launch the hotfix in .exe format.
2. Follow the installation instructions.
   ↳ You need to accept the licence conditions to carry out installation.

NOTE

Installation without Java components

The Java components (JCE) of the hotfix are not required for operation with the LSM.

- Deactivate the checkbox ☐ JCE during the installation routine.

4.1.2 VN host

The VN host accesses the LSM database and provides various functions without LSM itself being executed (including gateway).

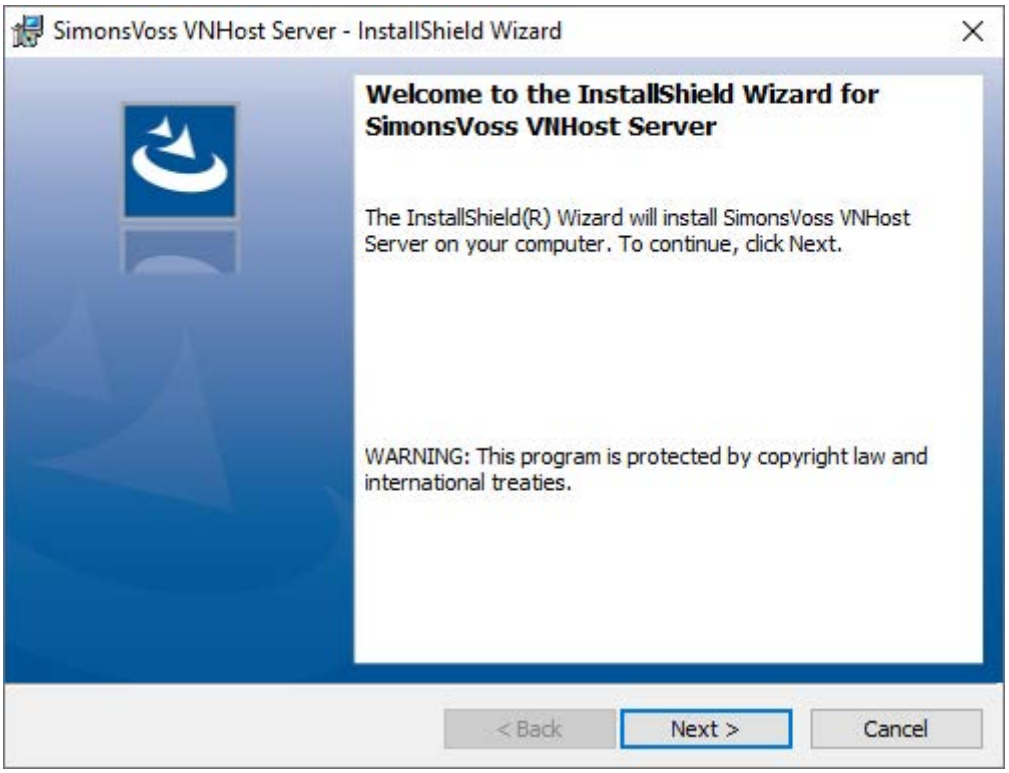
CAUTION

Install VN host after LSM

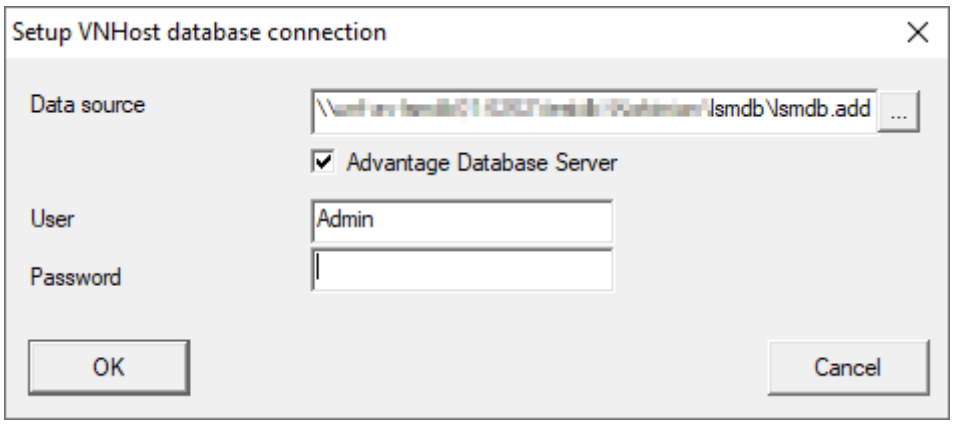
The VN host cannot access the database if LSM has not been installed yet and a locking system has been set up. If the VN host does not find a database it can access during installation, problems may arise.

1. Install LSM before the VN host.
2. Add a locking system.
3. Install VN host

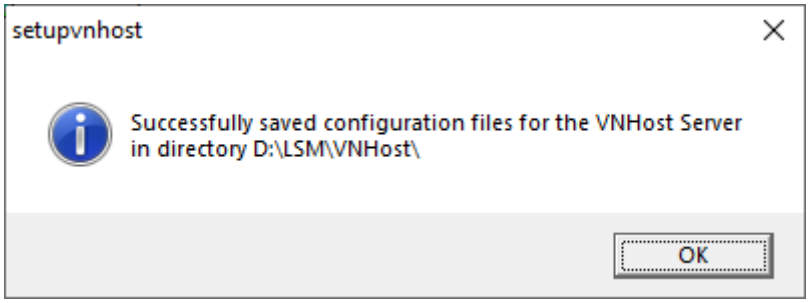
1. Execute the set-up file (vnhost_setup_3_5_sp3.exe).



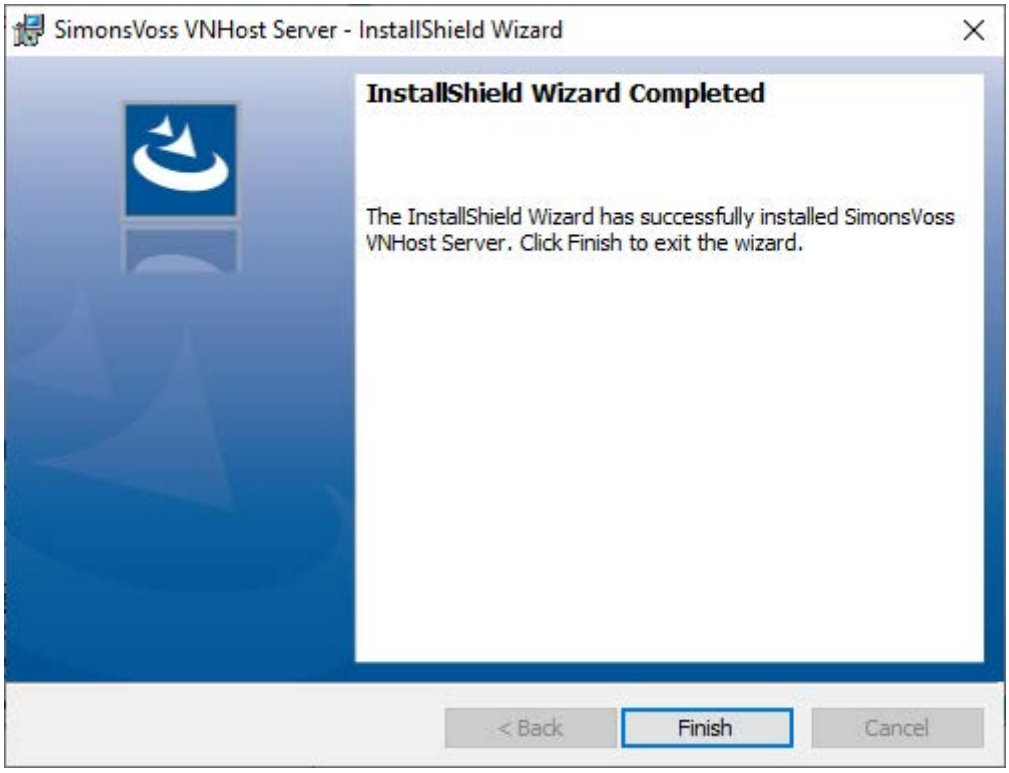
2. Follow the installation instructions and install the VN host on the server.
3. Enter the UNC path to your lsmdb.add (can be copied from the LSM login window) in the "Setup VN host database connection" window.



4. Enter your LSM user name and your LSM user password.
5. If your lsmdb.add is installed locally: disable the ☐ Advantage Database Server check box.
6. Click on the OK button.
   ↳ Connection is established between VN host and database.



↳ Installation complete.



4.1.3 CommNode

Install the CommNode server using the setup file. If the CommNode service is not then listed under the Windows services (SimonsVoss CommNode server), you must perform the installation with a batch file.

1. Go to the installation directory of the CommNode server (`C:\Program Files (x86)\SimonsVoss\CommNodeSvr_3_5`).
2. Execute the batch file install_CommNodeSvr with administrator rights.
   ↳ The command line opens.
   ↳ The CommNode server is installed.

↳ The CommNode server is installed and listed under Windows services.

4.1.3.1 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.

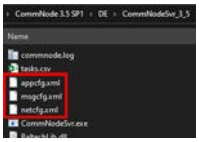
1. Open the LSM software.
2. Select | Network |/ Communication nodes .
3. Add "Name", "Computer name" and "Description",

```
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.

5. First steps after a new installation

5.1 Recommended approach to handling passwords

Two types of passwords are used in LSM software:

- **User password**

  The user password is required to log on to the locking plan or database.

- **Locking system password**

  The locking system password is programmed into all SimonsVoss components. This locking system password is saved to an encrypted section in the locking plan or database and cannot be read. Programmed SimonsVoss components can only be reprogrammed if the database knows the locking system password.

Two recommendations for managing passwords securely:

- To ensure optimum security for the whole locking system, the locking system password should be split into at least two parts, which are issued to different people on an individual basis.
- We strongly recommend writing the administrator and locking system password down and storing them securely in different places where they cannot be accessed by third persons.

The locking system operator should always be clear about one thing: what happens if the only person who knows the locking system password (or part of it) should suddenly no longer be available.

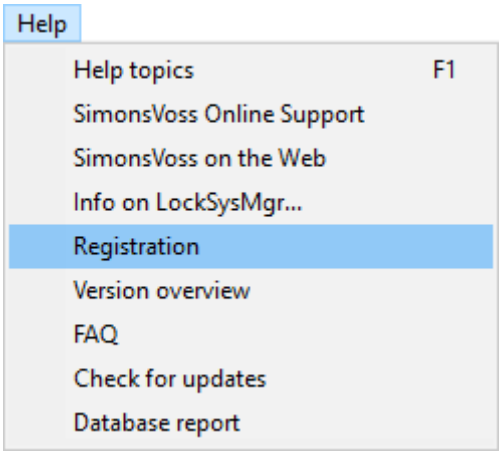
5.2 Register LSM

LSM needs to be registered. A registration file is created for this purpose and sent to a designated email address. You will then automatically receive a reply which contains your personal licence file. You can use this licence file to register LSM with the modules that you ordered.

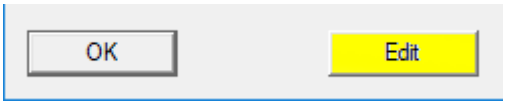
Procedure

- ✓ LSM installation is implemented.
- ✓ Delivery note with registration information is on hand.
- ✓ Sending mails is possible.

1. In the tab | Help | click on the Registration button.
   ↳ The Registration window opens.



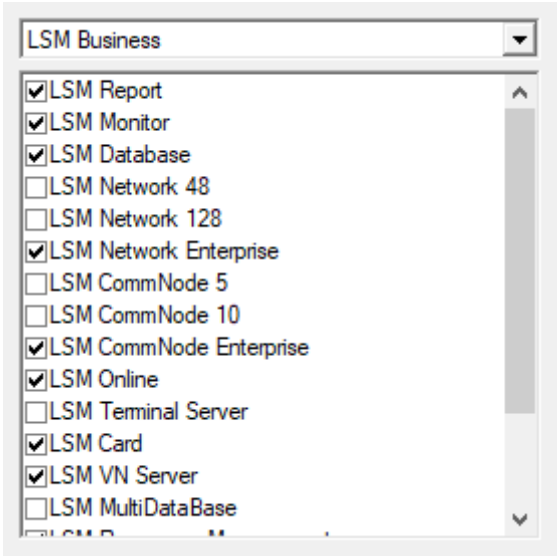
2. Click on the Edit button.



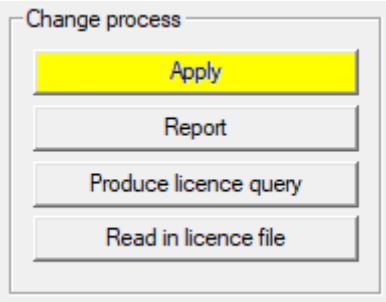
↳ The Edit registration window opens.

3. Complete the form.

4. Make sure the correct edition is selected (example: Business).

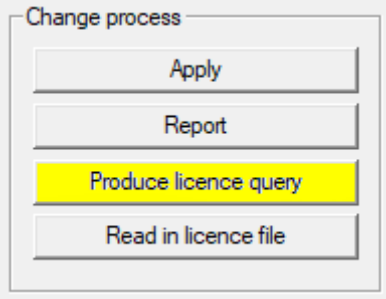


5. Click on the Apply button.

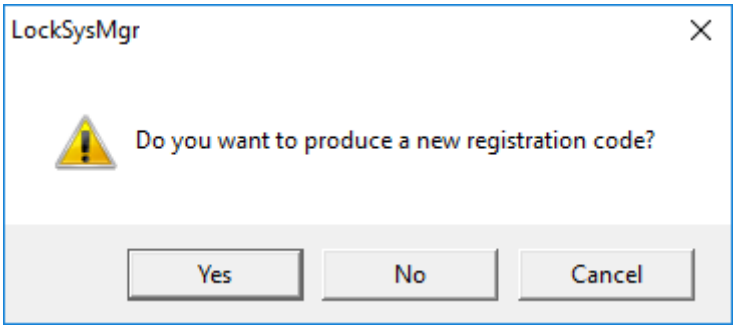


↳ The data record is saved.

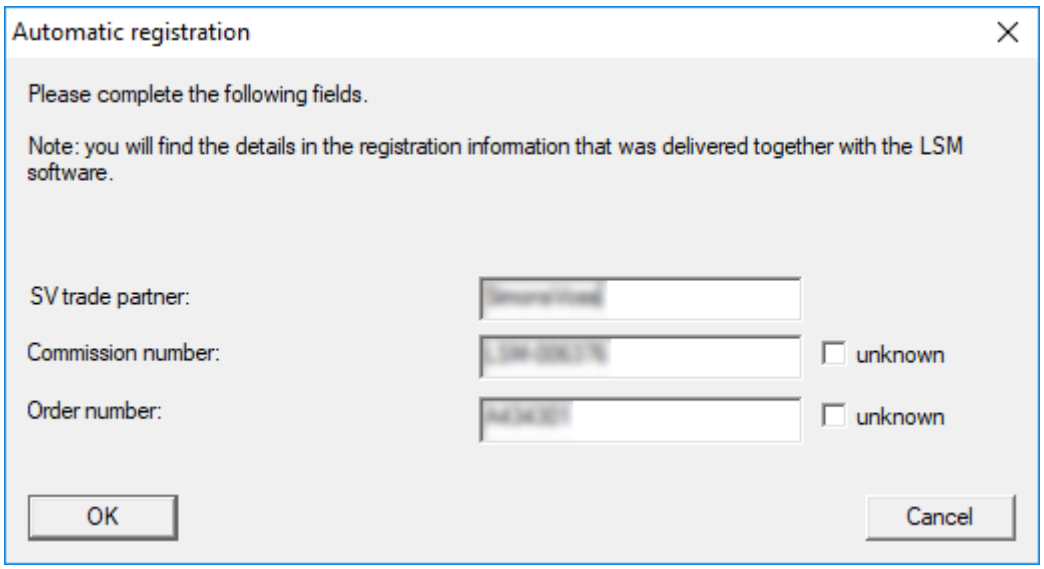
6. Click on the Produce licence query button.



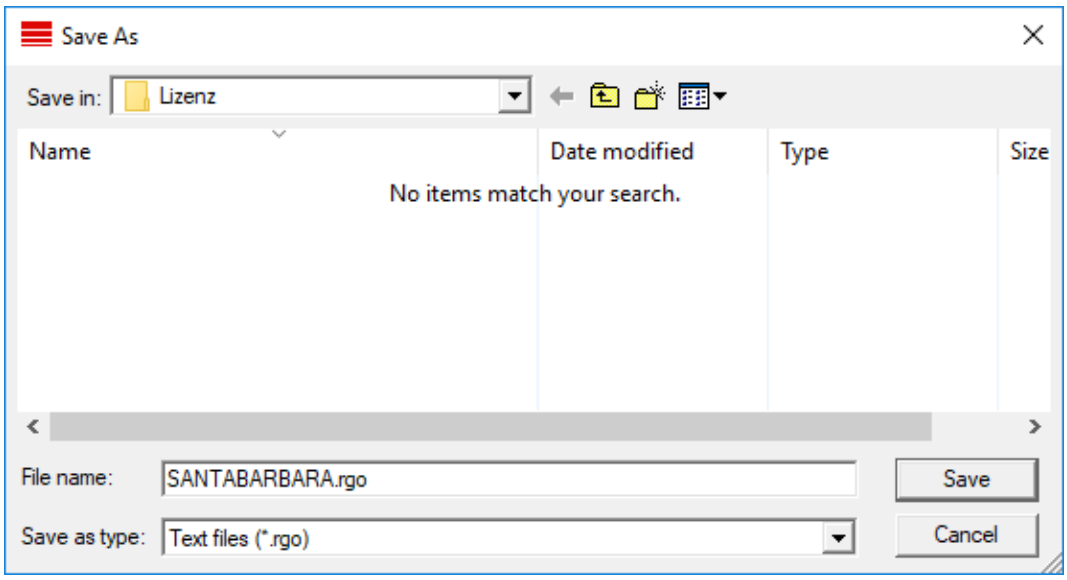
7. Click on the Yes button to accept the query prompt.



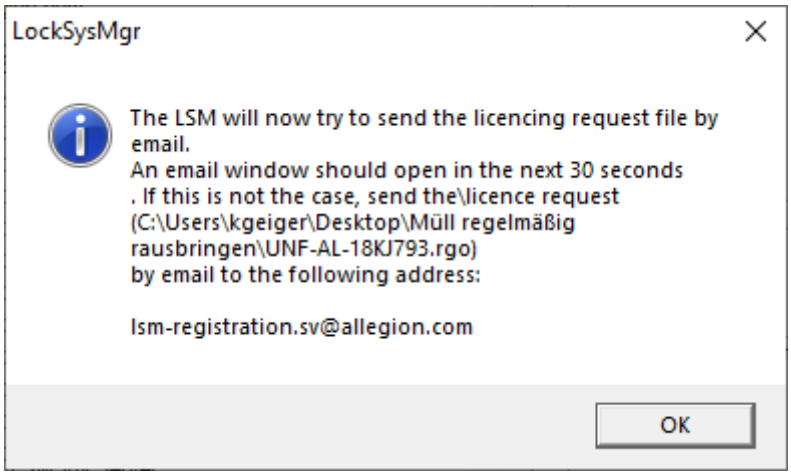
8. Complete the form (LSM consignment number in LSM-xxxxxx format; order number in Axxxxxx format).



9. Click on the OK button.
   ↳ The RGO file is created.
   ↳ The Explorer window will open.
10. Save the RGO file to a directory of your choice.

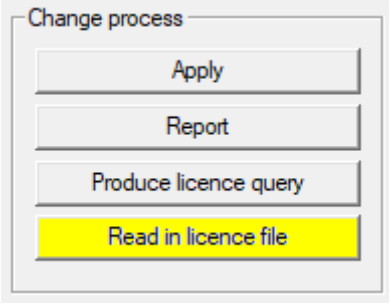


11. Click on the OK button.



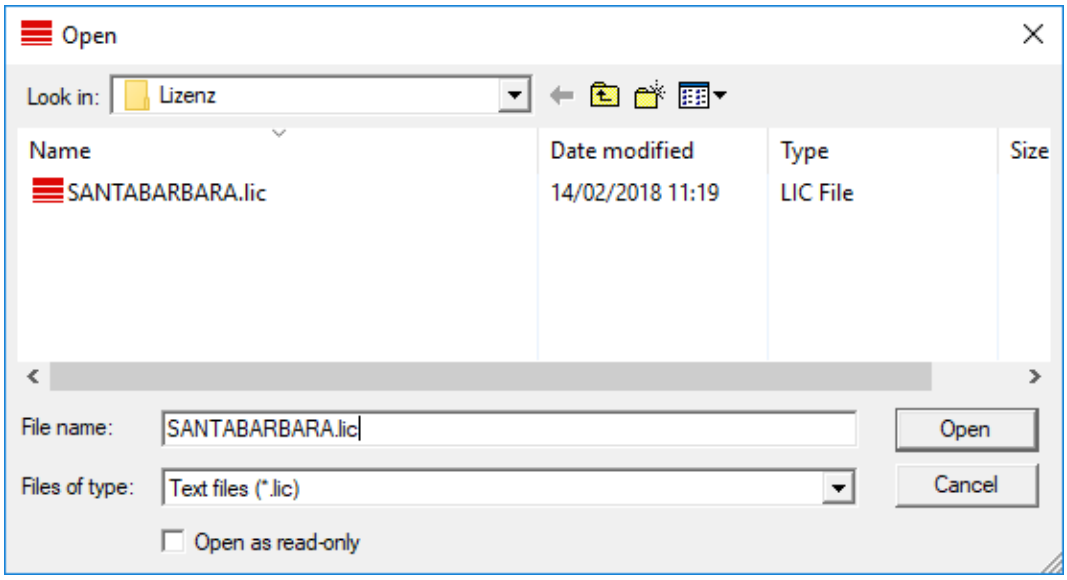
    ↳ The standard email client will open. An email is automatically generated with the RGO file attached.

12. If the RGO file is not attached, then attach it manually.
13. Send an email with the RGO file to lsm-registration.sv@allegion.com.
    ↳ Reply is automatically sent with the LIC file attached.
14. Save the LIC file to a directory of your choice.
15. Switch back to LSM.
16. Click on the Read in licence file button.



    ↳ The Explorer window will open.

17. Select the LIC file.



18. Click on the Open button.
19. Click on the OK button to accept the prompt notice.
20. Re-start LSM.

↳ Registration is implemented.

5.3 Add locking system

Establish password

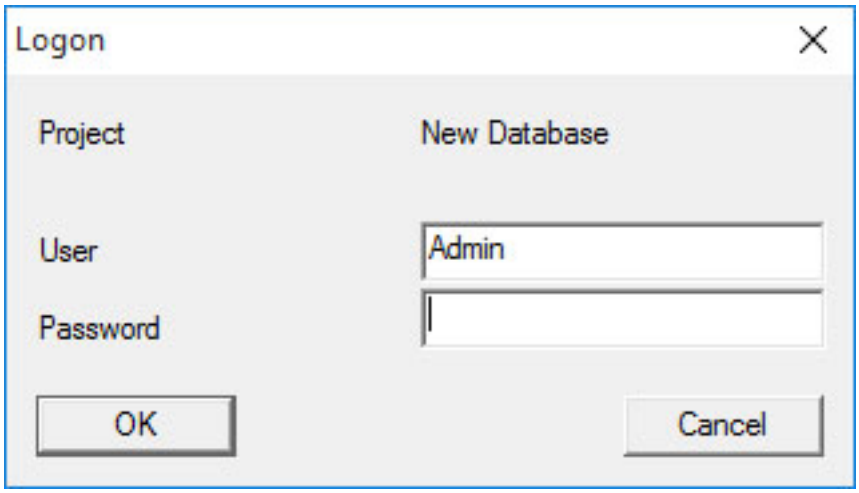
If you have already created a project, you can now create a locking system.

NOTE

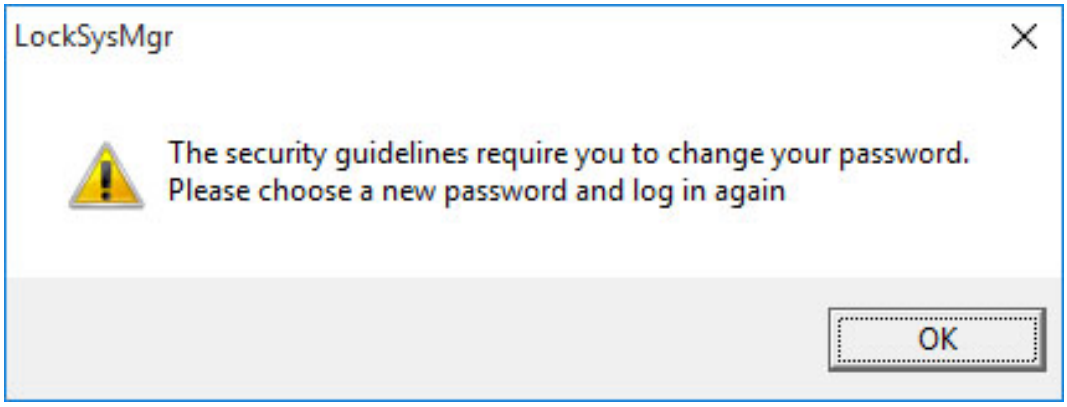
When creating the first locking plan in LSM Business or LSM Professional, licensing interrupts the process. The licensing of other modules is optional for LSM Basic.

1. Click on "Log on" in the main menu in the LSM software. Ensure that the right project is selected under "Setup" if necessary.

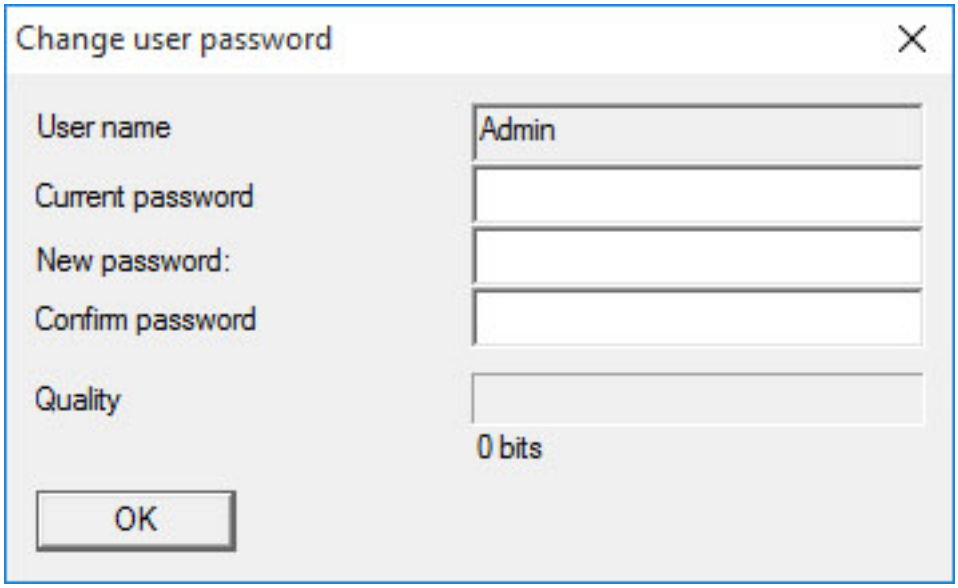
2. Enter the default password "system3060".



3. Click on "OK" to acknowledge the warning.



4. Re-enter the default password "system3060" and then establish a new user password.

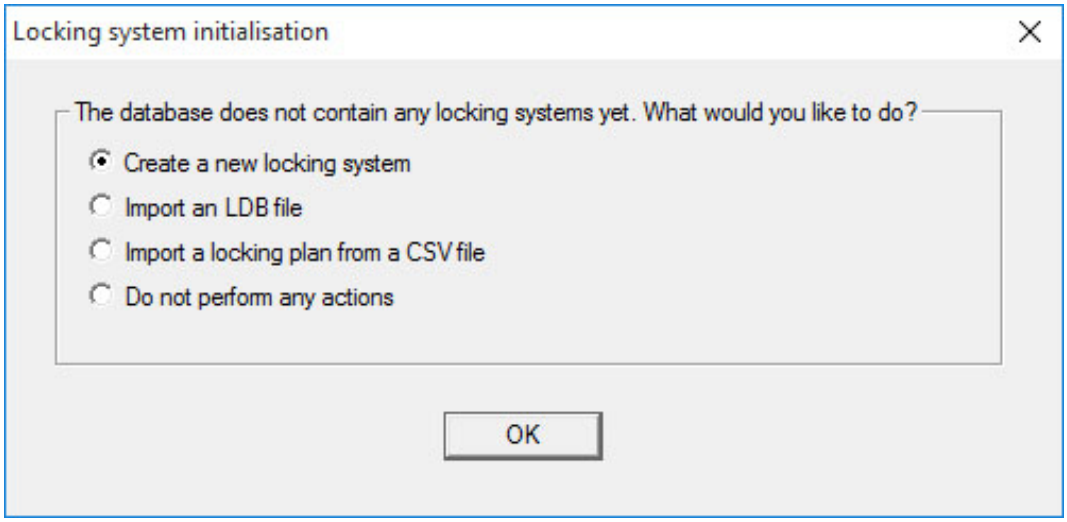


NOTE

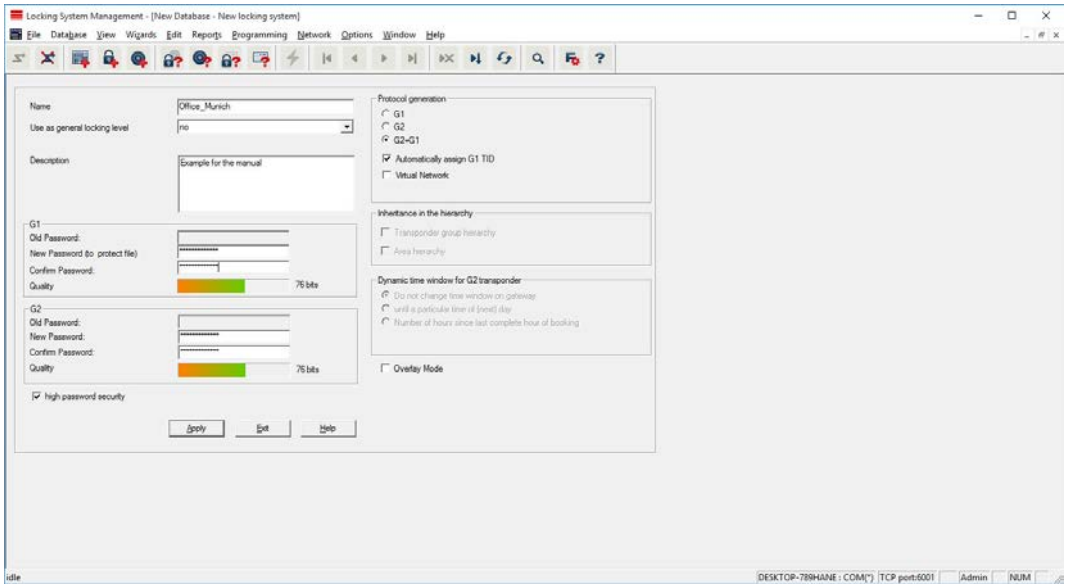
The user password will be requested each time that you log on to the database. Several users with different passwords and rights can be created for LSM Business.

Create locking system

1. A set-up wizard opens up once you have issued a new password:



2. Select "Create a new locking system" to add a completely new locking system. Confirm by pressing "OK".
3. Define the characteristics of the new locking system and issue secure passwords. *You can make changes at a later stage any time; however, this very time consuming after initial programming of components due to the programming requirements.*



4. Click on "Apply" to create the new locking system.

5. Click on "OK" to access the new locking system directly.

NOTE

The locking system password is programmed into all SimonsVoss components and managed with LSM software. You cannot make any changes to the programmed components without this locking system password, which is also indicated in the LSM software. *Observe the section on Recommended approach to handling passwords [▸ 26] to ensure that the locking system is operated without any problems.*

If the locking system password is changed, all programmed components must be reprogrammed.

5.3.1 Overview of protocol generations

	G1	G2
Access rights administration:	Locking devices	Locking device and ID medium (only ID medium in VN)
Number of locking devices:	16,000	64,000
Number of transponders:	8,000	64,000
Number of locking systems on a transponder:	3	4 x G2 + 3 x G1
Time zone groups:	5+1	100+1
Loggable access events in a locking device:	Cylinder: 1,000	Cylinder: 3,000; SmartRelay: 3,600 (200 as Gateway)
Physical access list on transponder:	No	1,000 per G2 locking plan (including date, time, locking device ID)
Procedure for group administration:	Adjustable; number is defined in the group	No pre-setting required; rights and exceptions are entered onto transponder
Replacement transponders:	7 replacement transponders using overlay mode	No pre-setting required
Network-capable:	Yes	Yes

	G1	G2
Virtual network:	No	Yes, circulate Block IDs in VN
Engage interval:	5 or 10 sec.	1 to 25 sec.; engage time can be doubled on an individual basis for transponders – max. 25 sec.
Time-restricted authorisation:	Yes	Yes
Battery warning:	Level 1; Level 2; storage mode	Level 1; Level 2; freeze mode
Battery replacement:	SmartCD	Battery replacement transponder together with authorised transponder or SmartCD
LSM/LDB:	All versions	LSM 3.0 and higher
Active/passive:	Yes / yes	Yes / yes

5.3.2 G1 locking system

The G1 standard is the first SimonsVoss protocol generation. This standard is compatible with the predecessor to LSM software: The LDB Locking Database Software.

NOTE

Only use this now obsolete protocol if you need to manage existing locking systems in a G1 environment. We recommend using G2 protocols with current G2 components for an up-to-date locking system.

5.3.3 G2 locking system

G2 is the current protocol generation used for SimonsVoss components. The G2 protocol offers many improvements compared to the preceding G1 protocol.

NOTE

Use the G2 protocol whenever possible. Using this protocol and its associated G2 components is the only way to set up and manage a locking system in line with the latest standards.

5.3.4 Mixed G2 + G1 system

The advantages of a mixed system *(using G1 and G2 components in a locking system at the same time)* also bring small disadvantages *(poor overview of components used; not a real G2 experience)*.

Mixed systems basically operate in a G1 environment. The only advantage of a mixed system is that G2 components can also be used at the same time. G2 components are limited in their use in a mixed system.

A mixed system can enable older G1 components and current G2 components to be used at the same time. The backward-compatible support for older components enables you to use existing components or components already in use efficiently. This function is specially designed for such special cases. However, you are not able to use individual, particularly convenient properties of G2 components.

5.3.5 Overlay mode

Overlay mode can only be activated in the G1" or "G2 + G1" protocol generations.

Overlay mode provides a very convenient feature for the restricted G1 protocol generation: the option of using newly programmed transponders directly without reprogramming the locking device. However, this feature only functions for up to 7 newly added transponders.

In the G2 protocol generation, such programming can be carried out using a transponder or a locking device.

7 further transponder IDs are added for each transponder ID if overlay mode is enabled:

Transponder IDs start at ID 64

- Transponder 1 with transponder ID 64: The Transponder IDs 65 - 71 are also reserved.
- Transponder 2 with transponder ID 72: The Transponder IDs 73 - 79 are also reserved.
- Transponder 3 with transponder ID 80: The Transponder IDs 81 - 87 are also reserved.
- and so on.

Example – replacement transponder: A replacement transponder needs to be programmed for Transponder 2 with Transponder ID 72 due to loss or theft. This replacement transponder is assigned the reserved Transponder ID 73. If the newly programmed replacement transponder is operated on an authorised locking device, the locking device engages and the "old" transponder 2 with Transponder ID 72 is blocked from use on the locking device. The process can be completed with a corresponding feedback signal to the LSM software.

It is possible to hold up to 1,000 transponders in reserve in this way.

5.4 Backing up the database automatically

Create resp. edit the batch script with a text editor to save the database automatically. Alternatively use the LSM installation toolbox.

The commands and the corresponding timeouts for Smart.XChange and the transponder terminal are optional:

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

You only need those if you actually use the services. Save the file with the extension .bat to the SimonsVoss folder. This batch script performs the following actions:

1. Stops services which use the database
2. Removes old backup
3. Copies database to the backup directory
4. Restarts services

Content of the batch script:

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

```
net start VNHostSvr /y
timeout /t 30
net start SVCommNodeSvr /y
timeout /t 30
net start TransTermSvr /y
timeout /t 30
net start Smart.XChangeService /y
```

Instad of the paths *C:\SimonsVoss\sv_backup* and *C:\SimonsVoss\sv_db*.** enter your own paths resp. network paths to your database respectively to your backup directory.

In order to create backups use the Windows built-in task planner to execute this batch script regularly (ideally daily). Select the created script to be executed. No further parameters are necessary.

Please note:

Default settings for security options

- Execution with the "system" account instead of an administrator account
- Enable: Execute independently of whether users are logged in or not
- Enable: Do not save the password
- Enable: Execute with the highest privileges

Contact your IT department. They are the system owner and therefore responsible for the correct execution of the backup jobs and the archivation of the backups.

6. Programming devices

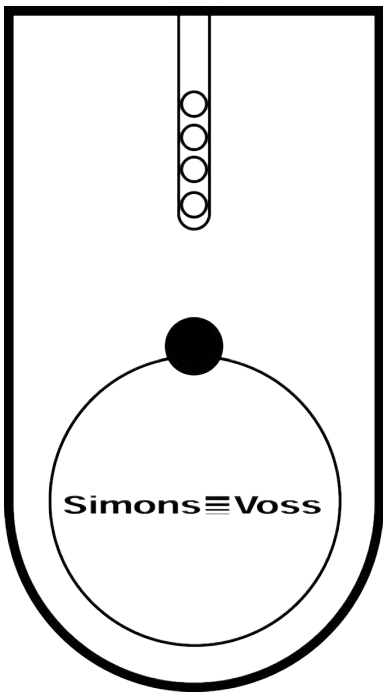
A programming device may be connected to any computer which has LSM software installed. All that is required is a USB port on the computer. The programming device is used to transfer settings and authorisations that you have made to SimonsVoss locking components. All components can also be easily read. You can also transmit settings and authorisations to components already programmed using LSM Mobile Edition or the SimonsVoss WaveNet network.

6.1 Identify programming devices and use properly

SimonsVoss programming devices are currently available in the following versions:

6.1.1 SmartCD.G2

The SmartCD.G2 is the standard programming device for active and hybrid components. You can use the SmartCD.G2 to programme all active SimonsVoss components. This programming device has a Bluetooth module and a rechargeable battery. It can also be easily used with LSM Mobile, so that it can be connected to a PDA or pocket PC. You can identify the SmartCD.G2 due to its SimonsVoss logo.



NOTE

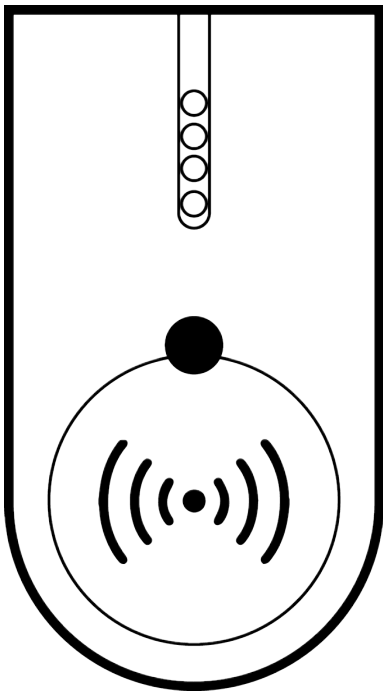
Initial charging of the built-in batteries.

The built-in rechargeable batteries are discharged when delivered.

- Charge the programming device for at least three hours before using it.

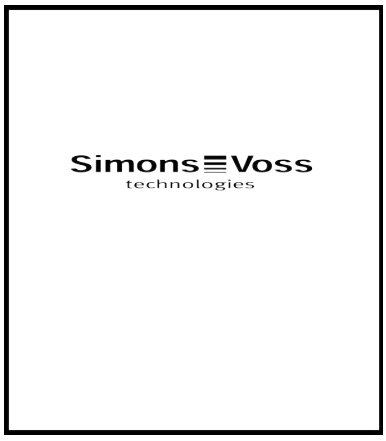
6.1.2 SmartCD.MP

You can use the SmartCD.MP programming device to programme and read passive components. Unlike the active SmartCD.G2, the SmartCD.MP is identified by the radio symbol. The SmartCD.MP can only be used via a direct USB connection.



6.1.3 SmartCD.HF

You can also use the SmartCD.HF card programming device to programme and read passive tags and cards.



6.1.4 SmartStick AX

The SmartStick AX is the standard programming device for all components with a BLE interface. All SimonsVoss AX components can be programmed using the SmartStick AX.

This programming device is connected and supplied with power via a USB cable.

Before programming, the AX components to be programmed must first be tapped with the SmartStick AX to wake up the BLE interface. The AX components are then recognised by the SmartStick AX for around 30 seconds and can be programmed.

6.2 Programming distance

A specific distance must be kept between the programming device and the components for successful programming and read processes.

SmartStick AX

After waking up the lock, the SmartStick AX has a range of up to 300 cm.

SMARTCD.G2

- The distance between SMARTCD.G2 and active components, such as locking cylinders or transponders, should be about 20 cm.
- Ensure that no other active components are in the immediate surrounding area during the programming or read process (radius of about 1.5 m to the SMARTCD.G2).

NOTE

The programming distance between SMARTCD.G2 and **SmartRelay or biometric reader** must be exactly 40 cm!

SMARTCD.MP

- The thumb-turn on the electronics side of the locking cylinder *(black ring between the thumb-turn and the profile cylinder housing)* must be held directly against the antenna symbol on the SMARTCD.MP.
- Hold the locking cylinder against the antenna symbol for the whole process.
- You can also use the SMARTCD.MP to programme cards by holding them directly on the programming device.

SMARTCD.HF

- Position the card or the tag, so that it is flush with the lower, left-hand corner of the SMARTCD.HF.

6.2.1 Programme hybrid locking devices

You use the SmartCD.G2 to programme hybrid locking devices. You also need to connect (and install) a SmartCD.MP or SmartCD.HF at the same time for programming.

Exception: The SmartHandle AX can also be programmed with the SmartCD.MP

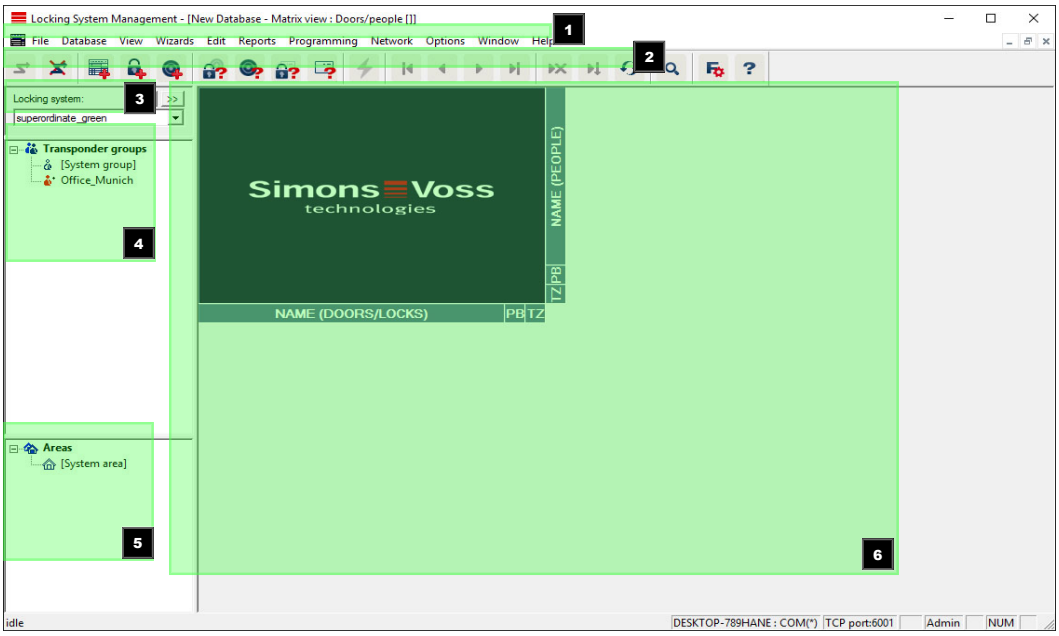
6.3 Check connection

You can use the LSM software to check that the programming device has been correctly connected and installed:

1. Select "Programming" in the menu bar.
2. Select the programming device to be checked, e.g. "Test SmartCD active" to test the SmartCD.G2.
   ↳ The test will start immediately.

7. User interface

The LSM software user interface is divided up into the following sections:



1. **Menu bar**

   Use the menu bar to open basic functions.

2. **Menu ribbon**

   You can use the menu ribbon to open important and frequently used functions directly.

3. **Locking system**

   This is where you can switch quickly between different locking systems in the project.

4. **Groups**

   Bring users together into groups to work more effectively.

5. **Areas**

   Bring locking devices together into areas to work more effectively.

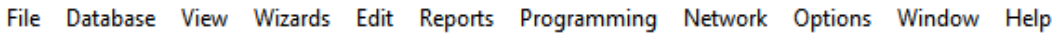
6. **Matrix**

   The matrix displays an overview of the selected locking systems.

NOTE

Some functions/entries may not be available, depending on the LSM software used.

7.1 Menu bar



7.1.1 File

7.1.1.1 Print Matrix

Prints the selected locking system.

7.1.1.2 Page view

Shows the matrix as a preview before printing.

7.1.1.3 Printer set-up

Set advanced print options, such as page size.

7.1.1.4 Change user password

This is where you can change the password for the user currently logged in.

7.1.1.5 Finish

Log off from project and exit LSM software.

7.1.2 Database

7.1.2.1 Log on

Log on to a project. *This function is only available if you are not currently logged on to a project.*

7.1.2.2 Log off

Click on "Log off" to log off from the current project.

7.1.2.3 Setup

This is where you can manage projects or databases. You have the following options open to you:

- Edit an existing project.
- Delete an existing project.
- Create a new project.
- A default project can be selected, which will load automatically.

7.1.2.4 Backup

You can used this function to back up your database and restore backed-up databases.

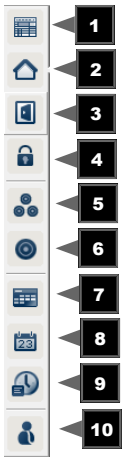
7.1.3 View

7.1.3.1 Status bar

Shows or hides a status bar on the lower edge of the screen. The status bar is shown by default. The status bar displays items such as the current locking system status, computer name and connection with the programming device.

7.1.3.2 Edit

You can use *View/Edit* to show an additional menu ribbon which provides quick access to the following functions:



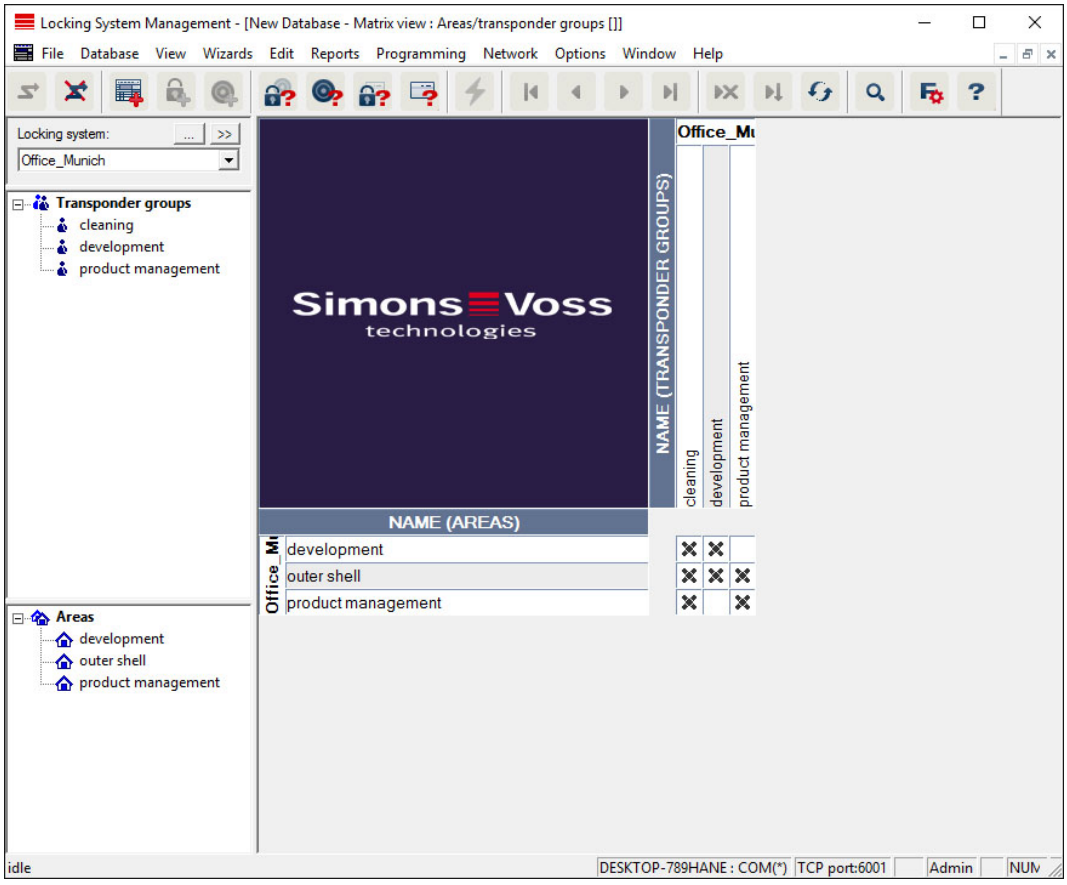
1. **Locking system properties**
2. **Area**
3. **Door**
4. **Locking device**
5. **Transponder group**
6. **Transponders**
7. **Public holiday list**
8. **Public holiday**
9. **Time zones**
10. **Person**

7.1.3.3 Areas/transponder groups

This view forms a matrix which provides a visual display of hierarchical personnel and room structures. The matrix is also able to authorise transponder groups for complete areas. This makes it quick and easy to issue basic authorisations in this matrix. The Doors/Persons view allows you to issue deviating authorisations in the form of individual extensions or restrictions.

If you need to work with transponder groups and areas in the locking system, this option provides you with the following decisive advantages:

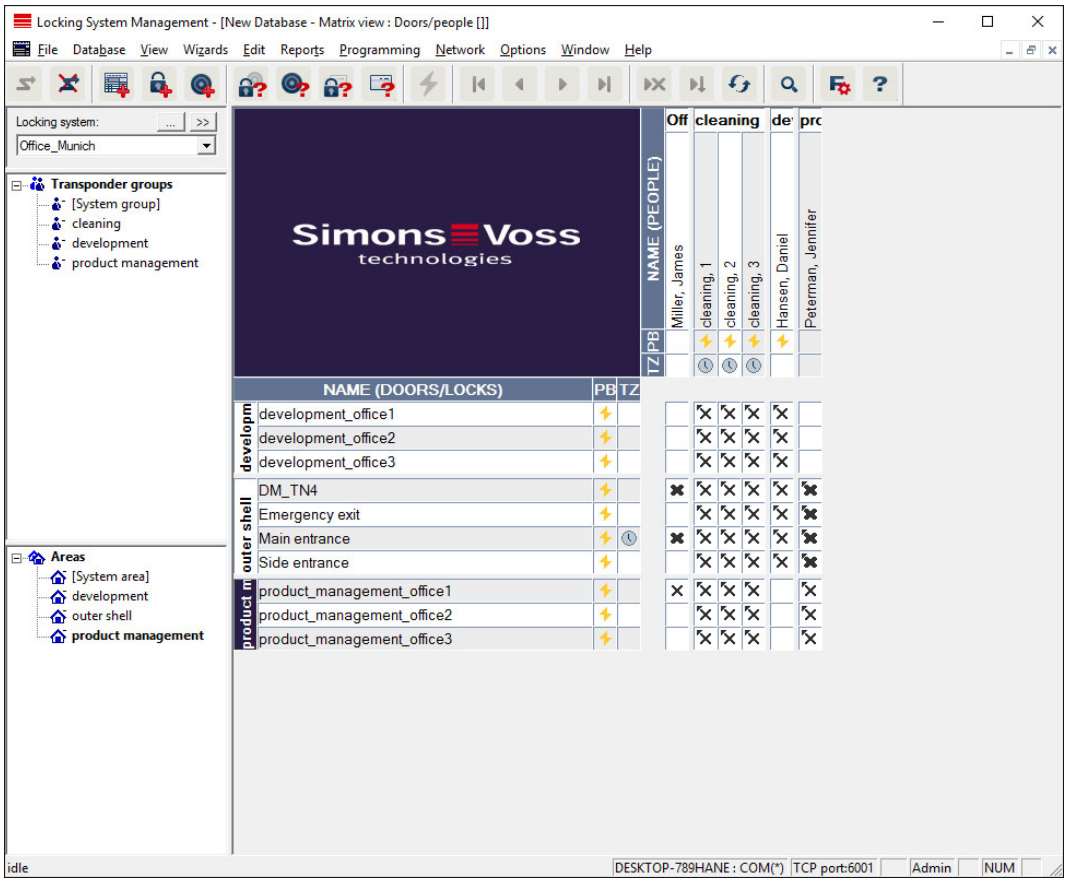
- Reduced view, where only transponder groups and areas are displayed. This makes it easier to find your way in the matrix.
- Issuing or withdrawing authorisations for entire areas from entire groups.
- Persons who are added to a group at a later stage receive all group rights automatically.



7.1.3.4 Doors/Persons

This view displays the individual authorisations for all persons for individual doors. Obviously, the matrix is extensive as a result. However, it allows precise setting of exceptional-case authorisations, enabling pre-set group

authorisations to be extended or even reduced. This view is thus suitable for implementing individual extensions or restrictions after the basic structure has been established at *Areas view/Transponder groups*.



7.1.3.5 All secondary areas/Open groups

This view setting opens all areas and groups, thus displaying all locking devices, even if individual areas have been hidden beforehand.

7.1.3.6 Log

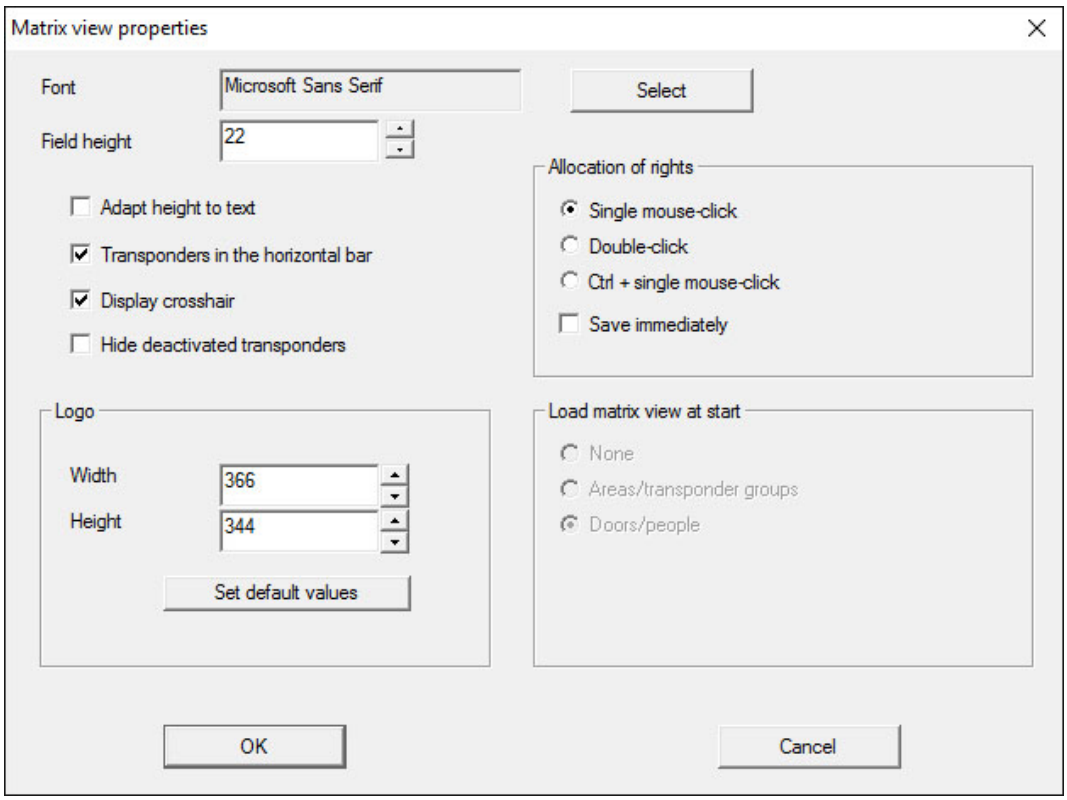
The log can be used to view all actions which have been carried out on the database. You can identify which user created or changed a particular locking device or view log-ons to the database, for example.

- Logs can be filtered as you require – by a time period, a user or an action.
- The list can then be sorted by clicking on the required column heading, e.g. by date, time or name.

7.1.3.7 Matrix settings

Each user has the option of setting up their preferred screen as their default screen. This screen is shown after logging on. Different basic settings can also be enabled here.

You can use the menu bar to adjust settings on the standard view at *View/ Matrix view properties*.



- **Font**

  You may select any fonts.

- **Field height**

  You can set the height for fields in points.

- **Adjust height to the typeface**

  Adjust the height automatically to the typeface.

- **Transponders in the horizontal bar**

  Transponders are displayed in the horizontal bar by default. You can change this setting if you wish to manage more locking devices than transponders.

- **Shows crosshair**

  Shows a crosshair for more precise navigation.

- **Hide deactivated transponders**

  Hides deactivated transponders.

- **Logo**

  Change the size of the logo.

- **Issuing of authorisations**

Mistakes can be quickly made with a mouse click, particularly in the case of large locking systems. In such cases, we recommend changing this setting.

Activate "Save immediately" if you wish to apply changes to authorisations immediately by simply clicking the mouse.

7.1.3.8 Additional columns

Additional columns can be added to the horizontal and vertical borders in the matrix to provide additional useful information to the user. The settings made only apply to the screen view in which they were configured. Different information is available, depending on the screen type. You can also set the sequence in which the data is displayed as you require. This is saved as a user-specific setting (Windows user).

This is how you unhide additional columns in the matrix:

1. Select the *View/Additional columns* menu bar followed by the required view, e.g. *Transponders/Persons.*
2. Highlight all other information which you wish to be displayed.
3. Sort the sequence using "Up" or "Down".
4. Click on the "OK" button to confirm your selection.

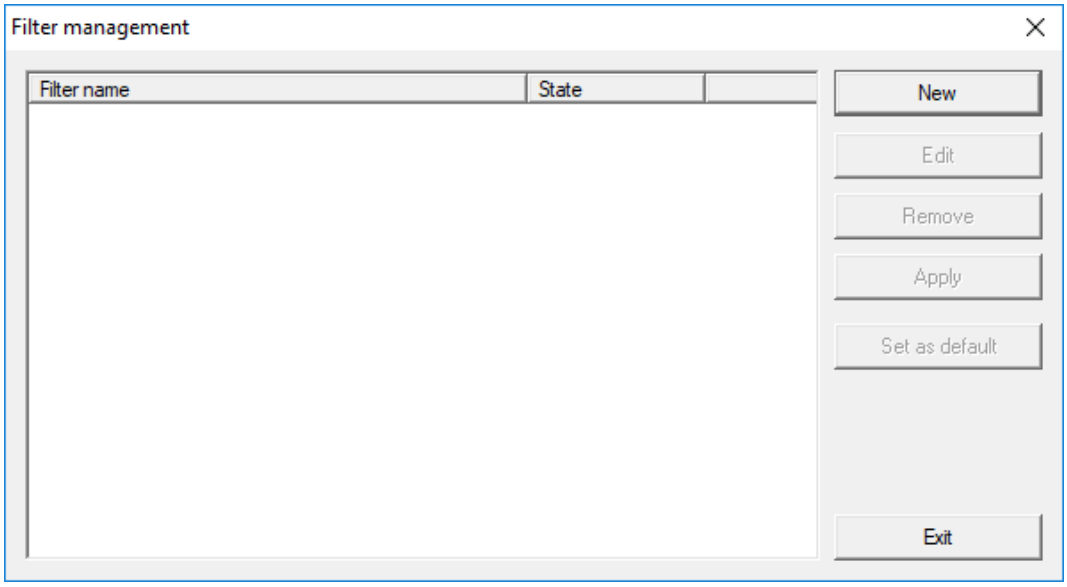
7.1.3.9 Refresh

Refreshes the matrix view.

You may need to update the matrix manually in exceptional cases, especially for extensive locking systems or special settings.

7.1.3.10 Filter

The introduction of filters has made it easier to manage a locking system. You can select a wide variety of filter options and apply these filters to an extensive variety of persons or person groups. This not only allows you to access more information by displaying optional additional columns, but the filter function also enables you to ensure that your views are clearly arranged.



- **New**

  Creates a new filter

- **Edit**

  Edits a selected filter

- **Remove**

  Removes a selected filter

- **Apply**

  Applies the selected filter. The button changes to "**Turn off**" if a filter is applied.

- **Set as default**

  This filter will be used by default

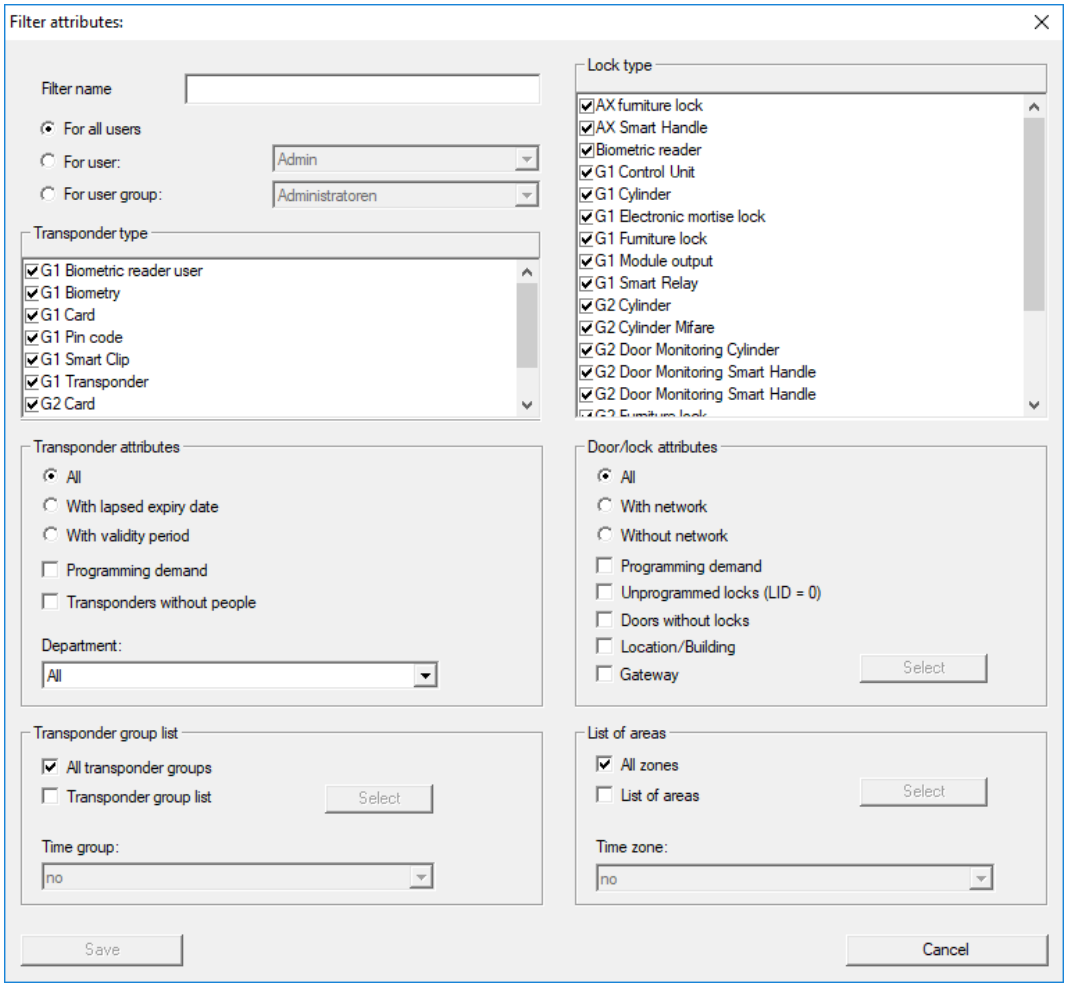
- **Finish**

  Exits from filter management and returns to the matrix

NOTE

A filter only remains active until it is switched off again.

You can use the "New" button to create a new filter:



- **Filter name**

  Enter a meaningful name for the new filter.

- **User restriction**

  User or user group which can apply the filter.

- **Transponder type**

  Type of transponder which should be displayed.

- **Transponder properties**

  Restrictions which concern the properties of the transponder (e.g. validity period or programming requirement).

- **Transponder group list**

  Restrictions which concern the transponder's assignment to a group (e.g. "Executive management" transponder group).

- **Locking device type**

  Type of locking device which should be displayed.

- **Doors/Locking system properties**

Restrictions which concern the properties of the locking device (e.g. with network or programming requirement).

- **Areas list**

  Restrictions which concern the locking device's assignment (e.g. "Reception" area).

7.1.4 Installation wizards

The installation wizards make it easier for new users to start using the LSM software. Experienced users also benefit from these wizards, which can be used to make all settings one after another from a central point.

7.1.4.1 Wizards/Door

This wizard can be used to add a new door step by step.

7.1.4.2 Wizard/Person

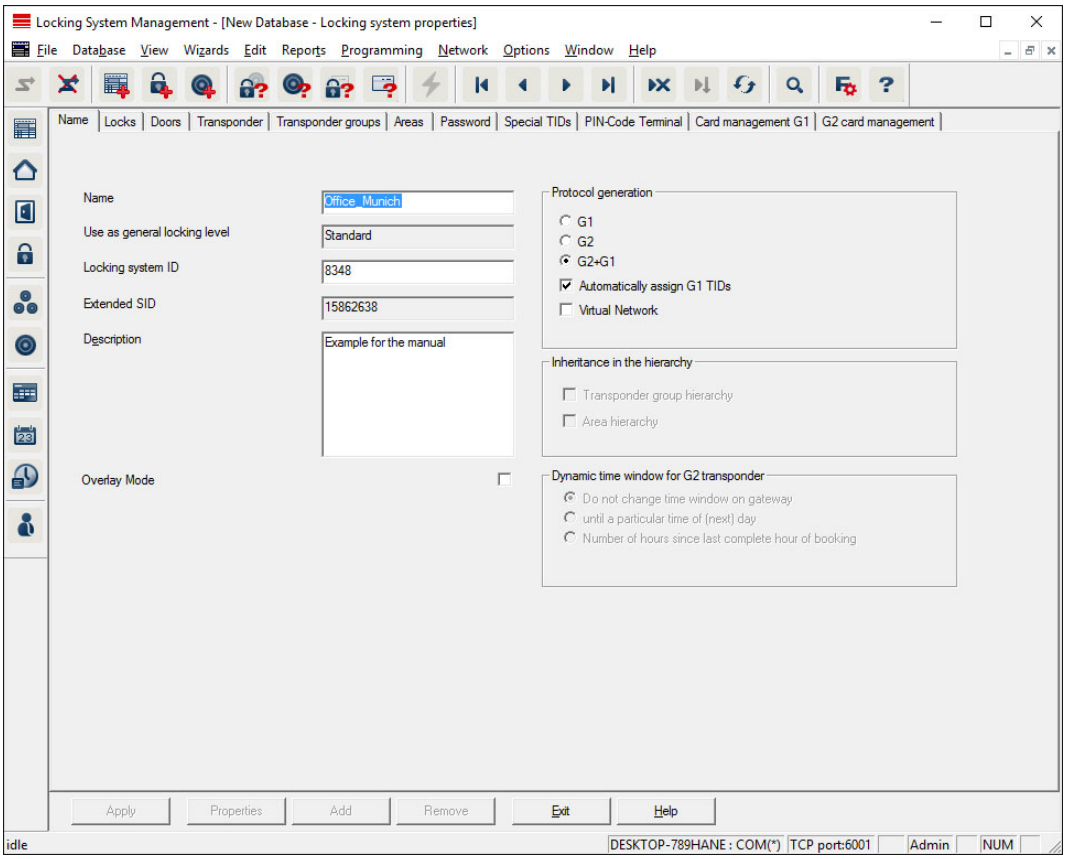
This wizard can be used to add a new person step by step.

7.1.5 Edit

7.1.5.1 Properties: Locking system

Settings for the currently selected locking system.

Name



- **Name**

  Name of the locking system

- **Use as a common locking level**

  Establishes the common locking level

- **Locking system ID**

  Locking system number

- **Extended SID**

  Additional distinctive feature of the locking system

- **Description**

  Blank field to describe the locking system

- **Operate in overlay mode (G1 only)**

  Activates the overlay mode. *This function must already be enabled when the locking system is created. You cannot change it afterwards.*

- **Protocol generation**

  Selects the extension variant for the hardware components

- **Inheritance in the hierarchy [LSM BUSINESS]**

  Select the inheritance areas

- **Dynamic time slot for G2 transponders**

  Advanced time settings for use with gateways:

  - **Do not change time window on the gateway**

    There is no time limit on the validity period for any G2 transponders able to book at the gateway.

  - **Until a specific time on the (next) day**

    There is a time limit on the validity period for all G2 transponders able to book at the gateway.

  - **Number of hours from the last full hour of the booking**

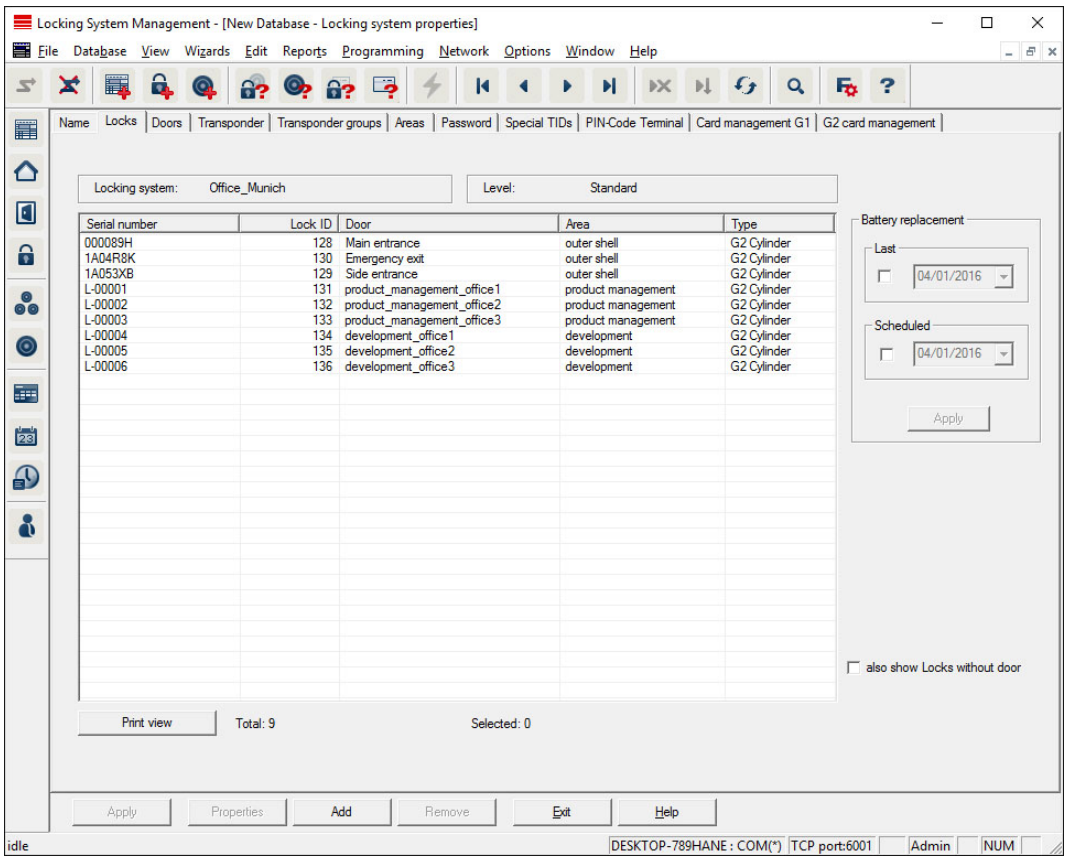
    The validity of all G2 transponders able to book at the gateway is extended by the specified number of hours.

NOTE

Virtual network not required

You do not need to configure a virtual network to use a gateway to manage time frames.

Locking devices

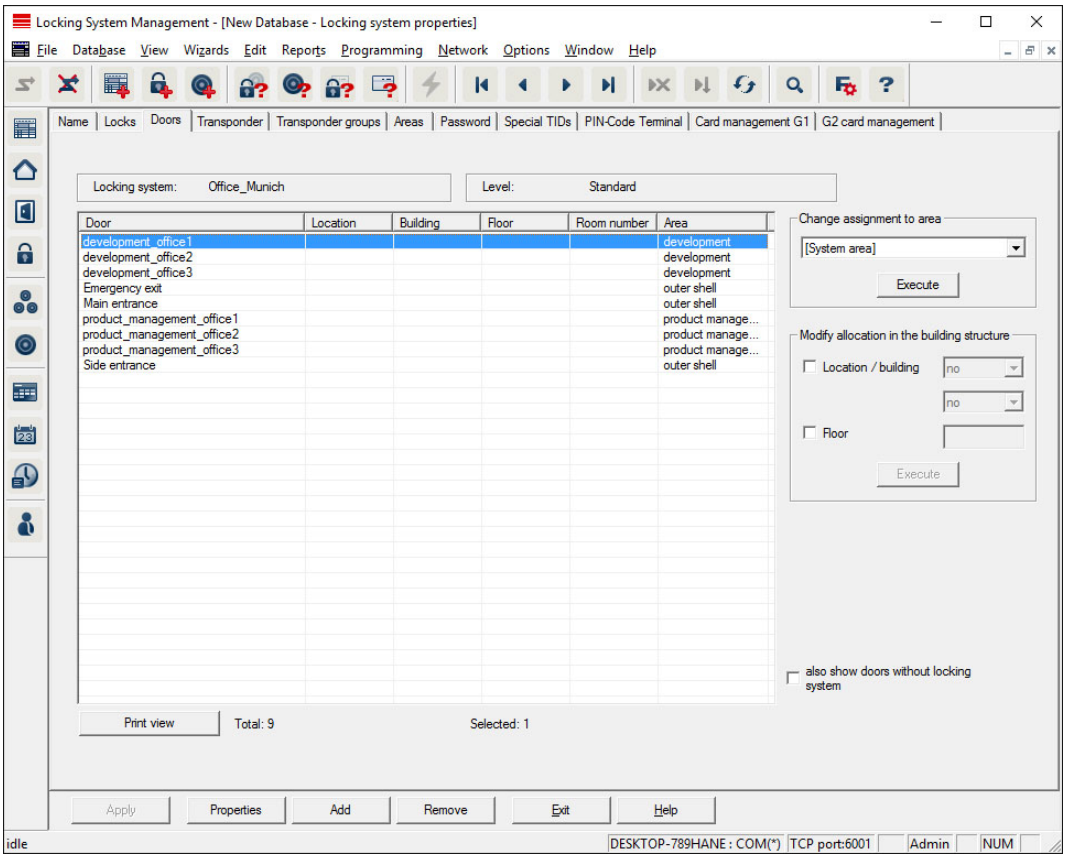


This tab gives you an overview of the locking devices used in the locking system. The devices are all displayed in detail in a table.

Notes on battery replacement can also be recorded:

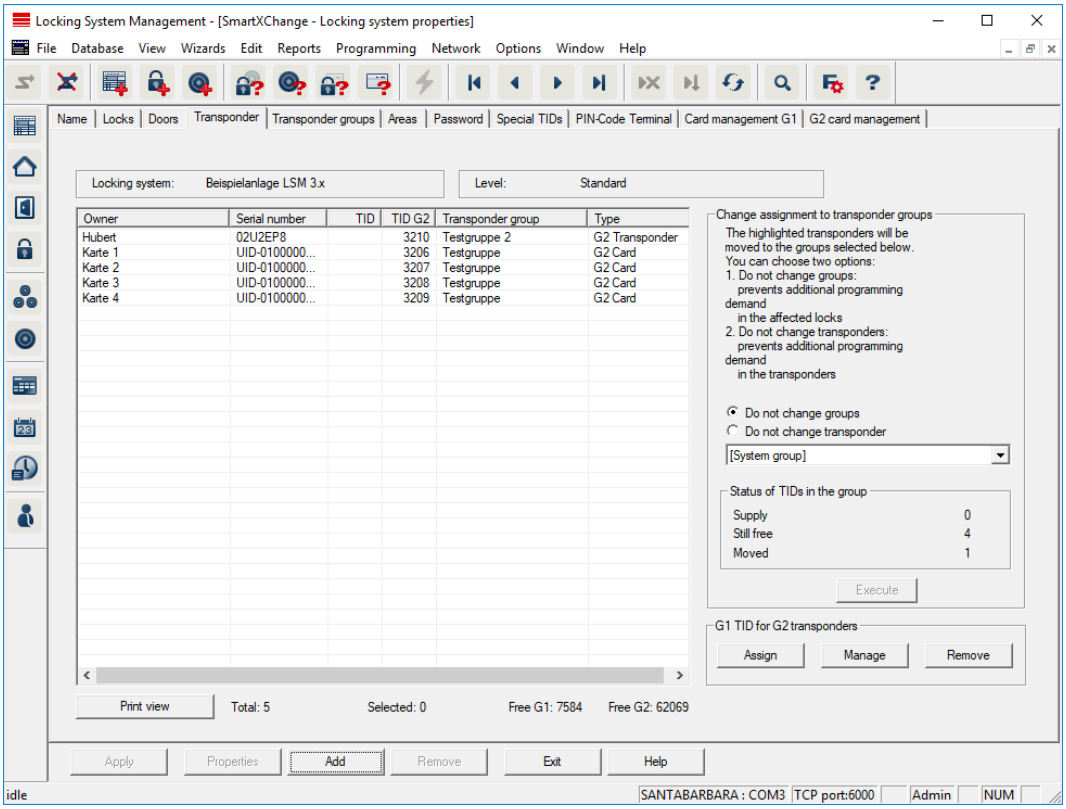
The scheduled battery replacement is displayed on the warning monitor and in the action list in the respective locking device. You also have the option of entering the scheduled battery replacement in the action list for the respective locking device in conjunction with a number of locking devices. You can enter a completed battery replacement for one or several locking devices under 'Last'.

Doors



This tab displays the correlation between the doors contained in the locking system and their assigned areas. The devices are all displayed in detail in a table. It is possible to select one or more doors and assign them to a specific area, location or floor. Ensure that the areas, locations or floors have already been added.

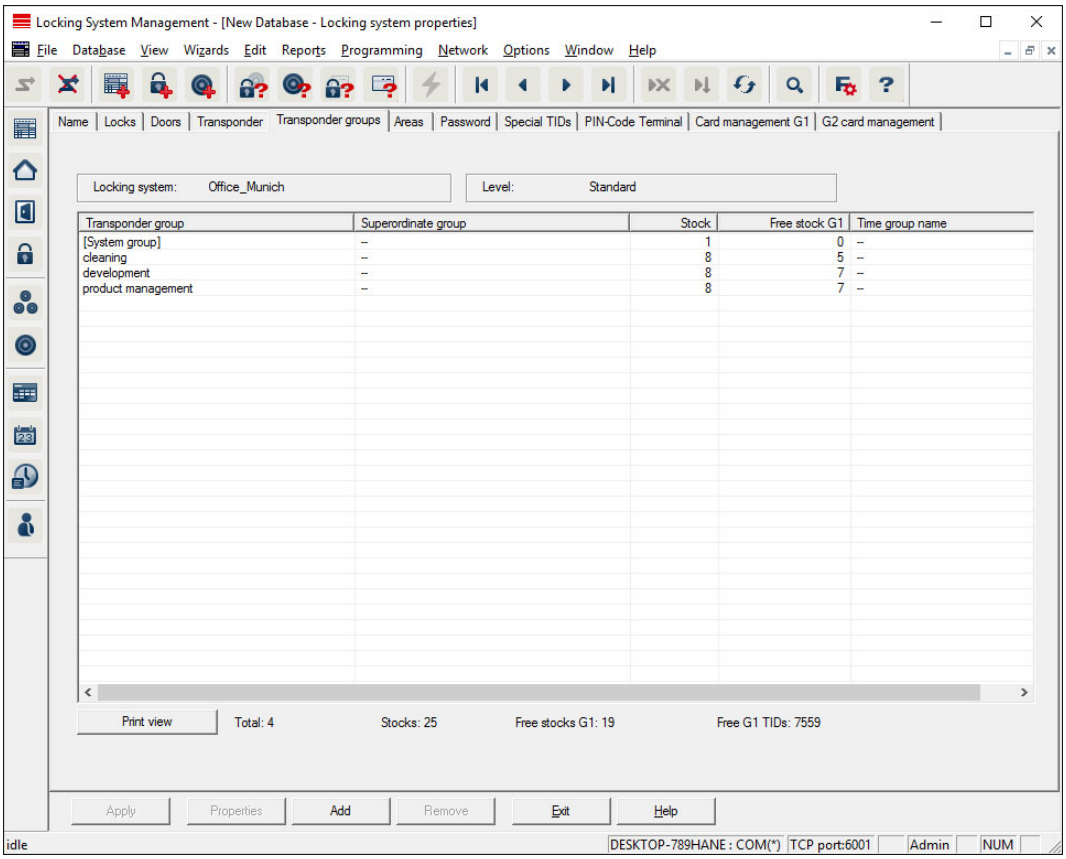
Transponders



This tab gives you an overview of the transponders contained in the locking system. The devices are all displayed in detail in a table.

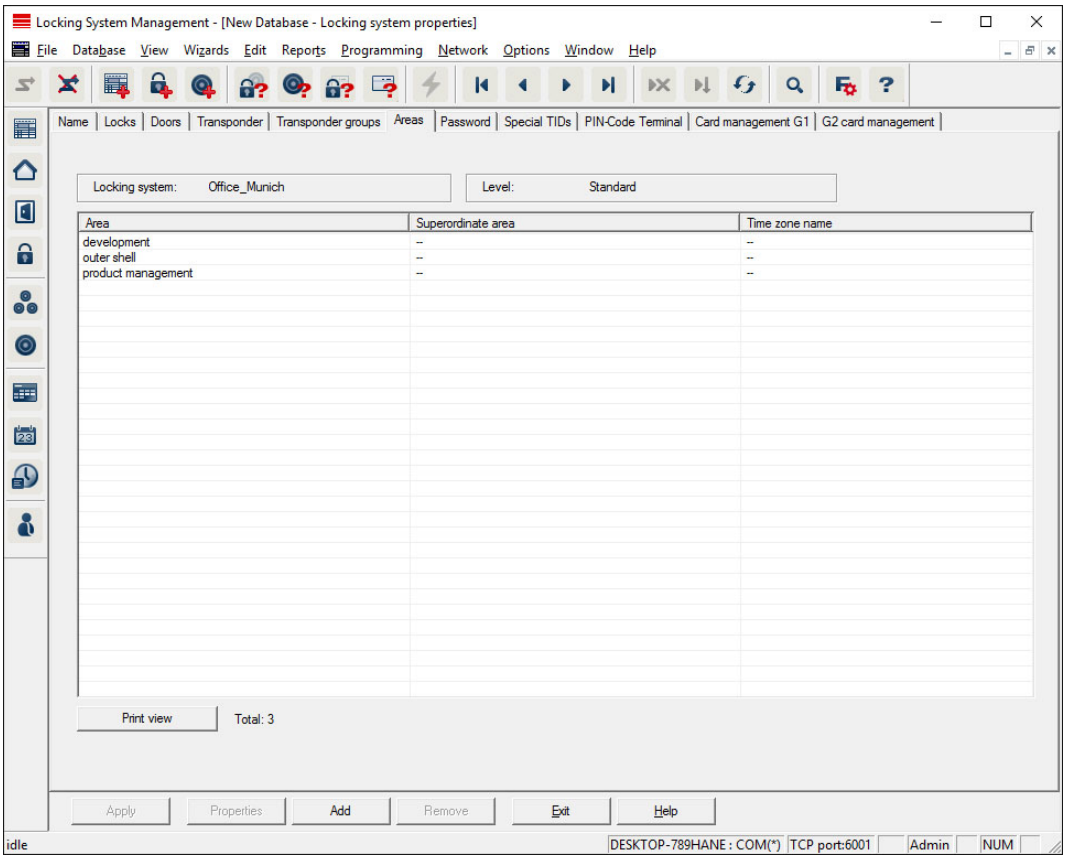
It is possible to select one or more transponders and assign them to another group. Ensure that the transponder groups have already been added.

Transponder groups



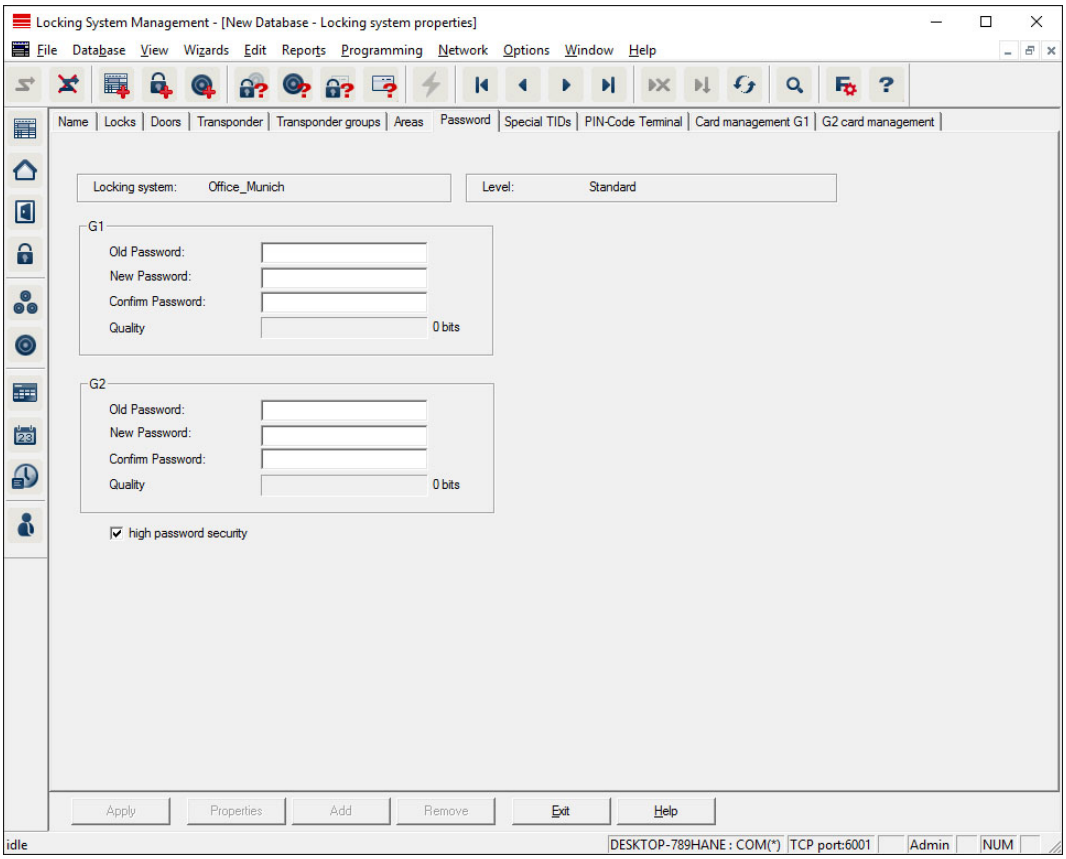
This tab gives you an overview of the transponder groups used in the locking system. The devices are all displayed in detail in a table.

Areas



This tab gives you an overview of the areas used in the locking system. The devices are all displayed in detail in a table.

Password



This is where you can change the locking system passwords used to change component programming.

CAUTION

Loss of locking system password

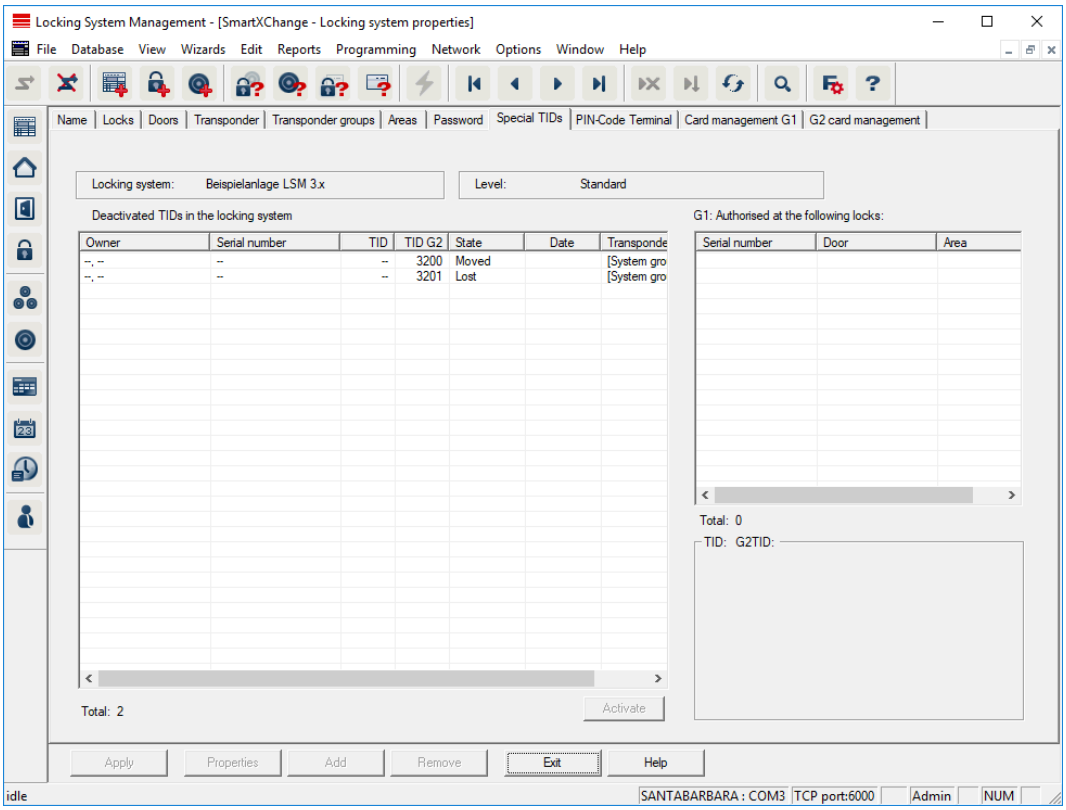
The locking system password is a central component of the security concept. The loss of the locking system password restricts the operation of the locking system and is a security risk.

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!

NOTE

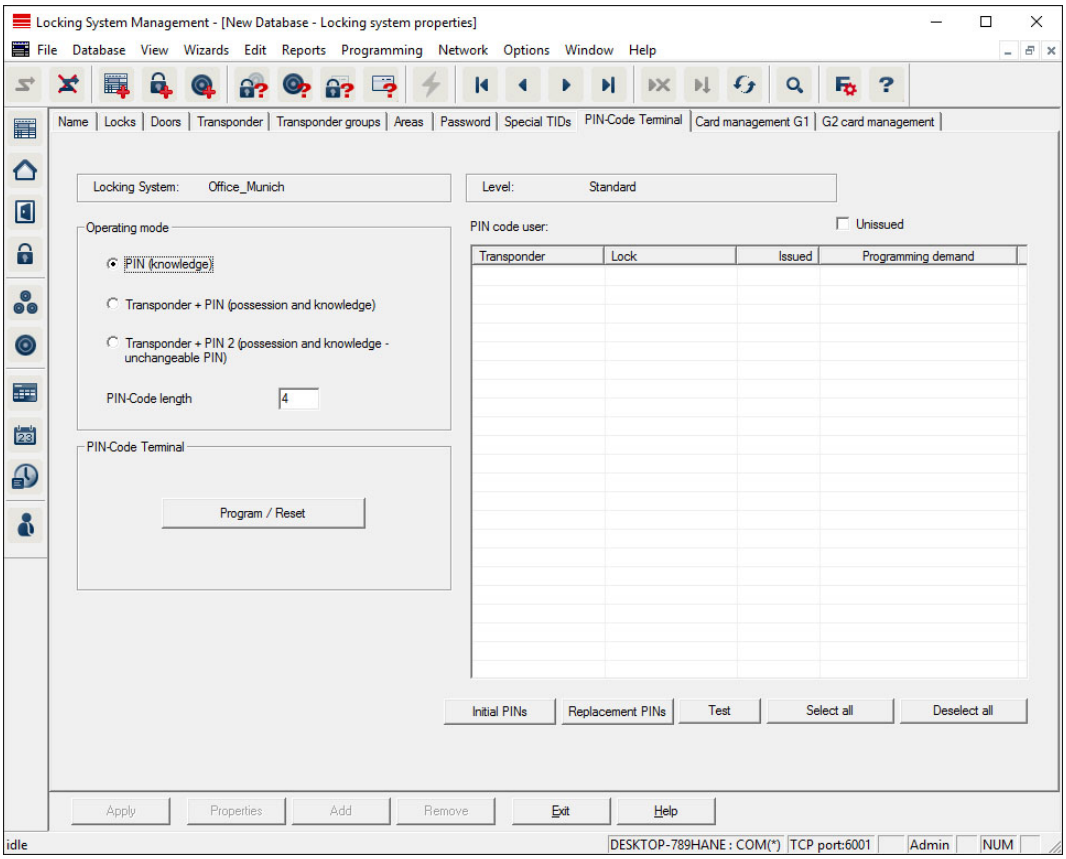
Components with different locking system passwords cannot communicate with one another.

Special TIDs



- The large, left-hand table shows an overview of the following transponders:
  - Deactivated transponders
  - Removed transponders
  - Lost transponders
  - Returned transponders
  - Temporarily deactivated transponders
- The smaller table on right-hand side shows all locking devices which the transponders selected in the left-hand table are authorised to use.
- The display pane under the small, right-hand table displays information and comments on the deactivated transponder.
- You can use the "Activate" button to re-activate a selected transponder *(depending on the pre-set status). In this case, a new TID is assigned to the transponder in the G2 protocol, which can generate programming requirements for the authorised locking devices.*

PIN code terminal



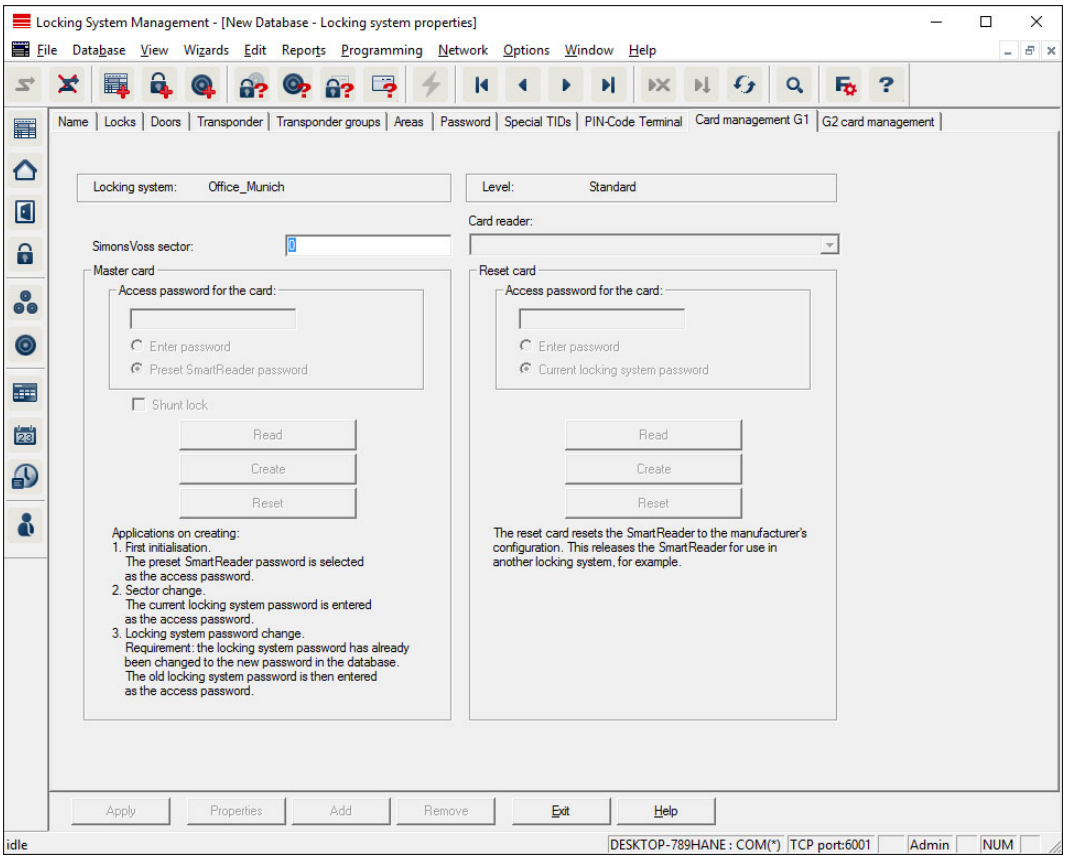
You can use this tab to add PIN code terminals and activate extended configurations.

For setting up the Pin Code Terminal, refer to the "Pin Code Terminal Manual" documentation, which you can find on the homepage:

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

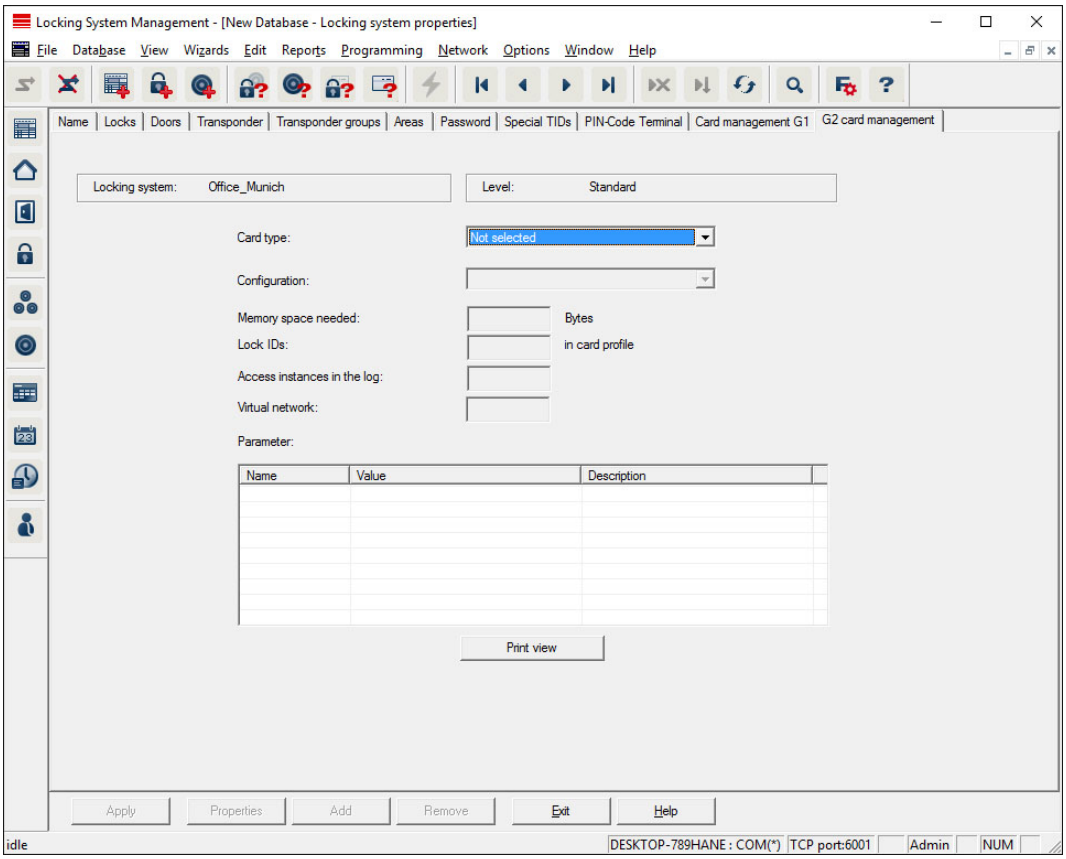
See *Help and other information [▸ 254]*.

G1 card management



Establish advanced properties and settings for your G1 cards (See *Card management [▸ 163]*).

G2 card management



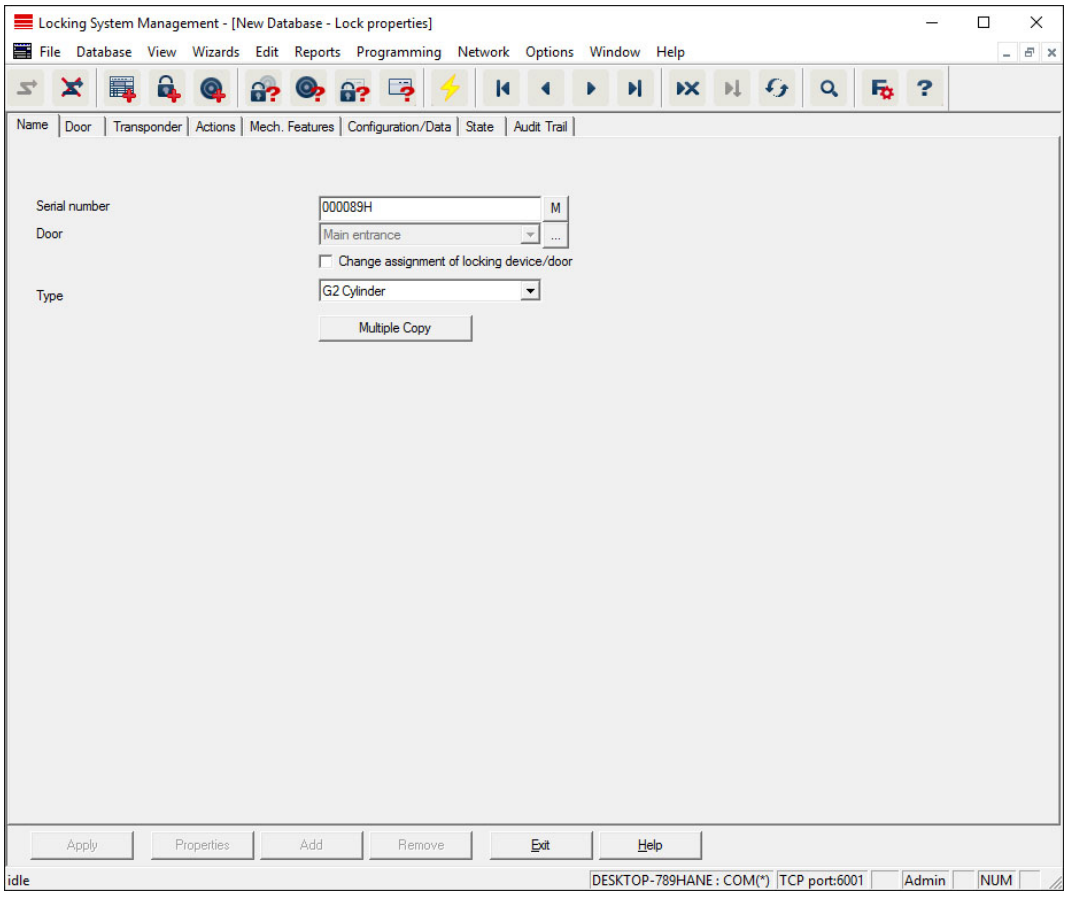
Establish advanced properties and settings for your G2 cards (See *Card management [▸ 163]*).

7.1.5.2 Properties: Locking device

Show and edit properties for the locking device currently highlighted.

A double click on the locking device opens the properties of the corresponding locking device directly.

Name



Serial number

Displays the locking device's serial number. The "..." button shows the door's properties.

Door

The door assigned to the locking device can be changed if the "Locking device assignment/Change door" checkbox is enabled. The "M" button shows the locking device in the matrix.

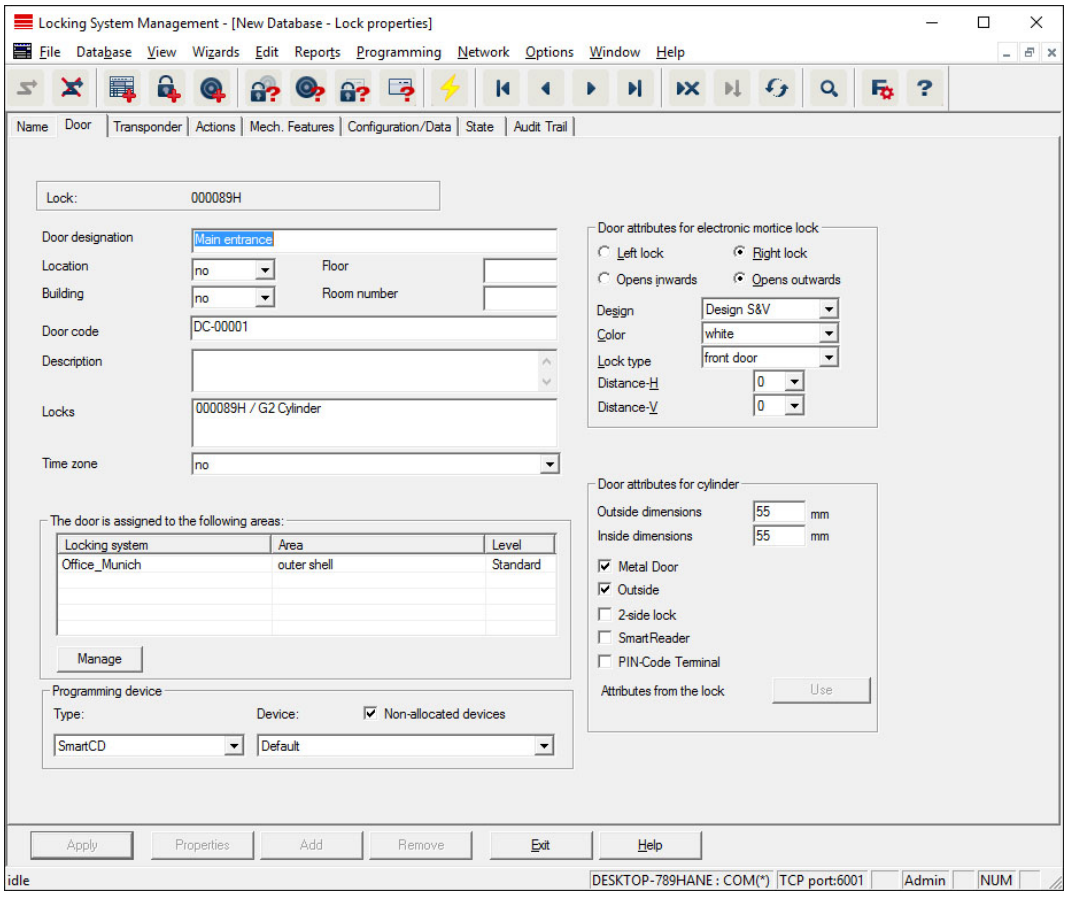
Type

Type of locking device.

Make multiple copies

Generates as many copies of the locking device with the same properties as required. A sequential number is also added to the name of the locking device.

Door



- **Door identifier**

  The name of the door.

- **Location**

  Location where the door is situated. (Locations need to have been added beforehand)

- **Building**

  Building where the door is situated. (Buildings need to have been added beforehand)

- **Floor**

  Floor on which the door is situated.

- **Room Number**

  The room number of the door.

- **Door code**

  Internal identifier for the door.

- **Description**

  Blank field to describe the door.

- **Locking devices**

  Locking devices which are assigned to the door.

- **Time zone**

  The door's time zone.

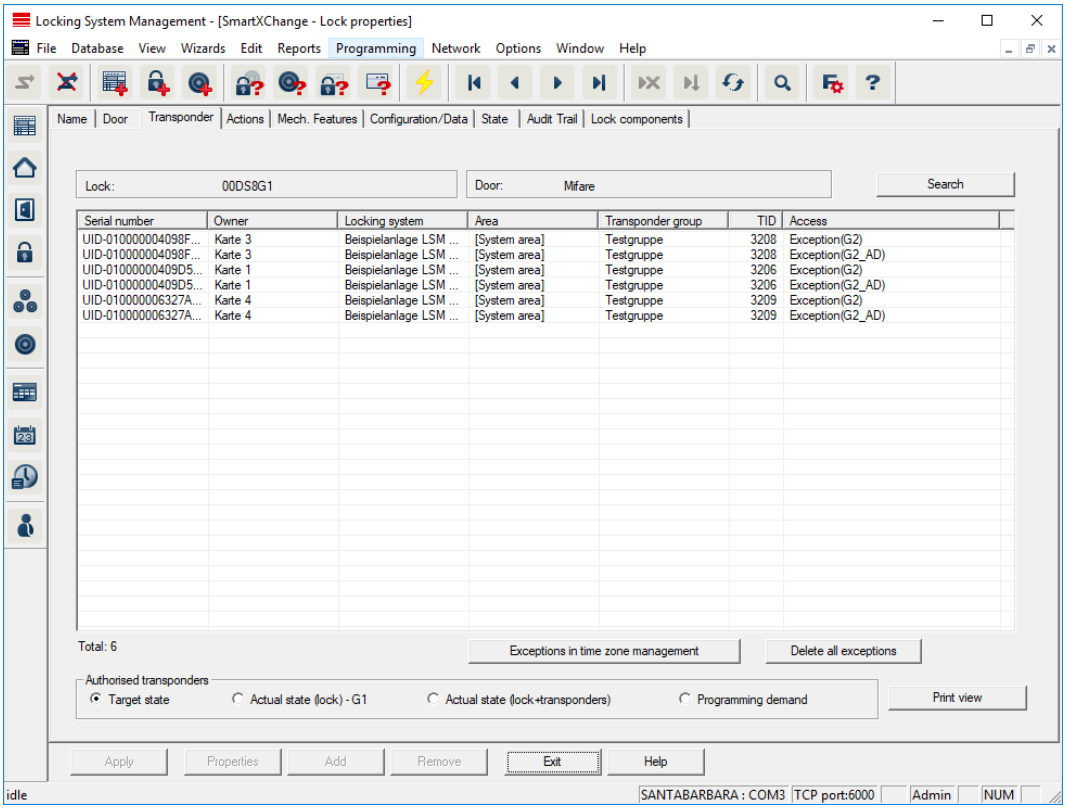
- **Programming device**

  Selects a specific programming device. (Particularly necessary for LON and WaveNet. Locking devices to which LON or WaveNet is assigned can also be programmed online wirelessly without a programming device.)

- **Door attributes**

  Information on the mortise lock and locking device. This allows you to see what replacement components are required if you need them.

Transponders



- **Table**

  Shows all transponders authorised for the locking device in a detailed list.

- **Authorised transponders**

  You can use the individual radio buttons to filter the table.

  - **Target state**

Displays the target status.

- **Current status (...)**

  Displays the current programmed status.

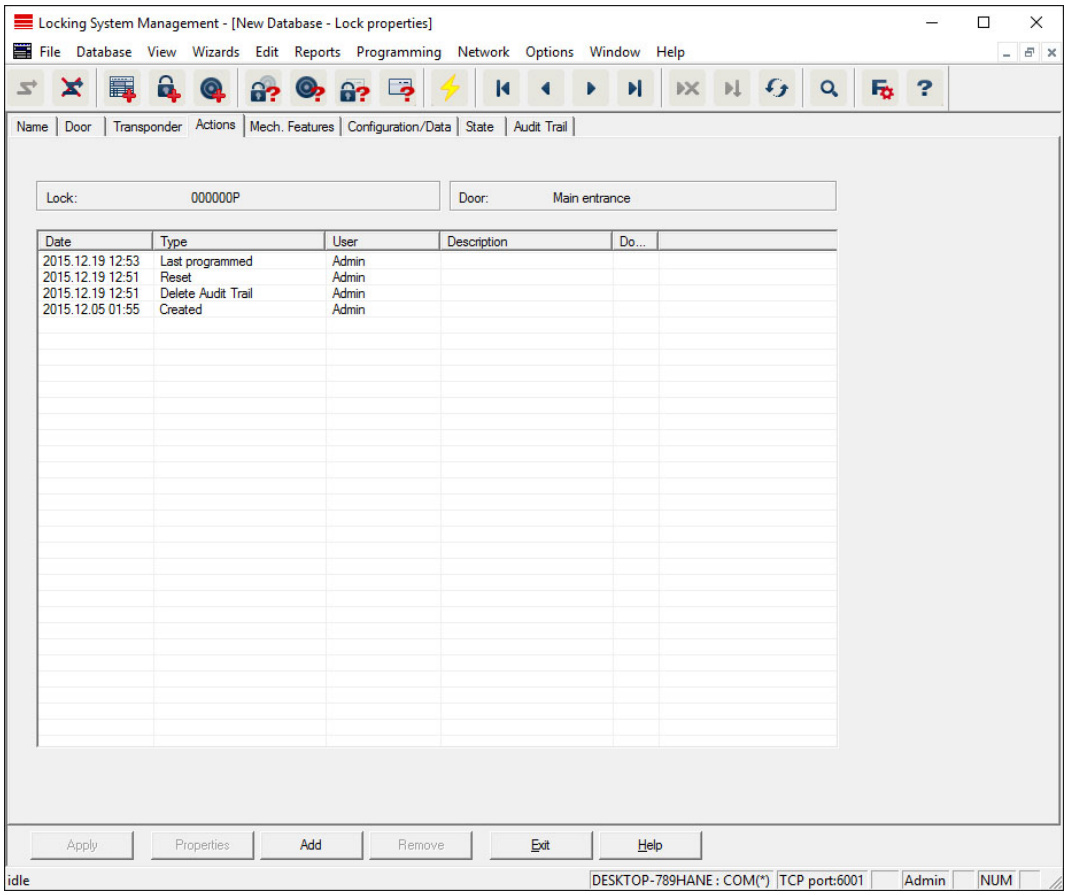
- **Programming requirement**

  Displays all transponders with programming requirements.

- Additional button "**Exceptions in time zone management**":

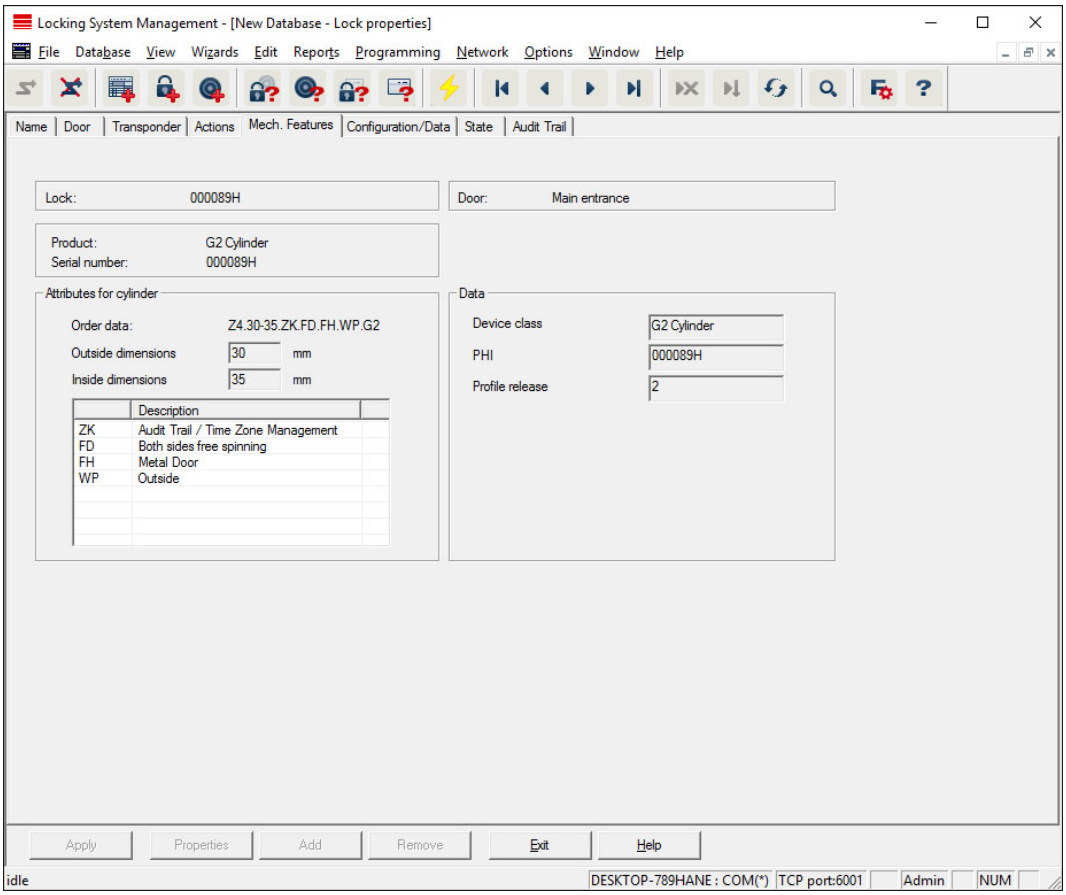
  This where exceptions for the transponder are displayed in time zone management.

Actions



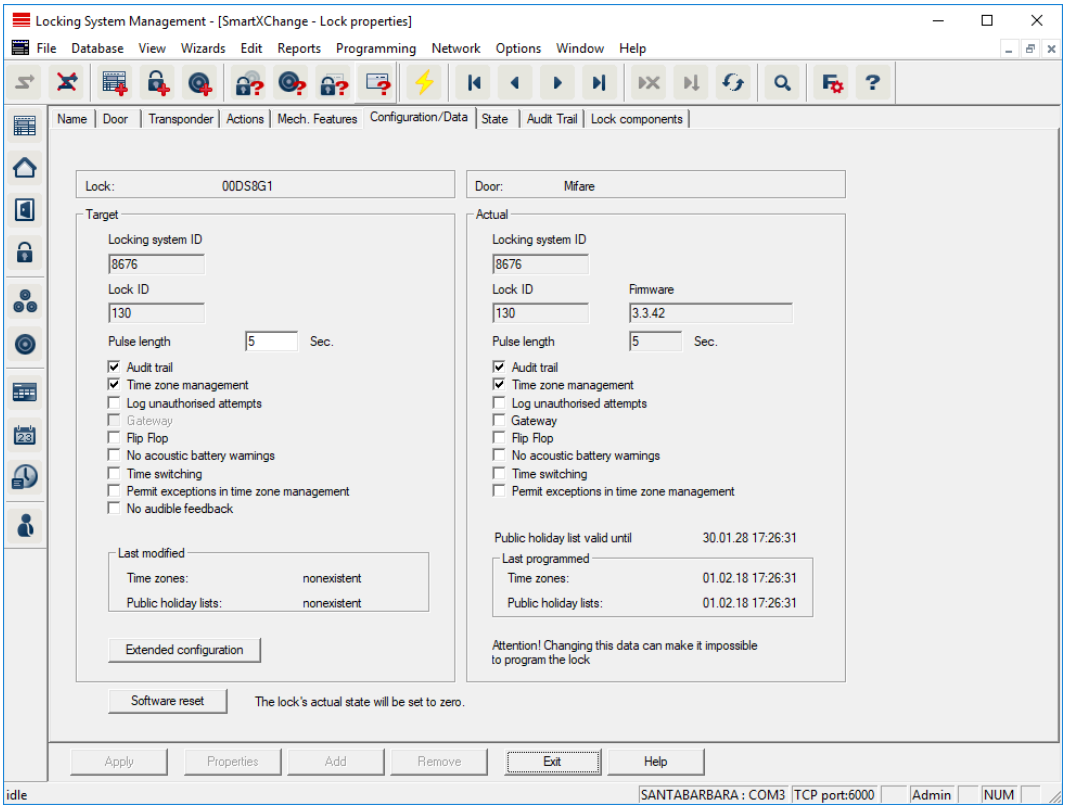
This table shows which actions (e.g. programming, authorization change, etc.) were carried out during locking. Different actions, such as "Last battery replacement", can also be added manually using the "Add" button.

Features



This tab shows the locking device's precise hardware options which are automatically entered during the initial programming.

Configuration/Data



This tab is divided into two sides:

- The left side shows the target status of the locking device – i.e. the desired status configured in the LSM software.
- The right side shows the locking device's current status – i.e. the status which was last programmed.

The following features can be enabled **depending on the locking device type**:

- **Access control**

  Option to log access events. *This function only works for components with an access control function.*

  Clarify whether the use of this option is allowed in your own particular environment, e.g. with the Works Council or the Data Protection Officer.

- **Time zone control**

  Option for control access for transponders in terms of time.

- **Logging unauthorised attempted access events**

  Rejected transponder bookings are retained in the locking device. This only applies to ID media which belong to the same locking system.

- **Gateway**

  Option for using gateways. *Only available with SmartRelay.*

- **Flip-flop**

  When a transponder is enabled, the locking device engaged ready for use and remains engaged until a transponder activates it again.

- **No audible battery warnings**

  If this function is enabled, there are no audible warnings indicating the battery status in components.

- **Time switch-over function**

  The locking device automatically changes status according to the settings under "Advanced configuration". *For access control versions only.*

- **No audible programming acknowledgement signals**

  The locking device does not acknowledge the process with audible signals when programming.

- **Card interface**

  Links card interface with locking device.

- **Extended configuration**

  Make advanced configuration settings, such as a time-controlled changeover of the locking device.

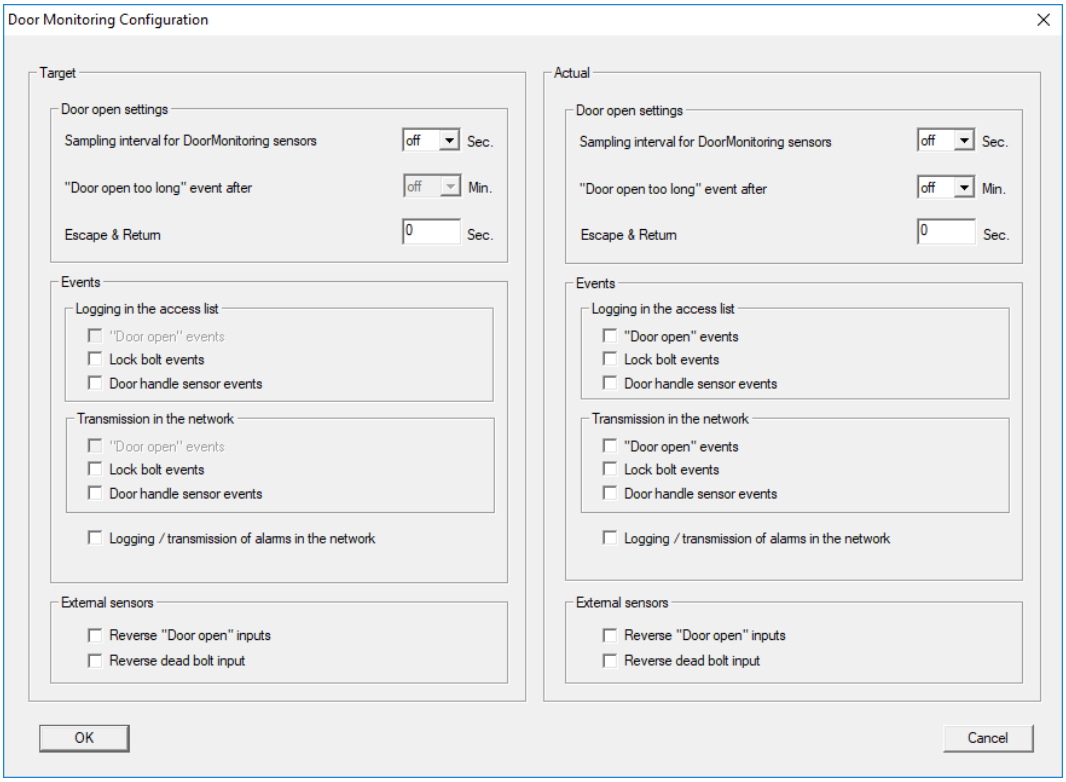
- **Software reset**

  Button to re-set the current status of the LSM software. This process is timed and shown on the left-hand side.

Configuration/Data: DoorMonitoring SmartHandle

You can configure the DoorMonitoring functions in the SmartHandle using the "Monitoring configuration" button on the "Configuration/Data" tab on the locking device (see also *Putting DoorMonitoring locks into operation [▸ 194]*).

This function is only available if the SmartHandle features the DM function and this function was also directly added into the LSM software as "G2 SmartHandle DoorMonitoring".



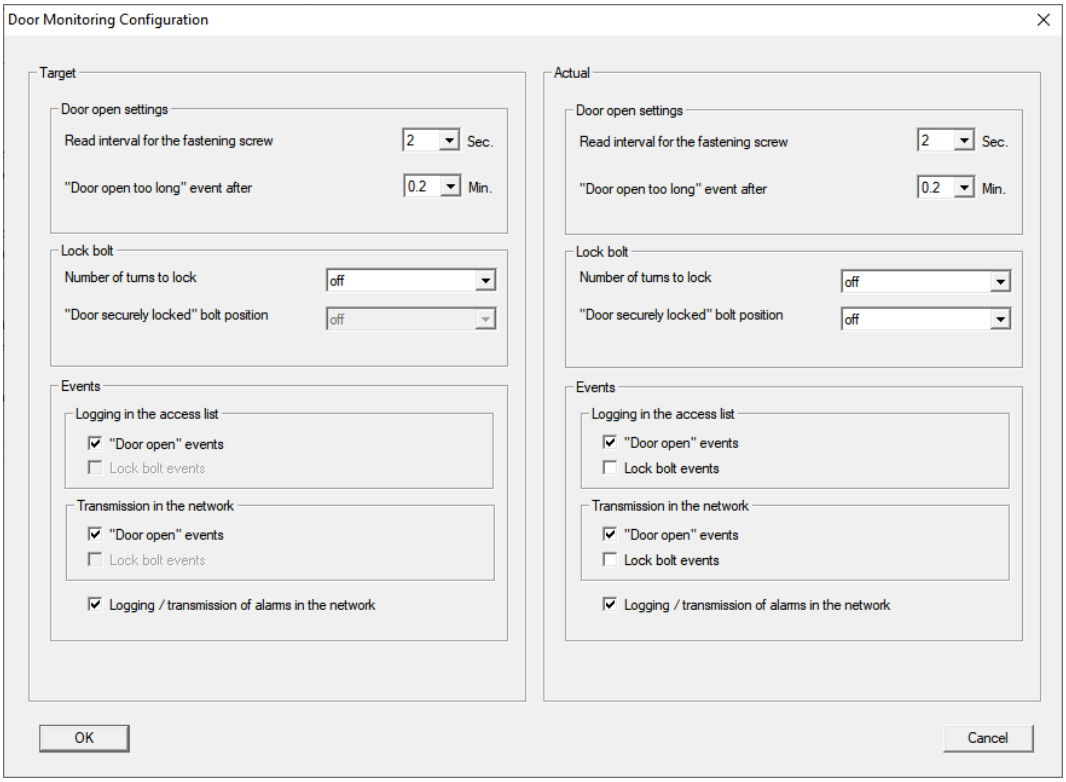
Activate the required changes in the left hand "Target area".

- **Escape & return:** Prolongs the time that the SmartHandle is engaged to open after the door has been detected as closed again.

Configuration/Data: DoorMonitoring locking cylinder

You can configure the DoorMonitoring functions in the locking device using the "Monitoring configuration" button on the "Configuration/Data" tab on the locking cylinder (see also *Putting DoorMonitoring locks into operation [▸ 194]*).

This function is only available if the locking cylinder features the DM function and this was also directly added into the LSM software as "G2 cylinder DoorMonitoring".

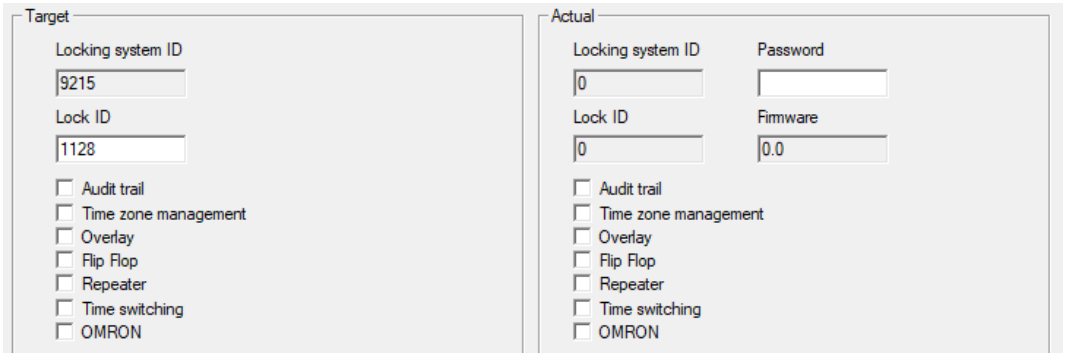


Activate the required changes in the left hand "Target area".

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

This tab ([Configuration/Data]) is divided into two sides:

- The left side shows the target status of the locking device ("Actual") – i.e. the desired status configured in the LSM software.
- The right side shows the locking device's current status ("Target") – i.e. the status which was last programmed.

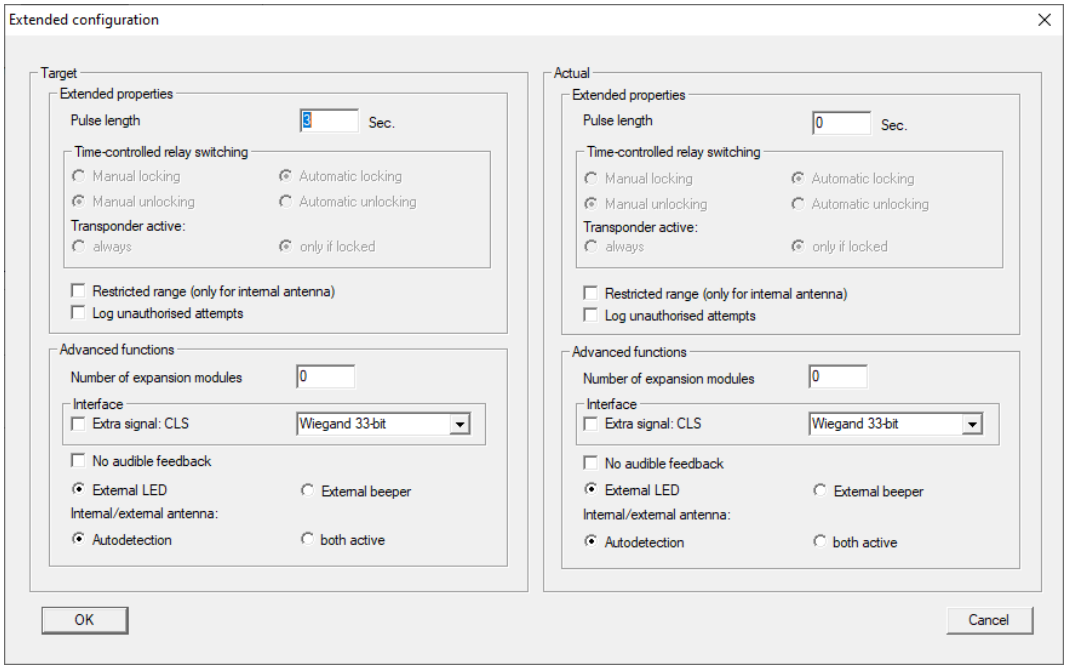


The following features can be enabled **depending on the locking device type**:

☑ Audit trail	Only possible in SREL.ZK and SREL.ADV versions. The 1,024 most recent transponder transactions are logged with the date and time.

☑ Time zone management	Only possible in SREL.ZK and SREL.ADV versions. A time zone plan can be uploaded and the transponders are approved or blocked according to their time zone group.
☑ Overlay	Replacement transponders can overwrite their corresponding original transponders. The original transponder is blocked once the replacement transponder is used for the first time.
☑ Flip Flop	Pulse mode (default setting) is switched off and the pulse duration no longer plays a role. When flip flop mode is activated, SmartRelay changes its status from on to off or vice versa each time it is activated using a transponder. This mode is ideal for switching lights, machines and other systems on and off. *Where applicable, you should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.*
☑ Repeater	The SmartRelay receives a transponder signal, which it amplifies and forwards. This function allows SmartRelay to be used to bridge longer radio transmission paths. The distance to the next SmartRelay can be up to 2 m.

☑ Time switching	For SREL.ZK and SREL.ADV only. A time zone plan needs to be uploaded when the time switch-over is activated. This allows SmartRelay to remain unlocked during the indicated times (in Group 5). During the day, the door can be used freely while only a transponder will open the door at night. *You should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.*
☑ OMRON	For SREL.ADV only Many access control and time-and-attendance systems feature serial interfaces to connect card readers. A SmartRelay can also be connected via these interfaces, thus also allowing you to use SimonsVoss transponders in third-party systems. Select this option on both the SmartRelay and the cylinder if you wish the SmartRelay to transmit transponder data to a third-party system and a remote opening command to be sent from SmartRelay to a cylinder after clearance by the third-party system. Set the type of external system under "Interface". Click on the Extended configuration button to do so.



Some settings can be specified using the Extended configuration button:

Pulse length	This is where you indicate the number of seconds for the duration of switch pulse. The value can be set at 0.1 to 25.5 seconds. If you enter 3 seconds, for example, an electric strike is released for 3 seconds before it locks again.
☑ Restricted range	If you select this option, the reader range from the transponder to the SmartRelay is reduced from 1.5 m to about 0.4 m. This option can be used when several SmartRelays are in close proximity to one another and individual transponders are authorised for use on several SmartRelays, for example.
☑ Log unauthorised attempts	For SREL.ZK and SREL.ADV only: Normally, only authorised transponder operations are logged. You need to select this option if you also wish to record attempts to open the door with non-authorised transponders.

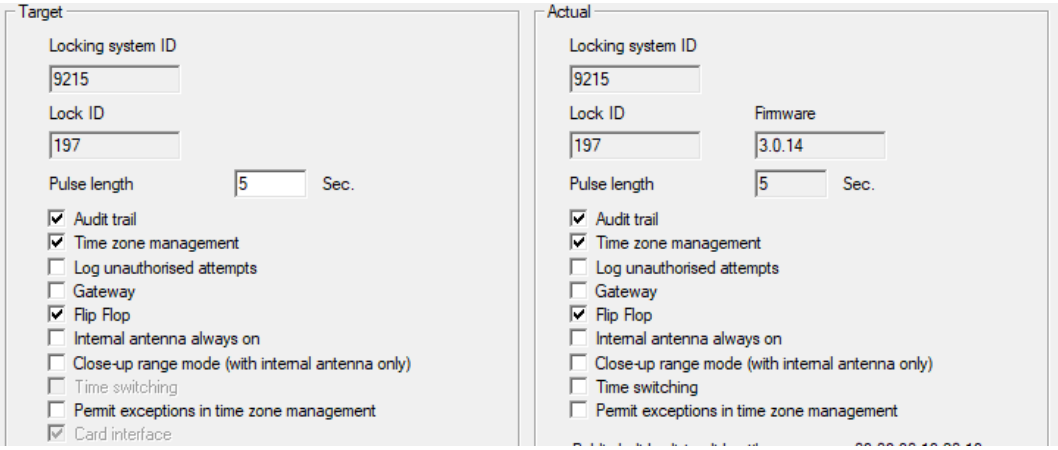
Number of extension modules	This where you indicate the number of external modules connected to the SmartRelay. These modules are connected to the terminals RS-485 C OM, RS-485 A and RS-485 B.
"Interface"	For SREL.ADV only: You can enter the type of card reader here which the SmartRelay is to simulate for operation as a serial interface. The following options are available: ■ Wiegand, 33 bit ■ Wiegand, 26 bit ■ Primion ■ Siemens ■ Kaba Benzing ■ Gantner Legic ■ Isgus
☑ No audible feedback	For SREL.ADV only: You should check this field if you do not want audible programming confirmation signals to be emitted from a connected buzzer or beeper while you are programming SmartRelay.
◉ External LED/ ◉ External beeper	For SREL.ADV only: This indicates which external component group is connected. In flip flop mode, SmartRelay emits a permanent signal when switched on if there is an external LED; in the case of a beeper, an audible signal is only emitted when there is a change of status.

◉ Autodetection/ ◉ both active	For SREL.ADV only ■ ◉ Autodetection If an external antenna is connected, this is the one which is used. SmartRelay switches off the internal antenna in such cases. If no external antenna is connected (standard case), SmartRelay functions with the internal antenna. ■ ◉ both active SmartRelay is able to use both antennas to verify transponder bookings.

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

This tab ([Configuration/Data]) is divided into two sides:

- The left side shows the target status of the locking device ("Actual") – i.e. the desired status configured in the LSM software.
- The right side shows the locking device's current status ("Target") – i.e. the status which was last programmed.



The following features can be enabled **depending on the locking device type**:

- **Pulse length**

  This where you indicate the number of seconds for the duration of switch pulse. The value can be set at 0.1 to 25.5 seconds. If you enter 3 seconds, for example, an electric strike is released for 3 seconds before it locks again.

- **Access control**

ZK and ADV possible. The most recent transponder transactions are logged with the date and time.

- **Time zone control**

  Only possible in SREL.ZK and SREL.ADV versions. A time zone plan can be uploaded and the transponders are approved or blocked according to their time zone group.

- **Logging unauthorised attempted access events**

  For ZK and ADV only: Normally, only authorised transponder operations are logged. You need to select this option if you also wish to record attempts to open the door with non-authorised transponders.

- **Gateway**

  SmartRelay can be used as a gateway.

- **Flip-flop**

  Pulse mode (default setting) is switched off and the pulse duration no longer plays a role. When flip-flop mode is activated, SmartRelay changes its status from on to off or vice versa each time it is activated using a transponder. This mode is ideal for switching lights, machines and other systems on and off.

  Where applicable, you should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.

- **Internal antenna always on**

  Even if an external antenna is connected, the internal antenna is still used at the same time.

- **Close range mode (for internal antennas only)**

  Close range mode is activated.

- **Time switch-over function**

  For SREL.ZK and SREL.ADV only. A time zone plan needs to be uploaded when the time switch-over is activated. This allows SmartRelay to remain unlocked during the indicated times (in Group 5). During the day, the door can be used freely while only a transponder will open the door at night.

  You should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.

- **Permit exceptions in time zone management**

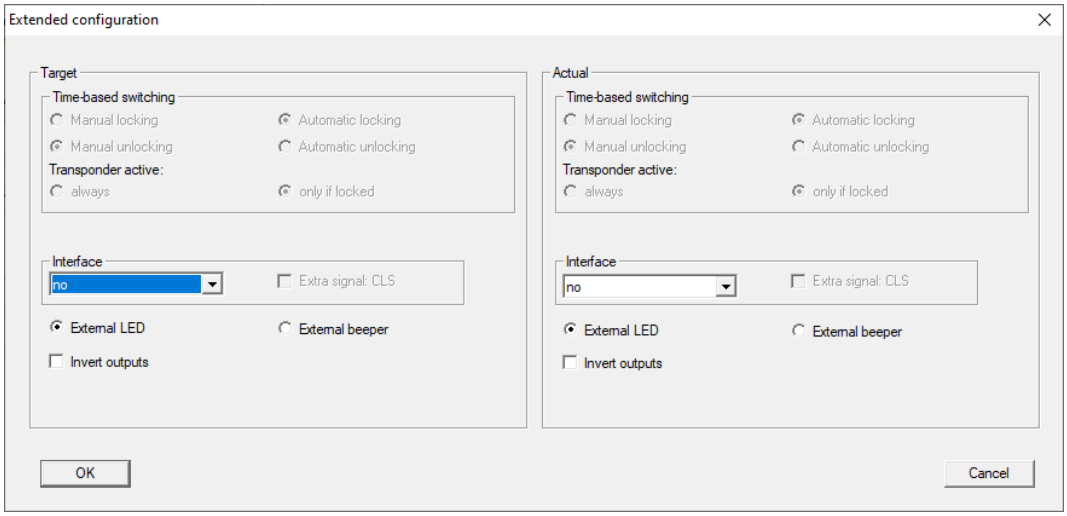
  Exceptions are permitted in time zone management if this checkbox is enabled.

- **Card interface**

This option is enabled for all G2 SmartRelays as standard. The LSM first adds a data record for an active locking device and checks whether the locking device has an interface during programming. If no card interface is detected, LSM automatically disables the checkbox. You no longer need to indicate whether you have an active or hybrid SmartRelay G2 for LSM 3.3 or higher.

NOTE

If you change the card interface setting manually, automatic detection will no longer function and warning messages will be emitted.



Some settings can be specified using the "Extended configuration" button:

- **Interface**

  You can enter the type of card reader here which the SmartRelay is to simulate for operation as a serial interface.

  The following options are available:

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

- **External LED/external beeper**

For SREL.ADV only: This indicates which external component group is connected. In flip-flop mode, SmartRelay emits a permanent signal when switched on if there is an external LED; if there is a beeper, an audible signal is only emitted when there is a change of status.

- **Invert outputs**

  You can use these settings to invert the relay output.

SmartRelay 3

This tab is split in two.

- The "Actual" section shows the locking device target status. This is the status that the operator wants and which is configured in LSM but possibly may not be configured in the SREL3 ADV system yet.
- The "Target" section shows the actual locking device status. This status is the last status programmed in SREL3 ADV system.

The following features can be activated, depending on the device type:

- Pulse length

  This where you indicate the number of seconds for the switch pulse duration (0 s to 25 s). If you enter three seconds, for example, an electric strike is released for three seconds before it locks again.

- ☑ Audit trail

  Access control is only available in the .ZK variant. The most recent transponder transactions are logged with the date and time.

- ☑ Time zone management

  Time zone control is only available in the .ZK variant. You can upload a time zone plan. Transponders are then approved or blocked according to their time zone group.

- ☑ Log unauthorised attempts

  Logging of unauthorised access attempts is only available in the .ZK version. If you enable this option, unauthorised transponders activations are also logged in addition to activations with authorised transponders.

- ☑ Gateway

  SmartRelay can be used as a gateway (see Gateway function).

- ☑ Flip Flop

  The relay used in the controller behaves in the same way as a monostable multivibrator (pulse generation) by default. If you enable this option, the configured pulse duration is ignored and the relay remains activated until an authorised identification medium is actuated again. This option is recommended if you wish to switch lighting, machinery and similar systems on and off.

IMPORTANT

Damage due to continuous current

Devices which are designed to generate pulses may not be suitable for continuous currents. Ensure that the power supply units and devices used, such as electric strikes, are suitable for operating with a continuous current.

- ☑ Close-up range mode

  Close range mode reduces the read range in the reader's B-field (see Near-field option).

- ☑ Time switching

  Time change-over is only available in the .ZK variant. You can upload a time zone plan. If you activate time change-over, the SREL3 ADV system can be automatically activated or blocked during the authorised or non-authorised times (in Group 5). The SREL3 ADV system will even switch automatically, depending on the setting. For example, a door can remain open automatically during the day but can only be opened with a transponder at night (see Time switch-over function).

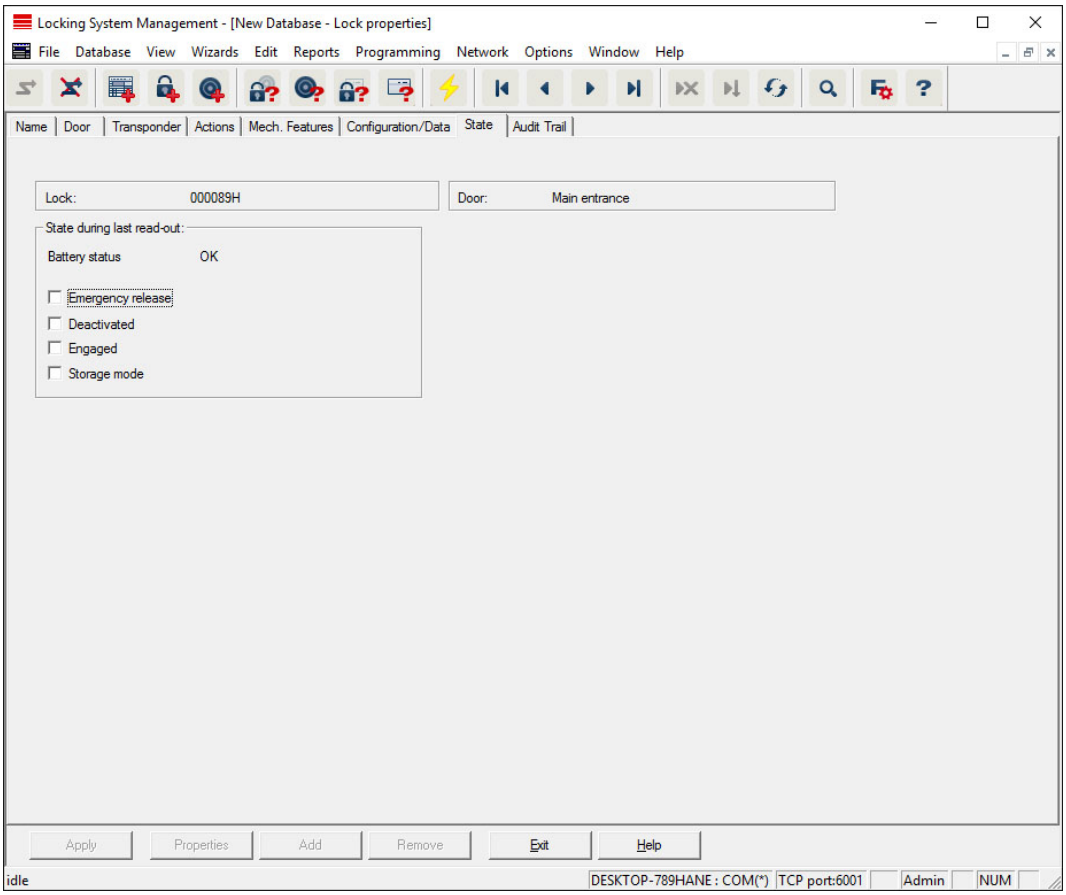
- ☑ Ignore activation or expiry date

  Transponders can be given a validity date. You can enable this option if you wish the transponders to also be valid beyond this validity date.

- ☑ Card interface

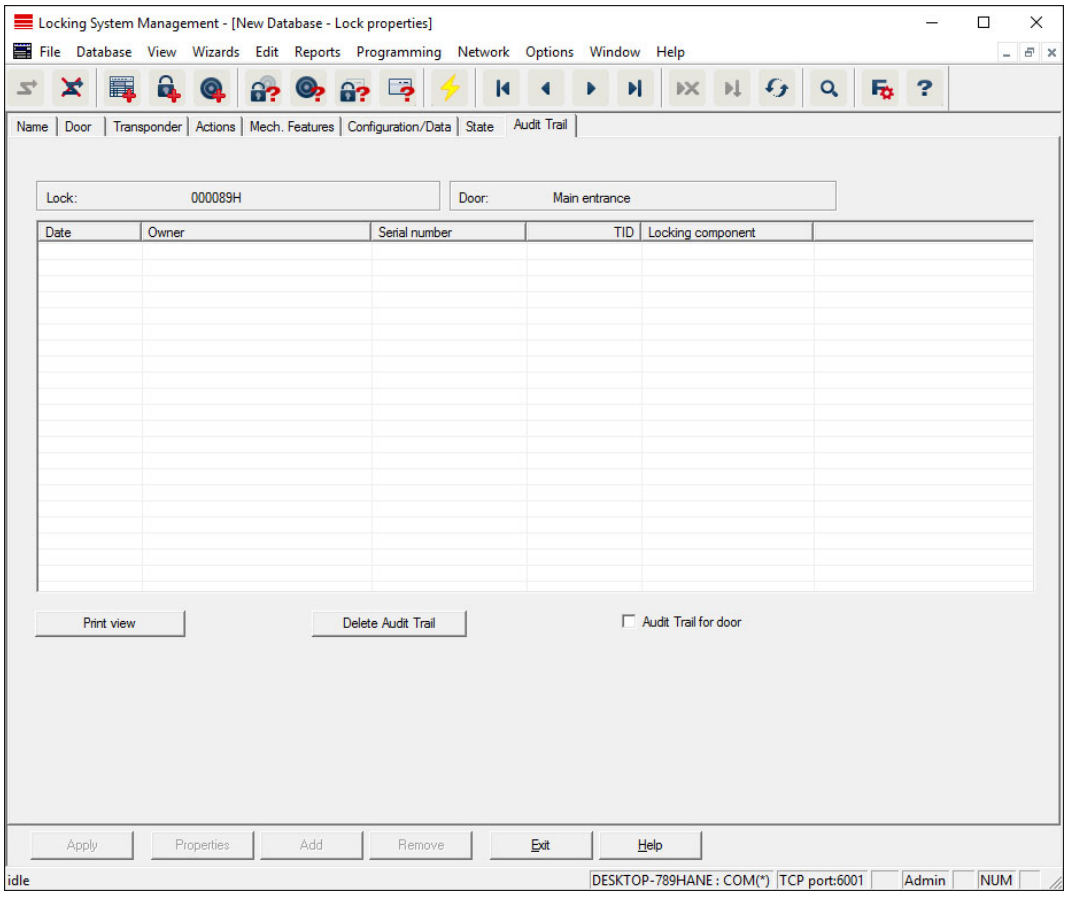
  This option should not be changed. It allows LSM to automatically detect whether the connected reader is a hybrid reader or not during programming. If you change this option manually, detection will no longer function.

Status



The last uploaded status of the locking device is displayed and is updated each time the locking device is read.

Access list



This tab can display the latest version of the access list. *The locking device must support the "Access control" function, which must be enabled in the locking device properties.*

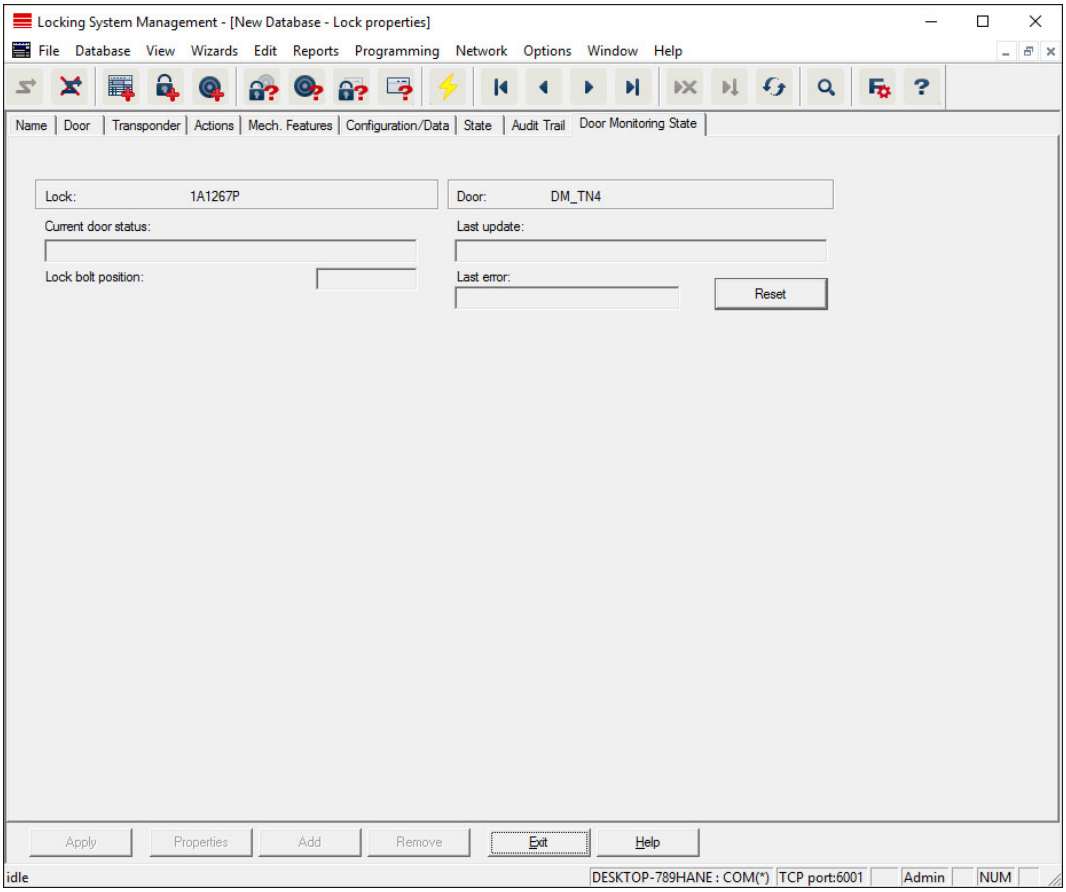
This is how you read the access list:

1. Read locking device using the *Programming/Read locking device* menu bar.
2. Click on the "Access list" button to launch the read process.
   ↳ The access system is automatically displayed and saved. It can now be displayed in the locking list properties in the Access list tab at any time.

DoorMonitoring status

The current status of the locking device can be displayed in the "DoorMonitoring status" tab in real time (see also *Possible (door) states [▸ 194]*). A configured WaveNet is required for this function.

This tab can only be selected if the locking device features the DM function and this was also directly added into the LSM software as "G2 DoorMonitoring/SmartHandle cylinder". The appearance may vary.



NOTE

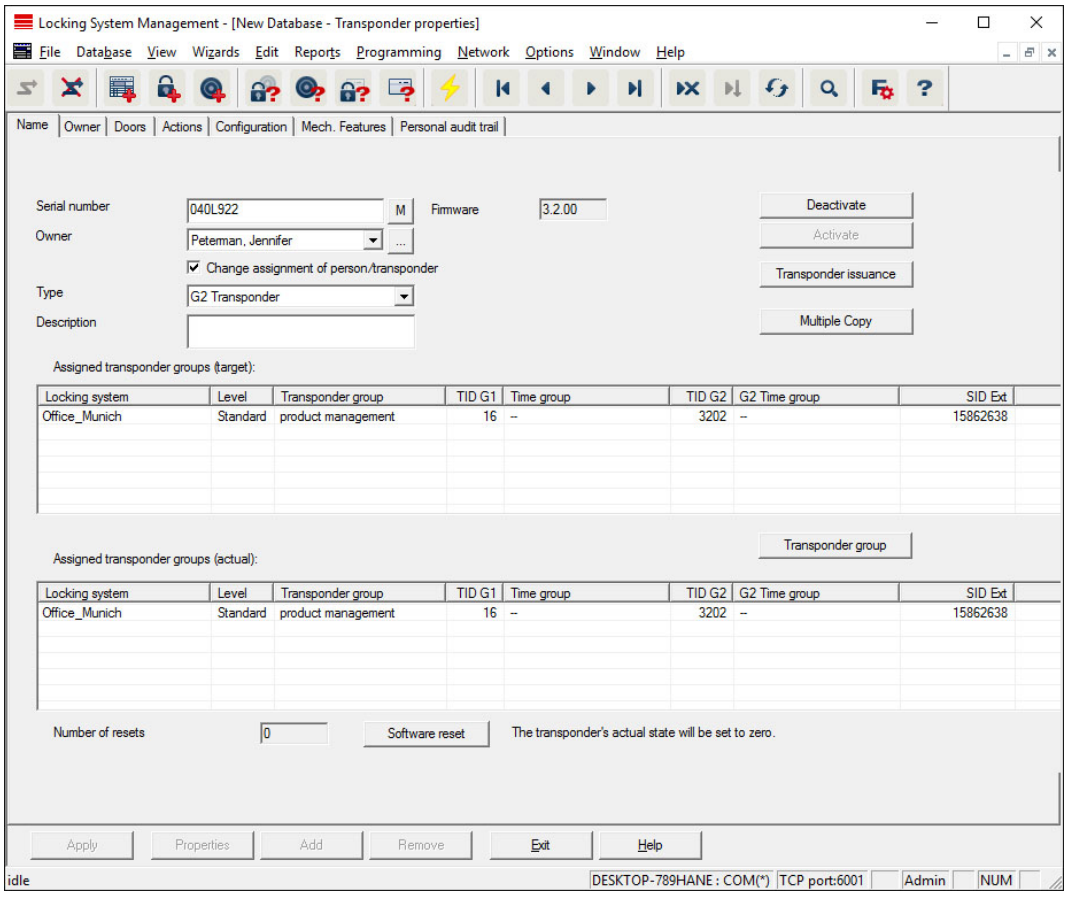
If you wish to monitor several locking devices at the same time, you can also use SmartSurveil to display locking devices and their respective door status in a table where they can be clearly seen.

7.1.5.3 Properties: Transponders

Show and edit properties for the transponder currently highlighted.

Double-click on a transponder to open its properties directly.

Name



- **Serial number**

  Transponder serial number. The "..." button shows the person's properties. The G2 transponder "internal serial numbers" (PHI number*Physical Hardware Identifier; embossed on the product*) are automatically applied when they are programmed.

- **Holder**

  The person that the transponder is assigned to. The "M" button shows the transponder in the matrix.

- **Type**

  Type of transponder.

- **Description**

  Blank field to describe the transponder.

- **Assigned transponder groups: Target state**

  Target status of the transponder group to which the transponder belongs.

- **Transponder group**

You can use this button assign the transponder to another transponder group.

- **Assigned transponder groups: Current status**

  Current status (last programming) of the transponder groups to which the transponder belongs.

- **Software reset**

  Button to re-set the current status of the LSM software. This process is timed and shown on the left-hand side.

NOTE

Only use this function if you are sure where the programmed components are. This action can be used if a transponder is defective. A correctly programmed, functional transponder which has only be reset in the software may still be authorised to operate locking devices. This poses a high security risk!

- **Disable**

  Button to disable a transponder.

- **Activate**

  Button to activate a transponder.

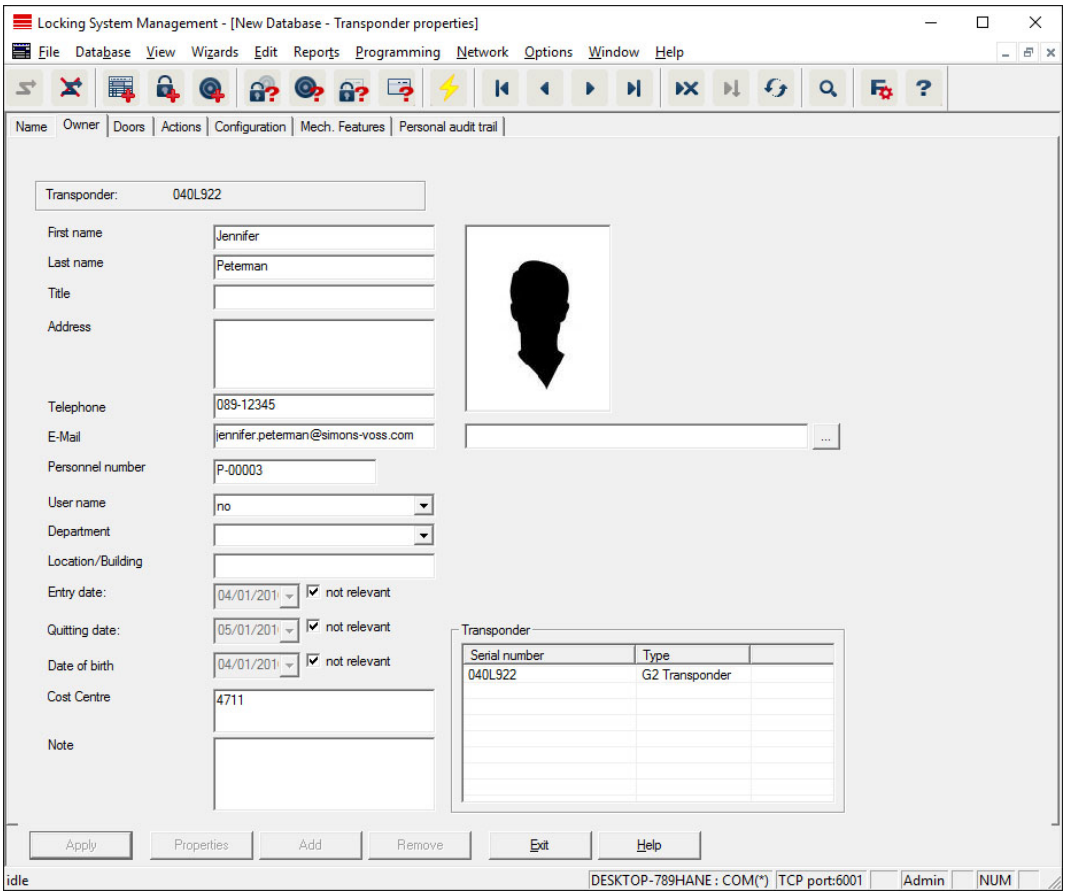
- **Issuing of transponders**

  Generates a form with signature for handover. The form also contains a list of all authorised doors.

- **Make multiple copies**

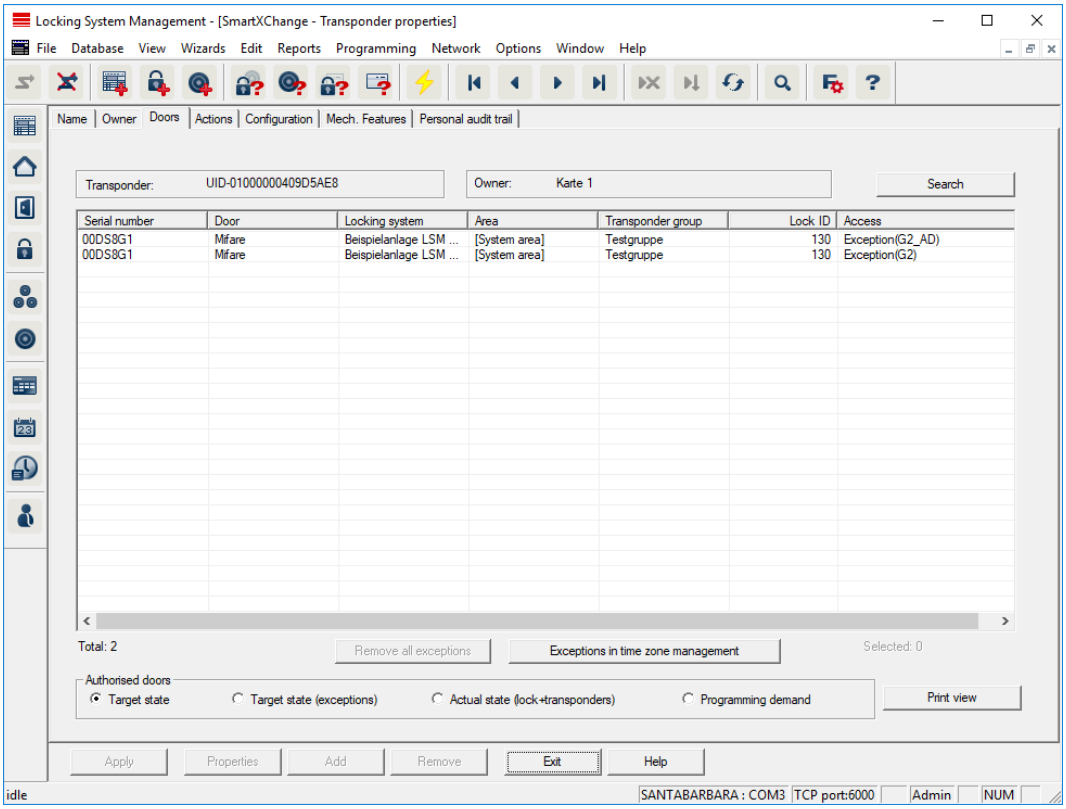
  Generates as many copies of the transponder with the same properties as required.

Holder



You can enter all information on the transponder's holder in the "Holder" tab. The "Transponder" table indicates how many transponders and which ones are assigned to the user. You can use the "..." to add a user photo. *We recommend using JPEG images no larger than 500 kB.*

Doors



This tab gives you an overview of the selected transponder's authorisations for doors. The devices are all displayed in detail in a table.

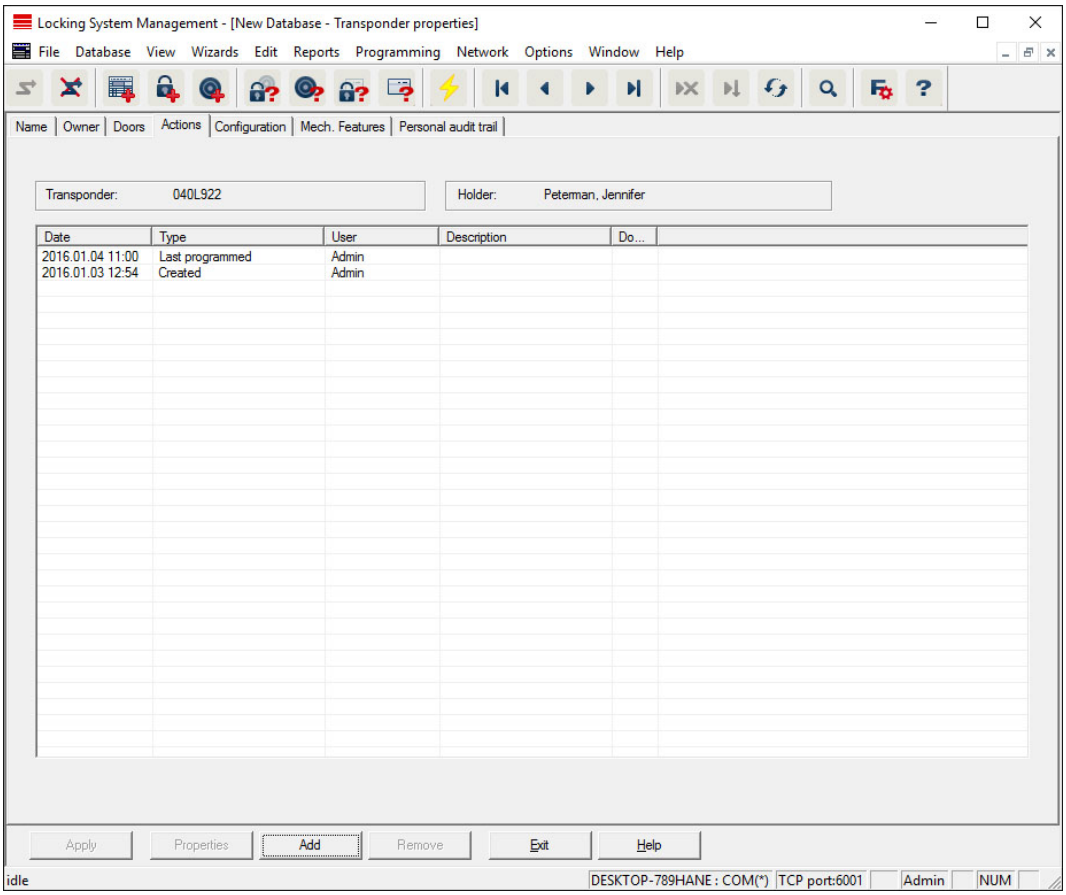
- **Table**

  Shows all the doors that the transponder is authorised to use in a detailed list.

- **Authorised doors**

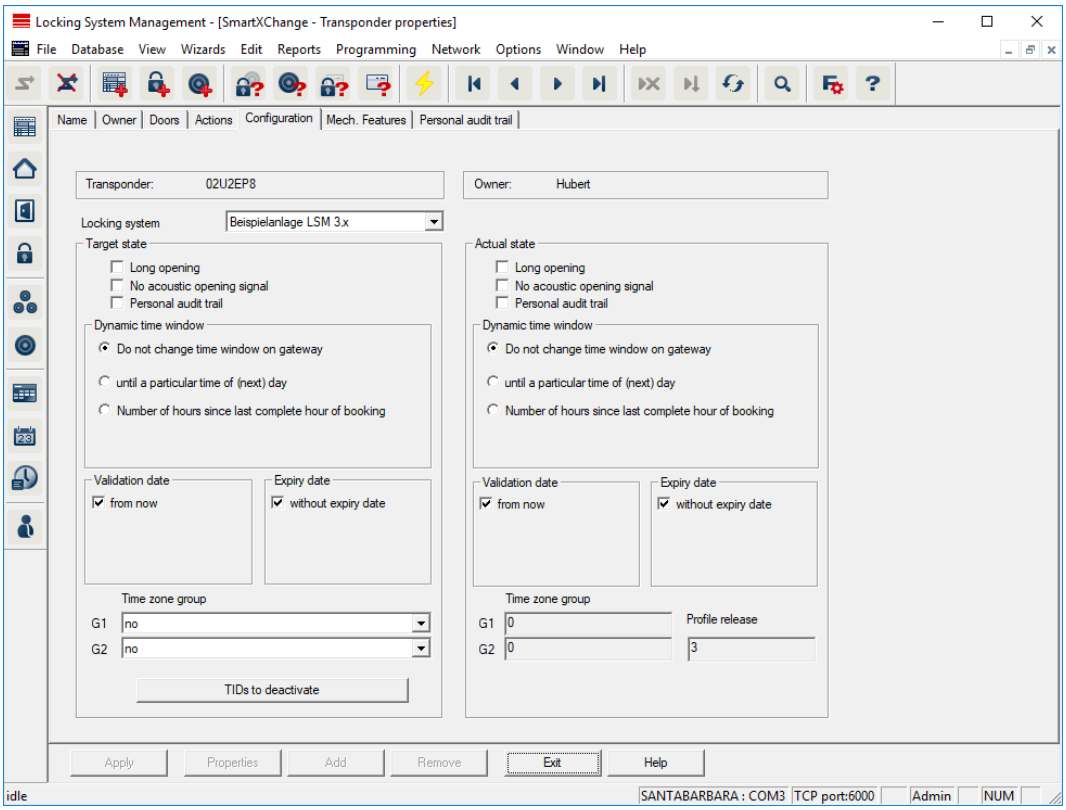
  You can use the individual radio buttons to sort and filter the table.

Actions



This table shows which actions, such as programming and authorisation changes, have been implemented using the selected transponder. Certain actions, such as "Scheduled return", can also be added manually using the "Add" button.

Configuration



This tab is divided into two sides:

- The left side shows the transponder's target status – i.e. the required status configured in the LSM software.
- The right side shows the transponder's current status, i.e. the status which was last programmed.
- **Locking system**

  Displays the transponder's currently assigned locking system.
- **Long opening**

  This allows the locking device to remain engaged to open for longer. The locking device impulse length is doubled. *Example: People with disability possibly require the door to be open longer.*
- **No audible opening signal**

  The locking device responds to the transponder without emitting an audible signal. *Example of use: assisted living accommodation. The duty nurse can enter the room at night without making a noise.*
- **Physical access list**

  Saves all access events on the transponder.
- **Do not change time window on the gateway**

There is no time limit on the validity period for this G2 transponder booking at the gateway.

- **Until a specific time on the next day**

  There is a time limit on the validity period for this G2 transponder booking at the gateway. Enter a time.

- **Number of hours from the last full hour of the booking**

  The validity of this G2 transponder booking at the gateway is extended by the specified number of hours. Enter the number of hours.

- **Activation date**

  Date and time from which the transponder is to be valid.

- **Expiry date**

  Date and time from which the transponder is to be no longer valid.

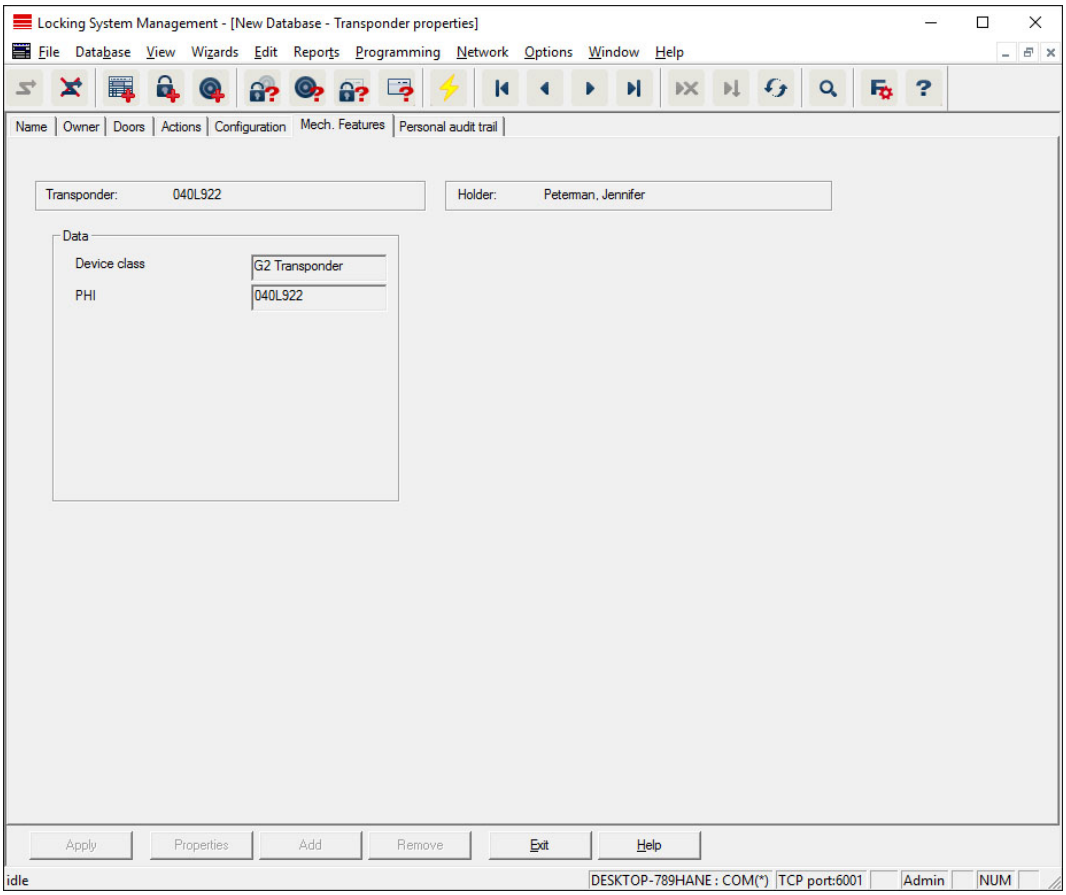
- **Time zone group**

  You can assign the transponder to a previously assigned time zone group.

- **TIDs to deactivate**

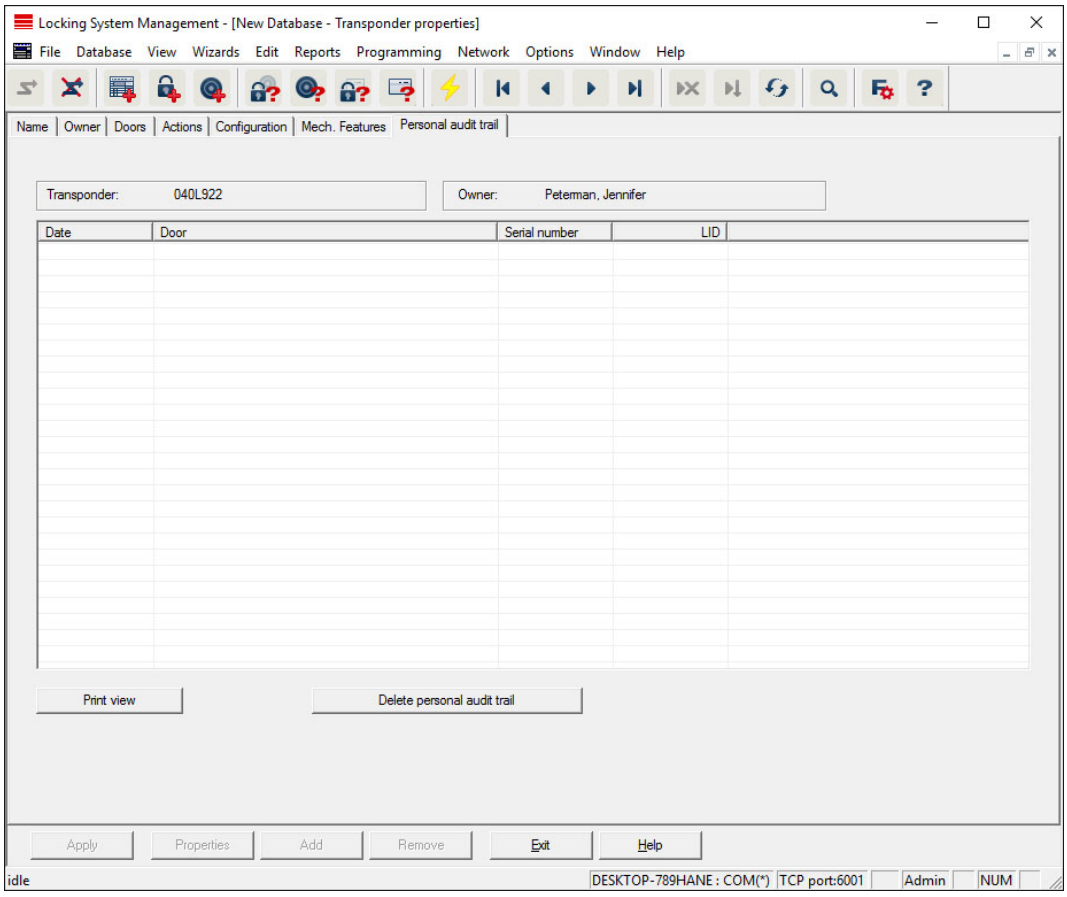
  You can save to the transponder ID for other transponders which have been deactivated. As soon as the transponder registers on a locking device, the deactivations will come into effect on the locking device in question.

Features



Check the transponder's exact specifications.

Physical access list



This tab can display the latest version of the physical access list. *The "Physical access list" function must be enabled.*

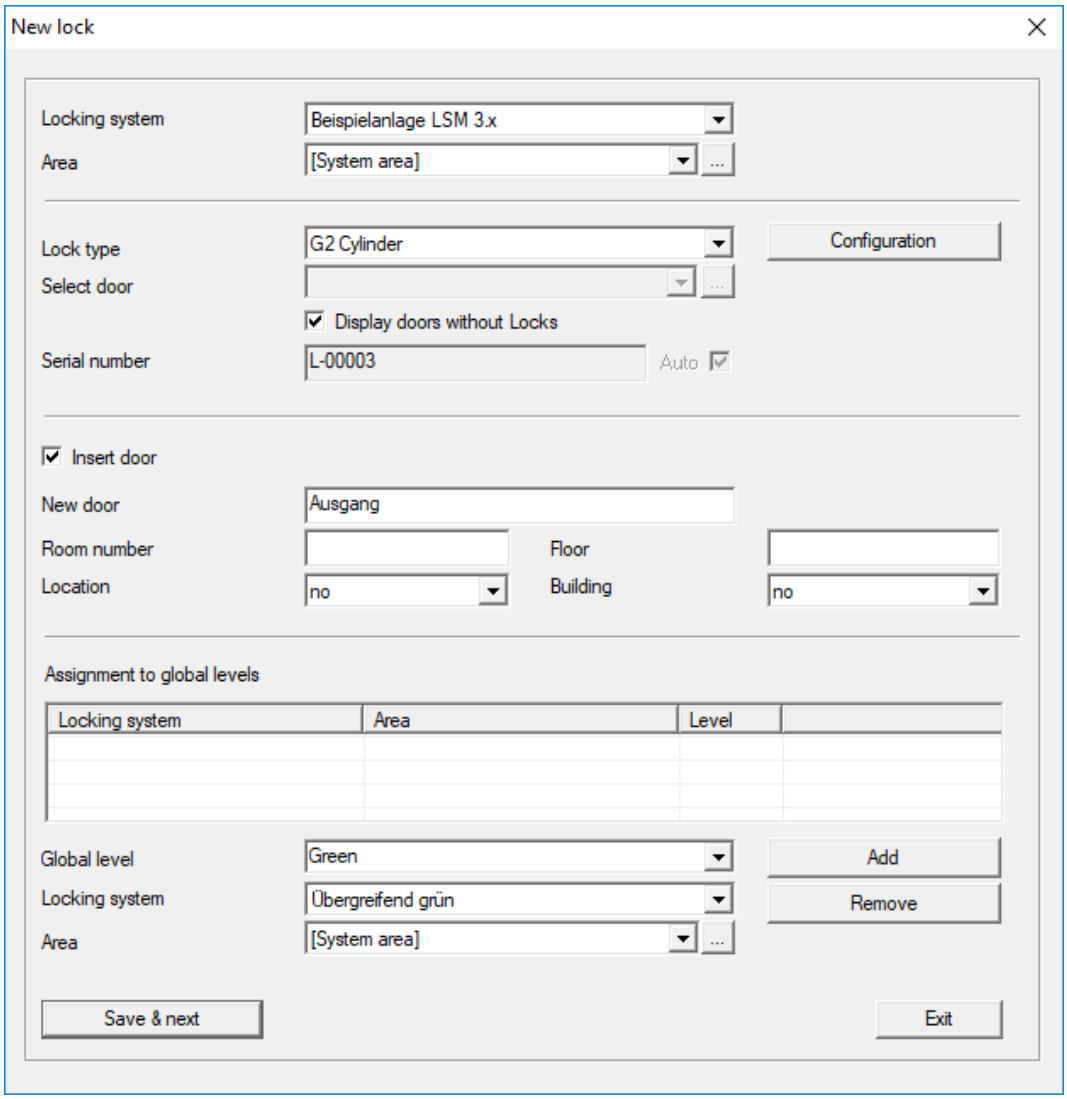
How to read the physical access list:

1. Read transponder using the *Programming/Read transponder* menu bar.
2. Click on the "Physical access list" button to launch the read process.
   ↳ The physical access list is automatically displayed and saved. It can now be displayed in the transponder properties in the Access list tab at any time.

7.1.5.4 Edit/New locking system

This is where you can add a new locking system within the project.

7.1.5.5 New locking device



Use this option to add a new locking device manually.

If several locking systems and common locking levels have already been created, the new locking device can be assigned to them directly. Drop-down lists provide corresponding options for this purpose.

- Optionally select a locking system and area to assign the locking device correctly immediately. Locking systems and areas must be defined beforehand. It is possible to change these settings at a later stage at any time.
- You can use the "Add door" button to create a new door. A door can contain a number of locking devices.
- You can use the "Save & next" button to add a new locking device to the locking plan. Select "Finish" to return to the matrix or add another door.

Different locking devices can be managed in the LSM software, depending on the hardware used. Select the type of locking device that you wish to add from Locking device type in the drop-down menu.

7.1.5.6 New transponder

Use this option to add a new transponder manually.

If several locking systems and transponder groups have already been created, the new transponder can be assigned to them directly. Drop-down lists provide corresponding options for this purpose.

- Optionally select a locking system and transponder group to assign the transponder correctly immediately. Locking systems and transponder groups must be defined beforehand. It is possible to change these settings at any time.
- You can use the "Configuration" button to make advanced settings such as the transponder validity.
- You can use the "Save & next" button to add the transponder to the locking plan. Select "Finish" to return to the matrix or add another transponder.

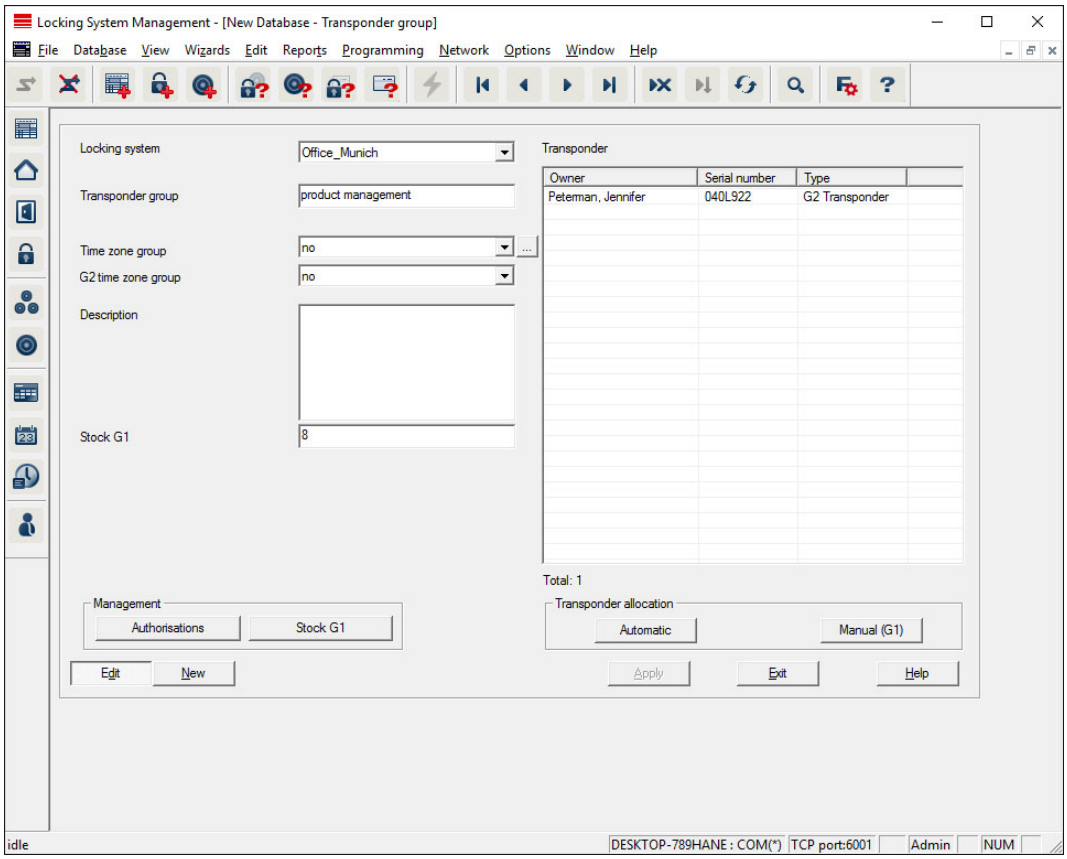
Ensure that each ID medium is basically marked as a transponder in the LSM software. Different ID media can be managed in the LSM software, depending on the hardware used:

G1 biometrics	Biometric transponder
G1 biometric reader user	Biometric reader user in G1 standard
G1 card	Card in G1 standard
G1 SmartClip	SmartClip in G1 standard
G1 transponder	Transponder in G1 standard
G2 card	Card in G2 standard
G2 PIN code user	User of a PIN code terminal
G2 transponder	Transponder in G2 standard
Undefined	Not yet determined G1 transponder

NOTE

Transponder must never be assigned to a locking system and a common level at the same time.

7.1.5.7 Transponder group



This menu displays the transponder groups already added. You can use the "Next dataset" and "Previous dataset" buttons on the menu ribbon to switch between individual transponder groups. You can use the "New" button to add more transponders.

- **Locking system**

  Selects the locking system added.

- **Transponder group**

  The transponder group name.

- **Global group**

  Transponder group which occupies a position higher up in the hierarchy.

- **Time zone group G1**

  Establishes the G1 time group for the transponder group.

- **Time zone group G2**

  Establishes the G2 time group for the transponder group.

- **Description**

  Blank field to describe the transponder group.

- **G1 reserve**

Total number of transponder IDs available in the transponder group.

- **Authorisations**

  Option of issuing the group authorisations.

- **Reserve (G1)**

  Option to manage G1 transponder IDs.

- **Automatic**

  Option to automatically assign a free transponder to the transponder group.

- **Manual (G1)**

  Option to assign a specific transponder to a specific transponder ID manually.

7.1.5.8 Person

This menu displays the persons already added. You can use the "Next dataset" and "Previous dataset" buttons on the menu ribbon to switch between individual persons.

The menu is the same as the "Holder" tab under *Edit/Properties: Transponder*.

You can also use the "New" button to add new persons.

7.1.5.9 Area

Use this menu to display the individual transponder areas. You can use the "Next dataset" and "Previous dataset" buttons on the menu ribbon to switch between individual transponder groups.

You can also use the "New" button to add new areas.

7.1.5.10 Door

This menu displays the doors already added. You can use the "Next dataset" and "Previous dataset" buttons on the menu ribbon to switch between individual doors.

The menu is the same as the "Door" tab under *Edit/Properties: Locking device*.

You can also use the "New" button to add new doors.

7.1.5.11 Building

You can use this menu to add a new building or edit an existing building to the locking system. Buildings can only be created if their location has already been added.

7.1.5.12 Location

You can use this menu to add a new location or edit an existing location in the locking system.

7.1.5.13 Public holiday list

This list applies universally to the project. This is where public holidays can be selected according to geographical location or where new ones can be created.

7.1.5.14 Public holiday

This is where individual public holidays can be created. This is where you can determine a new "public holiday" or a "holiday period". *Newly created public holidays must be assigned to a public holiday list in the holidays management.*

7.1.5.15 Time zone plan

You can create time zone plans in this section.

- **Name**

  Suitable, unique name for the time zone plan.

- **Description**

  Apt description of the time zone plan.

- **Public holiday list**

  Select a relevant geograPHIcal location.

- **Display names of groups for the locking system**

  Selects the locking system for which the time group names changed manually are displayed.

- **Time groups table**

  Up to 100 time groups may be defined for each time zone plan. First select a group and then edit the weekly program.

NOTE

The fifth group is intended for time change-over (see Time switch-over function).

- **Small tables on right at top**

  If the time zone plan has already been assigned to an area, this displayed in the two small tables.

NOTE

Next, always create a time zone plan first and later assign it to an area *or an individual locking device*. You can do this at *Edit/Area*, for example.

- **Weekly schedule**
  - Fields filled in blue indicate an authorisation at this time.
  - You can click on fields individually or select by holding down the mouse button to make changes.
- **Edit**

  This button needs to be enabled to edit the time zone plan. Changes can be saved by pressing the "Apply" button.

- **New**

  The "New" button creates a new, empty time zone plan.

7.1.5.16 Time group

The time group can display all the time groups issued in the time zone plan. This view is especially suitable for giving a complete overview of the locking system, time group, transponder group and transponders.

You can use the "Assigned transponders" button to print out an overview.

7.1.5.17 Local time zone

Enter your local time zone in this window if you manage locations in different time zones. The "Import from registration" button allows you to select from standard world time zones.

If a locking device has been programmed with a local time zone, this changes automatically between daylight saving time and standard time.

7.1.5.18 User

The first log-on to LSM automatically becomes the administrator ("Admin"). This role has all rights.

Different users can be added in LSM Business. Several users can thus manage a database or a locking system.

New users and their rights can be displayed under *Edit/Users* (see also *Administer users [▸ 162]*). You can use the "Previous dataset" and "Next dataset" button to switch between different users.

- "User account is blocked"

  If this checkbox is enabled, the user is currently blocked.

- "User must change password at next log-on"

  If this checkbox is enabled, the user needs to enter a new password when they next log on. Users can also enter a new password under *File/Change password* at any time.

- "User groups" button

  This is where the user can be assigned to one or several existing user groups. The user group determines what particular rights the user has.

- "Edit" button

  This button is used to change the user data.

- "New" button

  This button can be used to add a new user.

7.1.5.19 User group

Users are added to user groups. This is how rights are distributed to users. The first person to log on to LSM Business is the "Admin" user, who is assigned to the "Administrator" user group with all rights.

New user groups and their rights can be added or restricted under *Edit/User group*. You can use the "Previous dataset" and "Next dataset" button to switch between different user groups.

- Group name

  Name of the group.

- Description

  Description of the group.

- Users

  Users which have already been assigned to the user group. You can use the "Edit" button to add existing users to the user group. You can also add them using *Edit/Users*.

- Write access

  Data can be changed and programming implemented if this checkbox is enabled. You can only read or display data if the checkbox is not enabled.

- Role

  This is where user group rights can be issued. *The distribution of roles are described in more detail in the following section on Roles & rights [▸ 102].*

- "Edit" button

  This button allows you to make changes to "Rights" or "Group name".

- "New" button

  Creates a new user group.

Roles & rights

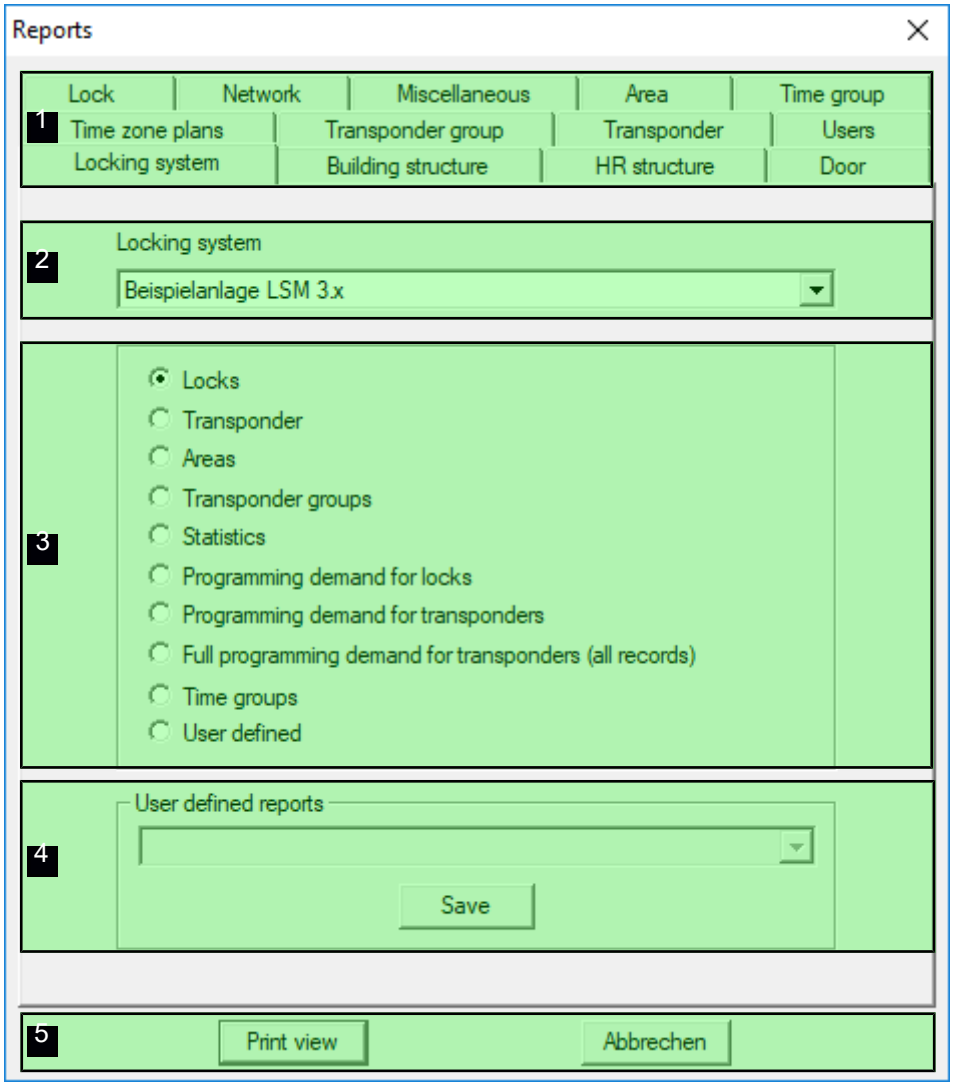
Role	Description
Locking system management	Manage authorisations in the matrix.
Programming/reading transponders	Allow communication between transponders and LSM using a programming device.
Programme/read locking devices	Allow communication between transponders and LSM using a programming device.
Edit transponders and groups	Edit transponders and transponder groups.
Edit locking devices and areas	Editing locking devices and areas.
Configure network	Create and edit network.
Manage network	Carry out tasks such as collective tasks or event manager via configured networks.
Access lists administration	Basic right to issue an authorisation to read access and physical access lists to a user group.
Manage access lists	Allow access and physical access lists.

HR management	Editing persons.
Use LSM Mobile	Allow export to or import from.
time management	Create and edit public holiday lists, time zones and time groups.
Print reports	Allow reports and labels to be printed.
Read log	Access to the "View/Log" menu.
Emergency opening	Allow emergency opening to be made.

7.1.6 Reports

To be able to use the comprehensive reporting system, you need at least LSM Basic Online or higher.

Each report type offers the following basic selection options:



1. Type of report, such as a SimonsVoss component, building or transponder group.

2. First limitation which should be reported.
3. Targeted limitation on what exactly should be reported.
4. Option of selecting a user-defined report and then saving it. *Customised, user-defined reports can be ordered from SimonsVoss Technologies GmbH.*
5. The "Display" button shows the report subject to the pre-set criteria.

The page headers and footers for reports can be customised under Options/Reports.

Displayed reports can be printed out directly or exported in different formats.

7.1.6.1 Locking system

7.1.6.2 Area

7.1.6.3 Transponder group

7.1.6.4 Door

7.1.6.5 Locking device

7.1.6.6 Transponder

7.1.6.7 Time group

7.1.6.8 Time zone plan

7.1.6.9 Network

7.1.6.10 Personnel structure

7.1.6.11 Building structure

7.1.6.12 User

7.1.6.13 Miscellaneous

List of present persons

From LSM 3.4 SP2 upwards you can generate a report which lists everyone being present in an area.

WARNING

Non-evacuation in case of danger

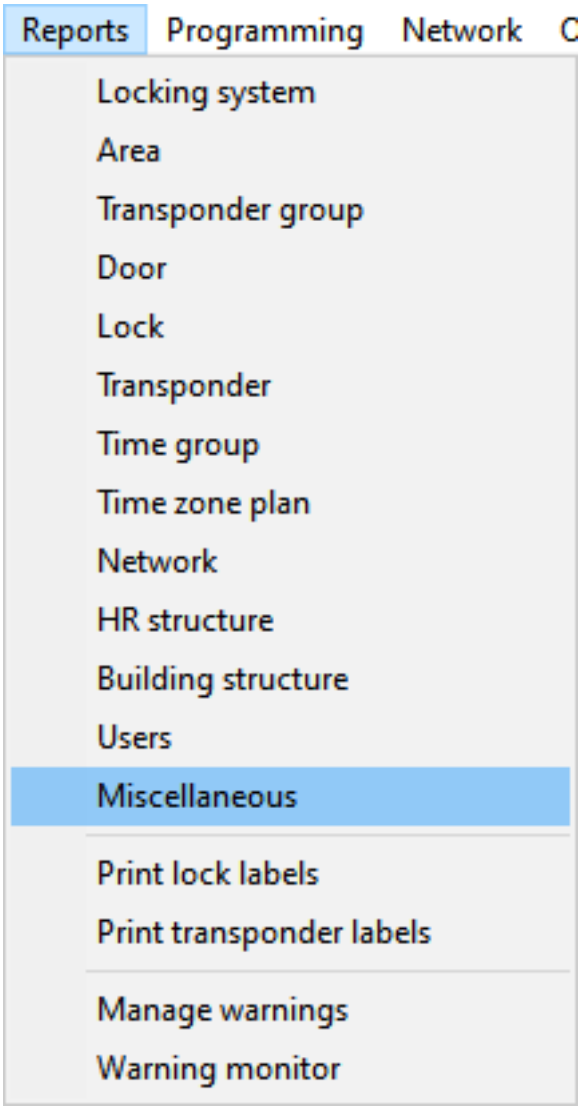
The report is based on data stored in the LSM database. This data does not necessarily display the actual conditions. For example, persons who enter through an already opened door won't be detected and thus won't be listed. Using a baffle gate like a turnstile at every entry and every exit increases the report's quality. However, it still doesn't guarantee that every person being presend in the building (respectively an area) is listed in the report.

If an evacuation is based on this report, then persons, which were not listed, may not be evacuated.

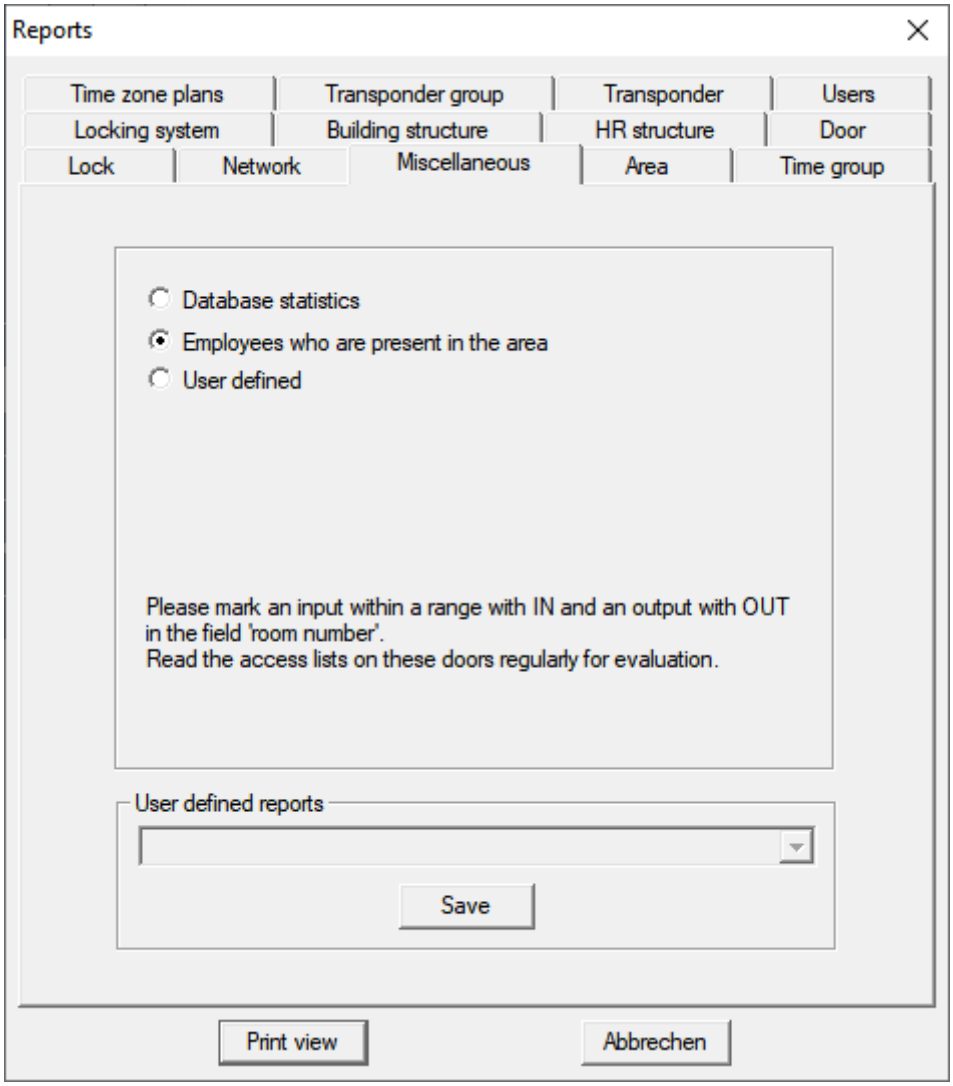
- Don't use this report instead of an evacuation list.

✓ LSM open.
✓ Doors and locks grouped to areas.
✓ Areas' names are recognizable without naming the locking system.
✓ Entrances and exits for the areas defined (see *Define entrances and exits for areas [▸ 108]*).
✓ Entrances and exits in the same area.

1. Choose via | Reports | the entry Miscellaneous.



↳ Window "Reports" opens and displays the register [Miscellaneous].



2. Mark the option ◉ Employees who are present in the area.
3. Click the button Print view.

↳ Window "Print view" opens.

The report contains the following informations:

- Area which this part of the report belongs to
  - Owner of the identification medium
  - Personal number of the owner
  - Time when the area has been entered (date and time)
  - Entered door
  - Site
  - Building
- Number of employees in the area
- Total number of employees

Define entrances and exits for areas

You may define areas. Starting with LSM 3.4 SP2 and upwards you may generate a list which shows persons being present in that area. However, you have to define which doors work as an entrance and which doors work as an exit for that area.

Defining entrances

You define an entrance with one of the following methods:

- You enter the expression */IN* instead of a door's room number in the lock's properties (register [Door]).
- You enter the expression */IN* instead of a name in the lock's properties (register [Lock components]).

Defining exits

You define an exit with one of the following methods:

- You enter the expression *OUT* instead of a door's room number in the lock's properties (register [Door]).
- You enter the expression *OUT* instead of a name in the lock's properties (register [Lock components]).

NOTE

Priority when interpreting definitions

You may enter any expression. The LSM first interprets the expression in the name field of the lock (register [Lock components]). If the LSM doesn't find one of the specified expressions (IN or OUT), then the LSM interprets the expression in the door's room number field (register [Door]).

7.1.6.14 Print locking device labels

A list of all locking devices is displayed first. You can select all locking devices or just individual ones.

You can use the "OK" button to select different label types for printing.

7.1.6.15 Print transponder labels

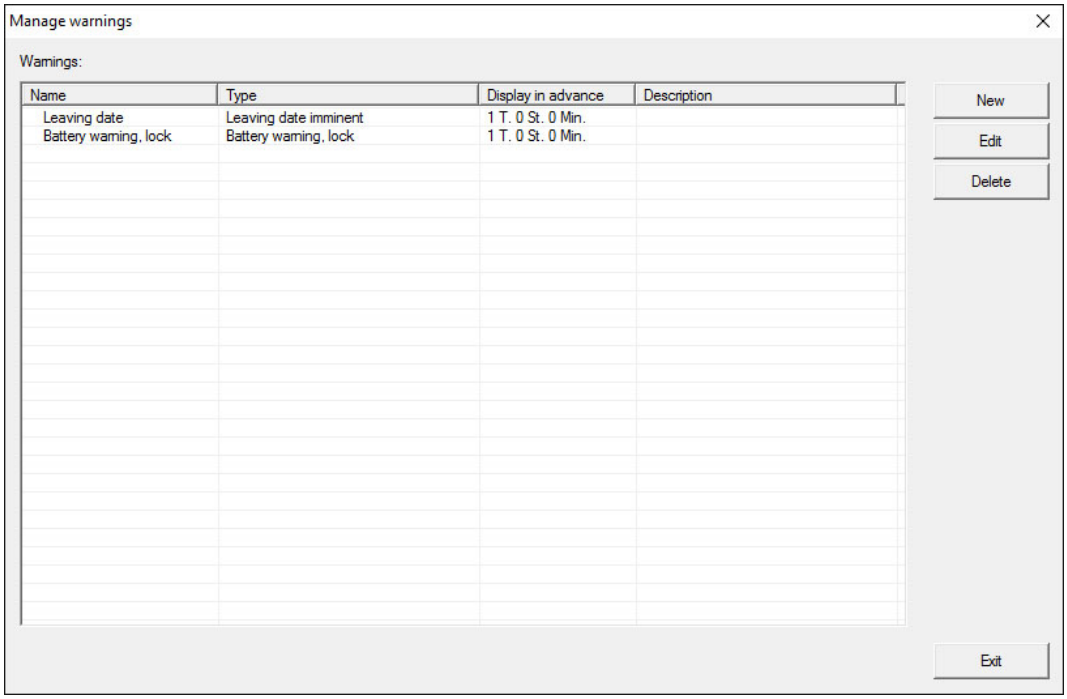
A list of all transponders is displayed first. You can select all transponders or just individual ones.

You can use the "OK" button to select different label types for printing.

7.1.6.16 Manage warnings

Available in LSM Business with enabled online module only.

The warning function provides help with working with LSM Business on a daily basis. You can configure the system to notify you of certain situations (e.g. return of transponder pending) or other events (locking device battery warning). Warnings are displayed in the warning monitor when LSM is launched. The warning monitor opens every 15 minutes.



- **Table**

  Overview of the added warnings.

- **New**

  Create a new warning.

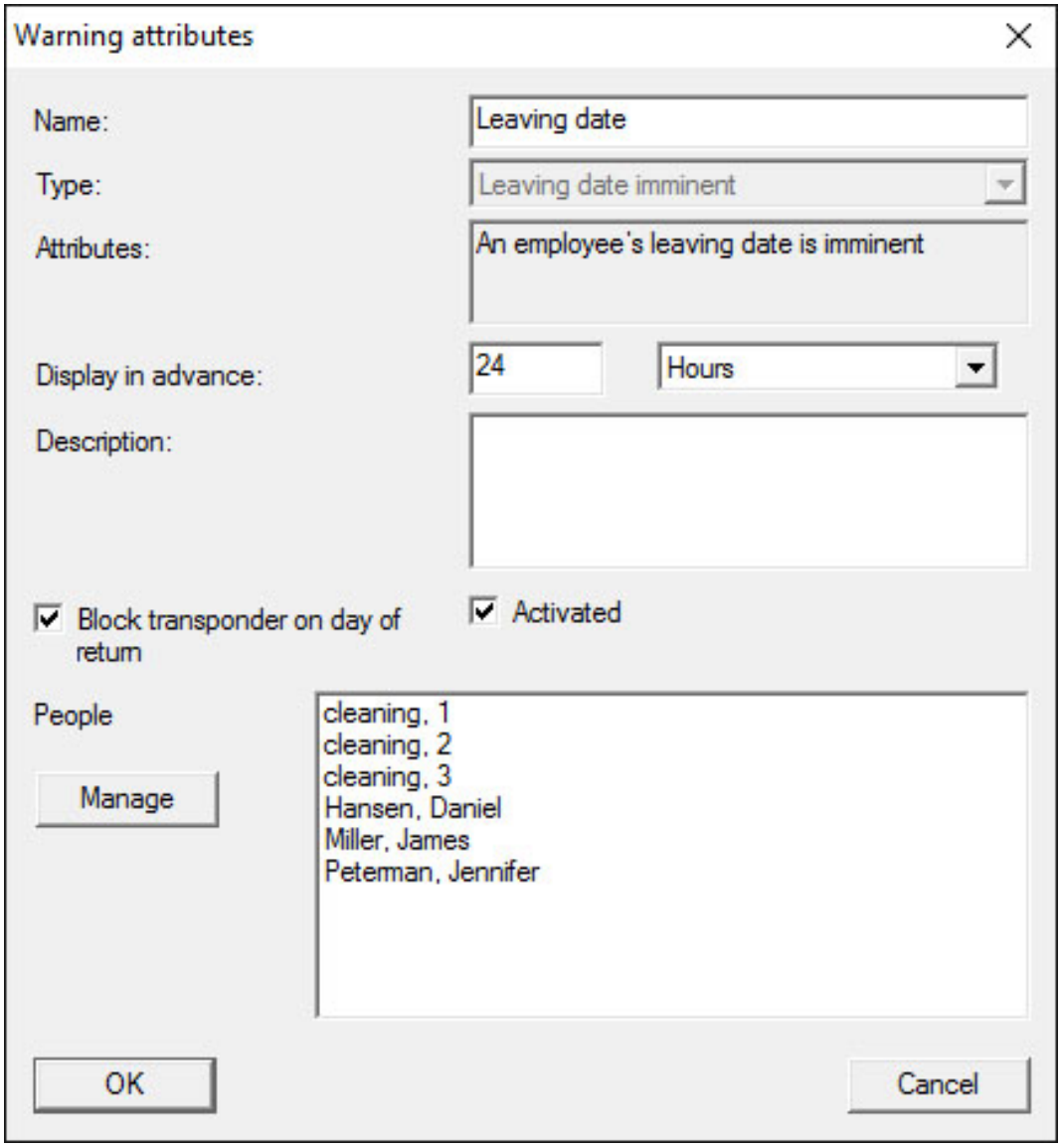
- **Edit**

  You can edit the settings after selecting the warning that you require.

- **Delete**

  You can delete the warning after selecting the one that you require.

You can use the "New" button to add a new warning:



- **Name**

  Name of the warning.

- **Type**

  Type of warning, such as locking device battery warning.

- **Properties**

  Are established based on the warning type.

- **Advanced notice**

  Time frame between the warning and the cause of the warning coming into effect.

- **Description**

  Blank field to describe the warning.

- **Block transponder on day of return**

Authorisations for locking devices are withdrawn from the transponders in the locking plan on the day of return -> Programming requirement.

- **Enabled**

  The warning is used if enabled.

- **Manage**

  Selects the objects to be monitored.

- **Table**

  Displays the selected components.

You can select the following warnings:

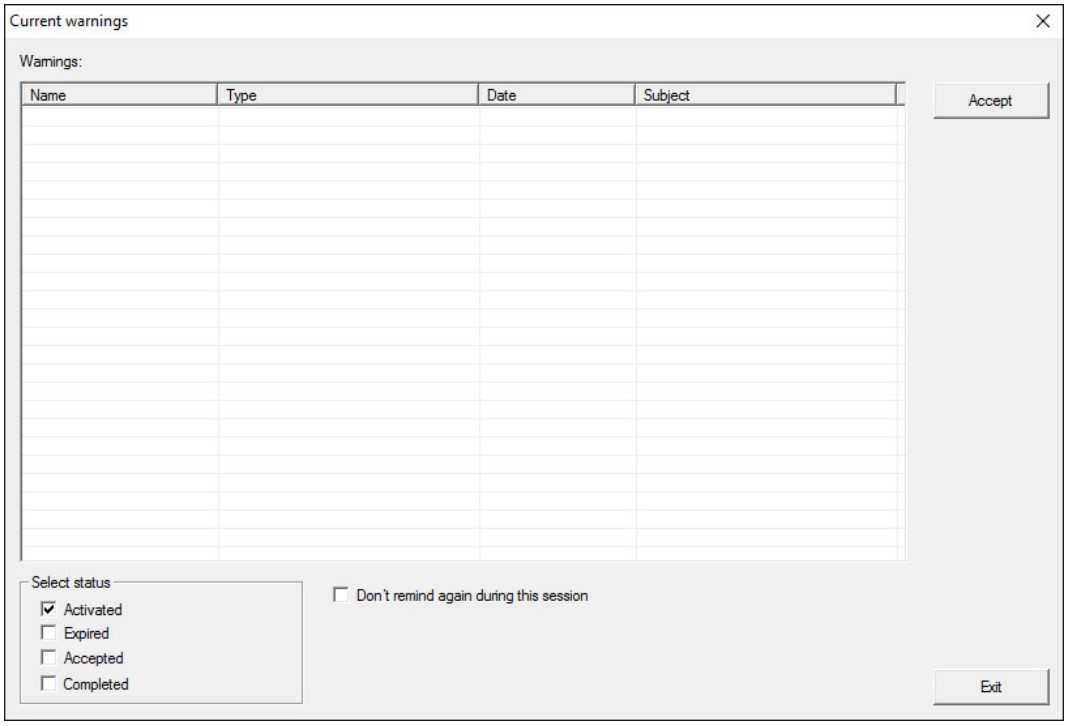
- Leaving date reached
- Battery warning for locking device
- Battery warning for transponders
- Export to handheld PDA
- Scheduled battery replacement
- Return of transponder pending
- Transponder expiry date

7.1.6.17 Warning monitor

Available in LSM Business with enabled online module only.

The warning monitor displays warnings which have been issued and are activated. The warning monitor starts up automatically after log-on and displays all accumulated warnings. If you select status display, you can also view already accepted or accumulated warnings. Double-click on the entry to open the properties of the respective object.

You can launch the warning monitor via *Reports/Warning monitor*.



- **Table**

  Overview of accumulated warnings.

- **Accept**

  You can accept individual warnings and they are then hidden.

- **Enabled**

  Only current warnings are shown.

- **Expired**

  Expired warnings are those warnings for which the pre-set time interval has already expired.

- **Accepted**

  This displays warnings that have already been accepted.

- **Processed**

  Processed warnings are those warnings which a follow-up task has dealt with, such as "Blocking of transponders".

7.1.7 Programming

7.1.7.1 Transponder

You can only select this function if you have selected a transponder in the matrix. The transponder which was selected in the matrix is displayed directly in the drop-down menu. Click on the "Programming" button to launch the programming process for the transponder selected in the drop-down list.

If you would like to programme a number of transponders one after the other, you can start with the first transponder and select the "Jump to the next transponder after programming" option.

7.1.7.2 Locking device

You can only select this function if you have selected a locking device in the matrix. The locking device which was selected in the matrix is displayed directly in the drop-down menu. Click on the "Programming" button to launch the programming process for the locking device selected in the drop-down list.

Select the programming device which you wish to use for programming in the "Programming device" field.

7.1.7.3 Read highlighted locking device/Set clock

Read the locking device selected in the matrix to set the clock time or read the access list.

7.1.7.4 Read locking device

You can use this command to read a locking device instantly using the standard SMARTCD.G2 programming device.

NOTE

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

7.1.7.5 Read MIFARE locking device

You can use this command to read a passive MIFARE locking device instantly using the passive SMARTCD.MP programming device.

NOTE

Hold the electronics side of the locking device (e.g. where the black ring between the profile cylinder housing and thumb-turn is located on the locking cylinder) directly against the antenna symbol on the programming device!

7.1.7.6 Read transponder

You can use this command to read a transponder instantly using the standard SMARTCD.G2 programming device. Observe the instructions in the LSM software.

7.1.7.7 Read G1 card

You use this command to read a G1 card instantly using the CD.MIFARE *(no longer available)*. Observe the instructions in the LSM software.

7.1.7.8 Read G2 card

You can use this command to read a G2 card instantly using the standard SMARTCD.HF programming device. Observe the instructions in the LSM software.

In the case of hybrid components, the SMARTCD.G2 also needs to be connected to the computer in addition to the SMARTCD.HF.

7.1.7.9 Special functions

Special functions/Read Compact Reader

Reads a Compact Reader.

Special functions/Activation transponder

You can use this function to create an activation transponder. You can use an activation transponder to reactivate deactivated locking devices. You also require an authorised transponder to open the locking device.

Special functions/G2 activation card

You can use this function to create a G2 activation card. You can use a G2 activation card to reactivate deactivated locking devices. You also require an authorised G2 card to open the locking device.

Special functions/G2 battery replacement transponder

If a locking device has changed to freeze mode due to a critical battery level, the locking device can only be reactivated with the aid of a battery replacement transponder. You also require an authorised transponder to open the locking device.

Special functions/G2 battery replacement card

A locking device can only be reactivated with the aid of a G2 battery replacement card after the locking device has changed to freeze mode due to a critical battery level. You also require an authorised G2 card to open the locking device.

7.1.7.10 Implement emergency opening

It is possible to open a locking device using the LSM software and the corresponding programming device. Note that you need to enter the locking system password to do so.

7.1.7.11 Test SmartCD active

You can use this function to test whether a connected SMARTCD.G2 functions correctly.

7.1.7.12 Test SmartCD Mifare

You can use this function to test whether a connected SMARTCD.MP or SMARTCD.HF functions correctly. Ensure that only one of the passive programming devices is connected when testing.

7.1.7.13 LSM Mobile

It is possible to export programming tasks from the LSM software if you have a Microsoft Windows-based laptop, netbook or PDA. You can thus programme several SimonsVoss components at the same time with mobile devices, for example.

LSM Mobile/Export to LSM Mobile

Exports the programming commands from a locking system.

LSM Mobile/Import from LSM Mobile

Exports the completed programming tasks back into the LSM software.

LSM Mobile/Exported tasks

Shows the current programming exports to LSM Mobile.

7.1.7.14 Virtual network

For further information see also here: *Managing the virtual network (VN) [▸ 220]*

Virtual network/Export to VN network

Virtual network/Import – synchronisation

Virtual network/Reset VN task

Virtual network/Exported VN tasks

7.1.8 Options

7.1.8.1 Working in compliance with data protection regulations GDPR

See *Working in compliance with data protection regulations GDPR [▸ 142]*.

7.1.8.2 Print Matrix

You can only print the matrix if the matrix view is currently being displayed.

7.1.8.3 Logging

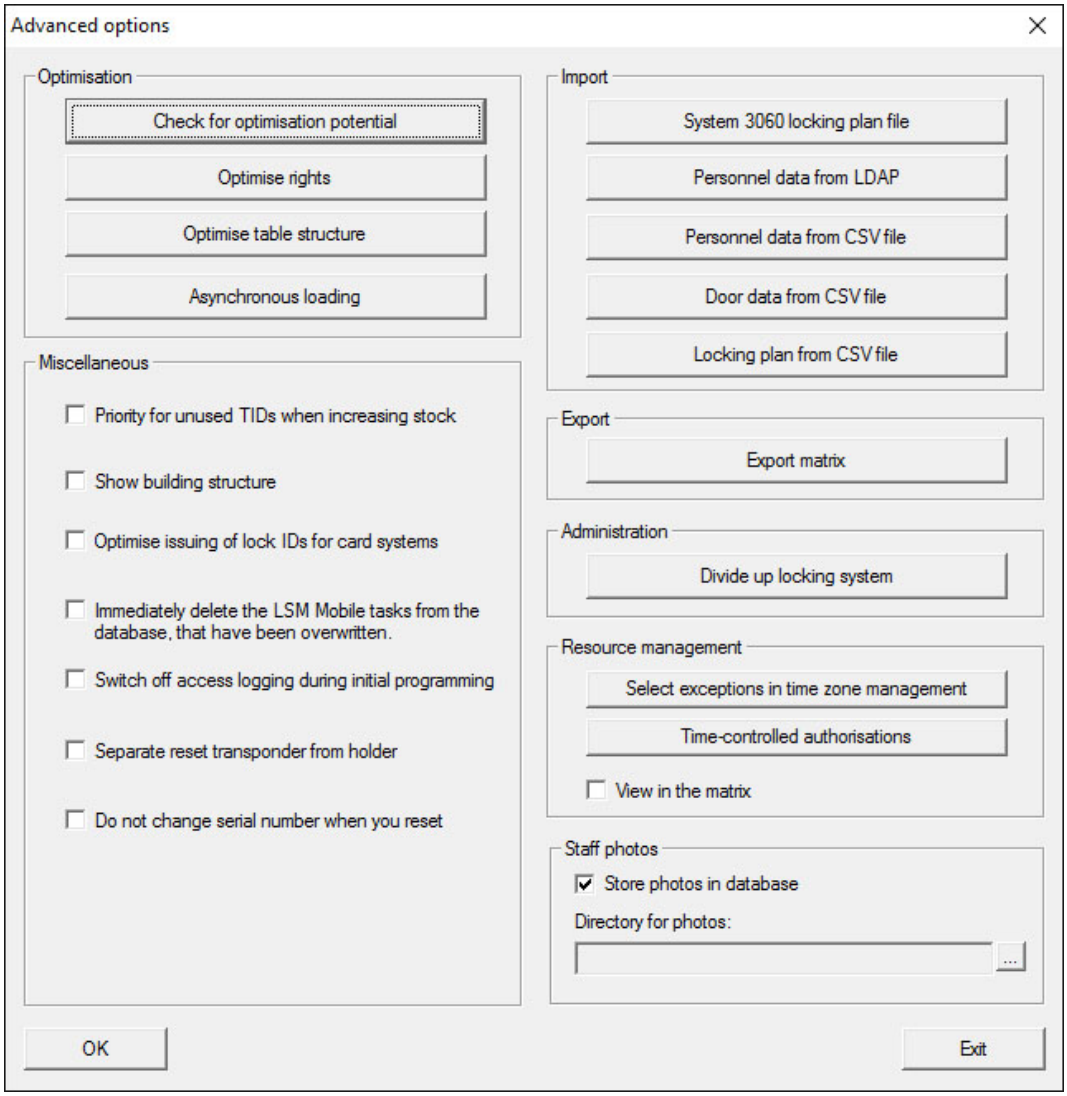
This is where you can indicate which log entries are saved and for what length of time. All log events are usually stored for 180 days. You can set time periods between 7 and 670 days.

7.1.8.4 Automatic numbering

New components are numbered sequentially by default. This option field allows you to define the syntax for different components.

7.1.8.5 Advanced

Ensure that you always have a fully functional, up-to-date data backup before optimising the database.



Check need for optimisation

Users who have been using the LSM software for some time may ask themselves whether the database application is performing correctly. Restructuring may cause more data (authorisation crosses) to overburden the database. For example, it is possible to give authorisation to a transponder group and an explicit individual authorisation to a person in this group. This just means that the person may have two existing authorisations for the same door which are separate from another. It is not just confusing but also unnecessary.

Click on the "Check need for optimisation" button to check whether the locking system needs to be optimised. Then follow the instructions in the LSM software.

Optimise authorisations

Implement this command if the check advises that you need to optimise.

Click on the "Optimise authorisations" button to check whether authorisations needs to be optimised. Then follow the instructions in the LSM software.

Optimise table structure

If a database is used for a longer period of time, this may lead to irregularities in individual tables. Optimising the structure resets the indexes in the table and removes any data inconsistencies.

Asynchronous loading

Currently not supported.

Miscellaneous

- **Preferably hold unused TIDs in reserve if reserve stock is increased**

  If the reserve of a transponder group is increased, TIDs are used which have never been used within the locking system (if TIDs are still available). If the checkbox is not enabled, TIDs which have already been programmed into a locking device before, but are not being used at the moment are also used.

- **Show building structure**

  If this checkbox is enabled, the abbreviations for the building and the floor of the door selected (if available) are displayed before the door name in the "Door" column in the "Manage WaveNet" mask.

- **Optimise issuing of locking device IDs for card systems**

If this checkbox is enabled and a configuration set in G2 card management with "L" or "L_AV", the LIDs must be issued as follows when new G2 locking devices are created:

- The next free LID is used in the case of hybrid and MIFARE locking devices.
- In the case of locking devices with active technology, an LID is issued which is above the LID range indicated for "Locking device IDs" in G2 card management.

- **Immediately delete the overwritten tasks for LSM Mobile from the database**

  If this checkbox is enabled, the previous export task for the same GUI user is deleted in the "Exported tasks" if a new task is carried out.

NOTE

Export tasks for the same user which were completed before the checkbox was enabled are not automatically deleted.

- **Switch off access control during initial programming**

  Enable this checkbox if you do not wish to have any access control in the locking system in general, but still want to use time zone control. This function is then automatically disabled when new locking devices are created.

- **Disassociate reset transponder from holder**

  Enable this checkbox if the transponder needs to be disassociated from its user when it is reset and the transponder's serial number is to be replaced by the current date and time.

- **Do not change serial number when reset**

  Enable this checkbox if a transponder's serial number should not be reset when reset (for auditing reasons).

System 3060 locking plan file

Import any locking plan from an LDB database *(predecessor to LSM software: Locking Database Software)*.

Employee data from LDAP

If employee data are provided on a server using LDAP, they can be imported using the "Employee data from LDAP" button in the LSM software.

Employee data from CSV file

You can used this button to import employee data, such as last name, first name, department and employee number, into the LSM software from a CSV file.

Door data from CSV file

You can used this button to import door data, such as the door, room number, area and inside dimension, into the LSM software from a CSV file.

Locking plan from CSV file

You can used this button to import locking plans into the LSM software from a CSV file.

Export matrix

This button allows you to export the matrix or the locking plan to a CSV file. Note that you can only export the contents of the areas and transponder groups open in the matrix.

Divide locking system

This is where you can divide an existing locking system into two systems. This is useful when a new tenant moves into a building, for example, and they would like to manage a part of the existing locking system themselves.

Select exceptions in time zone management

If a time group has been assigned to a transponder group, this function enables you to withdraw the assignment to the time group from individual transponders in this transponder group for specific G2 locking devices.

Time-controlled authorisations

You can use this function to authorise or block individual authorisation crosses at specific point in time (in their target state). This only makes sense in networked locking devices since the locking devices also need to be programmed promptly after the authorisations have been changed to make the change effective.

Employee photos

Employee photos are stored directly to the database by default. However, there is also the option to save employee photos to any directory.

7.1.8.6 Reports

Enter all data which are to be displayed with the report at this central point.

You can set the data on an individual basis or the same for all reports in LSM Business.

7.1.8.7 Access lists

You can place restrictions on access lists. It is possible to log during a specific time range in days or a maximum number of access events at a locking device.

Note how many access events can be stored on each particular locking device.

7.1.8.8 Security user password

This option provides even greater security for the whole locking system.

- **Password must be changed on a regular basis**

  Enable this option to require all users to change their password after a pre-defined period of time.

- **Use password history of the last 10 passwords**

  Enable this option to prohibit the use of the last 10 passwords.

- **Password entered incorrectly three times**

  Enable this option to block a user after the wrong password has been entered three times.

- **High password security**

  Only allow highly secure passwords.

7.1.9 Network

Working with networks such as WaveNet or virtual networks can be very complex. You can find information about working with networks in the WaveNet manual.

7.1.9.1 Locking device activation

This is where you can

- activate
- deactivate
- remote-open locking devices in the network

7.1.9.2 Collective tasks

The collective tasks item allows you to start a process such as programming for a larger number of locking devices at the same time.

7.1.9.3 Event manager

- *Setting up event management [▸ 210]*
- *Creating a response [▸ 213]*

7.1.9.4 Task manager

Available in LSM Business with enabled online module only.

- *Setting up event management [▸ 210]*
- *Read locking device [▸ 246]*

7.1.9.5 Email messages

Available in LSM Business with enabled online module only.

7.1.9.6 VN service

Advanced settings for the virtual network.

7.1.9.7 Communication node

You can select this option to specify communication nodes and their connection devices, such as Router- or CentralNodes.

7.1.9.8 Local connections

This is where you can manage the local connections to the PC/server.

7.1.9.9 Manage WaveNet

You can use "Manage WaveNet" to create the WaveNet topology and make other settings.

7.1.9.10 WaveNet Manager

This action launches WaveNet Manager. WaveNet Manager must be installed separately.

7.1.9.11 Import WaveNet topology

This action opens a window to import WaveNet topologies.

7.1.9.12 Manage LON network

This is where you can manage older LON networks centrally.

7.1.9.13 Terminal Server client settings

7.1.10 Windows

Switch between open windows.

7.1.11 Help

7.1.11.1 Help topics

Help topics for LSM software.

7.1.11.2 SimonsVoss online support

SimonsVoss provides online support for quick help. You can use this function to launch a free TeamViewer call over the Internet. The computer must have an Internet connection to use this function. After you have authorised access, a support employee will then access your computer to help you with your problem.

NOTE

Contact SimonsVoss Technologies GmbH first before you launch online support (see *Help and other information [▸ 254]*)!

7.1.11.3 SimonsVoss online

Shows the SimonsVoss homepage (See *Help and other information [▸ 254]*).You need an Internet connection to use this function.

7.1.11.4 Info about LockSysMgr...

Displays the software and driver version of the LSM software being used.

7.1.11.5 Registration

Displays the registered modules (See also Register LSM). You can also deactivate activated clients here.

7.1.11.6 Versions overview

Shows the versions of all the installations used with the LSM software.

7.1.11.7 FAQs

Displays the SimonsVoss FAQs database in the browser. You need an Internet connection to use this function.

7.1.11.8 Check for updates

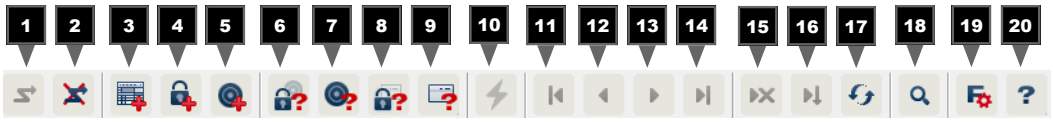
Checks the currently installed LSM software for updates. You need an Internet connection to use this function.

7.1.11.9 Database report

Exports a report in CSV format.

7.2 Menu ribbon

You can use the menu ribbon to open important and frequently used functions directly.



1. Log on
2. Log off
3. New locking system
4. New locking device
5. New ID medium *(e.g. transponder or card)*
6. Read locking device
7. Read transponder
8. Read MIFARE locking device
9. Read G2 card/tag
10. Programme
11. First dataset
12. Previous dataset
13. Next dataset
14. Last dataset
15. Remove
16. Apply
17. Update
18. Browse
19. Filter
20. Help

7.3 Locking system

This section allows you to choose between different locking systems within a project. It also allows you to view the locking system properties and edit them.

7.4 Groups and areas

These sections contain a navigation aid in which the two groups (transponder groups and areas) are mapped in two tree structures.

You can change the window size by dragging the separator line between Areas and Transponder groups and between the matrix and navigation pane.

Different symbols are displayed in the tree view depending on the display status to ensure that you can move around the tree structure as efficiently and reliably as possible:

	Locking system transponder groups
	Transponder group without transponders
	Transponder group which is hidden
	Transponder group which is displayed

	Locking system area
	Area with no doors
	Area which is hidden
	Area which is displayed

Procedure:

Subdivided areas and transponder groups with up to 6 levels are only possible in LSM Business.

- Click on the plus sign next to a red symbol and the next level down in the child grouping will appear.
- You can access further lower levels by continuing to click on the new plus signs. The maximum hierarchy depth is six levels.
- You can close the child levels by clicking on the minus sign on the left next to the blue symbol.
- You can close all opened groupings by clicking on the minus sign next to the locking system.
- If you double-click on an area or a group, this will change its respective view (display of contents in the matrix on or off).
- You can also quickly gain a complete overview by opening the whole tree structure:
  - View/All secondary areas/Open groups
- The uppermost group in the tree structure must be closed to also close all open areas or groups again.

Note that more time is required to process the data to be displayed and their display on the screen as the tree structure gets larger. You may experience this when reorganising the structure or refreshing the view.

7.5 Matrix

This view forms a matrix which provides a visual display of hierarchical personnel and room structures. The matrix is also able to authorise transponder groups for complete areas. This makes it quick and easy to issue basic authorisations in the Areas/Transponder groups view. The Doors/Persons view allows you to issue deviating authorisations in the form of individual extensions or restrictions.

Doors/Persons view

✕	Authorisation which has been configured, but not programmed into the locking device yet.
✕	Authorisation which has been programmed into the locking device.
✕	Authorisation which has been removed but not transmitted to the locking device yet.
✕	Yet to be programmed authorisations which are compliant with the locking system's group structure, i.e. they are from the group view, are marked with a small, black triangle.
✕	Programmed authorisations which are compliant with the locking system's group structure, i.e. they are from the group view, are marked with a small, black triangle.
✕	Withdrawn authorisations which are compliant with the locking system's group structure and have not been programmed yet.
✕	Authorisations which are not compliant with the locking system's group structure are indicated by a cross only and do not feature a black triangle (individual authorisation).
	Authorisations which have been withdrawn from the locking system's group structure at a later date feature the black triangle, but no longer feature an authorisation cross.
	Chequered (greyed-out) box: No authorisations can be configured. They do not feature any write accesses or the locking plan blocks this box (e.g. for deactivated transponders or G2 cards at the active cylinder).

Areas view/Transponder groups

✕	A black cross with a circle inside indicates a group authorisation.

	A grey cross with a circle inside indicates an "inherited" authorisation.

Group authorisation tree view

	Set manually (black)
	Direct inheritance (green)
	Indirect inheritance – inherited from child group (blue)
	Both direct and indirect inheritance (blue/green)

Programming requirement

A programming requirement may arise for a transponder or a locking device for different reasons. The programming flashes are shown in different colours to represent the different reasons for a programming requirement.

	Programming requirement for the component (yellow)
	■ Programming requirement for the transponder (red): ■■ Validity expired ■■ Deactivated ■ Locking device (red): ■■ Only common locking level assigned ■■ Not assigned to any door ■■ Not assigned to any locking system ■■ Door without locking device
	Programming requirement for a locking device after creating a replacement transponder in G1 system overlay mode

■ You can double-click on a component in the matrix to switch directly to the component's properties.

8. Background knowledge on LSM

This section describes the approaches to theory which should make it easier to gain understanding on how to work with the LSM software.

8.1 Group authorisations

A group authorisation enables you to authorise an entire transponder group for a whole area. This allows you to create basic authorisations in the locking plan very quickly in a clearly arranged way. It is useful to be clear about the planned use of the building and the company's organisational structure in advance when issuing the authorisations. A clearly structured system helps significantly to establish facts about possible access events quickly and precisely during day-to-day business at a later stage, allowing the company or organisation to run smoothly on a daily basis. You can add exceptions to group authorisations at *View/Doors/Persons* at any time at a later date by removing or adding an individual authorisation cross.

Areas and transponder groups

The following use case is quite frequently: A company consists of several departments with employess which need access to one, several or all departments. Of course it is possible to assign every employees' transponder to every door in the corresponding departments. However, this has a downside: The effort for managing such a locking system rises with the number of transponders and doors.

It's much more comfortable to use areas and transponder groups instead. Doing so, you only need to assign a transponder group or a door once. Every transponder in this group has the same rights as the group. The same applies to doors: Every door in an area has the same rights like the area which the door belongs to. This means: If you assign a new door to an area, then every transponder which is assigned to this area is also able to open this door.

Example: Facility management staff shall be allowed to enter the rooms of the support department. The company is split into several departments:

- Development
- Marketing
- Sales
- Support
- Restricted area
- Manufacturing

All transponders which belong to facility management staff are grouped to a group called facility management staff. Also all the doors which belong to departments are assigned to the corresponding departments (during their creation), for example support. For example, let's say the company has ten locks in the support department and the facility management team consists of ten persons. If one wants to assign everyone of this team to every door in the support department, then one has to assign and handle a whopping hundred authorisations (Ten transponders to ten doors).

Instead, one can use our transponder group facility management staff and assign this group to the area support. Thus, the number of authorizations to be assigned shrinks down to exactly one authorization.

8.1.1 Group reserves (G1 only)

Assigning a transponder to a group means that the transponder concerned immediately receives all the authorisations that have been allocated to the group. If a new transponder is assigned to a group, there is a programming requirement for the locking devices concerned. To avoid this situation, what are known as "Reserves of transponder IDs" can be assigned to groups when they are created and even at a later stage. Such transponder IDs are not assigned to any persons at this point in time. The reserves are saved to locking devices during programming and are then ready for use.

If a transponder ID from this reserve is then allocated to a person and the transponder programmed, there is no programming requirement for the locking devices. Transponders can thus be authorised automatically and activated in locking devices without the user needing to complete further steps such as programming the locking device.

8.1.2 Inheritance

Inheritance is one way of mapping the hierarchy of a company in the locking system. If inheritance is implemented correctly, it reduces the user's workload enormously. It enables certain processes to be automated by assigning a transponder from a specific transponder group. Inheritance can used when applying a hierarchy to areas and transponder groups. Group authorisations are taken into account during inheritance; the individual authorisations are not inherited.

8.2 Authorisations in the G2 protocol

Authorisations are stored on all components in the G2 protocol. This enables a new transponder to operate an authorised locking device without needing to reprogramme the locking device in question. Blocks (what are know as block IDs) can be transferred in the same way. When a new replacement transponder is activated on a locking device for the first time, its original authorisation is deleted from the locking device.

8.3 Time zone plans

The LSM software allows you to authorise transponders for locking devices for certain time periods only.

Example: A cleaner has a transponder which basically allows authorised access to the rooms to be cleaned. These rooms are to be cleaned between 16:00 and 20:00 hours on Mondays, Wednesdays and Fridays only.

This is where time zone plans come into play. An example is used below to give a brief explanation on how time zone plans are implemented. The example also tells you how time zone plans behave in different SimonsVoss components:

As a basic rule, time zone plans should be kept as simple as possible. In normal cases, time zone plans are created for locking devices. Individual time groups are then created in the locking device's time zone plan. These groups specify at what particular times each transponder may be authorised for use.

Entire areas are used instead of individual locking devices to keep the time zone plan as simple and general as possible. At the same time, whole transponder groups are assigned to specific time groups and not transponders on an individual basis. Such a process would look like this for the example:

Create time zone plan

- Create new time zone plan for the *Building shell* area. This area comprises all doors through which people can gain access to the building.
- A time group (e.g. Group 1) is selected in the new *Building shell* time zone plan. This group is named *Cleaning times*, for example.
- A time slot is now established in the time zone plan for the *Cleaning times* group. The relevant times can be selected from a weekly calendar as required.

Assign time zone plan to the area

- The *Building shell* time zone plan created and its defined *Cleaning times* time group are now assigned to the *Building envelope* area.
- The *Building envelope* area is then linked to the time zone plan. However, we still have not specified which transponder groups are assigned to the *Cleaning times* time group.

Assign time group to a transponder group

- The *Cleaning staff* transponder group then needs to be linked to the time zone group.

- A *Building envelope* time zone plan has now been created. Its associated *Cleaning times* time group is linked with the *Cleaning staff* transponder group.

Any number of time zone plans, complex or not, can be defined using this process. To finish off, we need to show what happens between the devices in the background:

- The time zone plan is programmed into each locking device in the *Building envelope* area that supports the access control function.
- The *Cleaning times* time zone group is saved to the transponders in the *Cleaning staff* transponder group.
- If the *Cleaning Staff 1* transponder is now activated on the *Main entrance* locking device, the transponder communicates its transponder ID and time group to the locking device.
- The *Main entrance* locking device checks in the first instance whether the transponder is actually authorised to use the locking device. In the second instance, the system checks whether the time group is authorised to use the locking device at the current time (day and time).
- If the response is positive for both queries, the locking device can be actuated. If the locking device check produces a negative response, access is denied.
- Both access events and rejected transponders can be saved in locking devices with the access control option.

8.4 Common locking level

Several locking systems may be managed within a project. Typical scenarios are shown here as an example:

- **A company with multiple locations/buildings**

  A company has individual branch offices in different locations. Employees normally always work in the same branch. However, special person groups need access to a number of branches or buildings.

  In this case, the individual branches or buildings are divided into separate locking systems. An employee from the main branch also needs to be authorised to use doors at other locations. This main branch employee is thus linked into the locking system at the other branch, where individual authorisations can also be configured.

- **A building with several occupants**

  A building has several occupants. The individual occupants need their own locking systems. However, the occupants need to share different locking devices, such as those on cabinets, turnstiles and the main entrance.

In this case, the individual occupants are divided into separate locking systems. A common locking level is also created, where all shared locking devices are added, for example. Persons and/or areas are added to the parent locking system and their corresponding authorisations are configured at the same time.

- **Fire service transponder for selected locking devices in all locking systems**

  Special fire service transponders to place in a key tube safe contain authorisations for all doors in a building. This allows the fire service to open all locking devices with a transponder in the event of a fire.

  In this case, a new common locking level is created, marked in red, where the area properties are used to add all required doors in the project. A "Fire service" transponder group is also created, which is authorised by clicking on all doors in the "red" common locking level.

General notes on comment locking levels:

- If a locking device or a transponder is linked into another locking plan, this linked object behaves in the same way as the original. If the original transponder or locking device is changed or deleted, this change in status has a direct effect on the linked object in the other locking system.
- The red level contains special characteristics, such as the opening of deactivated locking devices, which have been specially designed for the fire service. Only use this level for access in emergencies if at all possible.

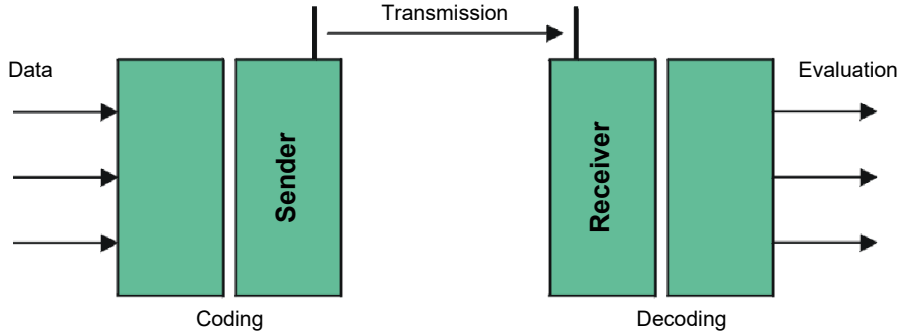
NOTE

All locking devices must be reprogrammed if pre-programmed locking devices are added to a common locking level. Look out for the newly generated programming requirement, which is indicated by a programming flash icon.

8.5 Encryption (WaveNet)

Advanced cryptography protects the data that is transported in your WaveNet.

Technical realization



End-to-end encryption

End-to-end means in this context: between central software and locking devices. The data is encrypted and leaves the central software. It is only decrypted again when the locking device is closed.

Communication	Encryption
End-to-end (general)	3DES (112 bit)
Access lists (against unauthorised reading)	Single DES (56 bit)
Broadcast signals	AES (128 bit)

Digitally signed data packages

The 128-bit signing of the data packets protects against manipulation on the radio link. If the signature of a data packet is not correct, the data packet is ignored.

Protection against replay attacks

Each safety-relevant data packet contains a counter. This counter is incremented for each new data packet. If a data packet with the same counter reading arrives again, the data packet is ignored. This means that if an attacker records a data packet and sends it again (replay attack), the counter of the data packet is the same as that of the original packet and the copy of the attacker is recognized and therefore ignored.

9. 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.

9.1 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 [▸ 130].*
3. Click on the "Apply" button.
4. Click on the "Finish" button.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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.

9.7.1 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.

9.7.2 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*

9.7.3 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.

9.8 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.

9.9 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.

9.10 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.

9.11 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.

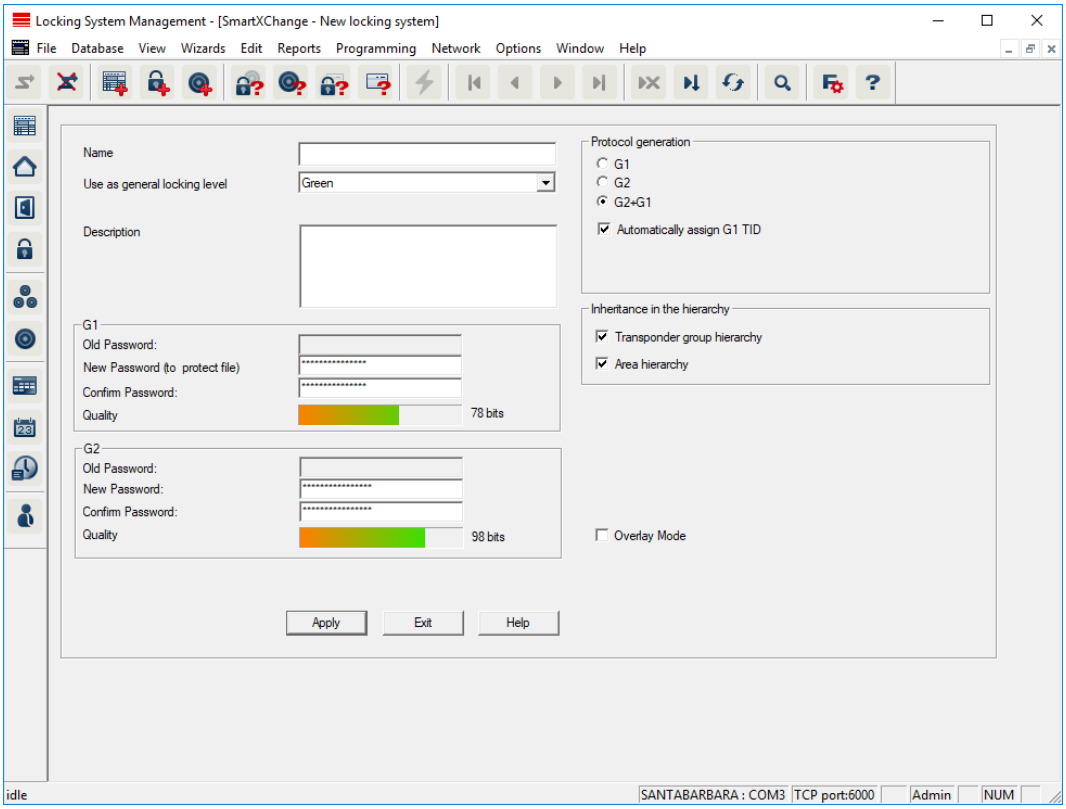
9.11.1 Add common locking level

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".

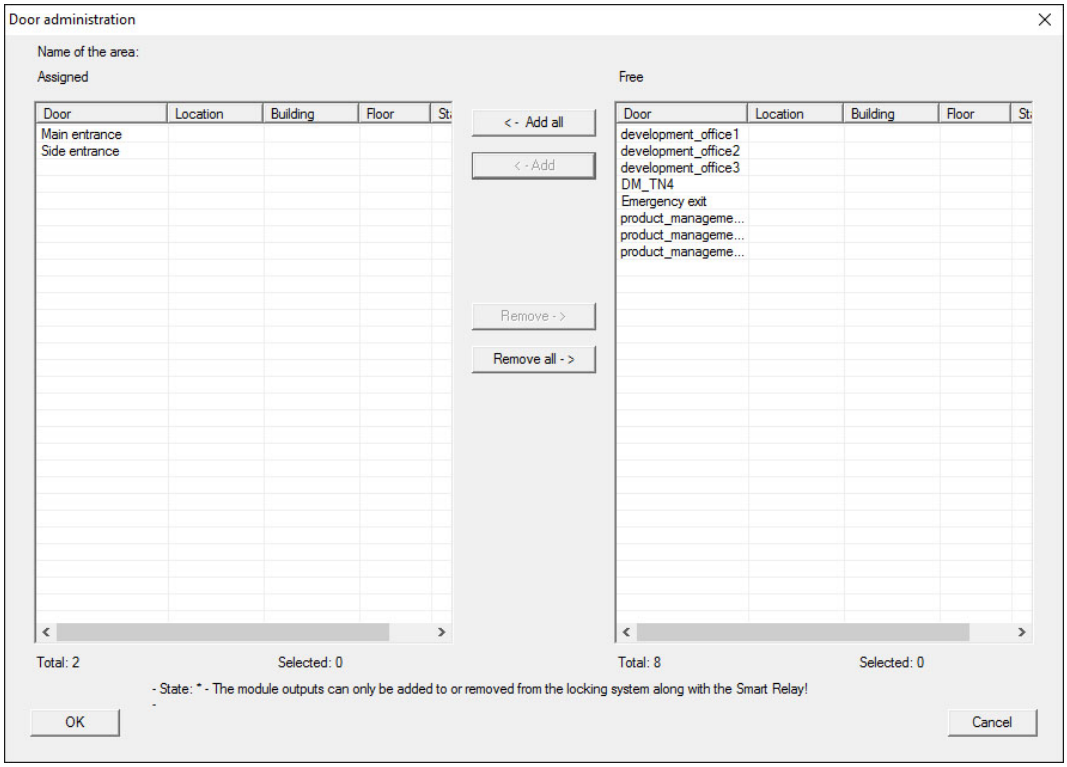


9.11.2 Link locking devices

✓ 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.



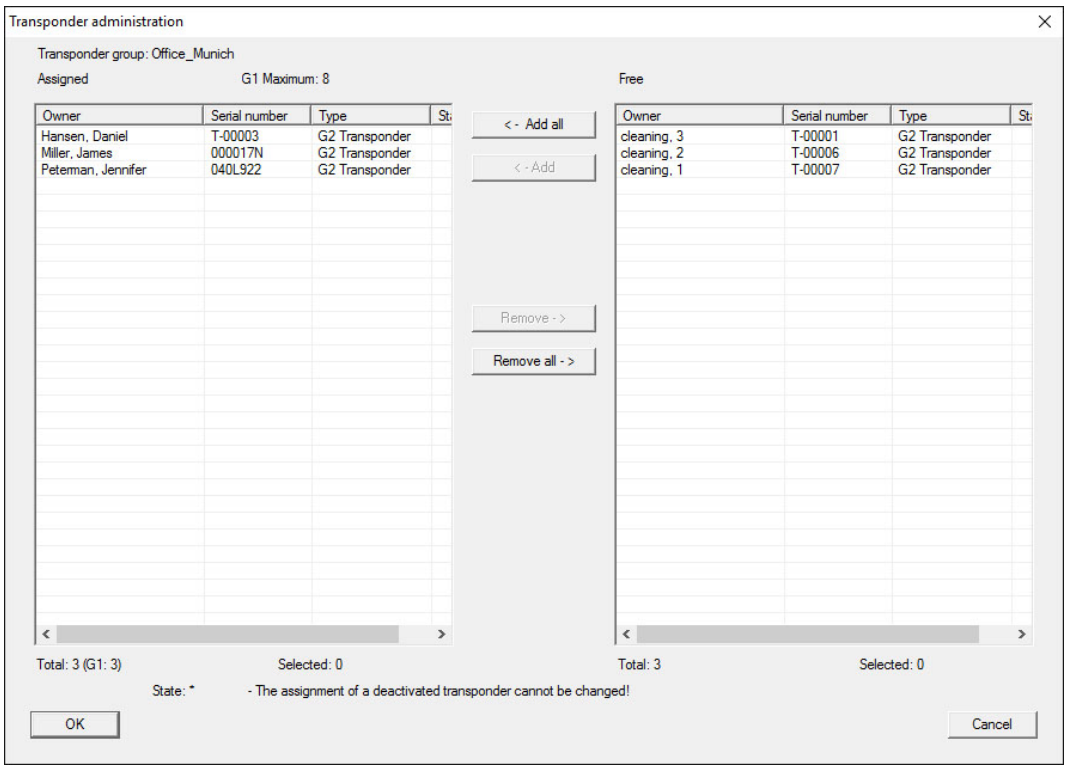
9.11.3 Link transponders

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.

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



9.11.4 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.

1. Open red common locking system.
2. Create transponder group which should be authorised for all areas relevant for the fire service.
3. Click on the "Authorisations" button in the transponder group properties in Administration.
4. Use the checkboxes to select all the areas/locking devices required to grant access through all doors to the transponder group.

9.12 Create fire service transponders

✓ You have already created at least one locking system.

1. Create a new "red" common locking level, using *Edit/New locking system*, for example.
2. Add a new area, such as "All locking devices", and use "Door administration" to assign all the locking devices required to this area.

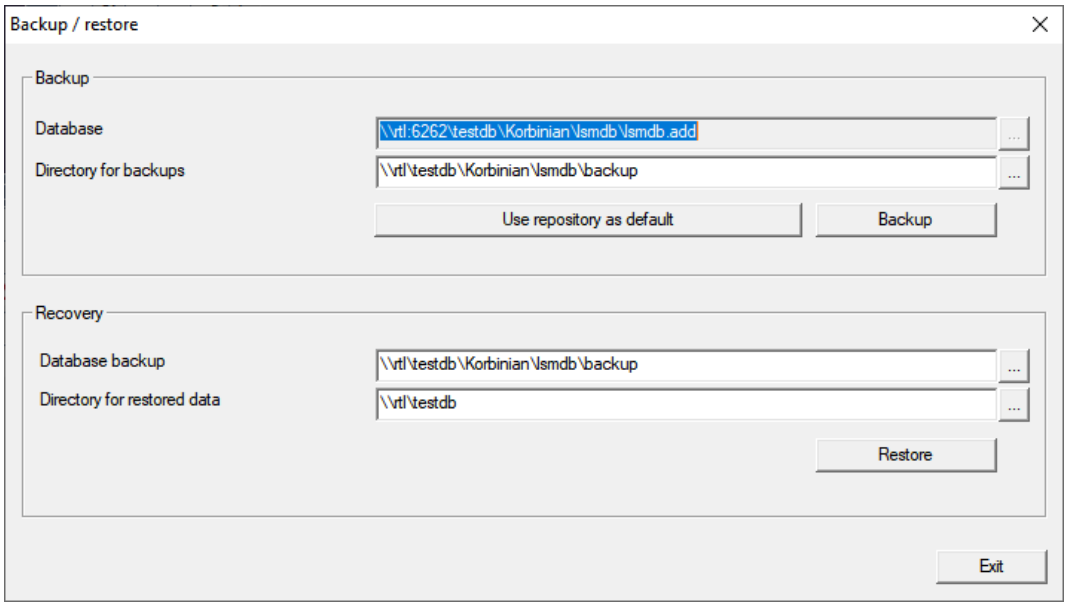
3. Add a new "Fire service" transponder group to the common locking level.
4. Click on the "Authorisations" button in the properties for the "Fire service" transponder group.
5. Enable the "All systems" checkbox to authorise this transponder group for all locking devices in general.
6. Click on the "OK" 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.

9.13 Backing up the database manually

✓ LSM opened.

1. Select via | Database | the entry Backup .
   ↳ Window "Backup / restore" opens.



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.

9.14 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 [▸ 116]*).

9.14.1 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:

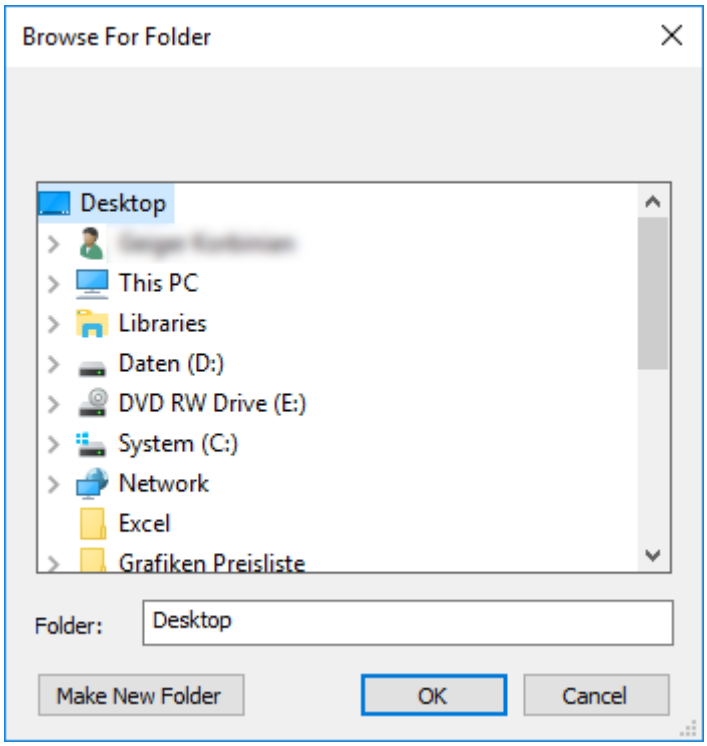
Person	This file contains personal data which can be used to identify the person (for example, surname, address or photo).
PersonHistory	This file contains the dates that the data record was created and erased.
PersonLog	This file contains different processing steps which have been performed on the person 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

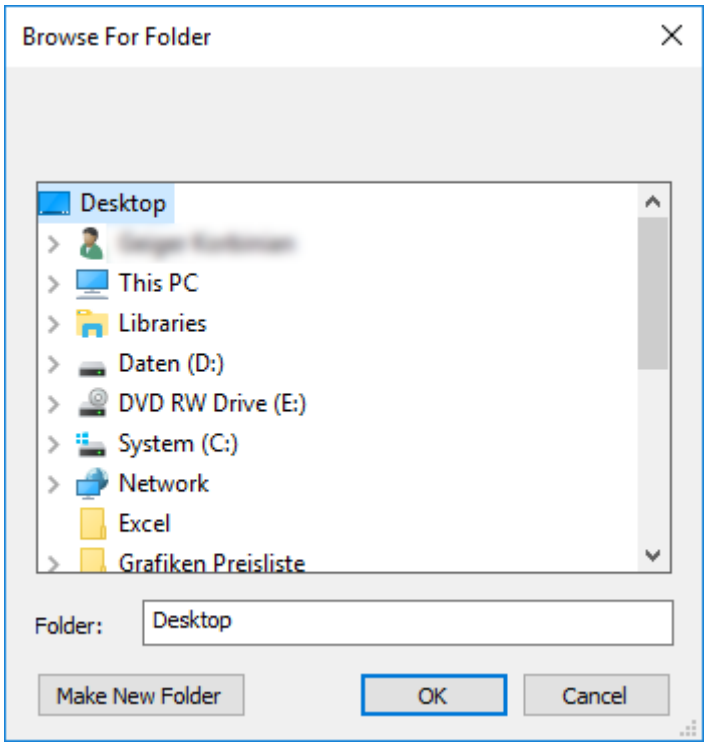
You can export the users' saved personal data as CSV files in the LSM software. Two files are generated during this process:

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.

9.14.2 Deleting Data

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

Persons

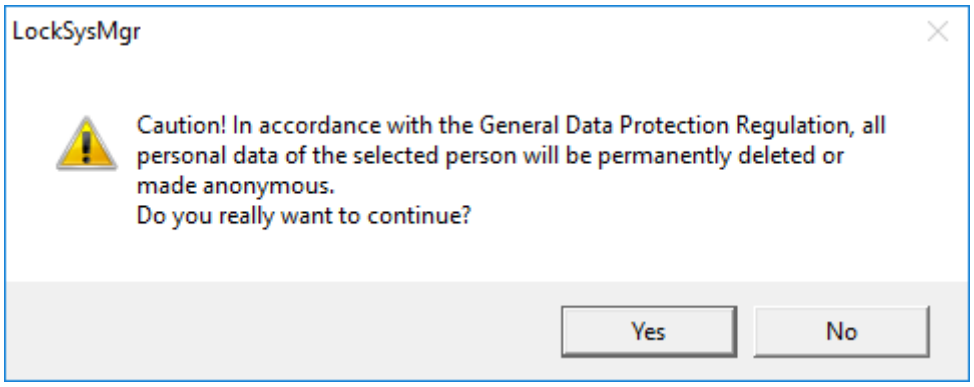
NOTE

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

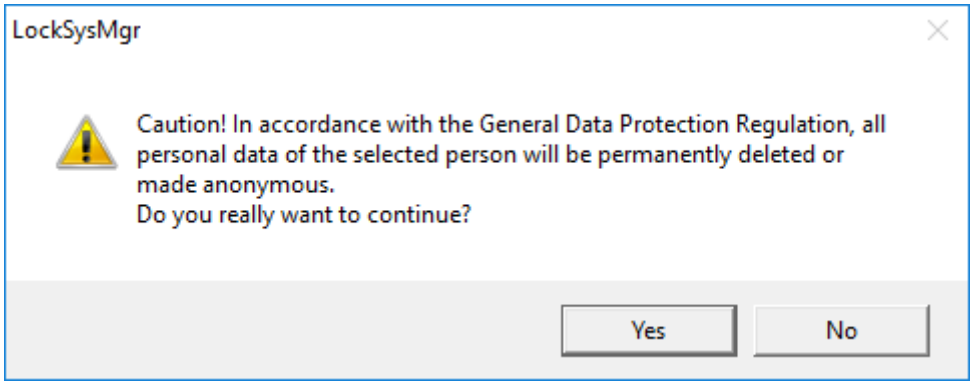
You can also use the button in the [Name] tab in the assigned identification media to erase personal data. Unlike erasure using the GDPR module, this button does not delete logs, which will remain in the system. This means that only a part of personal data is erased. People who are deleted in this way 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.

9.14.3 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.

9.14.4 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).

9.14.5 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.

9.14.6 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.

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

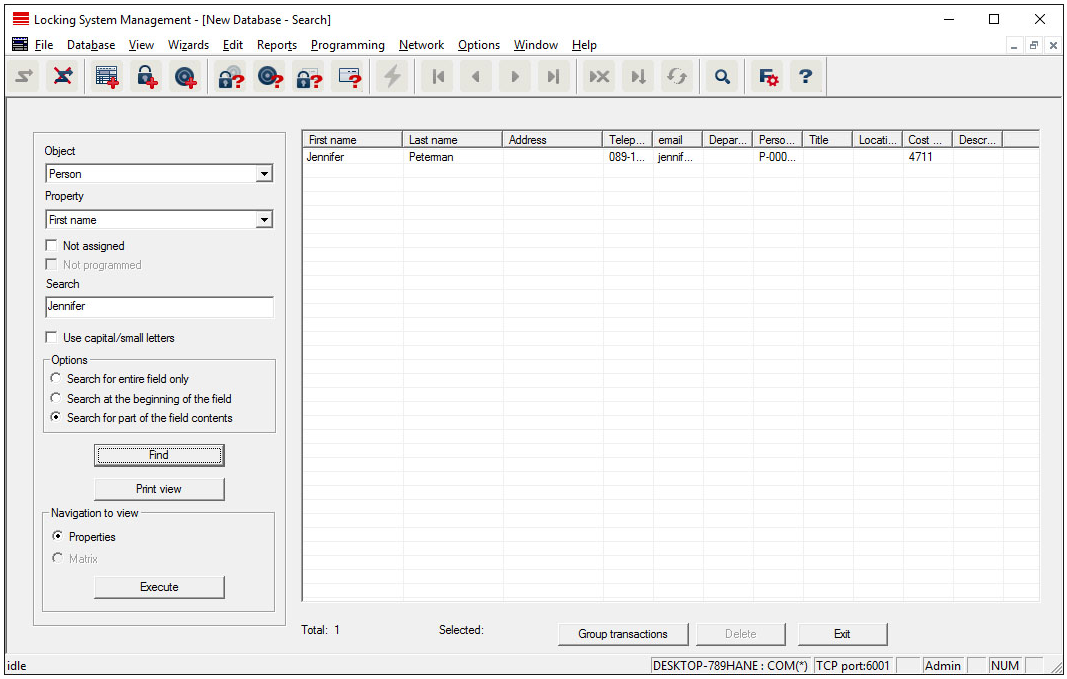
All collected data on a data subject can be made available as a copy by means of an export function (Art. 15 GDPR).

9.14.8 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.

9.15 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.

9.16 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.

9.17 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 [▸ 154]*).

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.

9.18 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.

9.19 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.

9.19.1 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.

9.20 Define time zone plan (with public holidays and company holidays

NOTE

Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to ± 15 minutes per year.

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.

9.21 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.

9.22 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.

9.23 Block transponders

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

- *Block transponder permanently and create replacement transponder [▸ 154]*

- *Block transponder temporarily [▸ 157]*

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.

9.23.1 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.
3. Update the matrix. The programming requirement has now disappeared.

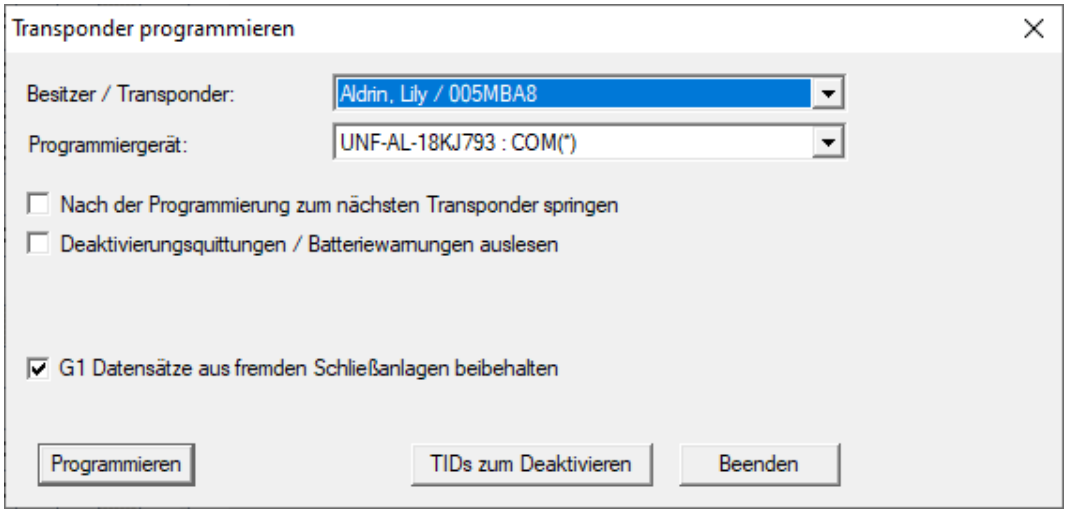
With LSM 3.5 SP3 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

Programme the TIDs to be disabled directly

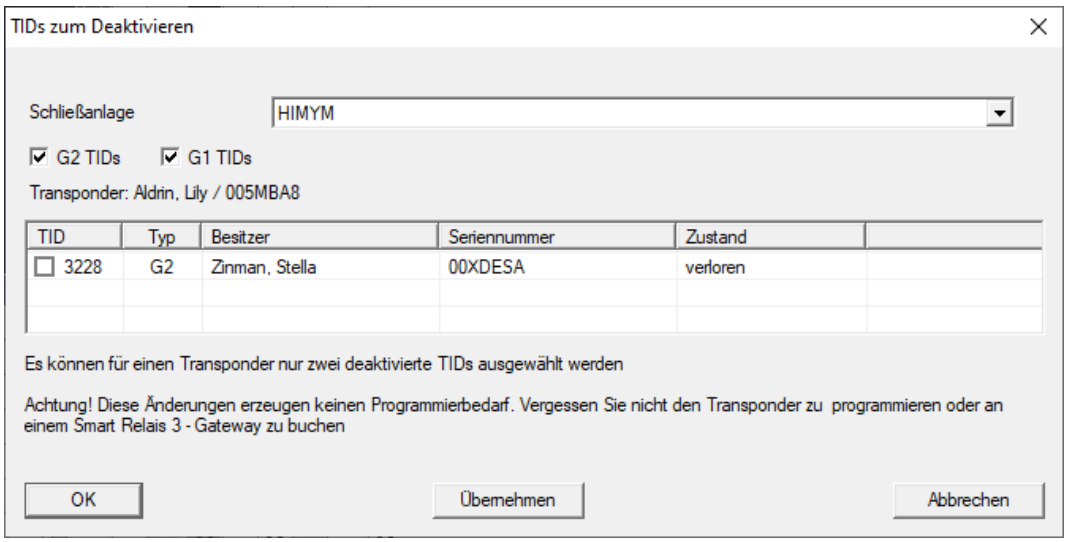
The IDs to be disabled are saved on the transponder during the programming process.

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

1. Click on the TIDs to deactivate button.



↳ The list will open.



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.

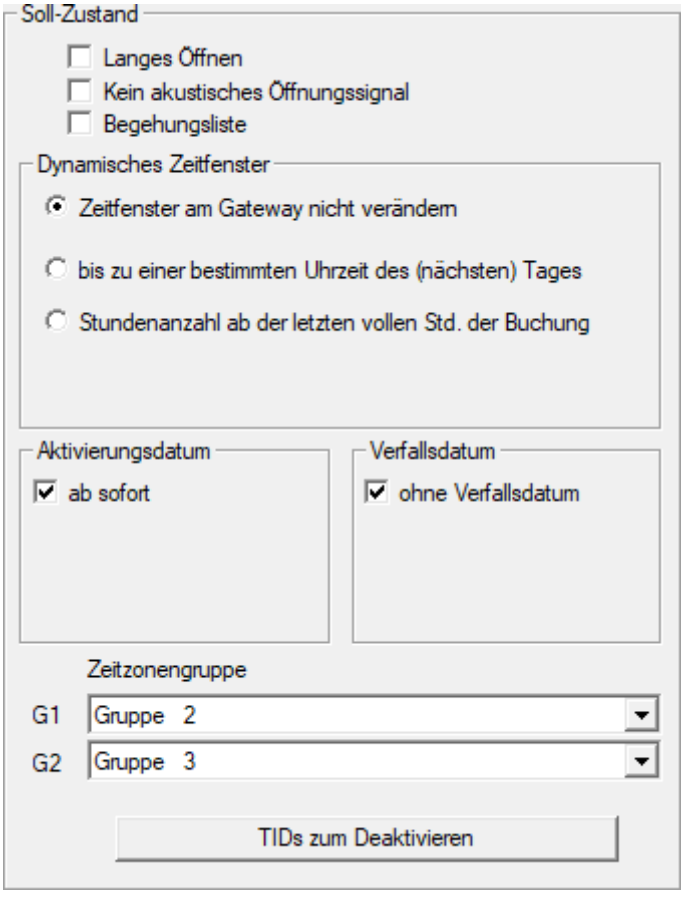
↳ The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

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.

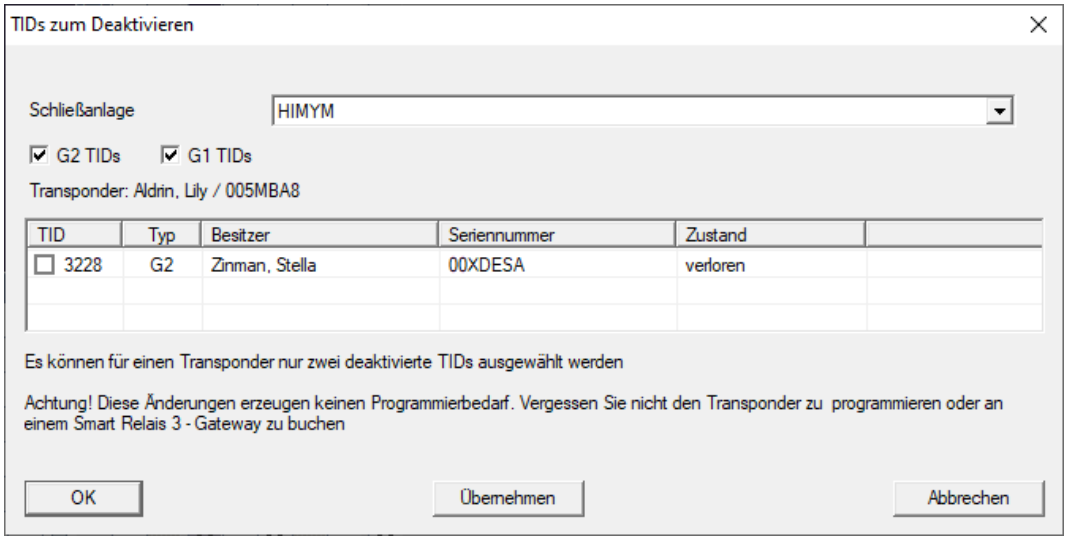
✓ The transponder's properties window is open.

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



2. Click on the TIDs to deactivate button.

↳ The list will open.

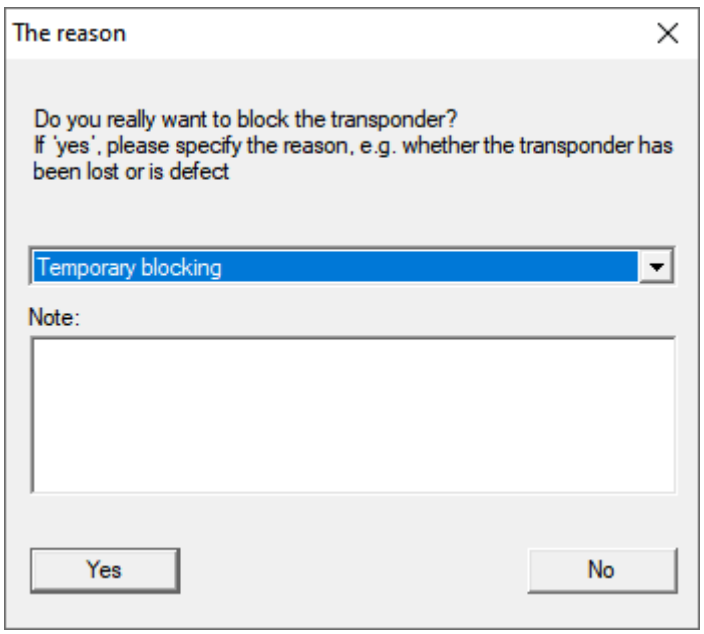


3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
4. Click on the OK button to confirm your input.

↳ The checked TIDs are saved on the transponder either during the next programming process or the next booking on a gateway.

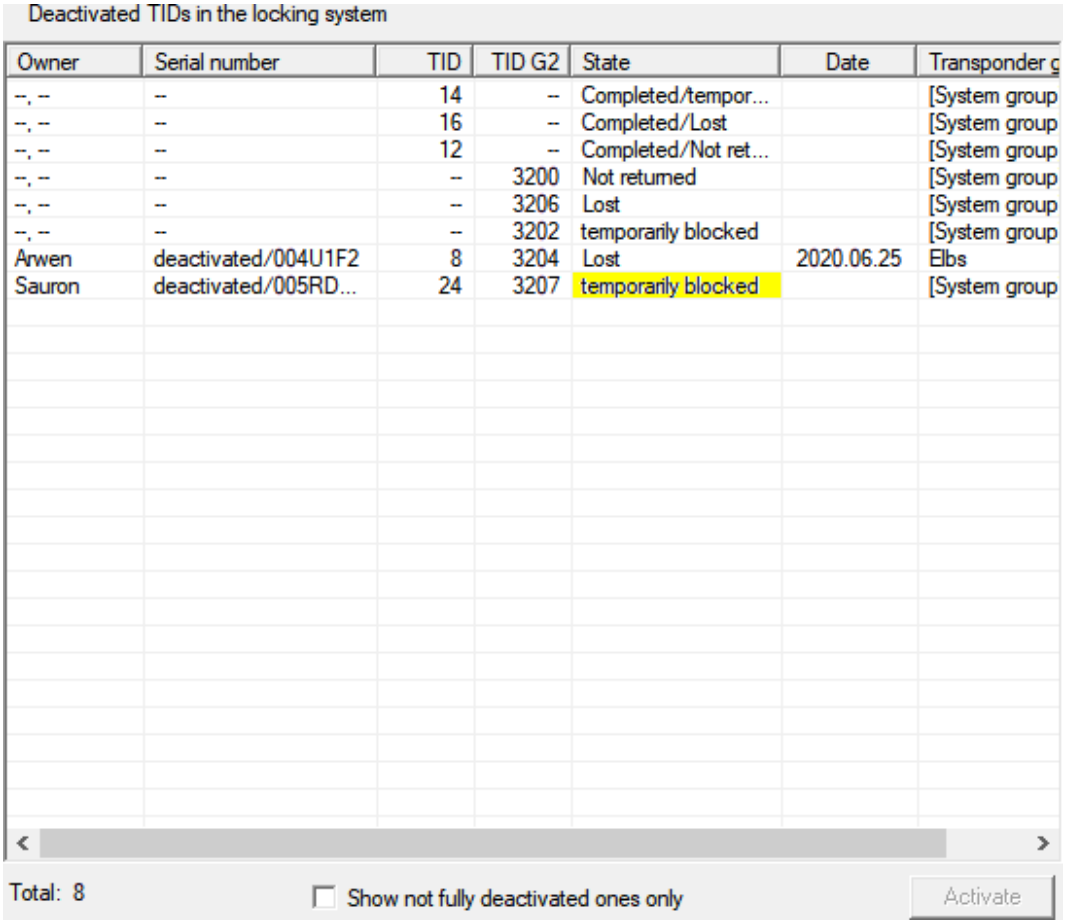
9.23.2 Block transponder temporarily

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 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].



9.24 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.

9.25 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.

9.26 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 [▸ 114]*).
✓ 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.

9.27 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 [▸ 162]*.

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.

9.27.1 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 [▸ 246]*).

9.28 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.

9.29 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.

9.29.1 Change configuration

You have two options for using cards.

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

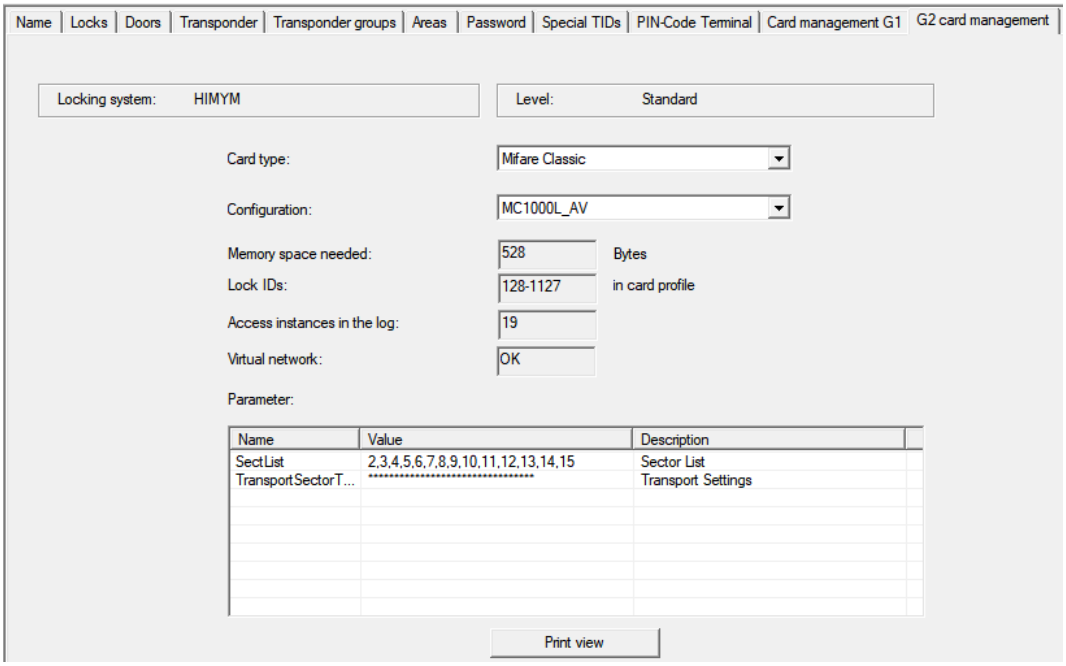
In both cases, enter the card type, the configuration and, if necessary, the sectors to be described (see *Overview [▸ 164]*).

Configuring the card

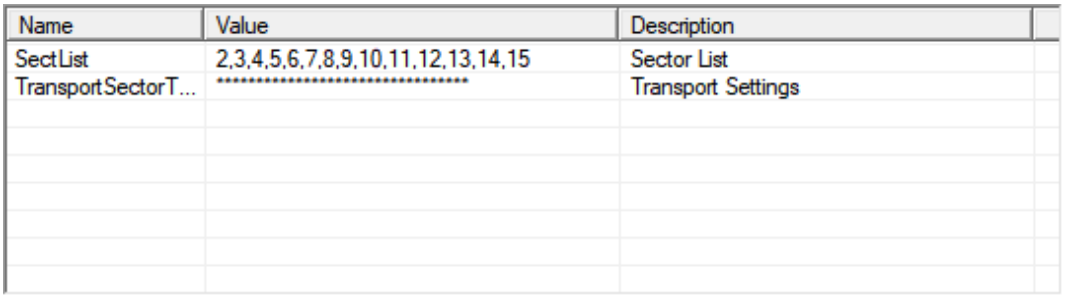
✓ LSM open.

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].



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).



7. Click on the Apply button.

↳ You have changed the configuration.

9.29.2 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_AV	✕	✓	✓	✕	✓
MC2400L_AV	✕	✓	✓	✕	✓
MC8000L_AV	✕	✓	✓	✕	✓
MBasic	✕	✕	✕	✓	✕
M1200L	✕	✕	✕	✓	✕
M3800L	✕	✕	✕	✓	✕
M1000L_AV	✕	✕	✕	✓	✕
M4000L_AV	✕	✕	✕	✓	✕
M8000L_AV	✕	✕	✕	✓	✕
M10000L_AV	✕	✕	✕	✓	✕

	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
MC3800L	G2	128-3927	3800	✕	2-15	528	✕
MC1000L_AV	G2	128-1127	1000	19	2-15	528	✓
MC2400L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✕	✕	✕	2-15	48	✕
M1200L	G2	128-1327	1200	✕	2-15	192	✕
M3800L	G2	128-3927	3800	✕	2-15	528	✕
M1000L_AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✕	✕	✕	2-15	48	✕
MD1200L	G2	128-1327	1200	✕	2-15	192	✕
MD3800L	G2	128-3927	3800	✕	n.a. (DES-Fire)	528	✕
MD2500L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	✓
MD4000L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	✓
MD1000L_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	128-32127	32000	470	n.a. (DESFire)	7000	✓
MD2400 L_AV	G2	128-2527	2400	34	n.a. (DESFire)	830	✓
MD3650 L_AV	G2	128-3777	3650	2	n.a. (DESFire)	830	✓

9.30 Forwarding USB programming devices to terminal servers (LSM Professional)

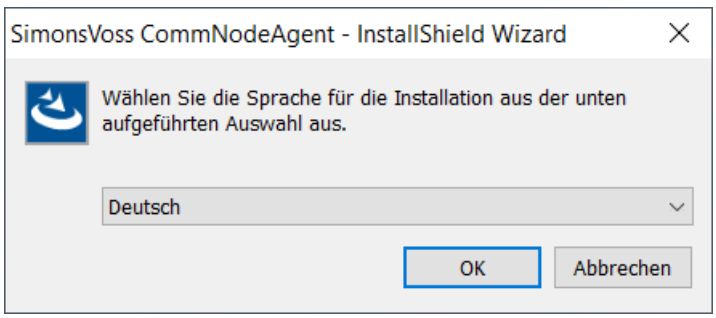
9.30.1 SmartCD.G2 / SmartCD2.G2

9.30.1.1 CommNodeAgent

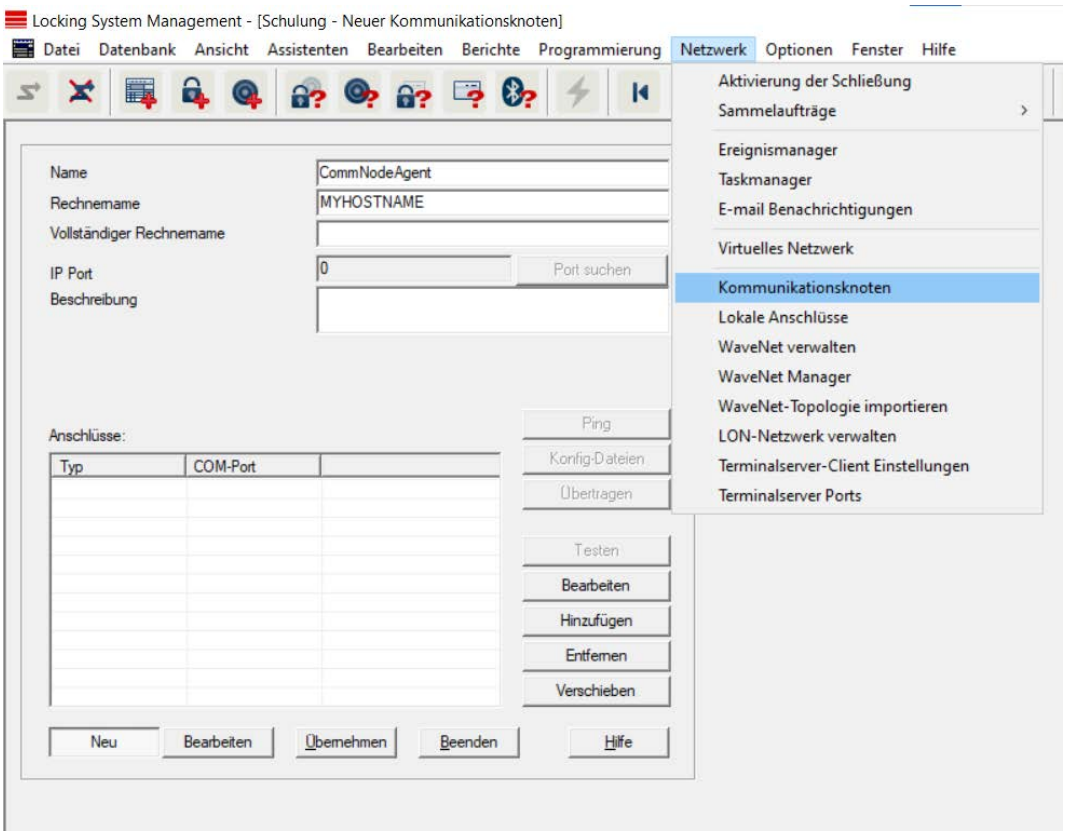
The CommNodeAgent is an SimonsVossapplication (only for full Windows systems, not for Windows RT) that uses the active SmartCD (SmartCD.G2 / SmartCD2.G2) in a remote desktop session. The CommNodeAgent forwards the USB SmartCD to the desired remote desktop session. The CommNodeAgent must be installed on the terminal-client and configured accordingly in LSM.

- ✓ Free USB port on terminal client
- ✓ Port release in the firewall (see SimonsVosscommunication matrix)
- ✓ Bidirectional DNS resolution client ↔ server
- ✓ CommNodeAgent version is identical or compatible with the LSM version

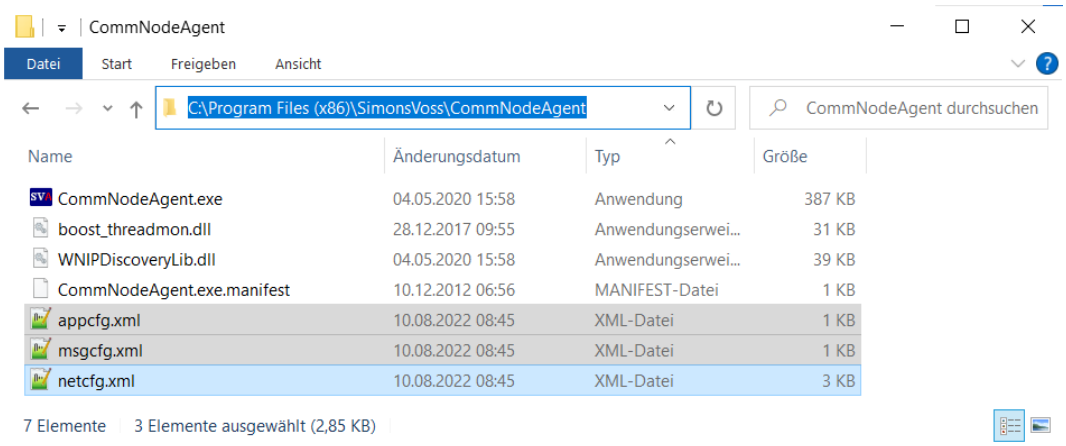
1. Install the CommNodeAgent and the SmartCD driver on the terminal client.



2. Go to | Network | in the top toolbar to select Communication nodes.

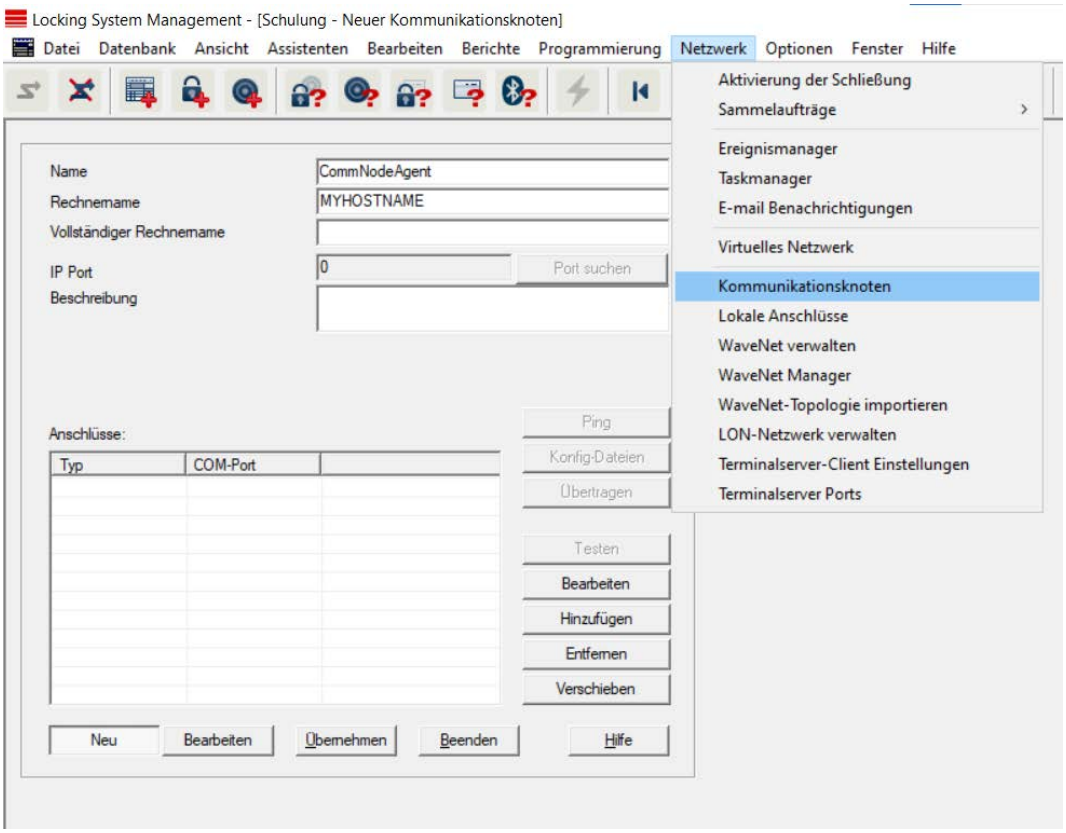


3. Click the button New.
4. Enter a user-defined name for the communication node in the input field Name [offen], e.g. CommNodeAgent.
5. Enter the terminal client hostname in the input field Rechnername [offen].
6. Click the button Apply.
7. Click the button Config files to save files as required.
8. To transfer the config files, copy the three generated XML config files from the above steps to the CommNodeAgent installation folder.

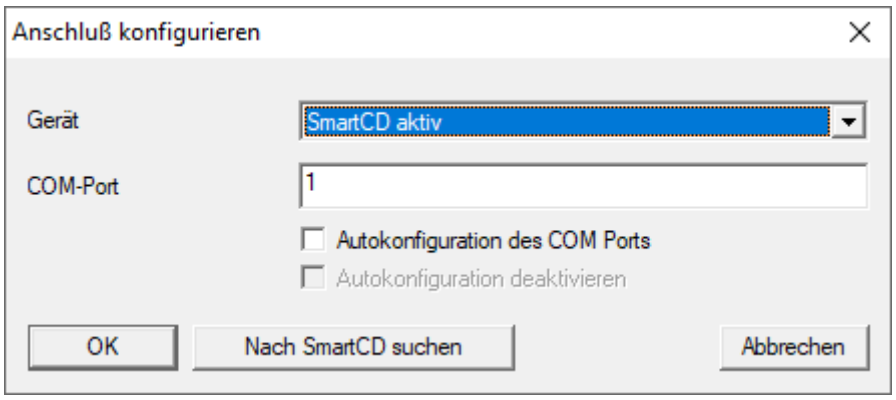


9. Run CommNodeAgent.exe as administrator.

10. To add SmartCD to the CommNodeAgent, select the | Network | entry in the upper program toolbar Communication nodes.

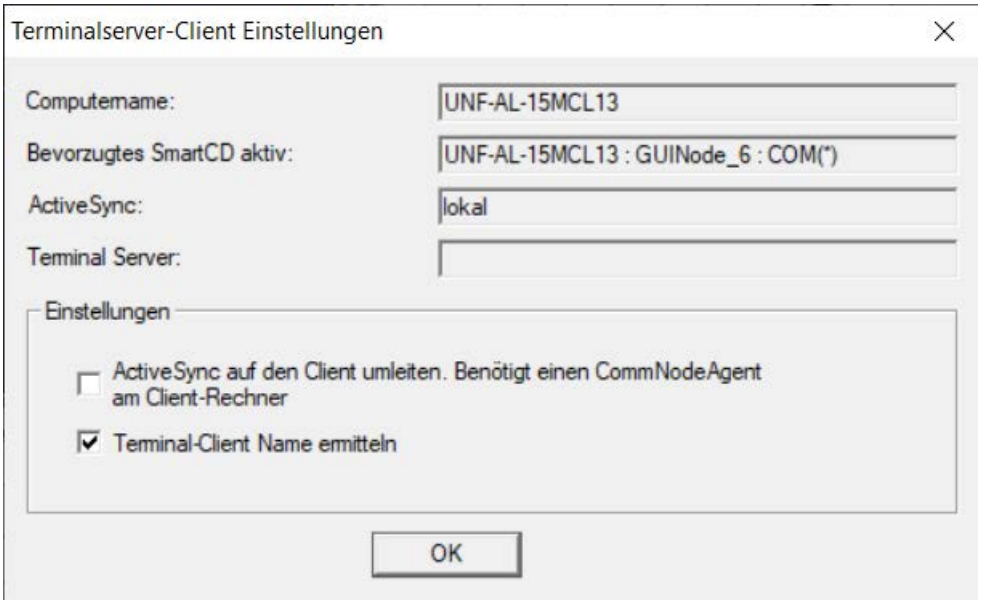


11. Click the button Add.
    ↳ The "LSM Hinzufügen Kommunikationsknoten: Anschluß konfigurieren [offen]" window will open.

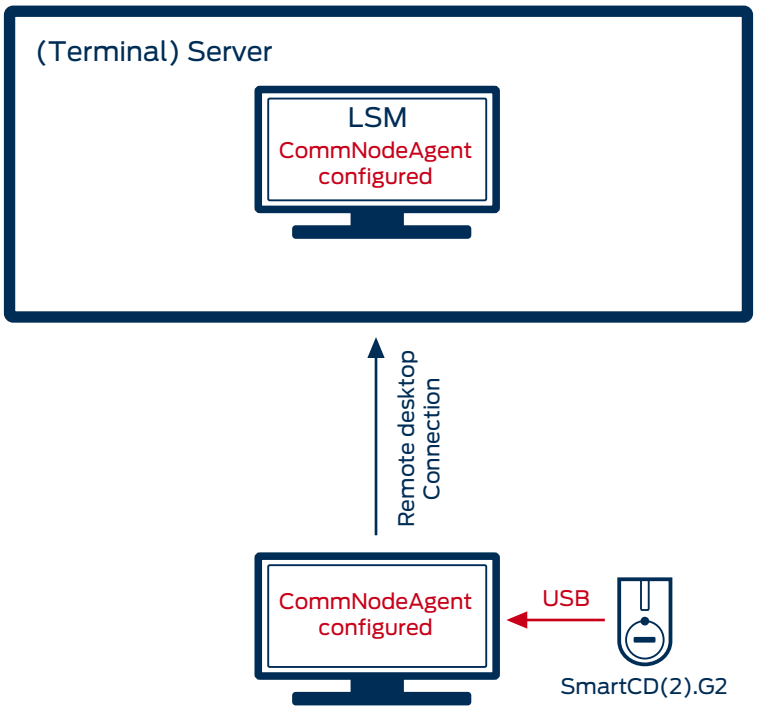


12. In the following dialogue ▼ **Device** select an entry from the drop-down menu "SmartCD".
13. Activate the ☑ LSM Kommunikationsknoten hinzufügen: Autokonfiguration des COM Ports [offen] check box.
14. Click on the OK button.
15. Click the button Transmit.

16. Go to | Network | in the top toolbar to select Terminalserver-Client Einstellungen.
17. Activate the ☑ Netzwerk: Terminal-Client Name ermitteln [offen] check box.



↳ The terminal server client settings are checked.



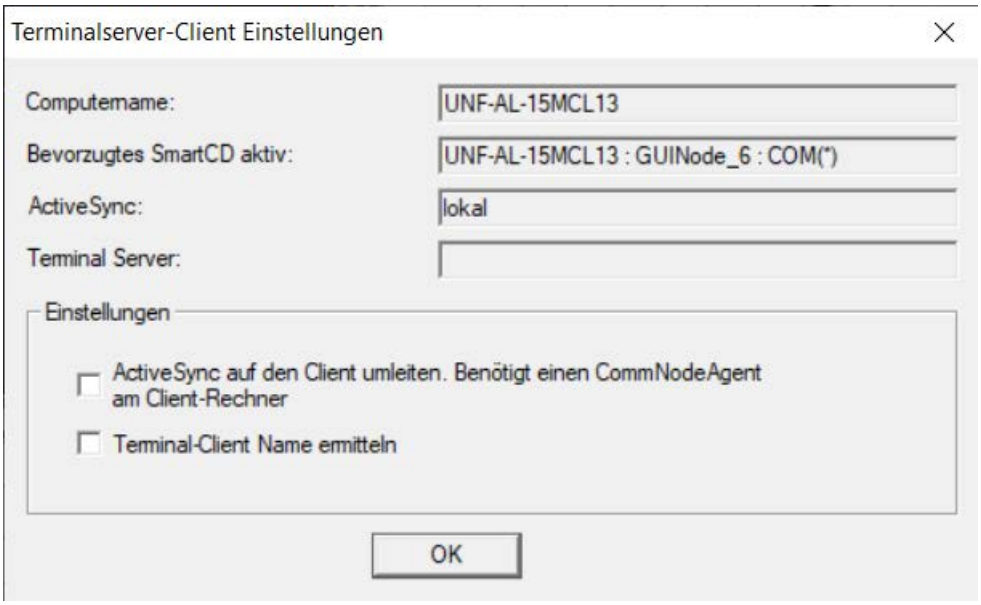
9.30.1.2 USB / Ethernet Server

USB devices can be forwarded to a (terminal) server via the customer network using a USB/Ethernet server.

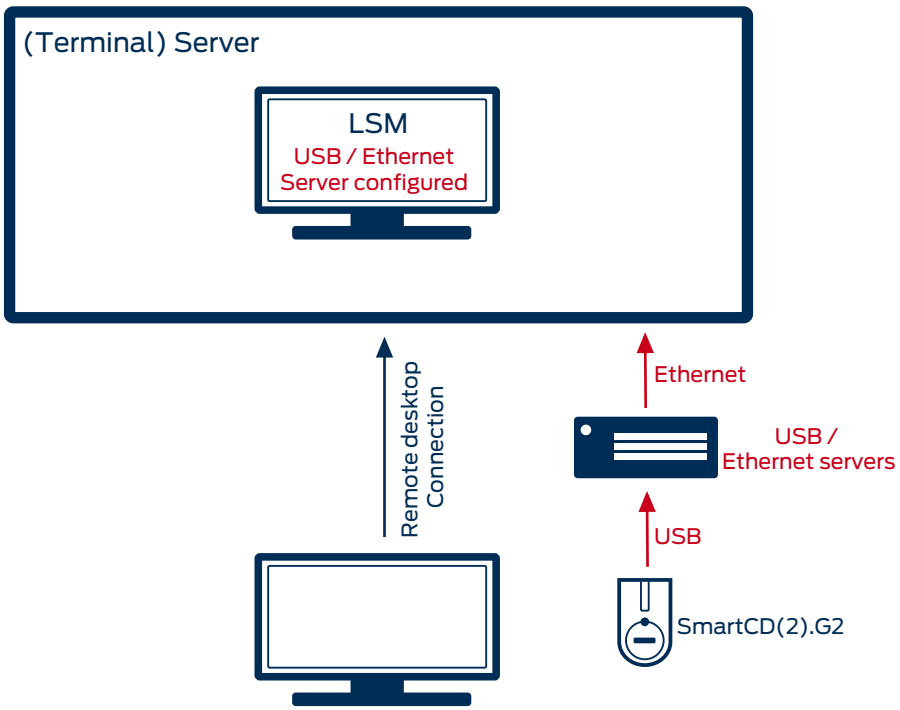
No installation is required on the terminal client.

✓ The USB server software must be set up centrally on the server.
✓ The USB server itself requires a corresponding network configuration.

1. Go to | Network | in the top toolbar to select Terminalserver-Client Einstellungen.
2. Disable the check box ☐ Netzwerk: Terminal-Client Name ermitteln [offen].



This is not a SimonsVosshardware, therefore setup/support cannot be provided by SimonsVoss. Reputable manufacturers of such devices include Silex and W&T.

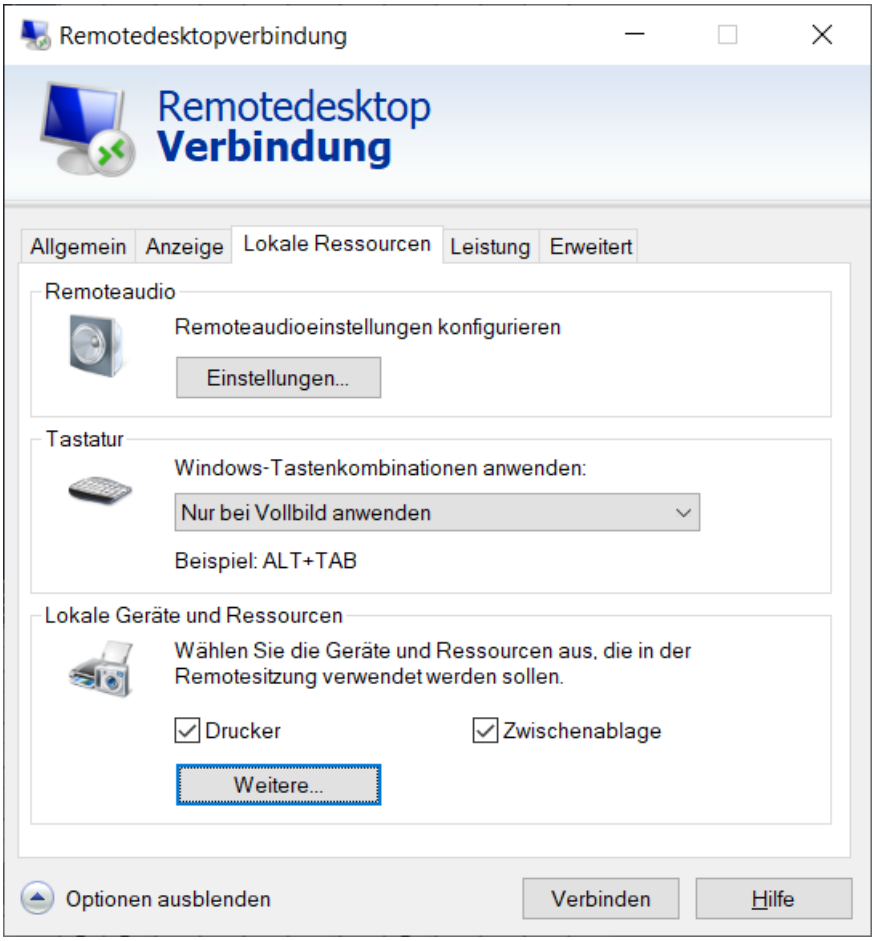


9.30.2 SmartCD MP / HF

9.30.2.1 Remote desktop connection (up to LSM 3.5 SP1)

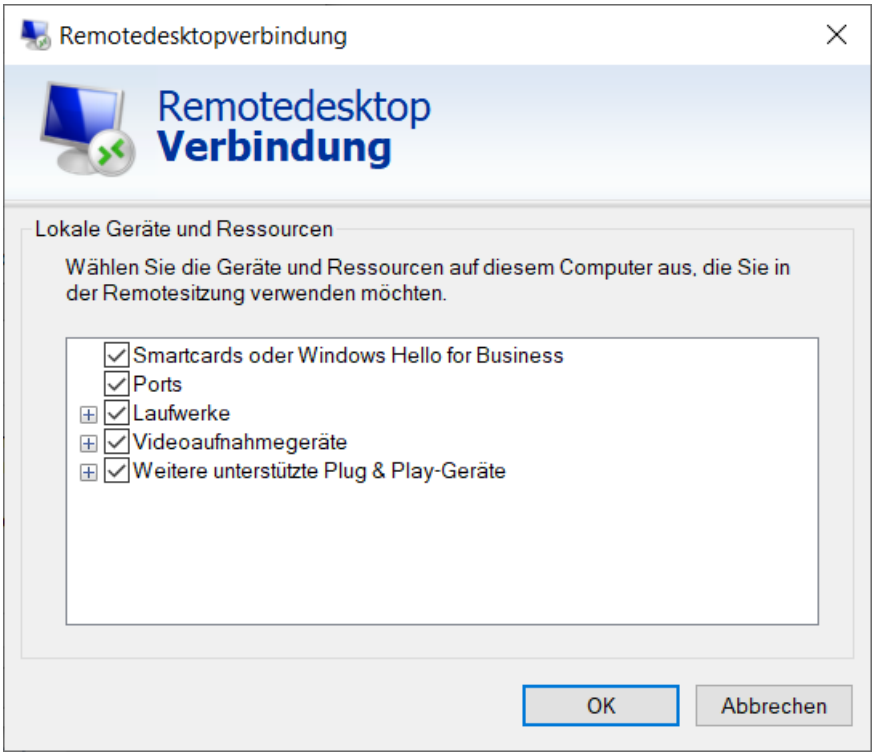
✓ SmartCD.MP and SmartCD.HF cannot be routed through via the CommNode-Agent. Forwarding takes place directly via the remote desktop connection.

1. Open the connection settings of the Remote Desktop session.
2. Click the button remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen] to show options.
3. Change to the tab [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

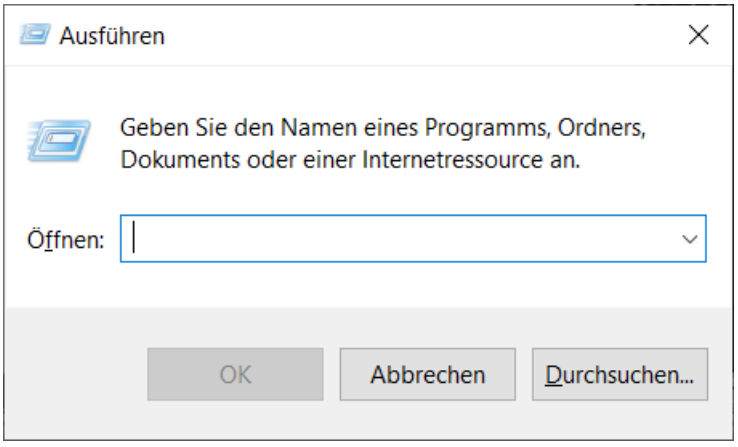


4. Click the button Remotedesktop Einstellungen lokale: Weitere [offen].

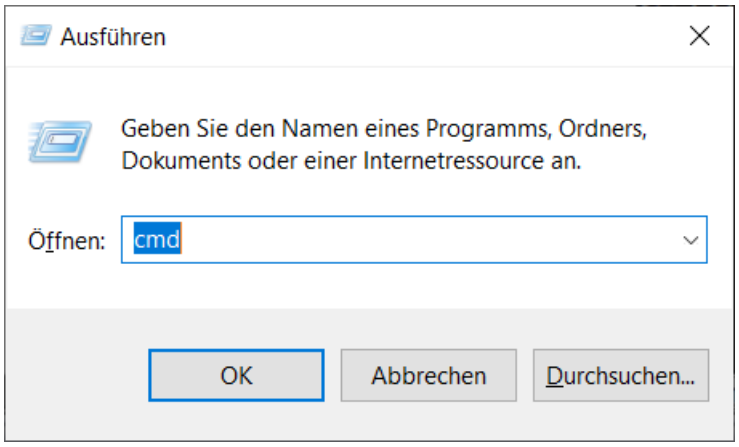
5. Make sure that the checkbox ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] is activated.



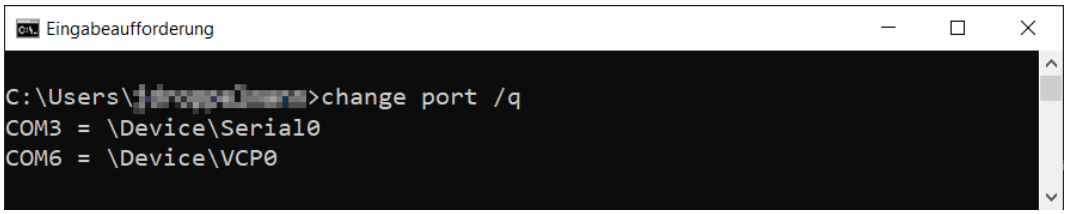
6. Click on the OK button.
7. Connect to the remote desktop.
8. Press the Windows key and R at the same time.
   ↳ The "Run" window will open.



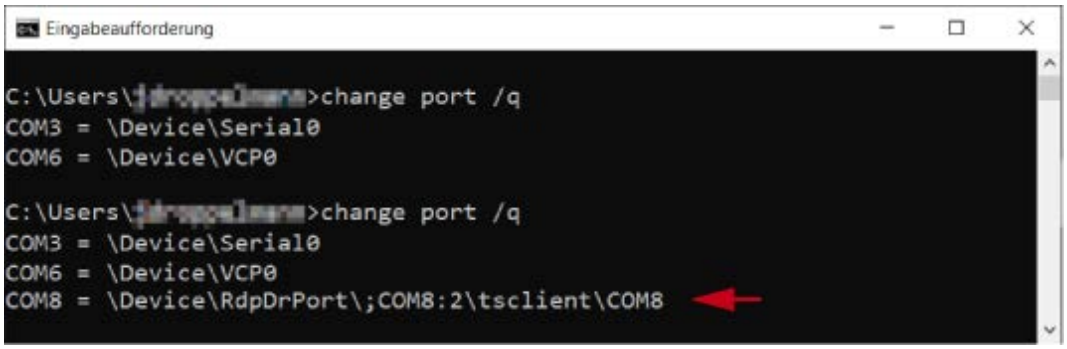
9. Enter a **CMD** in the input field.



10. Click on the OK button.
    ↳ The "Terminalserver: Eingabeaufforderung [offen]" window opens.
11. Unplug SmartCD.MP/SmartCD.HF from the terminal client.
12. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

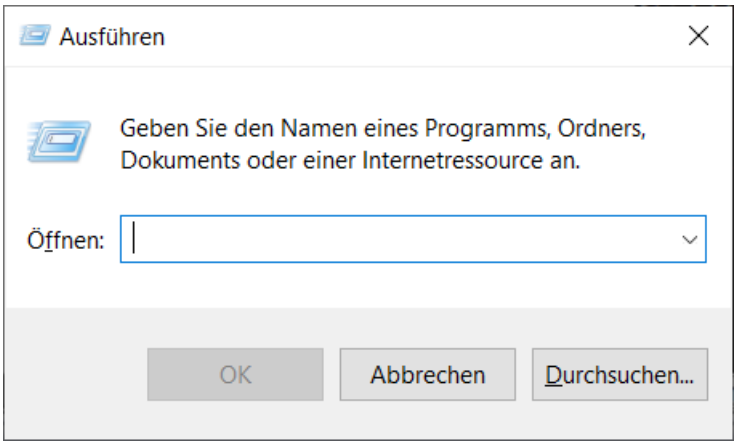


    ↳ The command displays the output without SmartCD.MP/SmartCD.HF connected.
13. Reconnect the SmartCD.MP/SmartCD.HF to the terminal client.
14. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

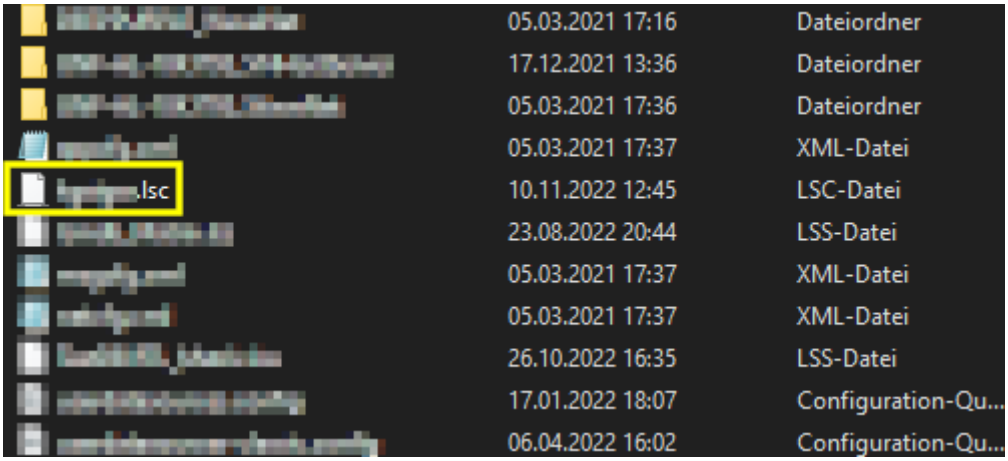


    ↳ The second command displays the output with SmartCD.MP/SmartCD.HF connected. A new port has been added.
    → In this case, COM port 8 is the forwarded SmartCD.MP/SmartCD.HF.

15. Press the Windows key and R at the same time.
    ↳ The "Run" window will open.



16. Enter the path to the LSM user directory:
    %localappdata%\SimonsVoss\LockSysMgr\config\.
17. Click on the OK button.
    ↳ Explorer displays the directory of LSM users.



NOTE

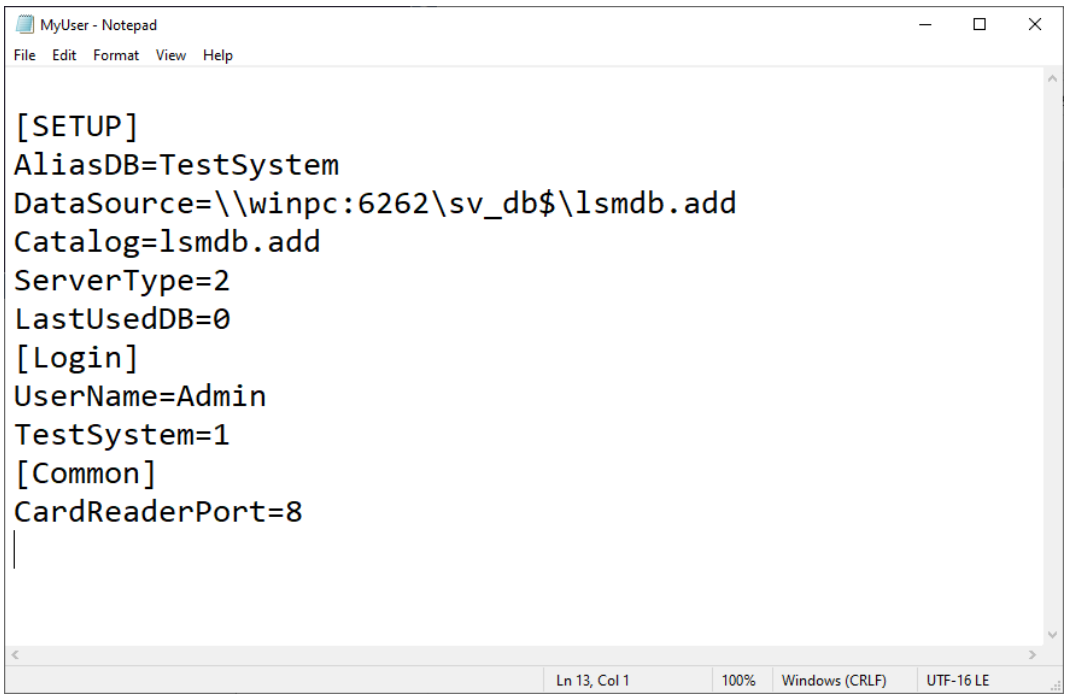
LSC file for LSM users

The LSM creates a configuration file (.lsc) for each user who has logged in at least once.

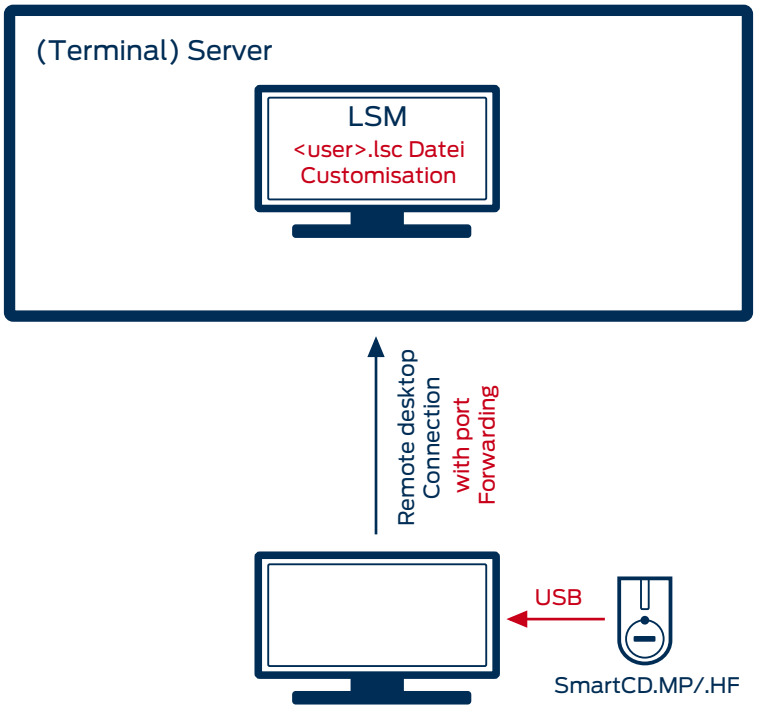
- If a configuration file is not yet available for a user, ask the user to log into LSM.

18. Double-click to open the configuration file.
19. Add the line [Common] to this file:
    CardReaderPort=<PORT>

20. Replace **<PORT>** with the previously "Terminalserver: Eingabeaufforderung [offen]" determined value.



21. Save the modified configuration file.
22. If necessary, also add the row for all other users in their configuration files.
23. If necessary, end the LSM session.
24. Restart the remote desktop session.

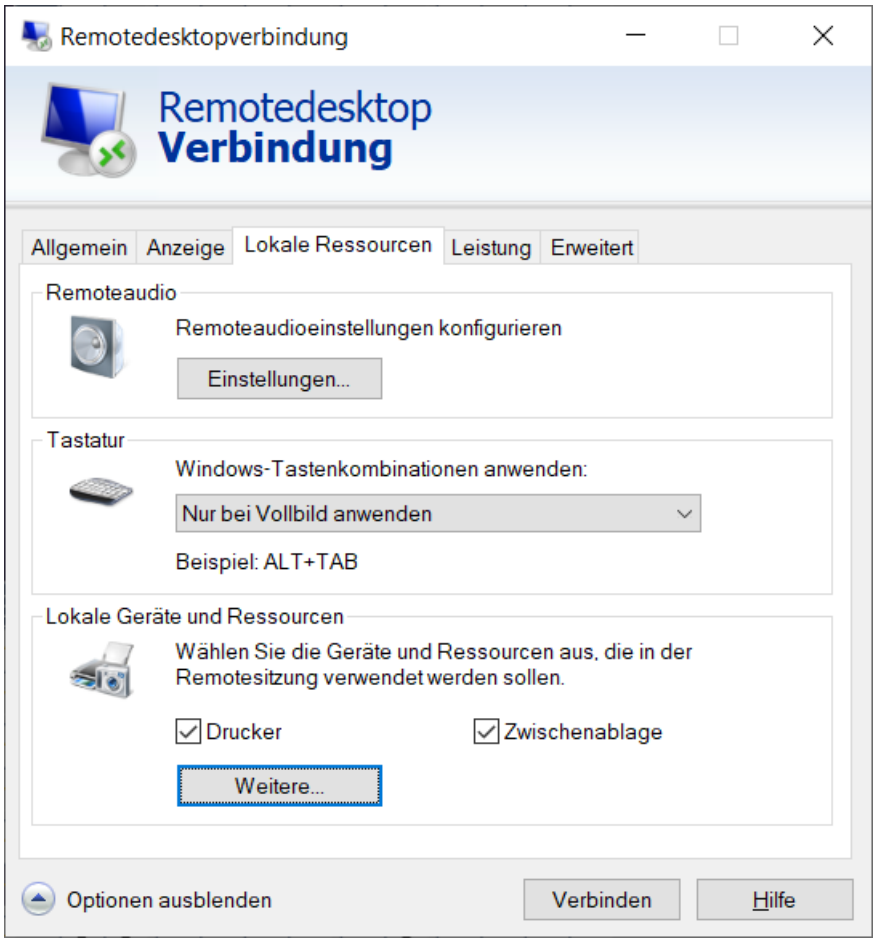


9.30.2.2 Remote desktop connection (from LSM 3.5 SP2)

From LSM 3.5 SP2, you will be able to manage the forwarded remote desktop ports for each hostname directly from within LSM.

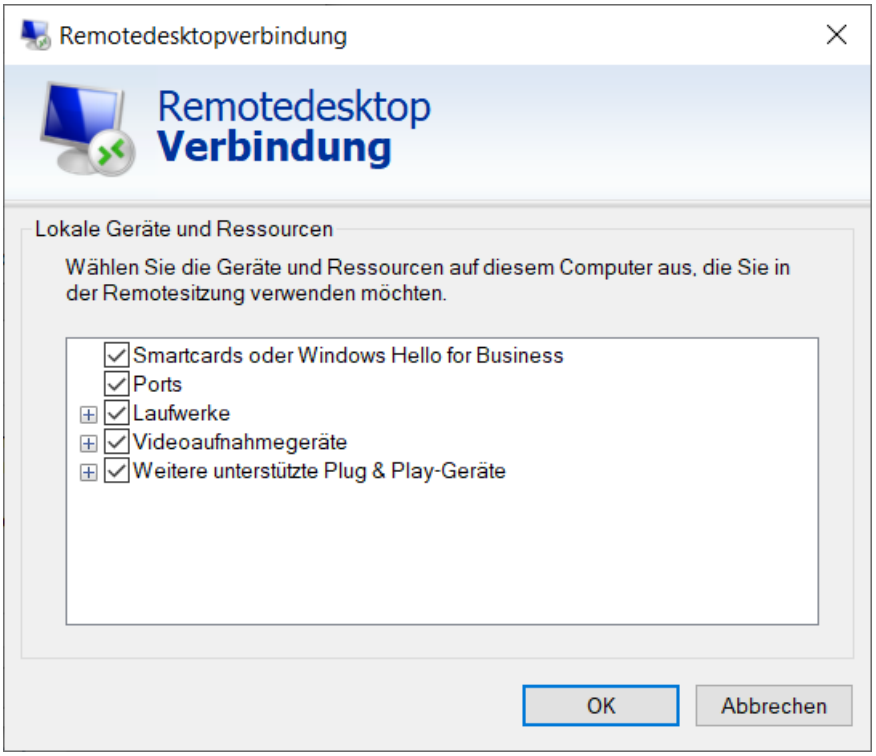
✓ SmartCD.MP and SmartCD.HF cannot be routed through via the CommNode-Agent. Forwarding takes place directly via the remote desktop connection.

1. Open the connection settings of the Remote Desktop session.
2. Click the button remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen] to show options.
3. Change to the tab [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

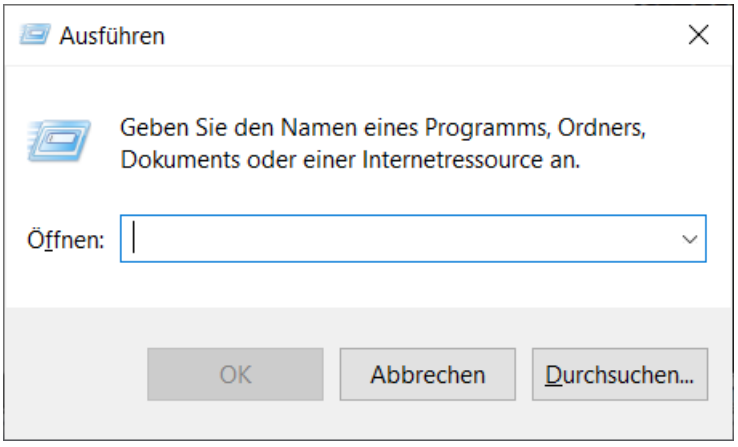


4. Click the button Remotedesktop Einstellungen lokale: Weitere [offen].

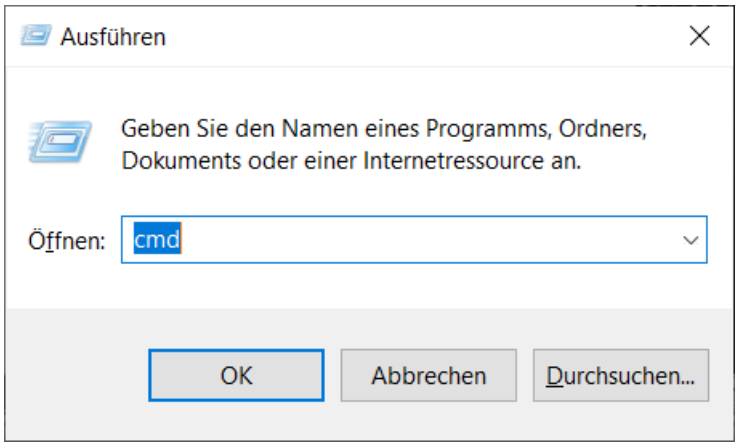
5. Make sure that the checkbox ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] is activated.



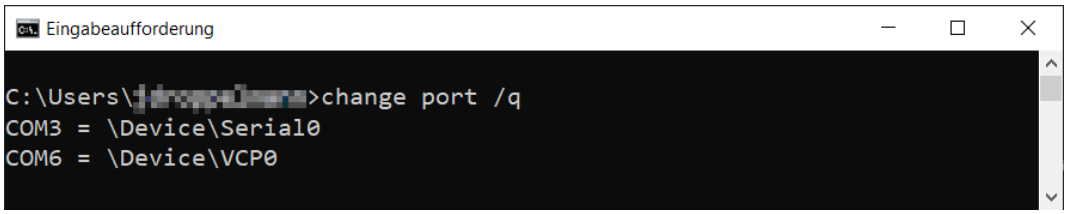
6. Click on the OK button.
7. Connect to the remote desktop.
8. Press the Windows key and R at the same time.
   ↳ The "Run" window will open.



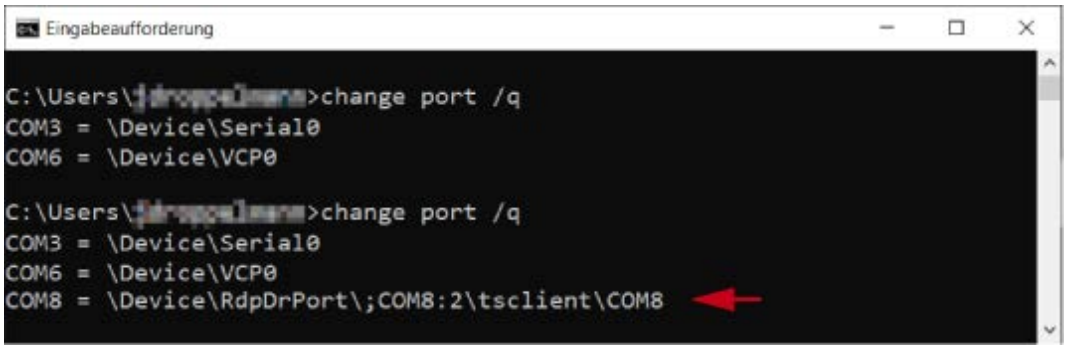
9. Enter a **CMD** in the input field.



10. Click on the OK button.
    ↳ The "Terminalserver: Eingabeaufforderung [offen]" window opens.
11. Unplug SmartCD.MP/SmartCD.HF from the terminal client.
12. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

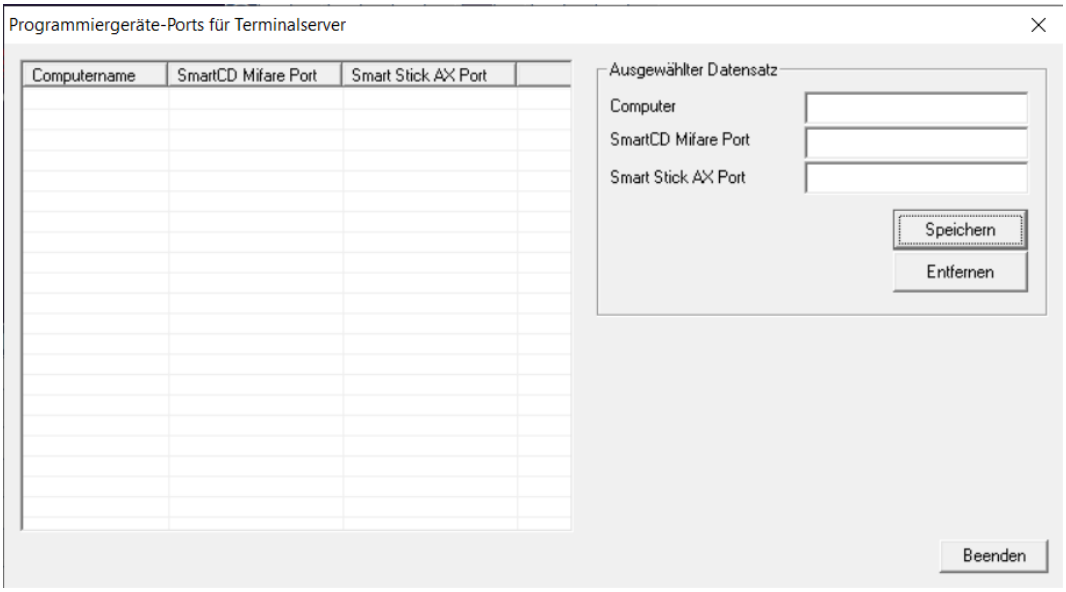


    ↳ The command displays the output without SmartCD.MP/SmartCD.HF connected.
13. Reconnect the SmartCD.MP/SmartCD.HF to the terminal client.
14. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

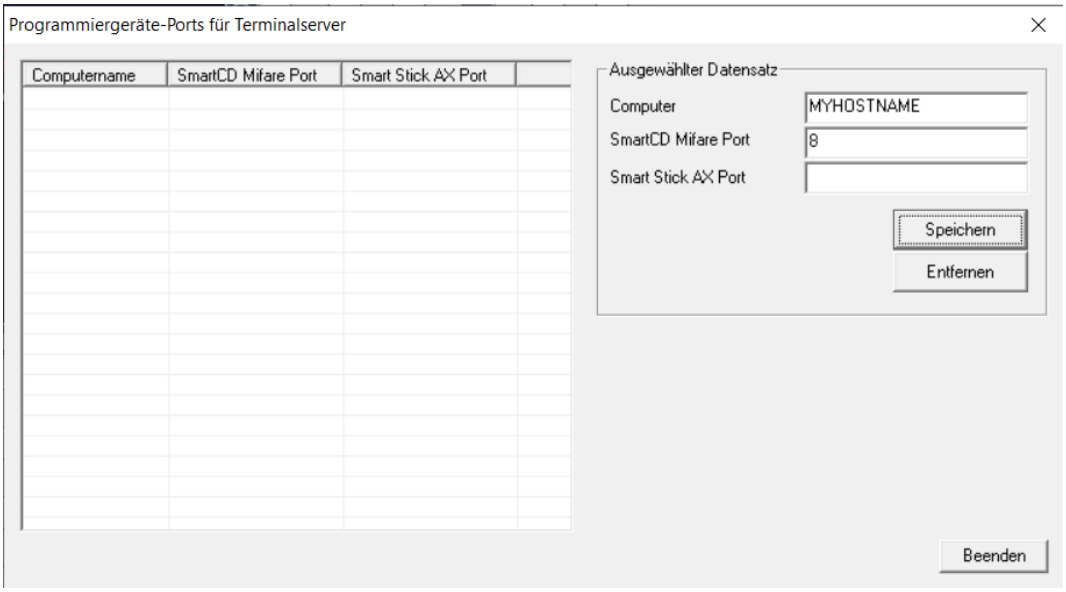


    ↳ The second command displays the output with SmartCD.MP/SmartCD.HF connected. A new port has been added.
    → In this case, COM port 8 is the forwarded SmartCD.MP/SmartCD.HF.

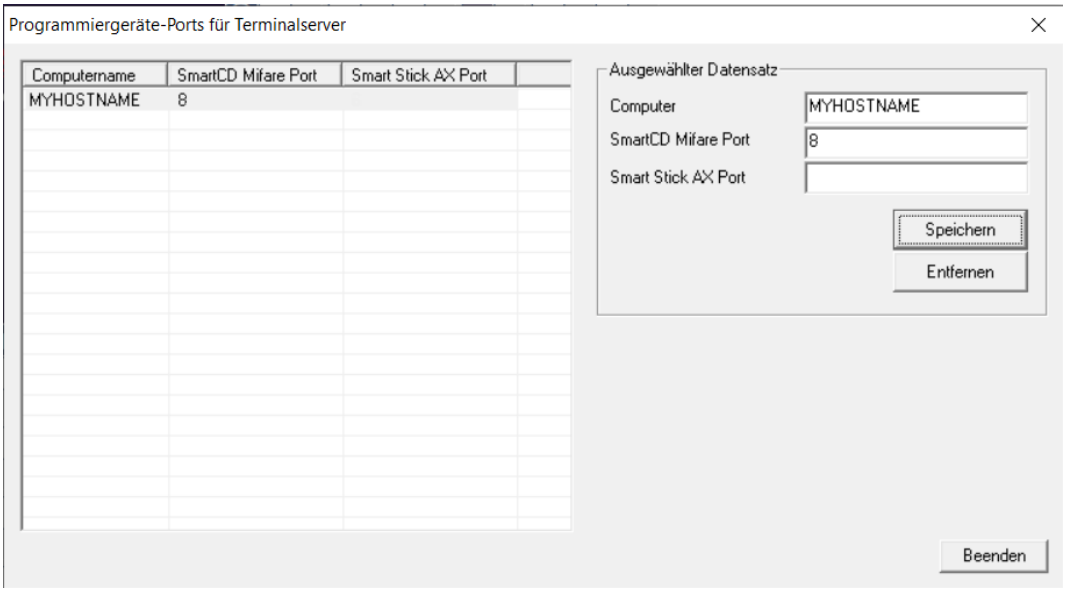
15. In the LSM, select the entry | Network | in the top toolbar Terminalserver Ports .
    ↳ The "LSM: Netzwerk - Programmiergeräte-Ports für Terminalserver [offen]" window will open.



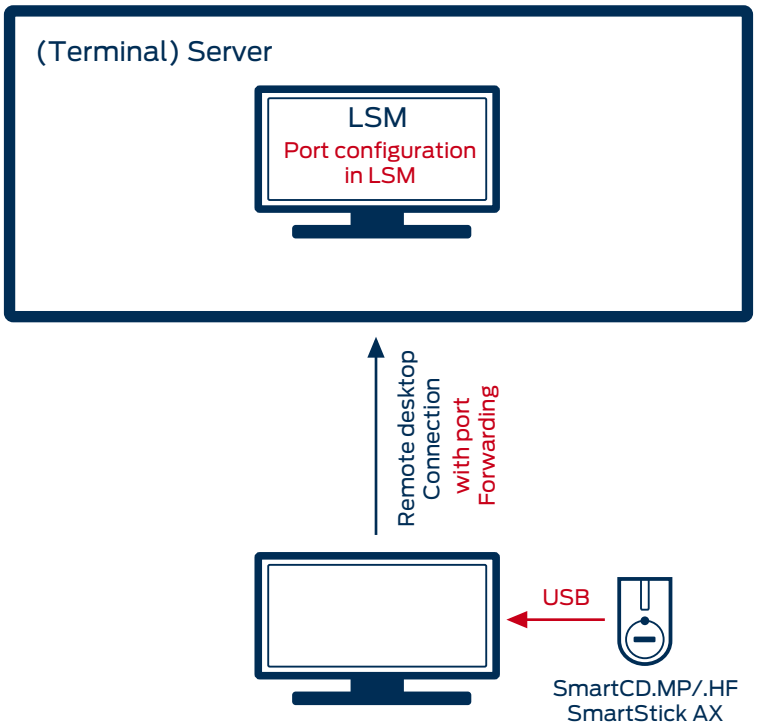
16. Enter a hostname Computer [offen] in the input field.
17. Enter the port determined from the LSM Terminalserver Port+Hostname: SmartCD Mifare Port [offen] window into the "Terminalserver: Eingabeaufforderung [offen]" input field.



18. Click the button LSM Netzwerk Port für Terminalserver und Hostnamen eingeben: Speichern [offen] .
    ↳ A line is created for hostname and port.



19. If necessary, end the LSM session.
20. Restart the remote desktop session.



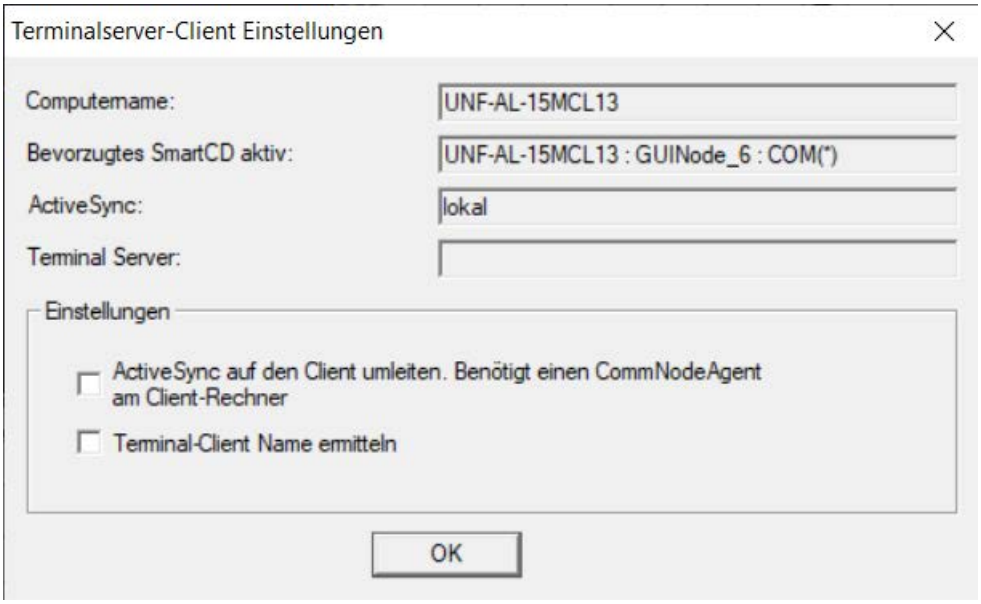
9.30.2.3 USB / Ethernet Server

USB devices can be forwarded to a (terminal) server via the customer network using a USB/Ethernet server.

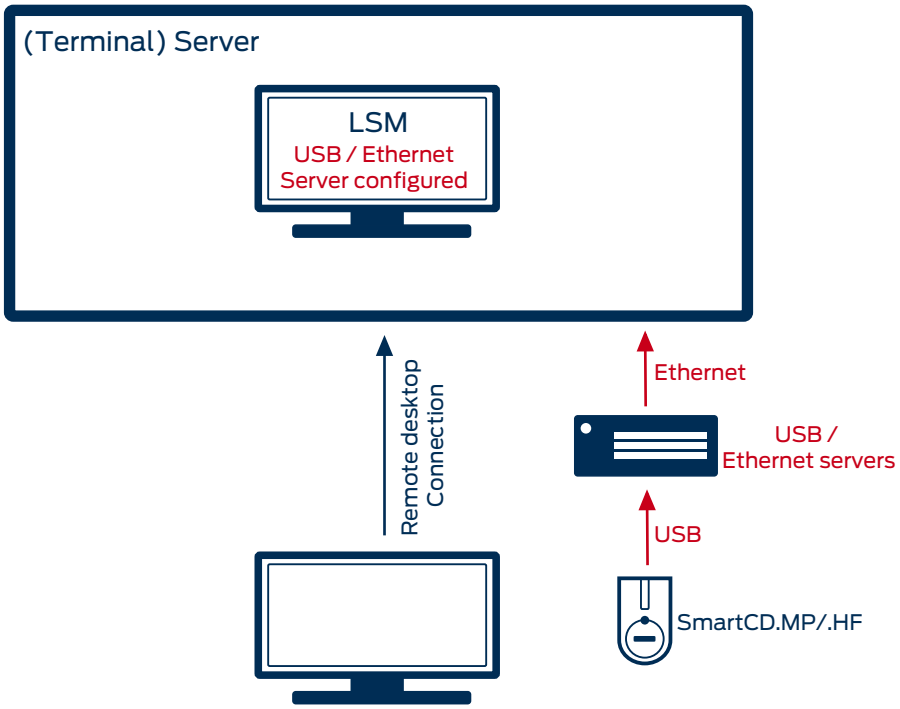
No installation is required on the terminal client.

✓ The USB server software must be set up centrally on the server.
✓ The USB server itself requires a corresponding network configuration.

1. Go to | Network | in the top toolbar to select Terminalserver-Client Einstellungen.
2. Disable the check box ☐ Netzwerk: Terminal-Client Name ermitteln [offen].
   ↳ The modification of a configuration file (*.lsc, see *Remote desktop connection (up to LSM 3.5 SP1) [▸ 172]*) may lead to malfunctions; the changed entries there may have to be removed.



This is not a SimonsVosshardware, therefore setup/support cannot be provided by SimonsVoss. Reputable manufacturers of such devices include Silex and W&T.



9.30.3 SmartStick AX

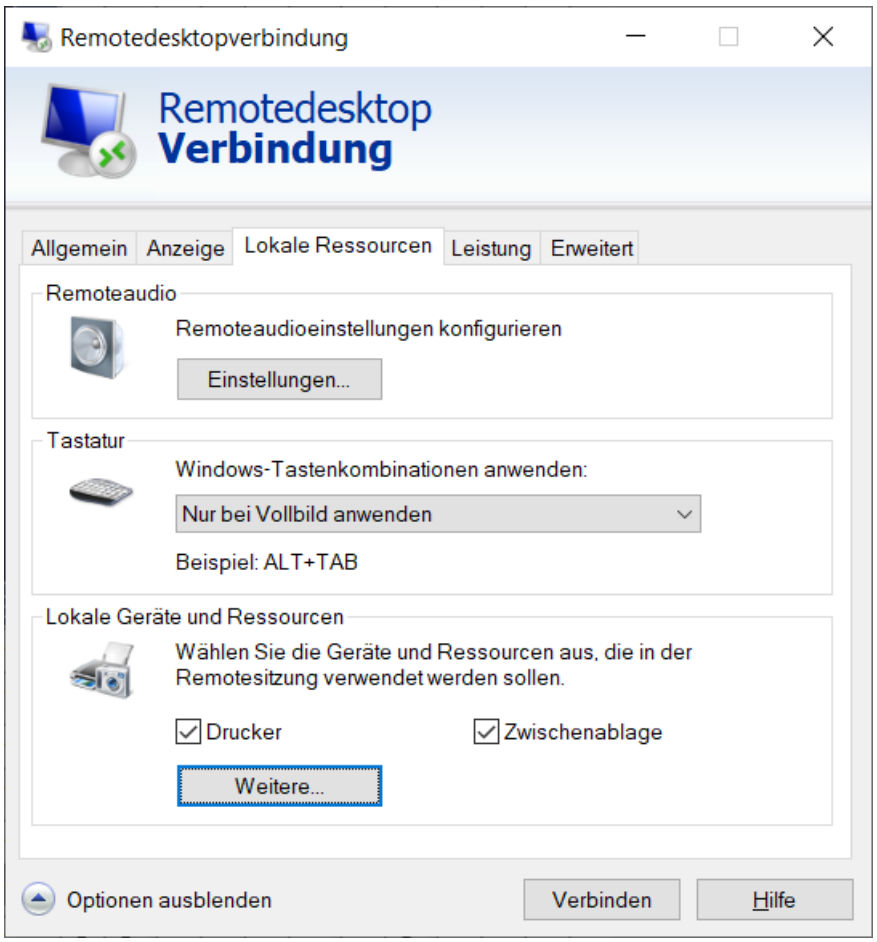
9.30.3.1 Remote desktop connection (from LSM 3.5 SP2)

From LSM 3.5 SP2, you will be able to manage the forwarded remote desktop ports for each hostname directly from within LSM.

✓ The SmartStick AX cannot be routed via the CommNode-Agent. Forwarding takes place directly via the remote desktop connection.

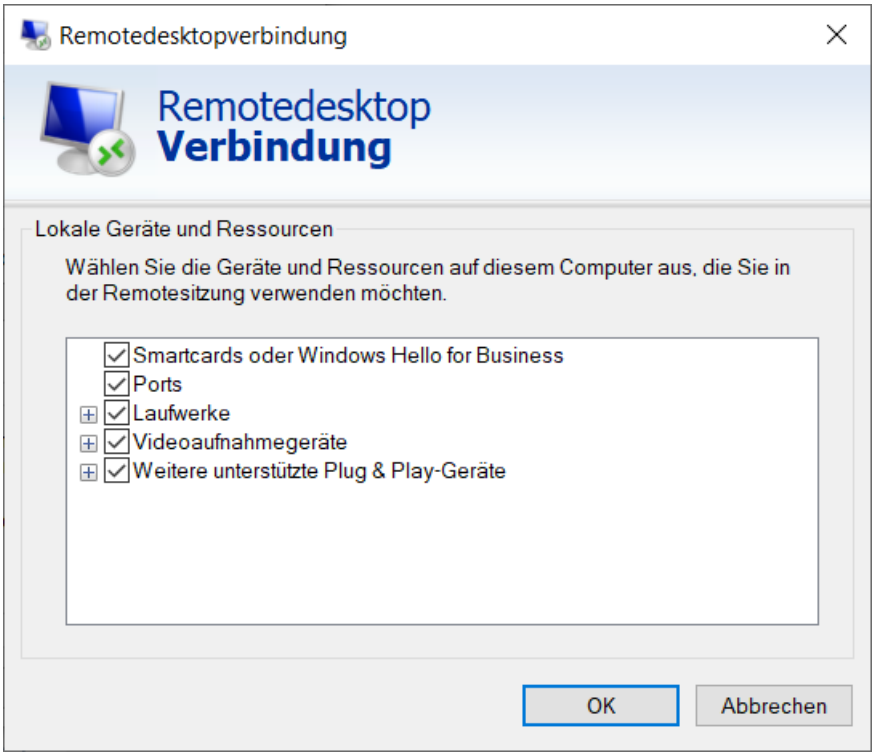
1. Open the connection settings of the Remote Desktop session.
2. Click the button remotedesktop-sitzung verbindungseinstellungen: Optionen einblenden [offen] to show options.

3. Change to the tab [Remotedesktop Einstellung Registerkarte: Lokale Ressourcen [offen]].

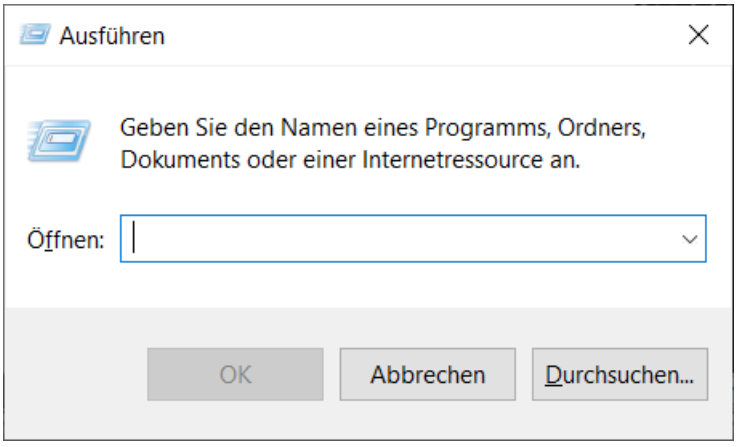


4. Click the button Remotedesktop Einstellungen lokale: Weitere [offen].

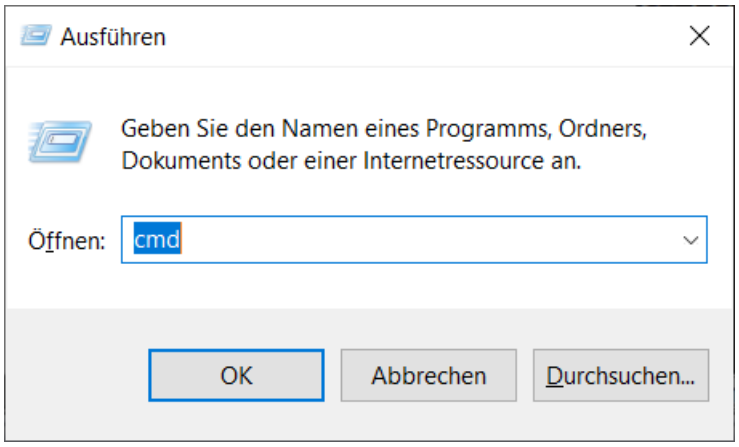
5. Make sure that the checkbox ☑ Remotedesktop-Sitzung Ressourcen: Ports [offen] is activated.



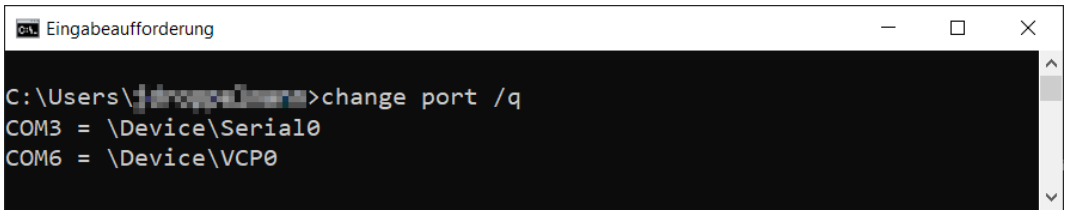
6. Click on the OK button.
7. Connect to the remote desktop.
8. Press the Windows key and R at the same time.
   ↳ The "Run" window will open.



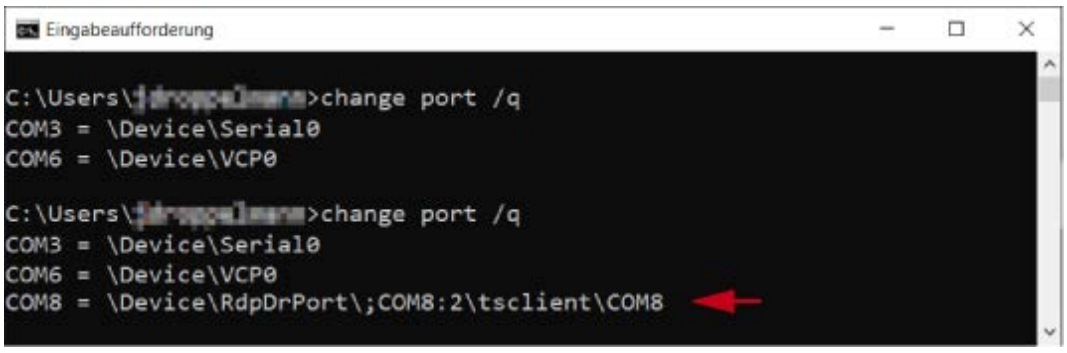
9. Enter a **CMD** in the input field.



10. Click on the OK button.
    ↳ The "Terminalserver: Eingabeaufforderung [offen]" window opens.
11. Unplug the SmartStick AX from the terminal client.
12. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

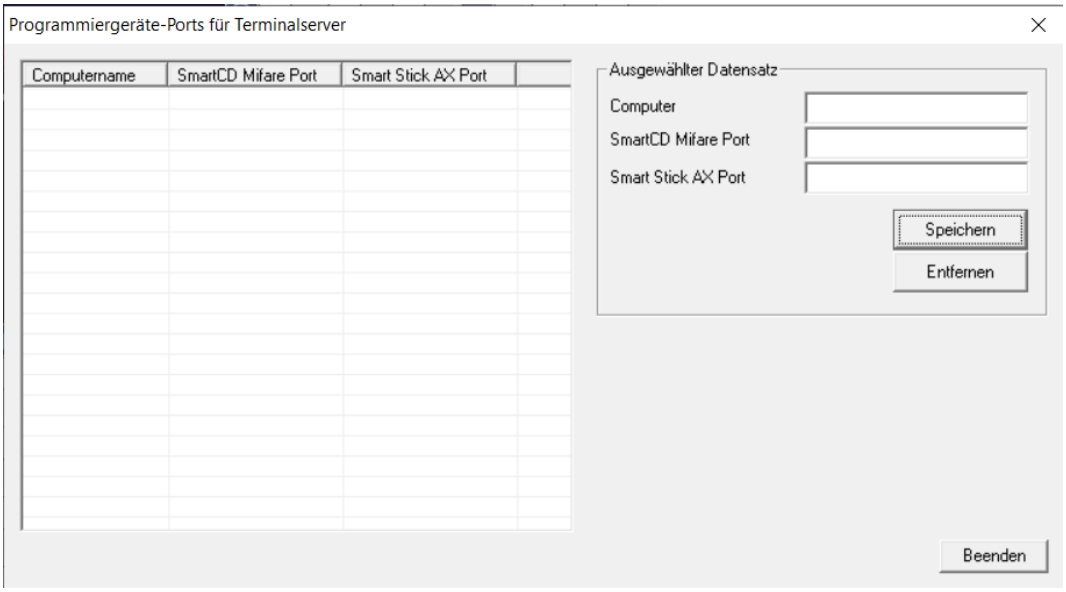


    ↳ The command shows the output without connected SmartStick AX.
13. Reconnect the SmartStick AX to the terminal client.
14. Enter *Portweiterleitung im CMD-Fenster prüfen für LSM: change port /q [offen]*.

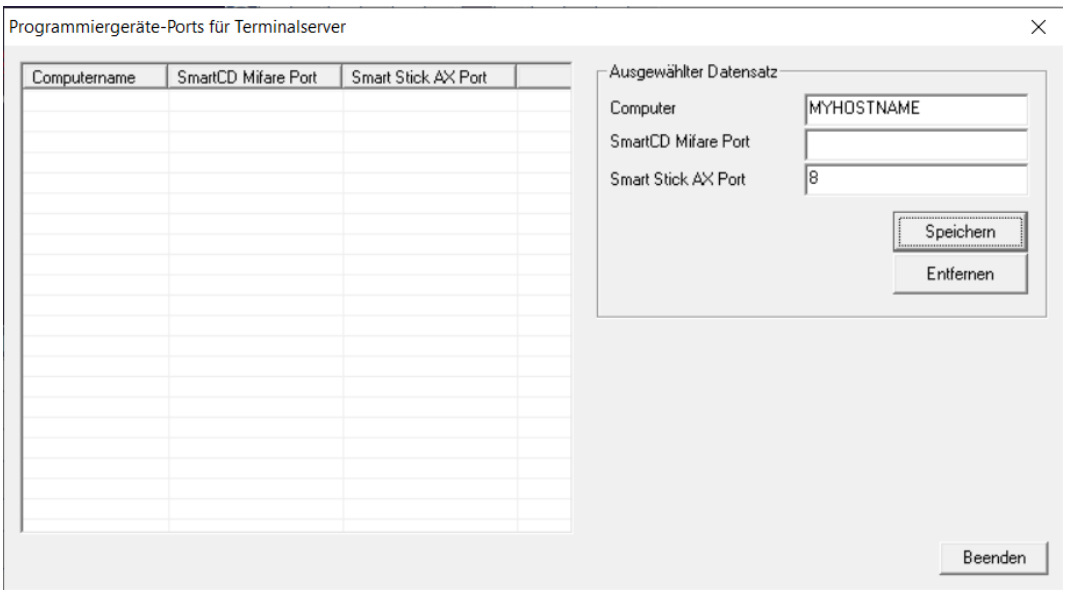


    ↳ The second command shows the output with SmartStick AX connected. A new port has been added.
    → In this case, the forwarded COM port 8 is the SmartStick AX.

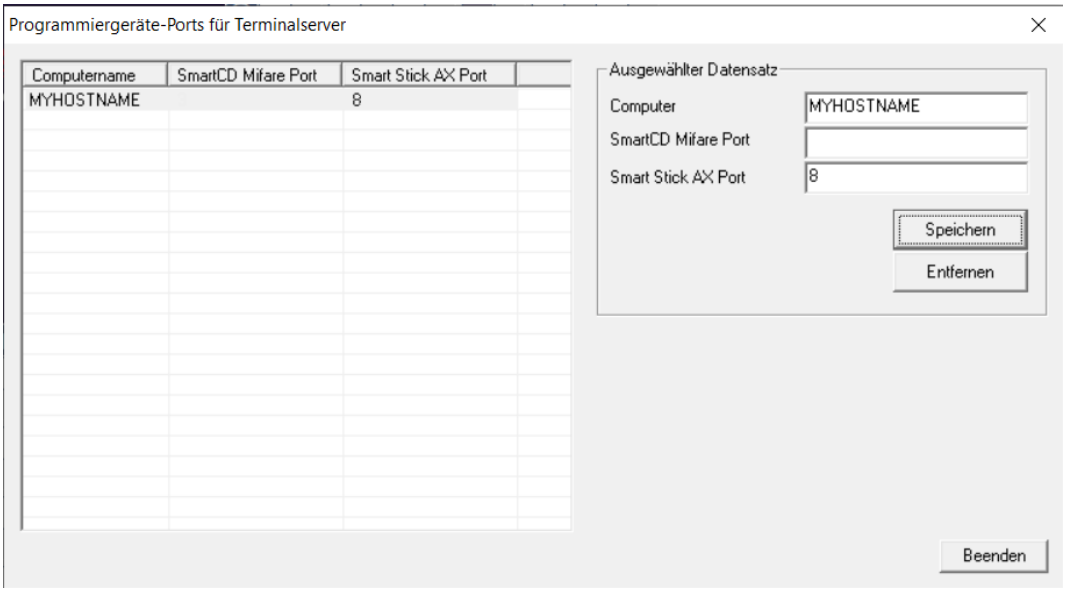
15. In the LSM, select the entry | Network | in the top toolbar Terminalserver Ports .
    ↳ The "LSM: Netzwerk - Programmiergeräte-Ports für Terminalserver [offen]" window will open.



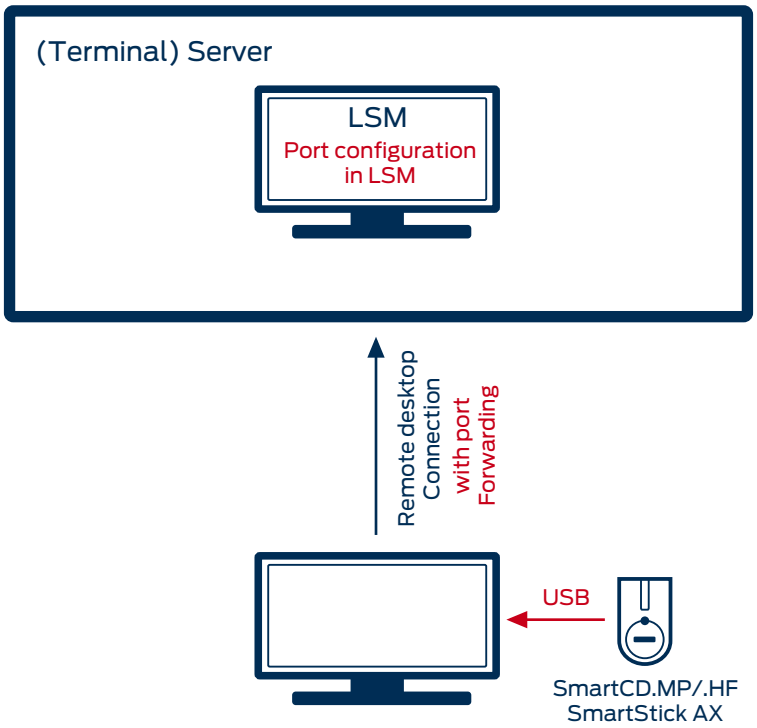
16. Enter a hostname Computer [offen] in the input field.
17. Enter the port determined from the LSM Terminalserver Port+Hostname: Smart Stick AX Port [offen] window into the "Terminalserver: Eingabeaufforderung [offen]" input field.



18. Click the button LSM Netzwerk Port für Terminalserver und Hostnamen eingeben: Speichern [offen] .
    ↳ A line is created for hostname and port.



19. If necessary, end the LSM session.
20. Restart the remote desktop session.



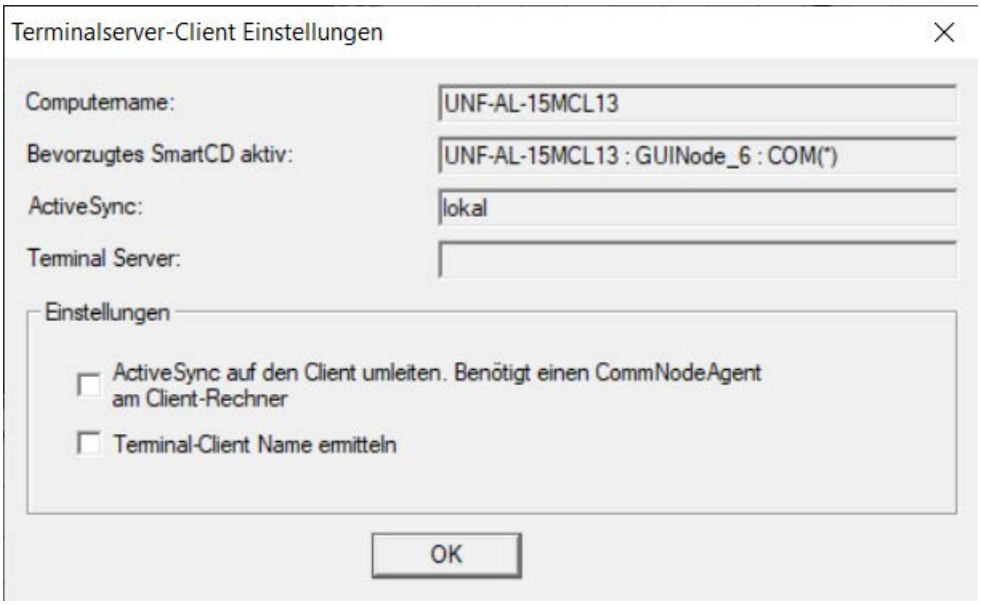
9.30.3.2 USB / Ethernet Server

USB devices can be forwarded to a (terminal) server via the customer network using a USB/Ethernet server.

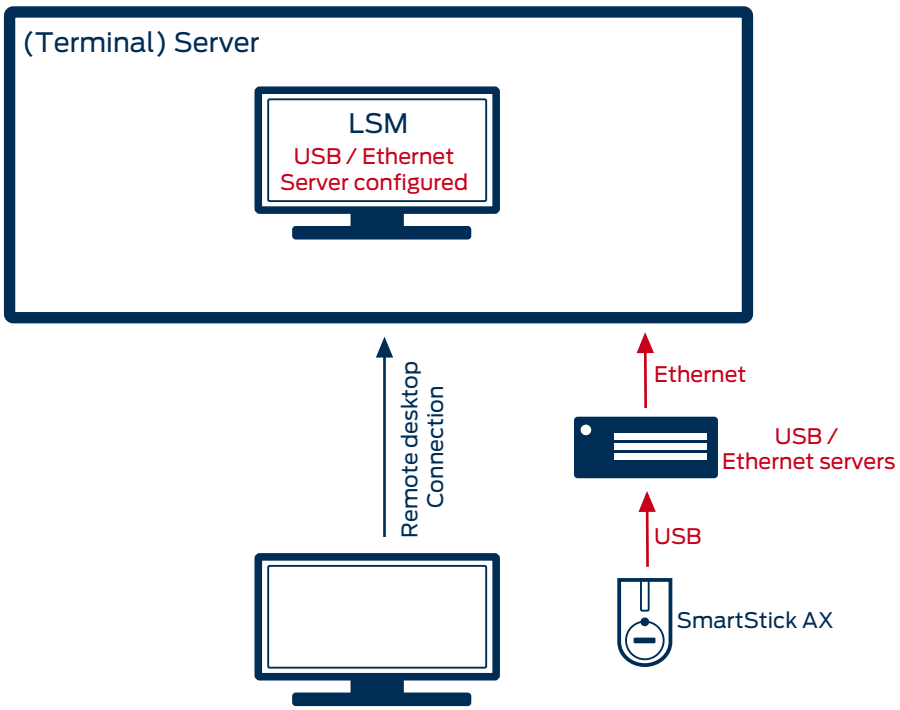
No installation is required on the terminal client.

✓ The USB server software must be set up centrally on the server.
✓ The USB server itself requires a corresponding network configuration.

1. Go to | Network | in the top toolbar to select Terminalserver-Client Einstellungen.
2. Disable the check box ☐ Netzwerk: Terminal-Client Name ermitteln [offen].



This is not a SimonsVosshardware, therefore setup/support cannot be provided by SimonsVoss. Reputable manufacturers of such devices include Silex and W&T.



10. 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.

10.1 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.

10.1.1 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.

10.1.2 Initial programming of the locking components

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

10.1.2.1 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.

10.1.2.2 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.

10.1.3 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.

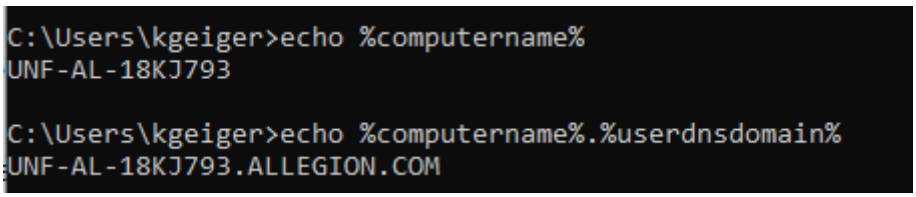
NOTE

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

10.1.4 Creating communication nodes

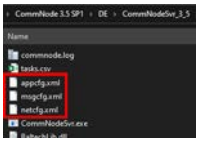
The communication node forms the interface between the CommNode server and the LSM software. You must launch the LSM software using an administrator account to add the configuration XMLs.

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



   ↳ *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.

10.1.5 Setting up the network and importing into LSM

10.1.5.1 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.

10.1.5.2 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.

10.1.5.3 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.

10.1.5.4 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.

10.2 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 [▸ 190]*".

10.2.1 Possible (door) states

States may differ for different components.

10.2.1.1 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

10.2.1.2 Possible DoorMonitoring states of locking cylinders

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

10.2.1.3 Possible DoorMonitoring states of SmartRelais 3

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

- *Sabotage detection [▸ 197]*

10.2.1.4 Possible states RouterNode 2 / GatewayNode 2

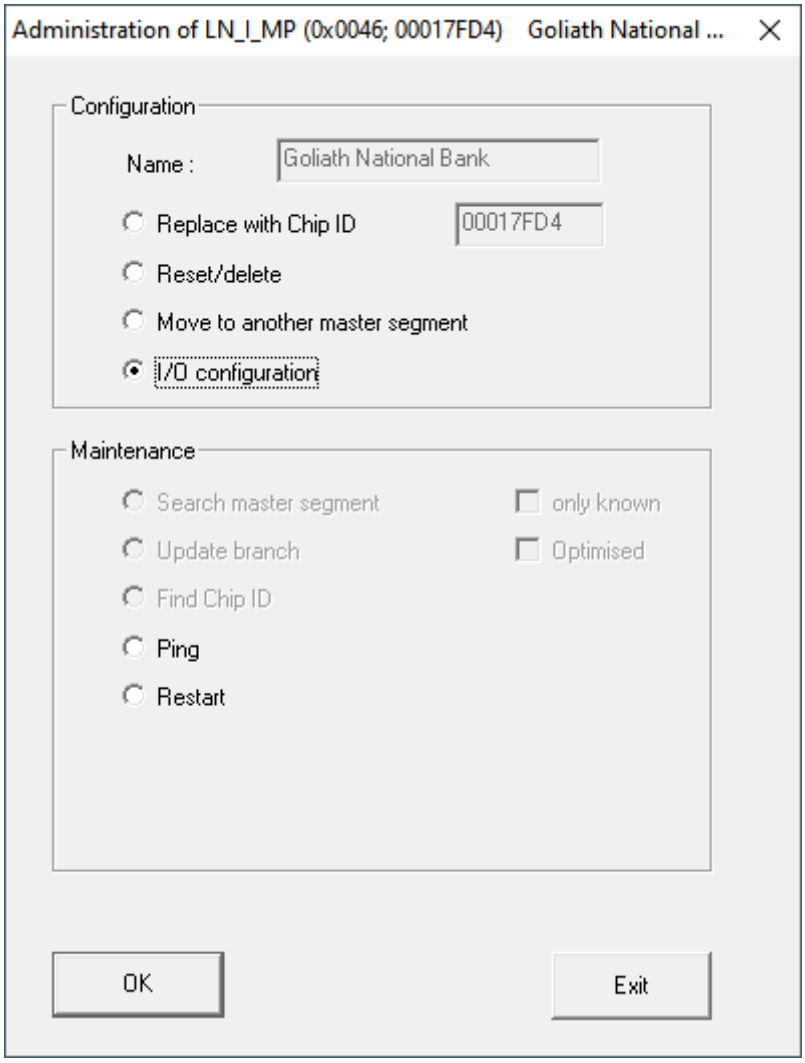
- Input active/inactive
- Analogue voltage input above/below threshold

10.2.2 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.

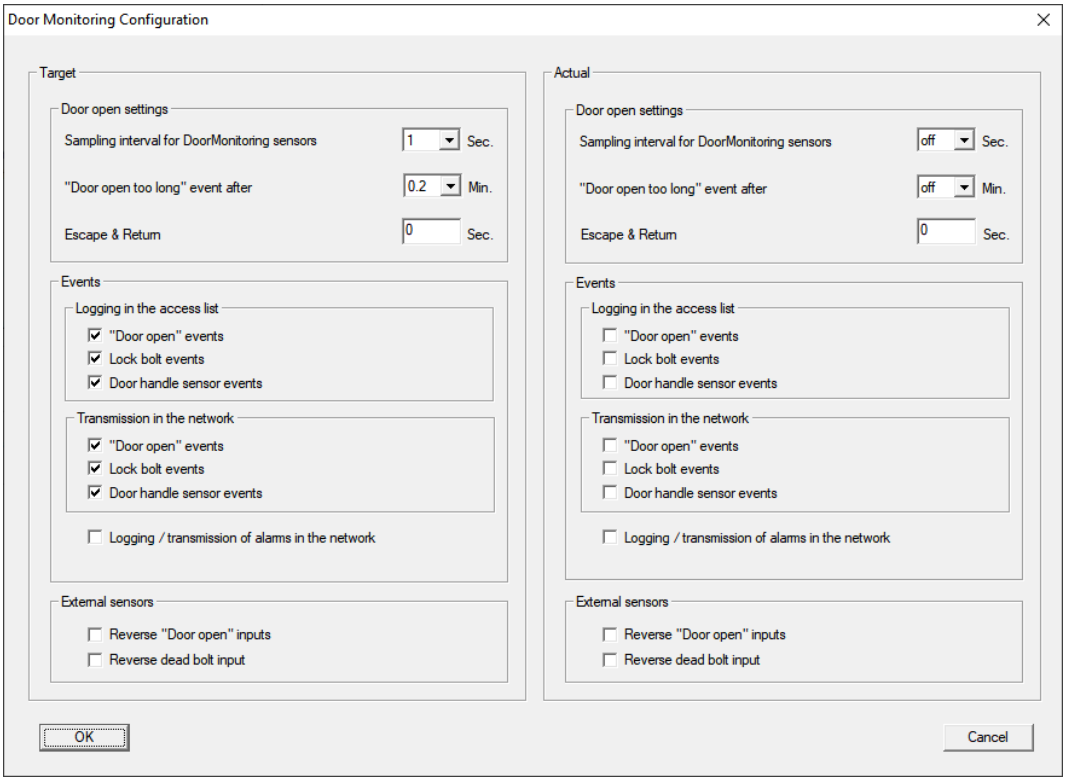
10.2.3 DoorMonitoring SmartHandle

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.

10.2.3.1 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 [▸ 210]*).

10.2.3.2 DoorMonitoring (SmartHandle) - Door handle events

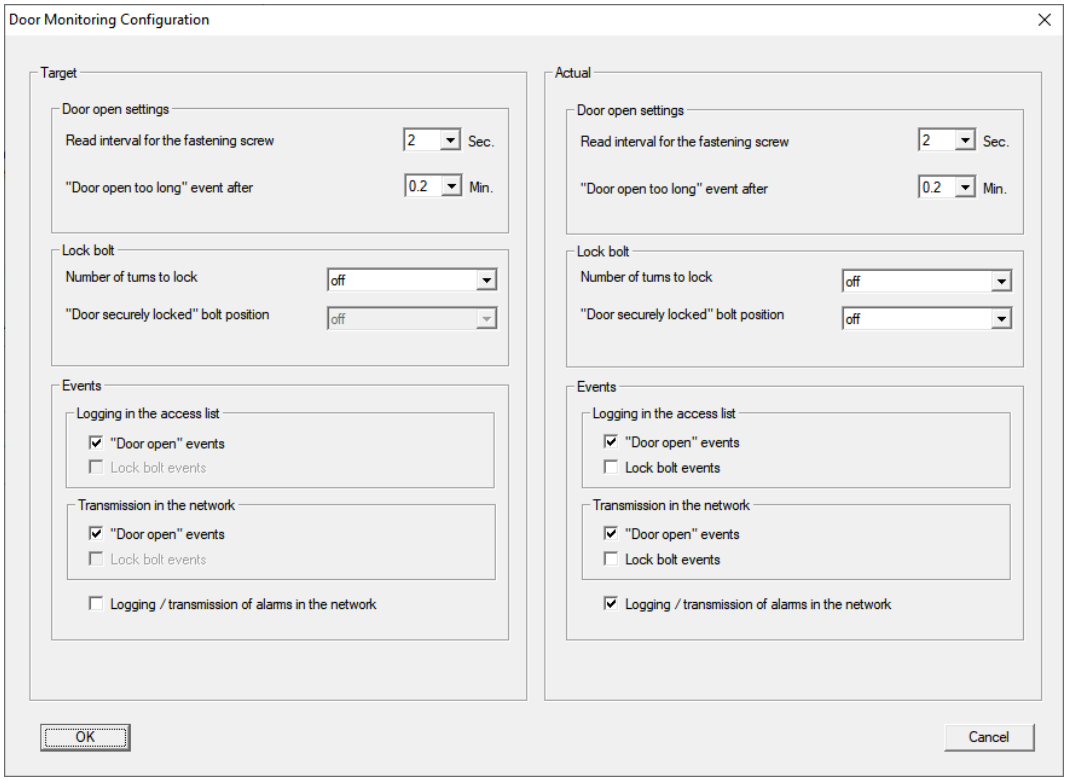
From LSM 3.5 SP3 onwards, you can see the state of the handle on the SmartHandle AX. When the trigger is pressed, the electronics detect this and send the information to LSM. If you want to evaluate the information, you can set up an event for it and then respond to it (see (*Setting up event management [▸ 210]*).

10.2.4 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.

10.2.5 Evaluating controller inputs

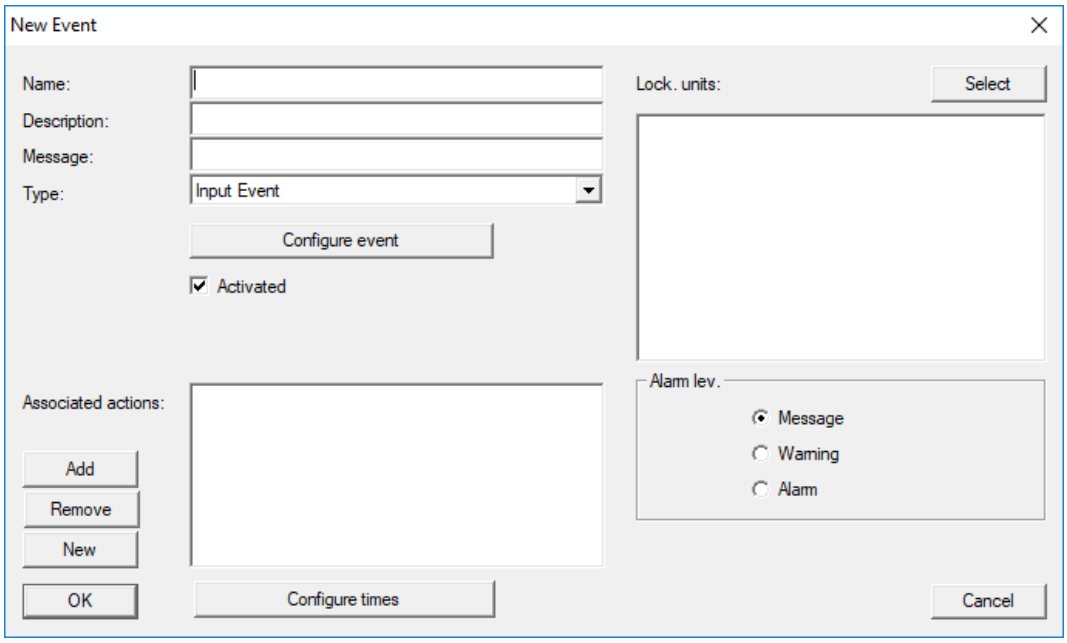
The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

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.

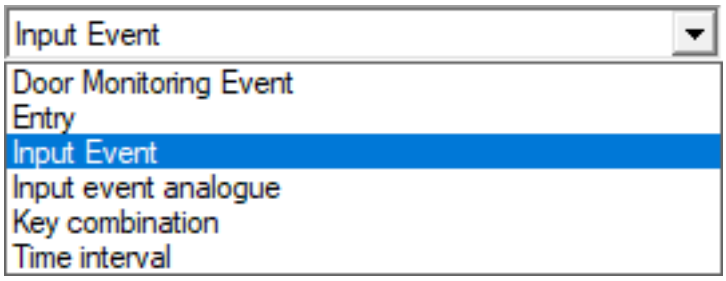
✓ LSM open.
✓ SREL3 ADV System added to the matrix.

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.

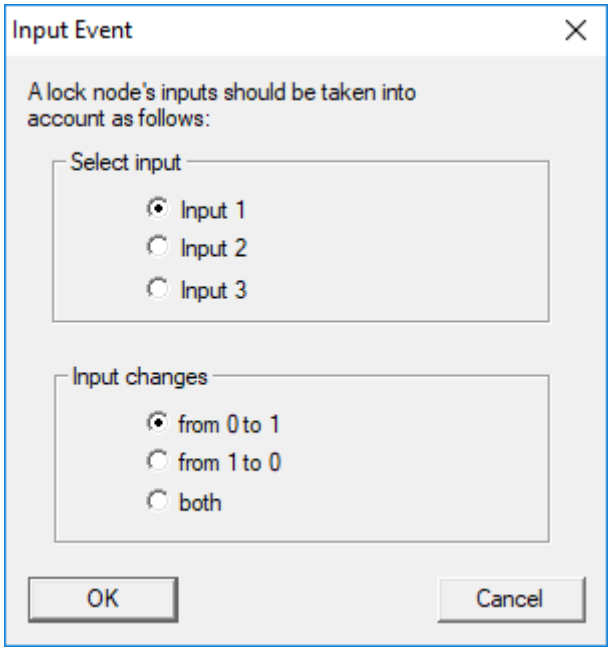


3. Enter a suitable name for the event.
4. Enter an optional description for the event.
5. Enter an optional message.
6. Open the ▼ **Type** drop-down menu.

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.

10.2.6 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.

10.2.7 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.

10.2.8 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.

10.3 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.

10.3.1 Preparing RouterNode for RingCast

NOTE

Firmware dependent availability of RingCast for RouterNodes

RingCast support is firmware dependent (see Firmware information).

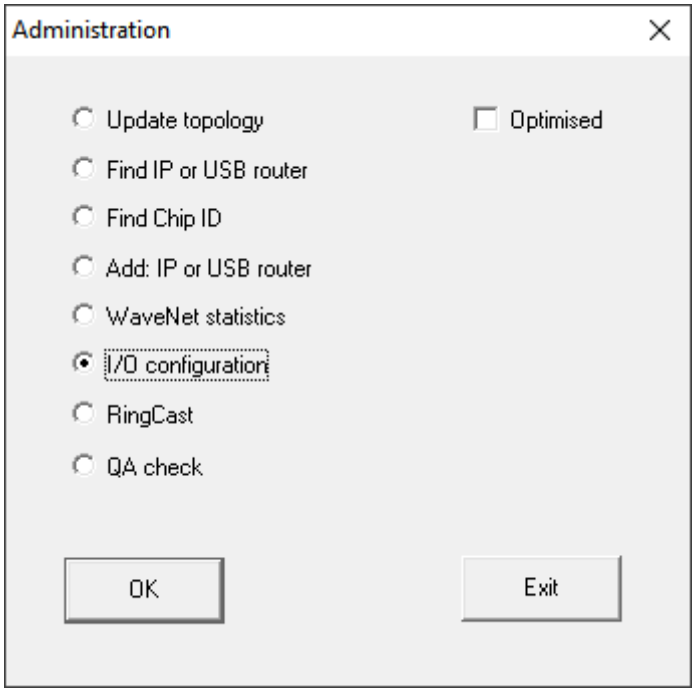
- If necessary, update the firmware (see Updating firmware).

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.

10.3.2 Adding a RingCast

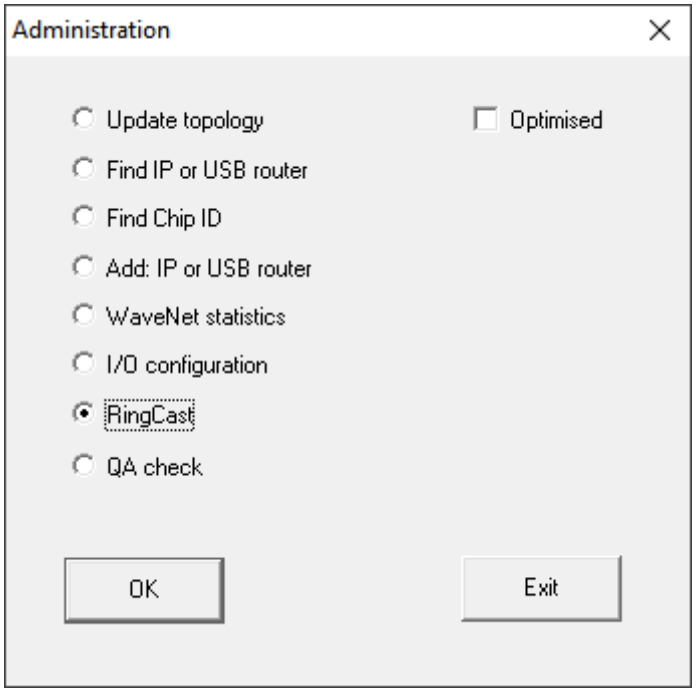
NOTE

Recalculating the RingCast

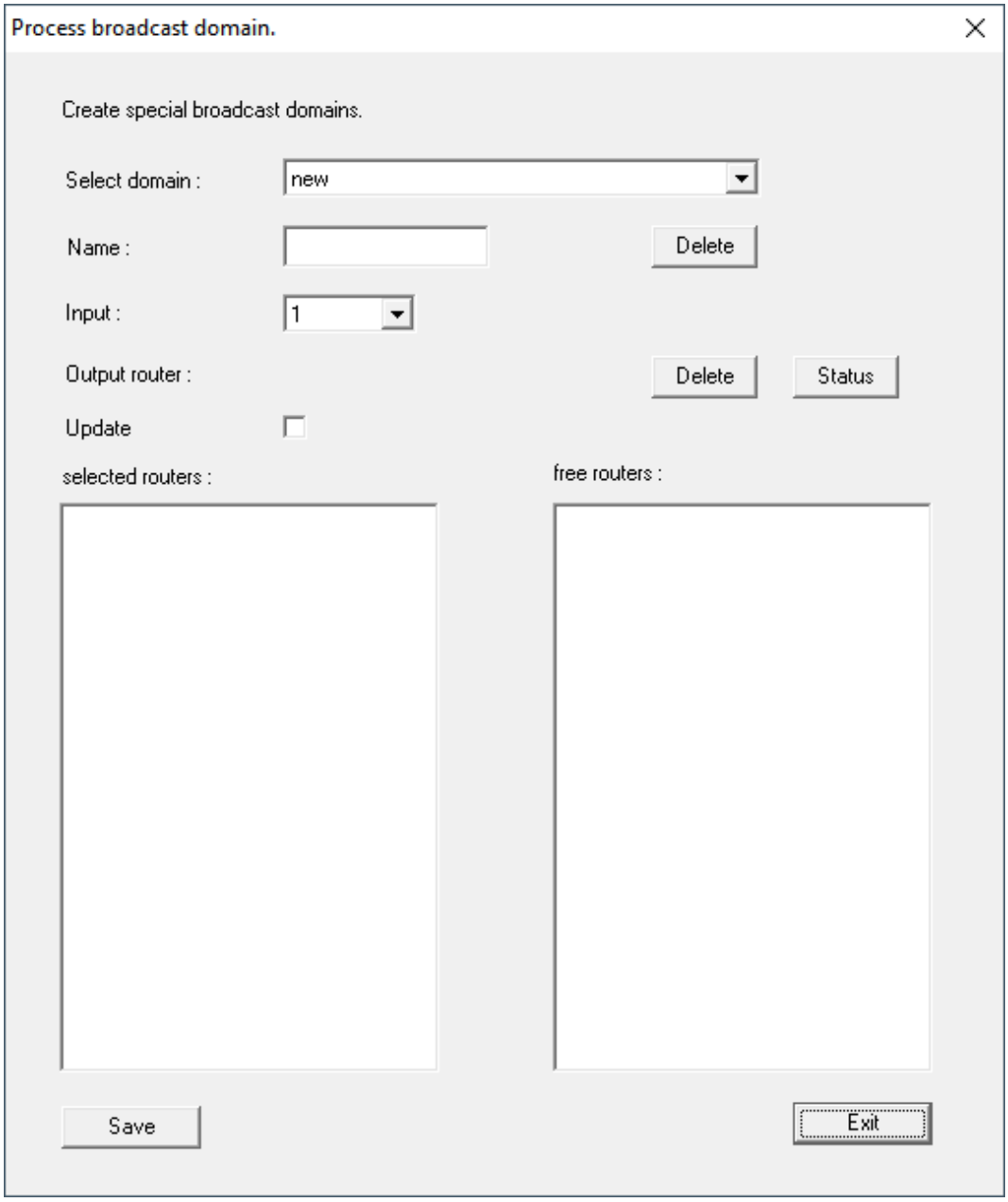
If you replace or delete a RouterNode in the RingCast or change its RingCast-relevant IO configuration, the RingCast is automatically recalculated after saving the changes and confirming the request.

- ✓ 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 [▸ 202]*).

1. Right-click on the WaveNet XX_X entry.
   ↳ The window "Administration" opens.

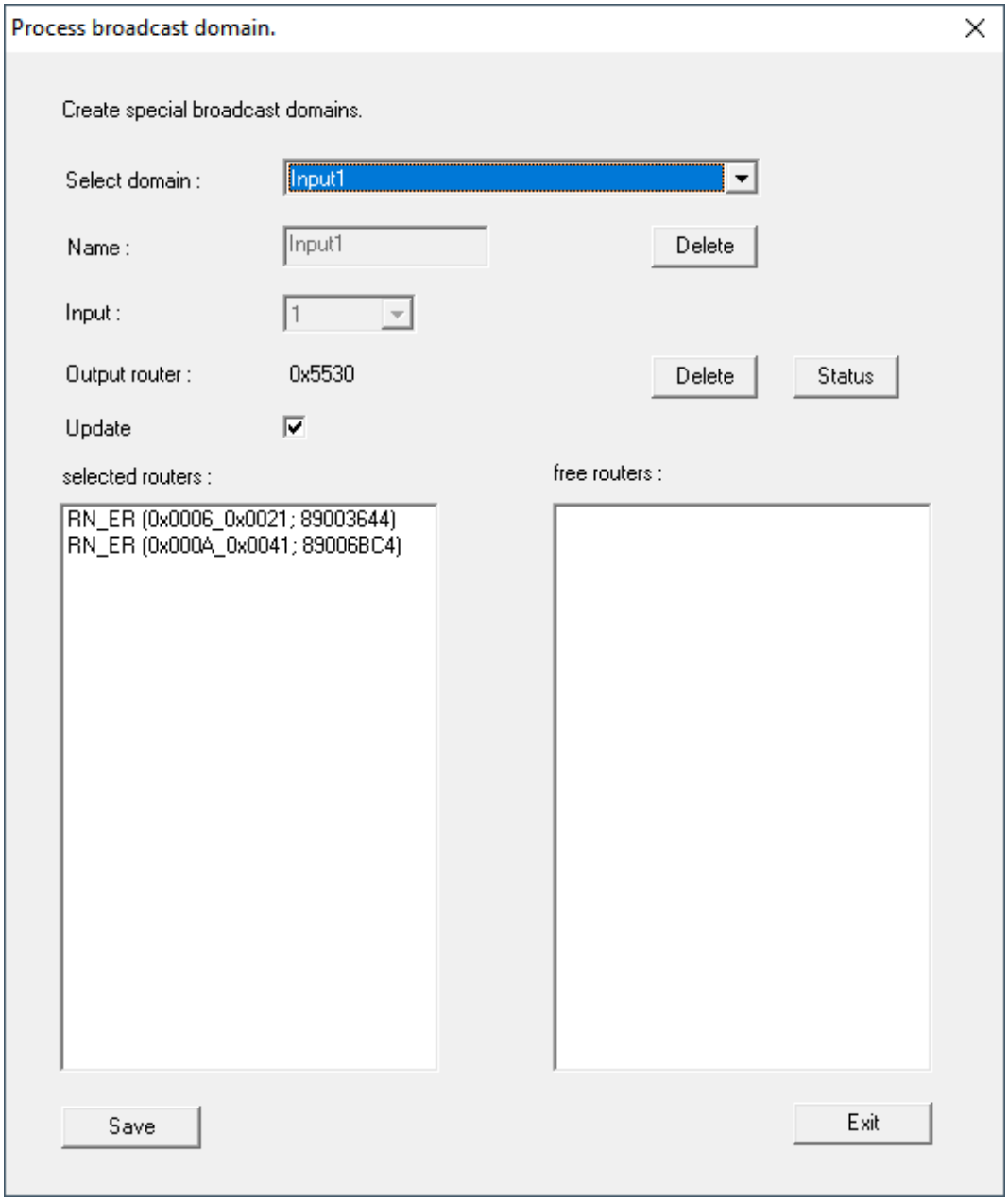


2. Select the option ◉ RingCast.
3. Click on the button OK.
   ↳ The "Administration" window closes.
   ↳ The window "Edit radio domains" opens.

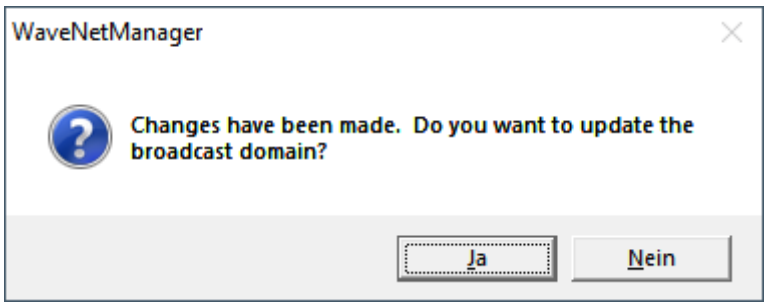


4. In the dropdown menu ▼ **Select domain** select an input for which in ▼ **Delay [s]** you have selected "RingCast".

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

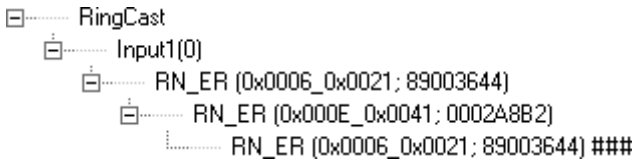


5. Click the button Save.
6. Click the button Exit.
   ↳ The "Edit radio domains" window closes.
   ↳ The window "WaveNetManager" opens.



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.

10.3.3 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 [▸ 207]*).
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 [▸ 207]*).

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

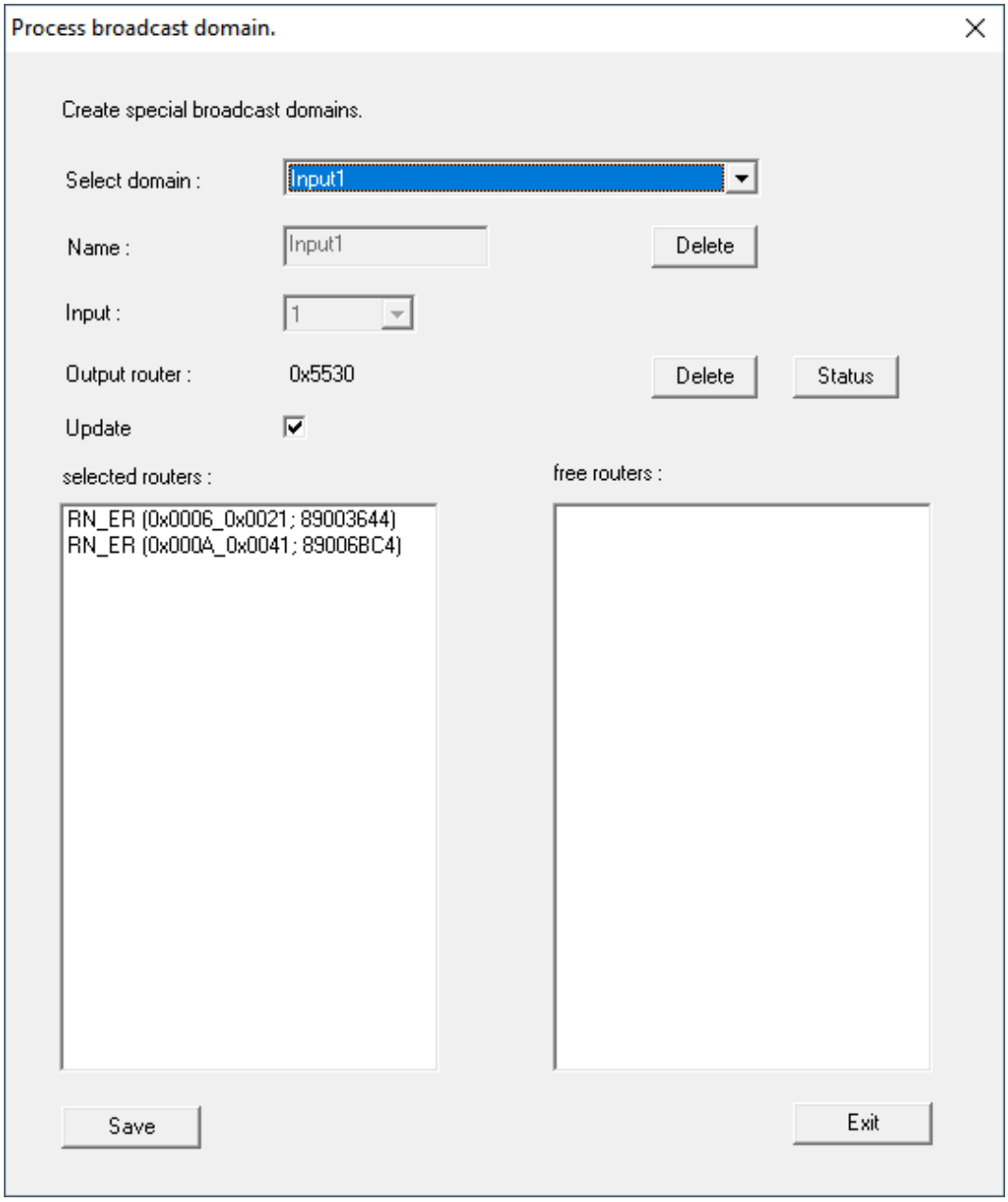
The central output router receives the input acknowledgement of the participating router nodes exclusively via an Ethernet connection. The central output router therefore ignores the status of router nodes that are not Ethernet router nodes (.ER). If you are using the central output router and your RingCast 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:

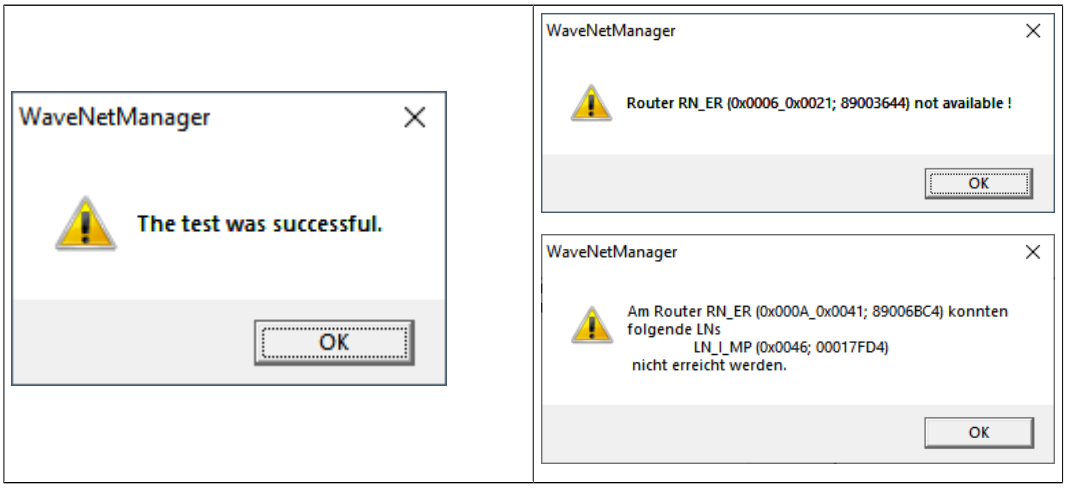
✓ WaveNet Manager opened via LSM (see Best Practice: From the LSM software)

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.



3. Click on the button Status.

↳ RingCast is tested.



The RingCast was able to address all locking devices.	The RingCast could not be closed. Possible causes (see also Central output router): ■ 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. 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).

10.4 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 [▸ 190]*.
- Forwarding of locking device events has also been activated as in *Activating the locking device's input events [▸ 201]*.

10.4.1 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.

10.4.2 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.

10.4.3 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.

10.4.4 Forward input events via the SREL3 ADV system

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

10.4.4.1 Evaluating controller inputs

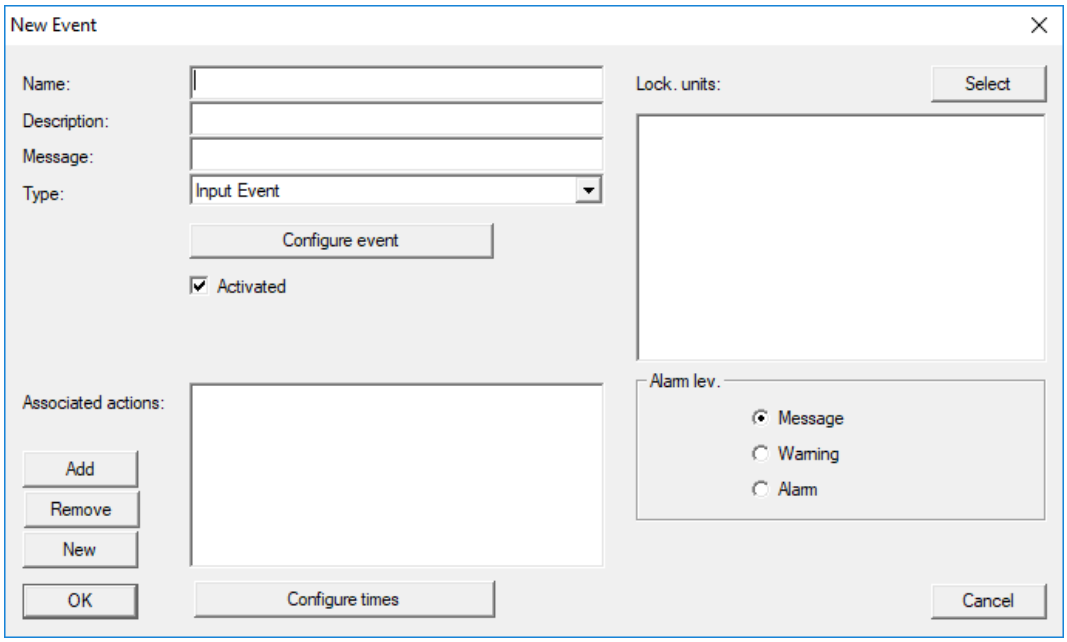
The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

Adding an event

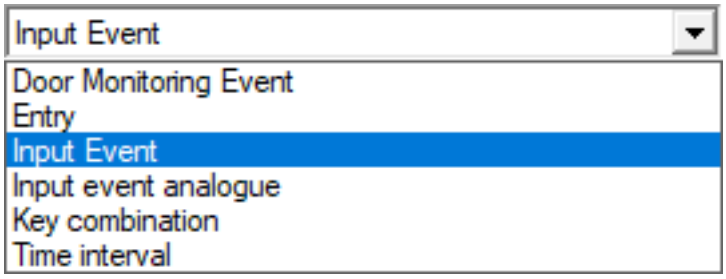
If you wish to use LSM or SmartSurveil (see SmartSurveil) to evaluate an input, you first need to create the corresponding input as an event in LSM. Only then will changes to the input also be saved in the LSM database.

✓ LSM open.
✓ SREL3 ADV System added to the matrix.

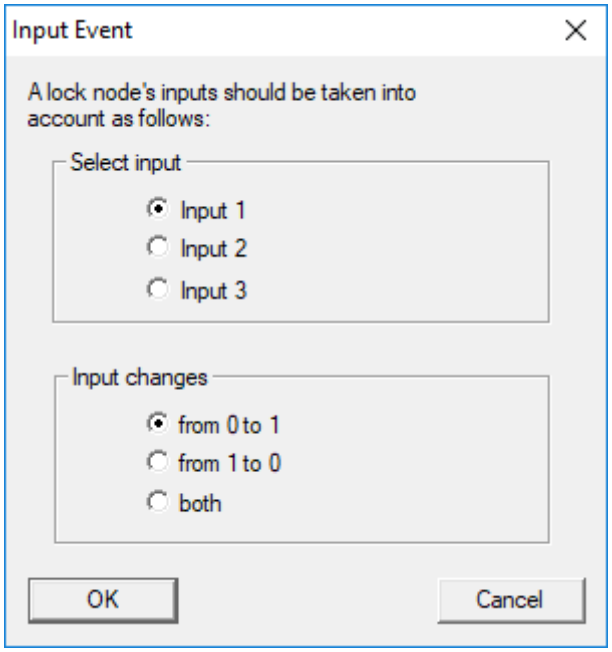
1. Use | Network | to select the Event manager item.
   ↳ The "Network event manager" window will open.
2. Click on the New button.
   ↳ The "New Event" window will open.



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.

10.4.5 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 us 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.

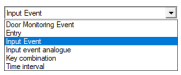
10.4.6 Creating an event

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.

10.4.6.1 Possible door events

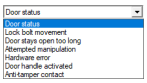
In the window "New Event" can be found in the drop-down menu ▼ **Type** different events available.



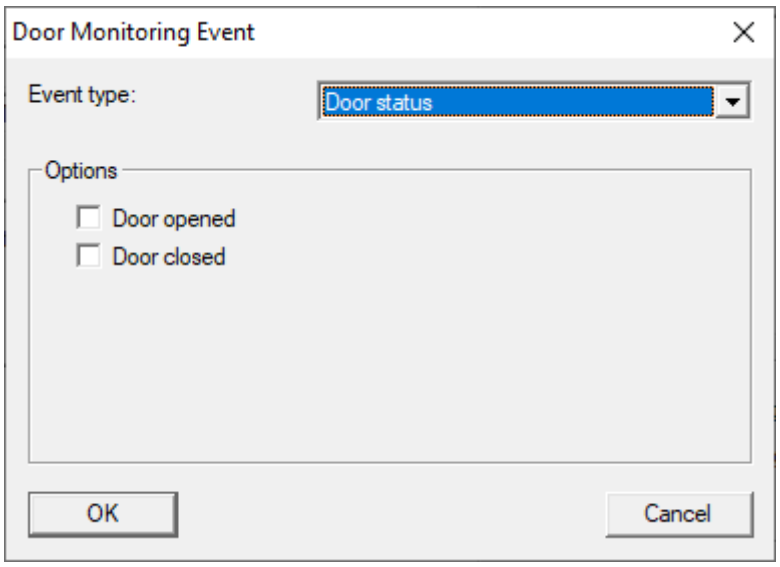
You need a DoorMonitoring-capable locking device (DM) for DoorMonitoring events.

Door monitoring event type

The following DoorMonitoring events are available to you:



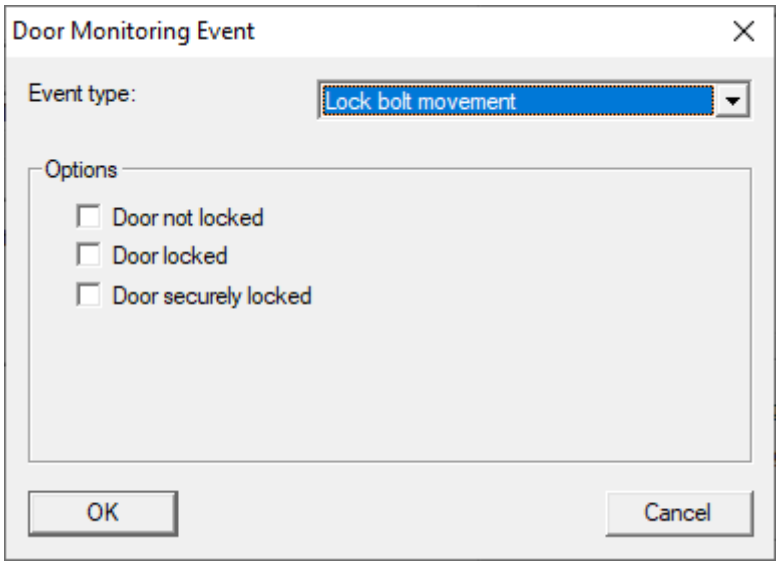
Door status



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

- ☑ Door open
- ☑ Door closed

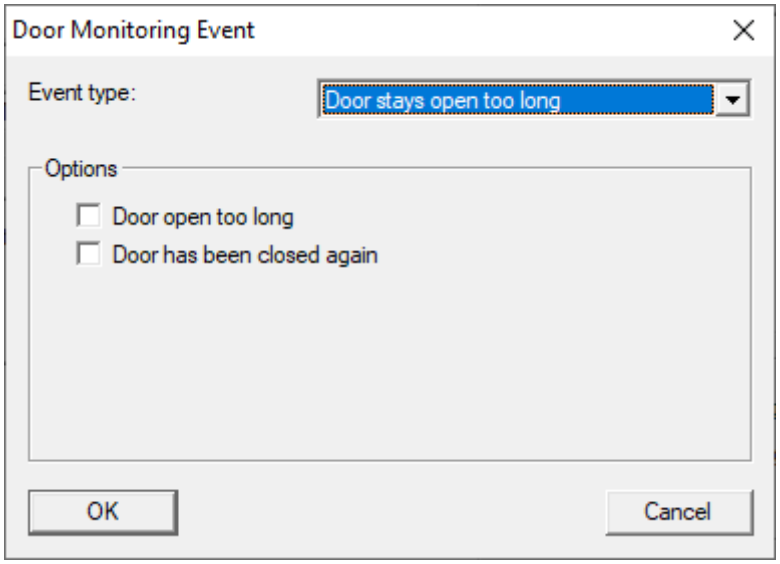
Lock bolt movement



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

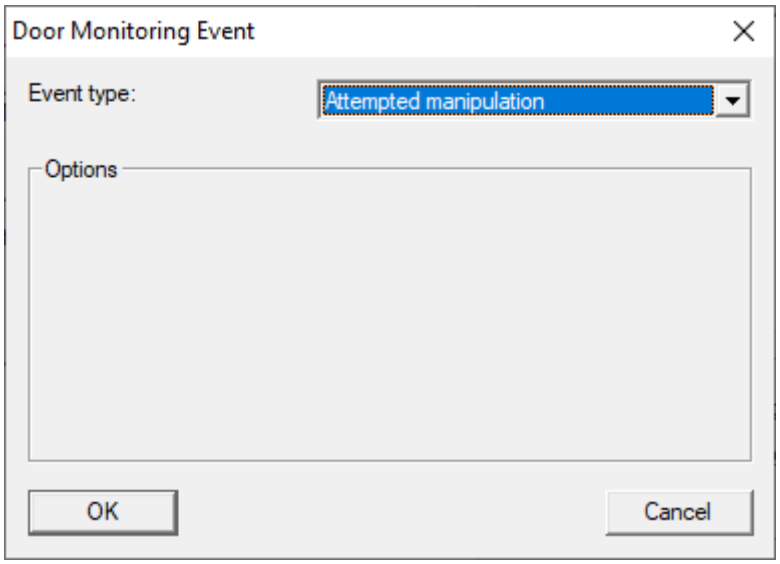
Door stays open too long



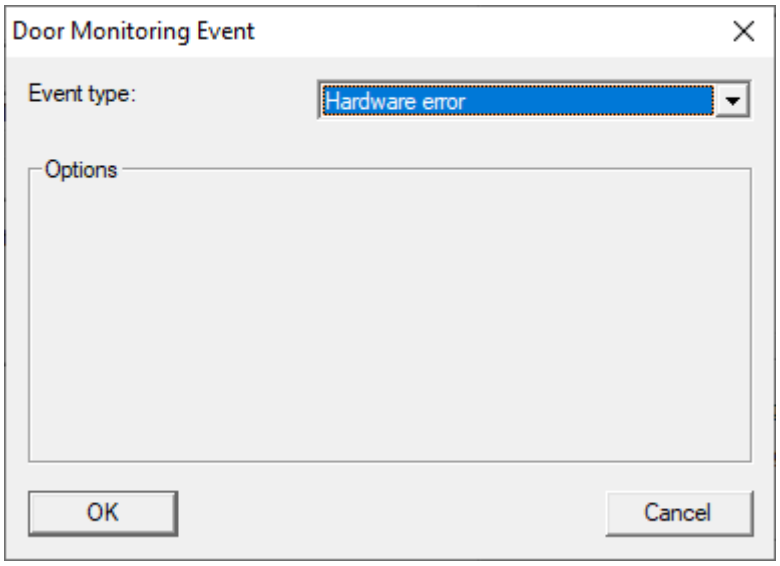
The following states can be detected. A check mark triggers the event as soon as the condition occurs:

- Door open too long
- Door closed again

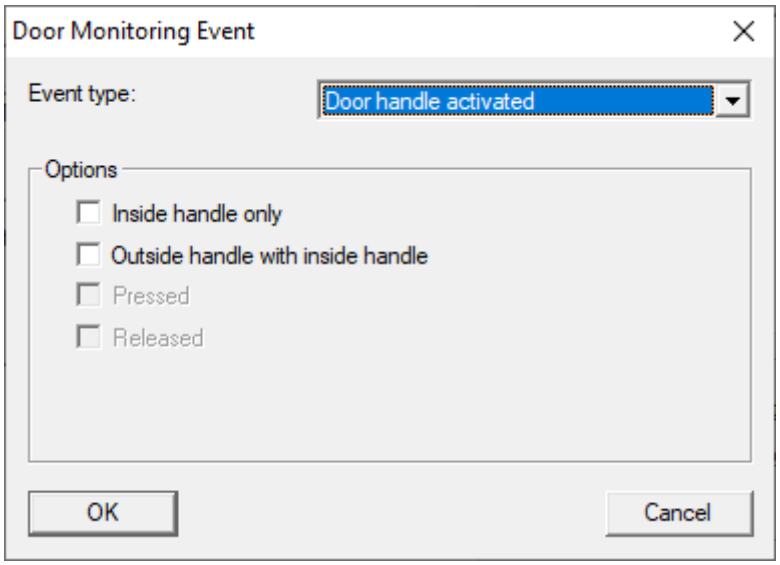
Attempted manipulation



Hardware error



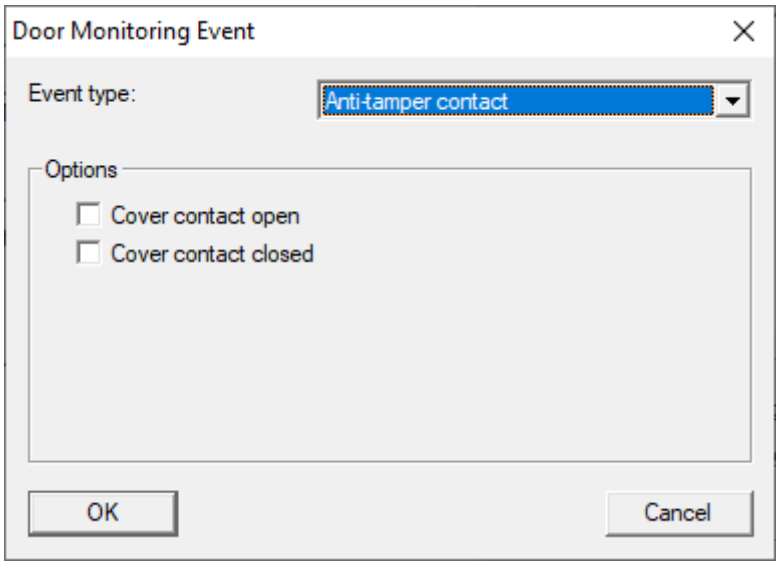
Door handle activated



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

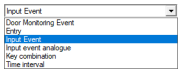


The following states can be detected. A check mark triggers the event as soon as the condition occurs:

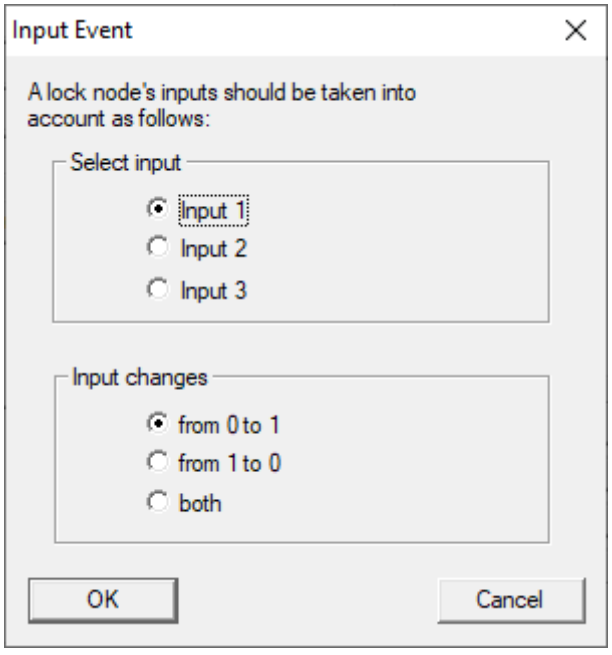
- Cover contact open
- Cover contact closed

Default Events

The following standard events are available:



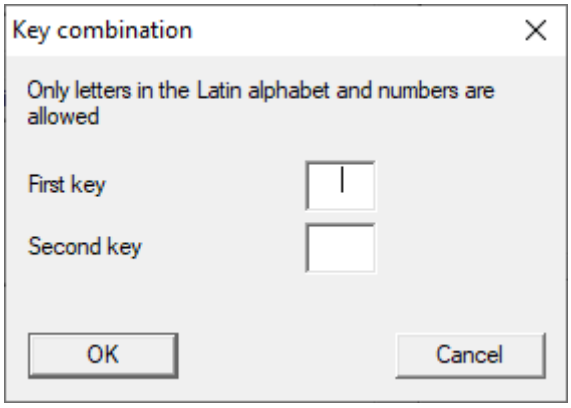
Input Event



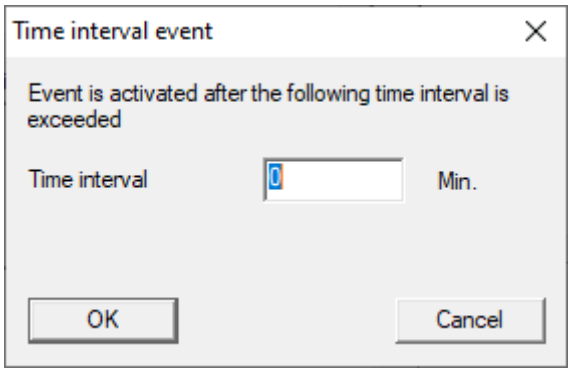
Analog input event

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

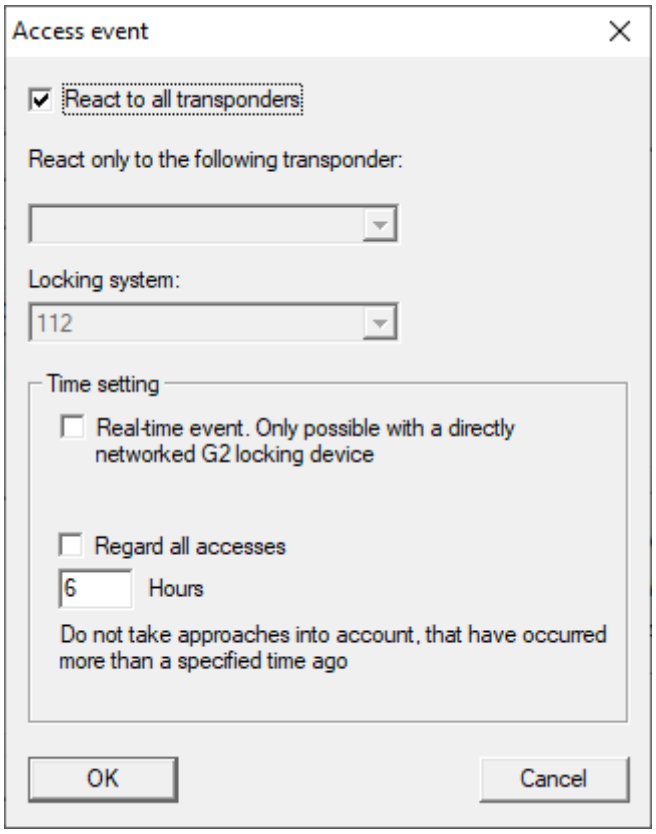
Key shortcut



Time interval



Access



10.5 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).

10.5.1 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 [▸ 8]*).

10.5.1.1 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 [▸ 226]*).

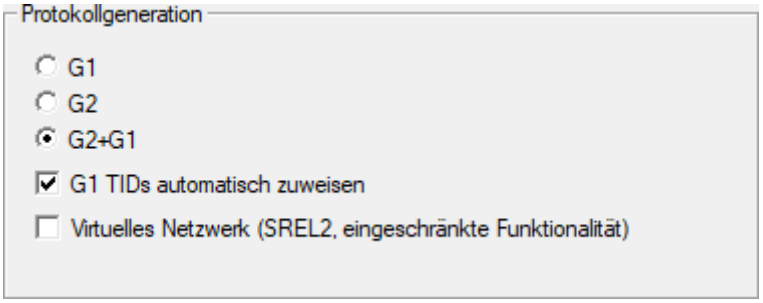
10.5.1.2 Setting up a locking system

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

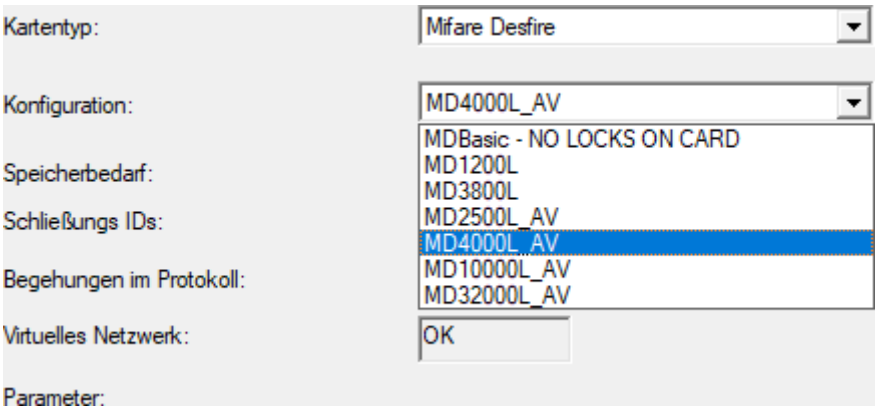
The ☐ Virtual network (SREL2, limited functions) checkbox must not be activated in the locking system properties.

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.



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



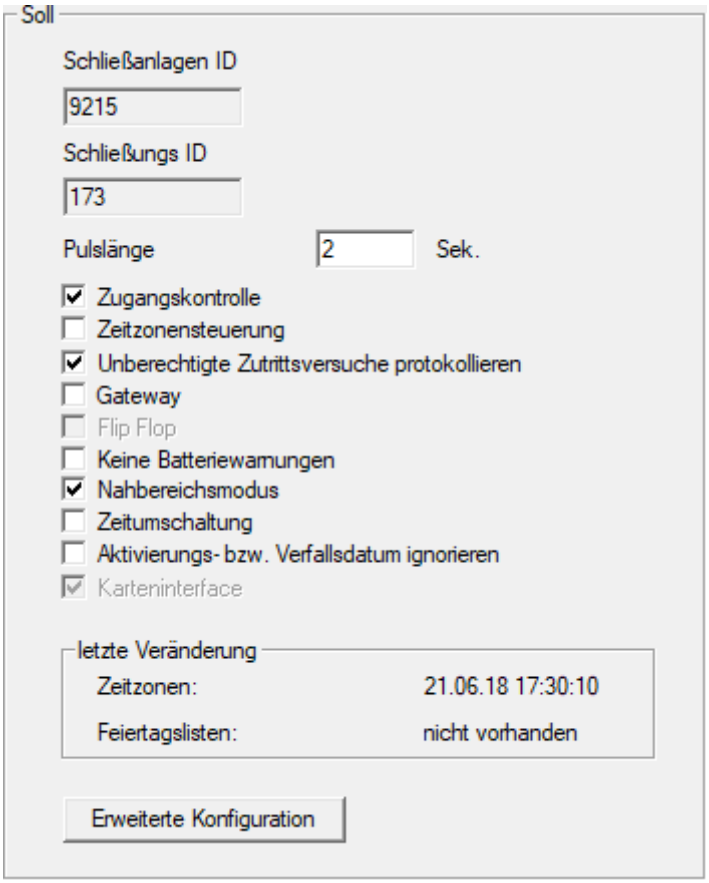
6. Click on the Apply button.

10.5.1.3 Setting up the gateway and VN host server

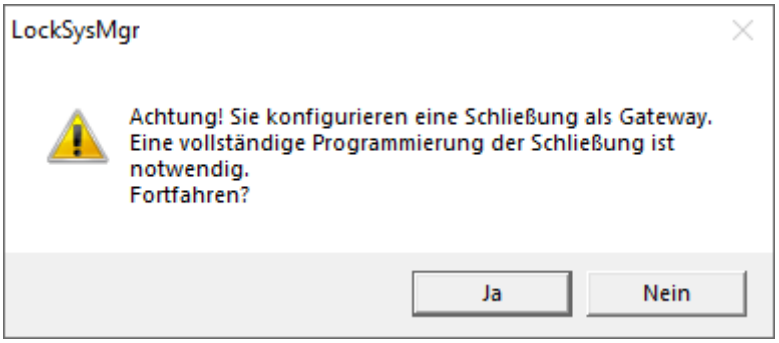
✓ Locking system created (see *Setting up a locking system [▸ 221]*).
✓ SmartRelais 3 Advanced configured and networked (see system manual for SmartRelais 3 Advanced).
✓ VN host installed (see *VN host [▸ 22]*).

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

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

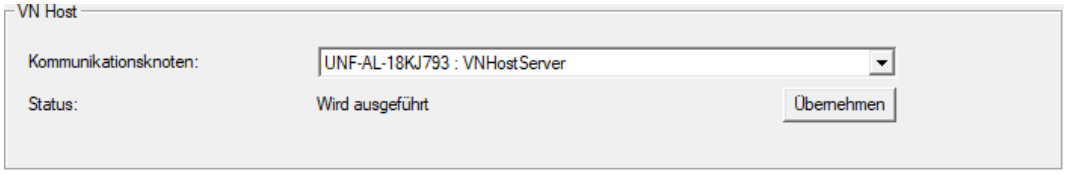


3. Activate the ☑ Time zone management and ☑ Audit trail checkboxes.
4. Activate the ☑ Gateway check box.
   ↳ Warning about pending programming will open.



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

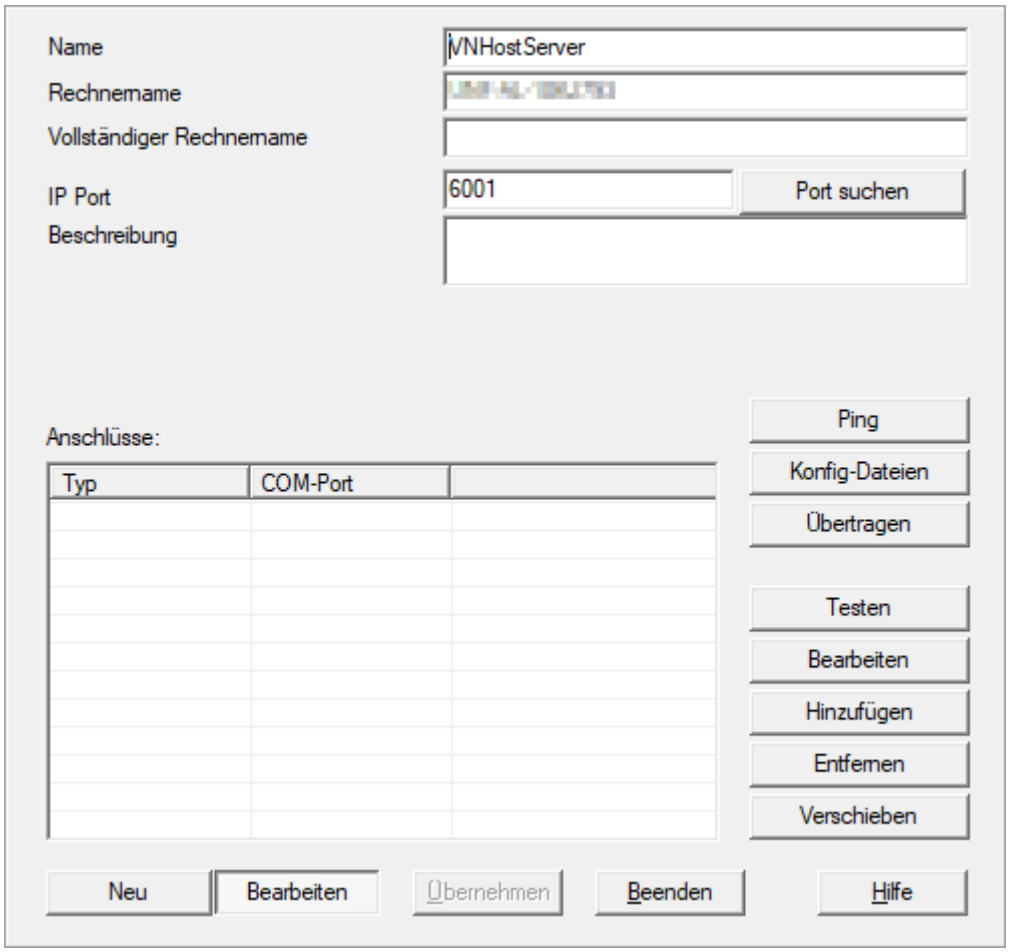
Different communication nodes on the SmartRelais 3 Advanced

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.

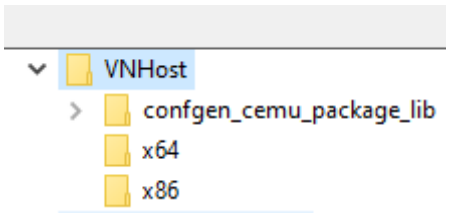
- Select the "VN host server" entry for the virtual network even if your SmartRelais 3 Advanced is using another communication node.

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.

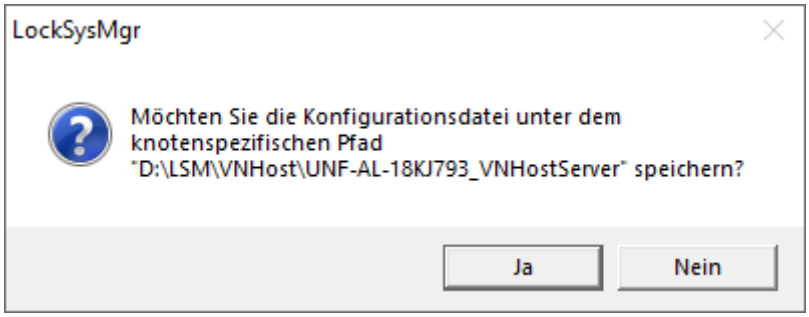
14. Switch to the VN host server communication node using the ▸ and ◂ buttons.



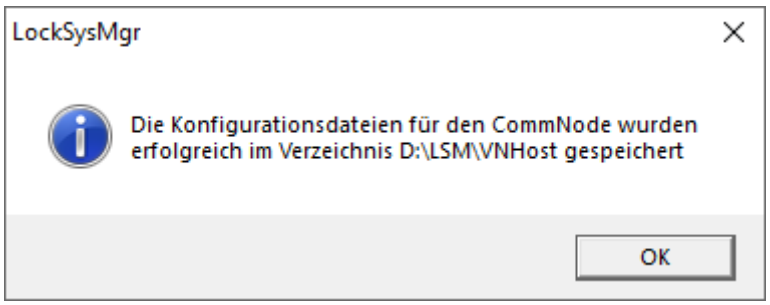
15. Click on the Config files button.
    ↳ The Explorer window will open.
16. Select the VN host server's installation folder.



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 [▸ 226]*).

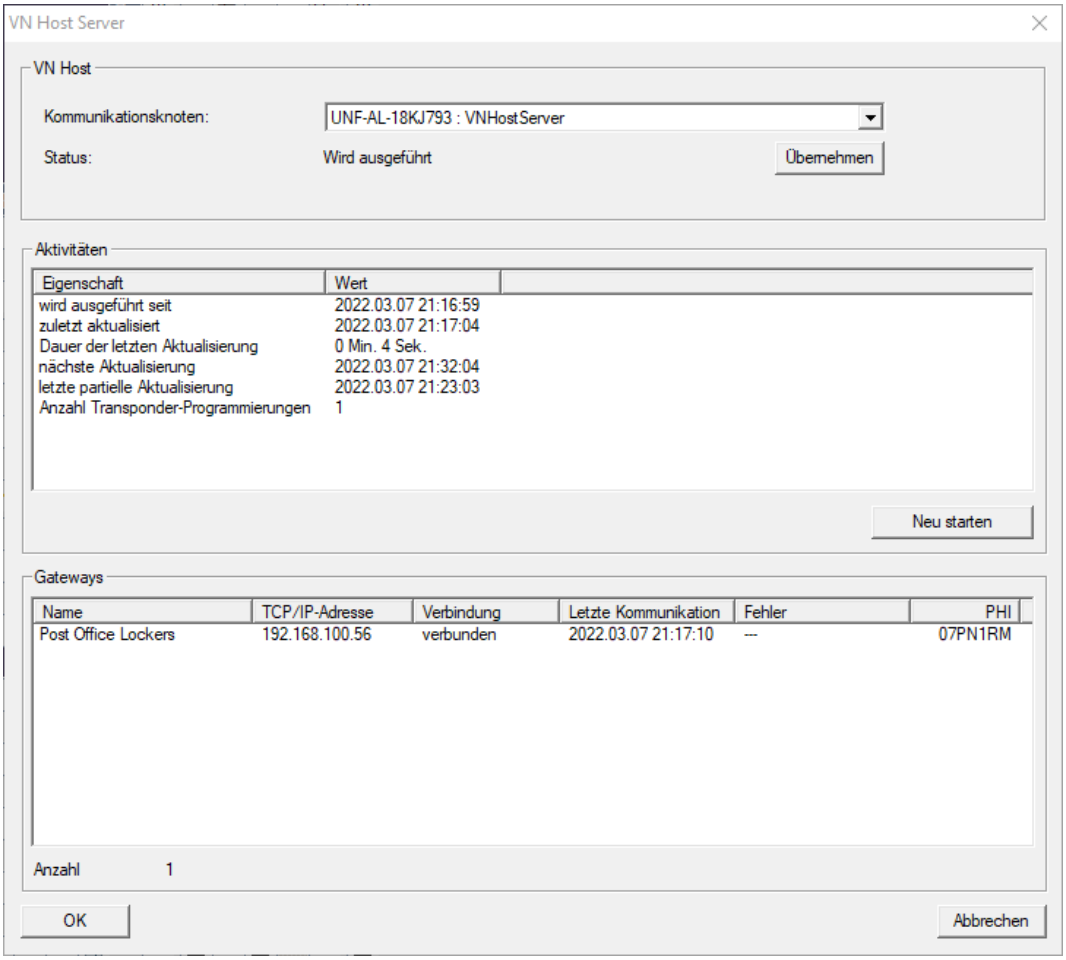
10.5.1.4 Check virtual network status

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

✓ Virtual network configured (see *Setting up a locking system [▸ 221]* and *Setting up the gateway and VN host server [▸ 222]*).

- 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

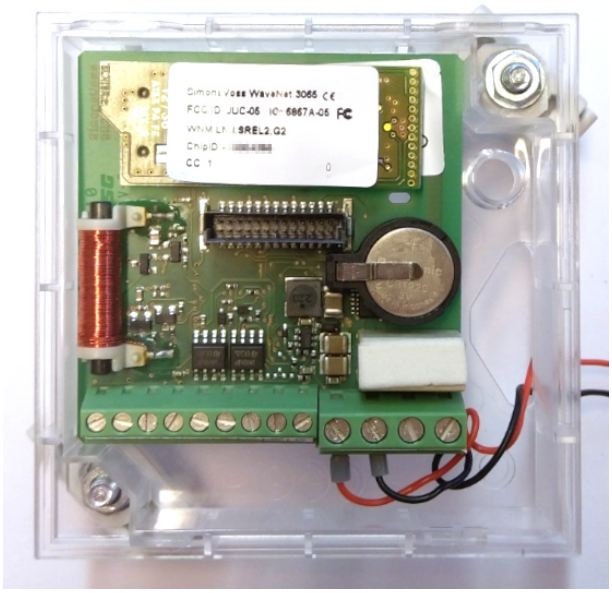
You will find a list of all SmartRelais 3 Advanced configured as ☑ Gateway and their statuses in the section.

10.5.2 Virtual network with SmartRelay 2 G2

10.5.2.1 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 [▸ 233]*).

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.



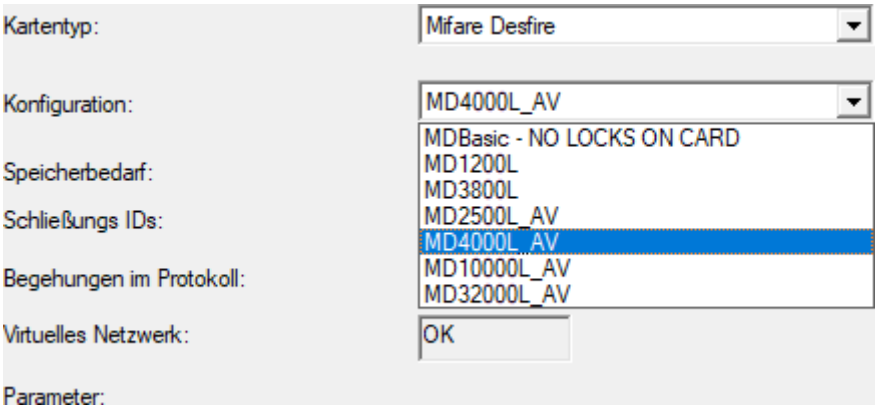
Identification media which are actuated on the gateway then distribute the data to the locking devices.

10.5.2.2 Setting up a locking system

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

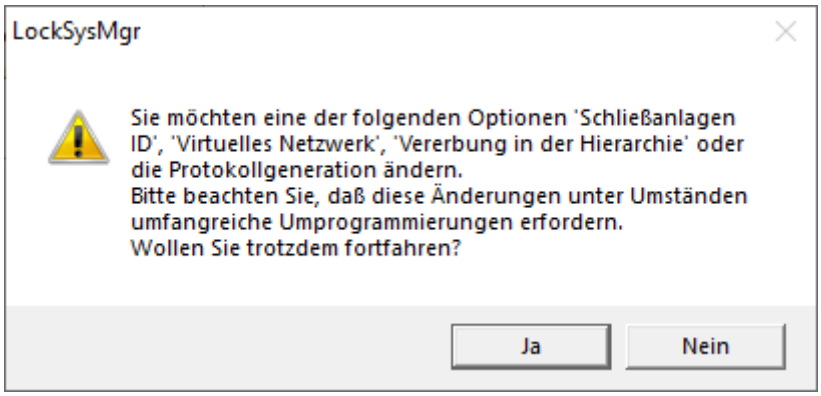
1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the "[Name]" tab.
3. Activate the checkbox in "Protocol generation" the area ☑ Virtual network (SREL2, limited functions).

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



↳ 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.



10.5.2.3 Setting up a VN service

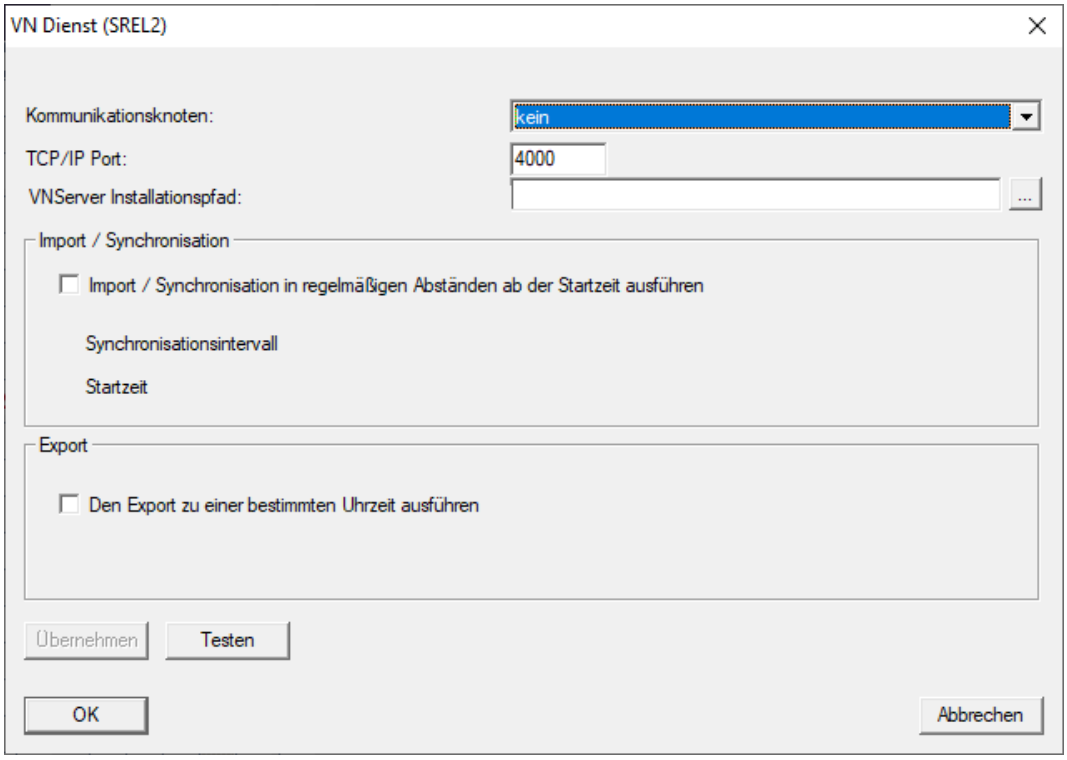
✓ Locking system configured (see *Add new locking system [▸ 133]*, *Add new transponder [▸ 133]* and *Add new locking device [▸ 190]*).

✓ ☑ Virtual network (SREL2, limited functions) checkbox activated.

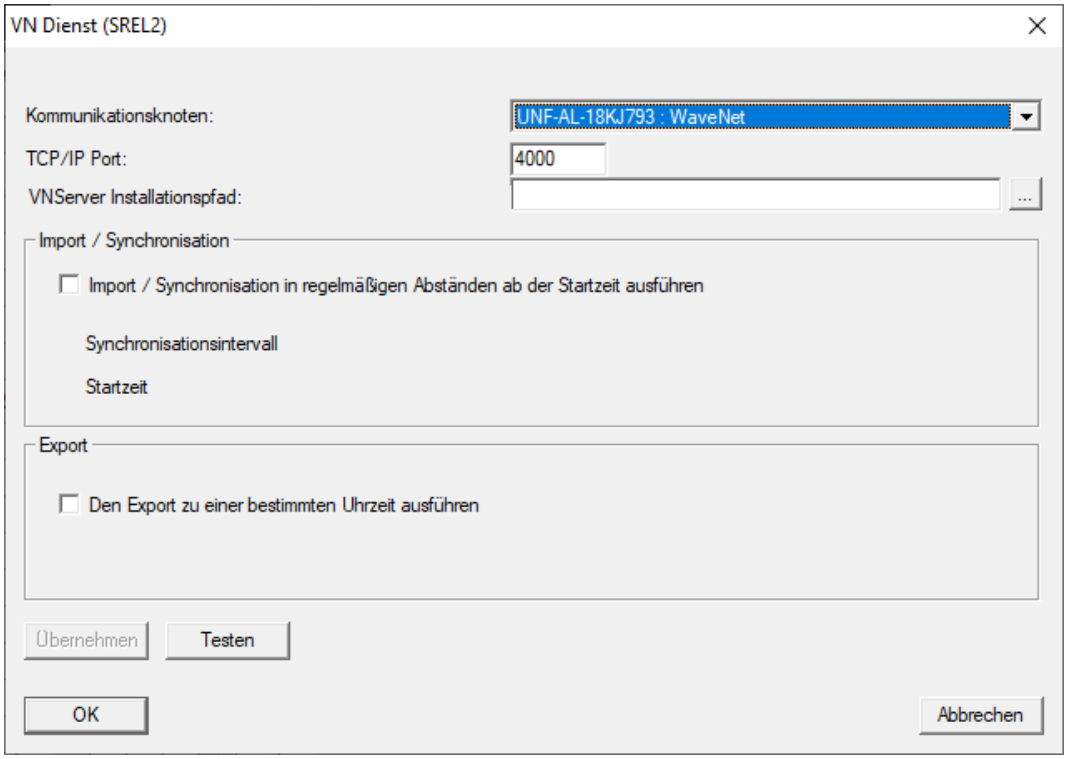
✓ All components programmed (see *Programme transponder [▸ 149]* and *Programme locking device [▸ 191]*).

✓ SmartRelay 2 G2 networked (see WaveNet manual).

1. Use | Network | to select the VN service (SREL2) input.
   ↳ The "VN service (SREL2)" window will open.

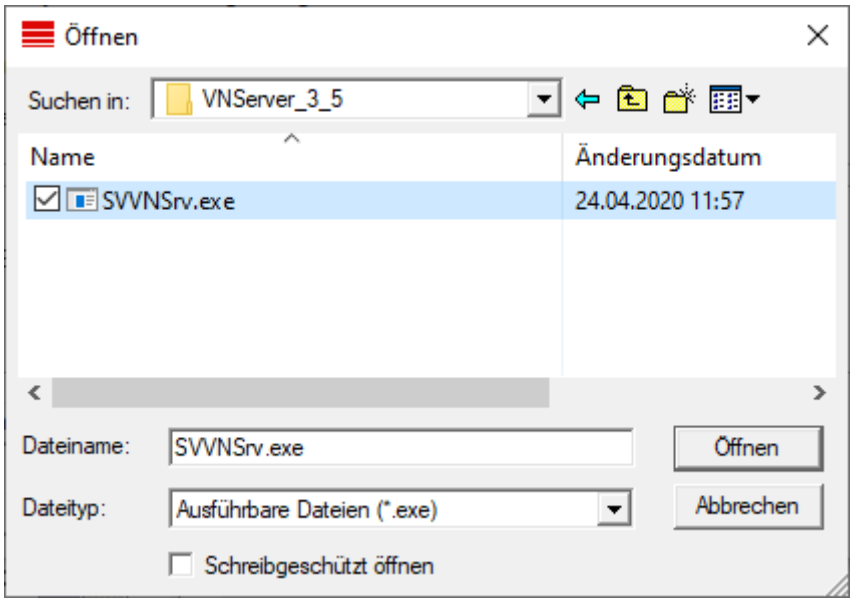


2. Select from the ▼ **Communication nodes** drop-down menu the communication node to which WaveNet with RouterNode 2 and SmartRelay 2 G2 is connected.

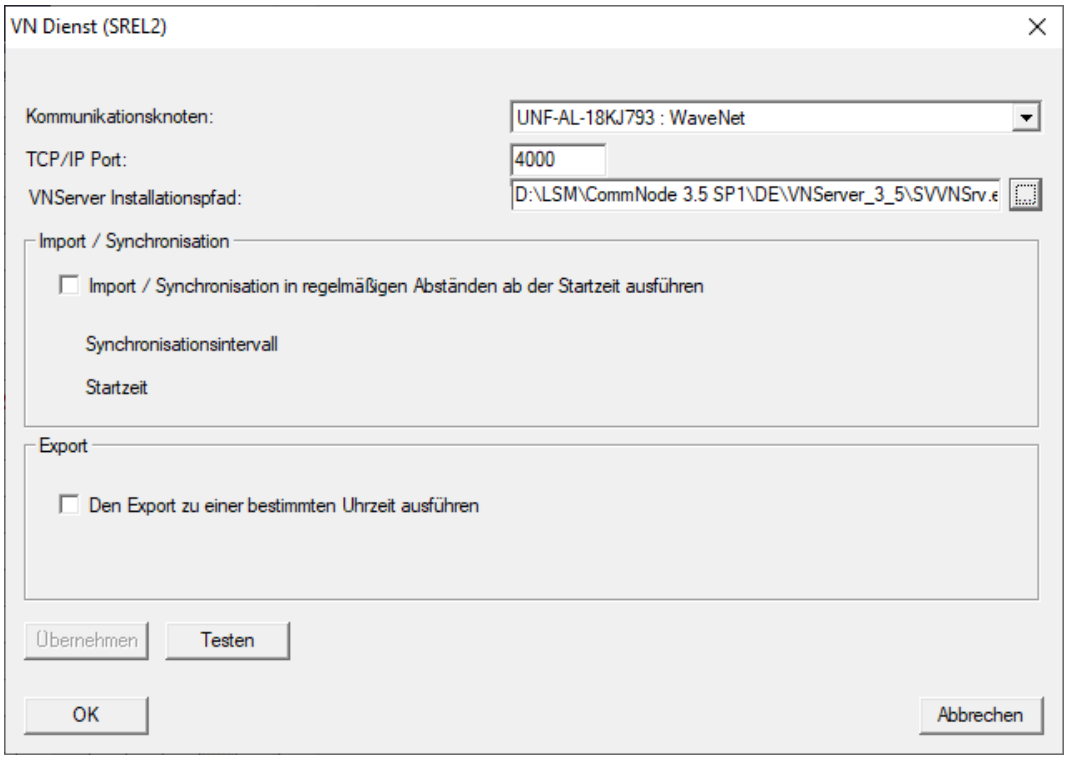


3. Ensure that the TCP/IP port is set to 4000.
4. Click on the ... button to open Explorer.

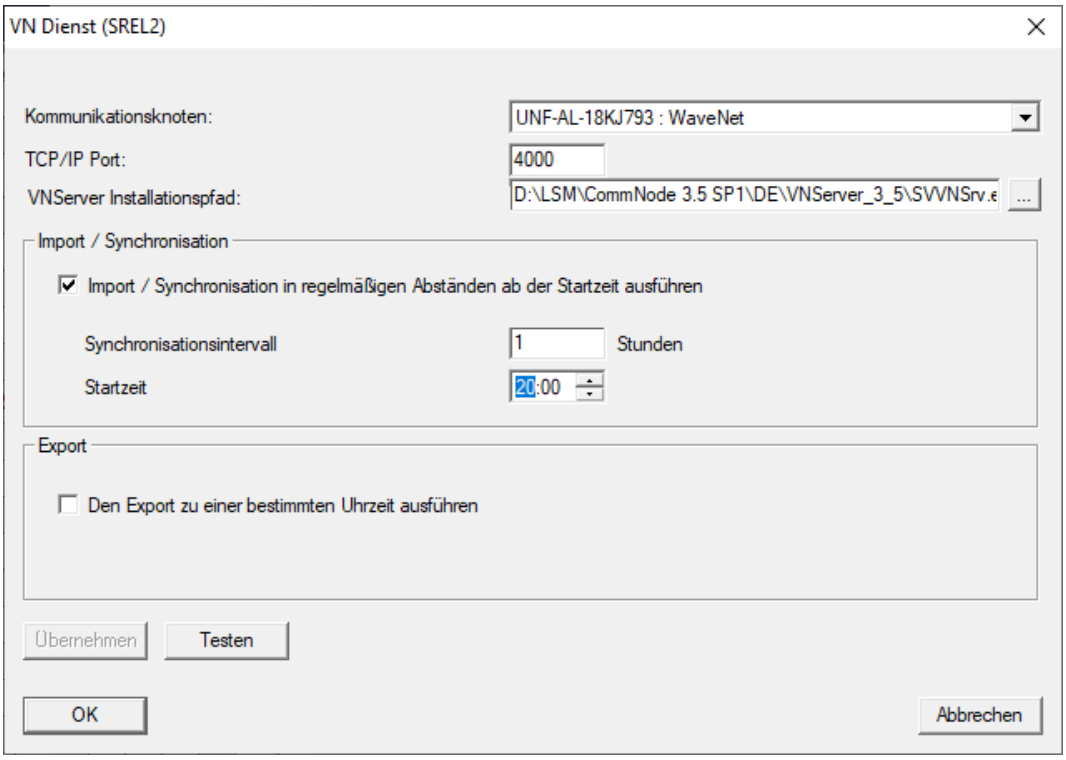
5. Select SVVNSvr.exe.
   SVVNSvr.exe is installed together with the CommNode server. Default directory: (C:\Programs(x86)\SimonsVoss\VNServer_x_x)



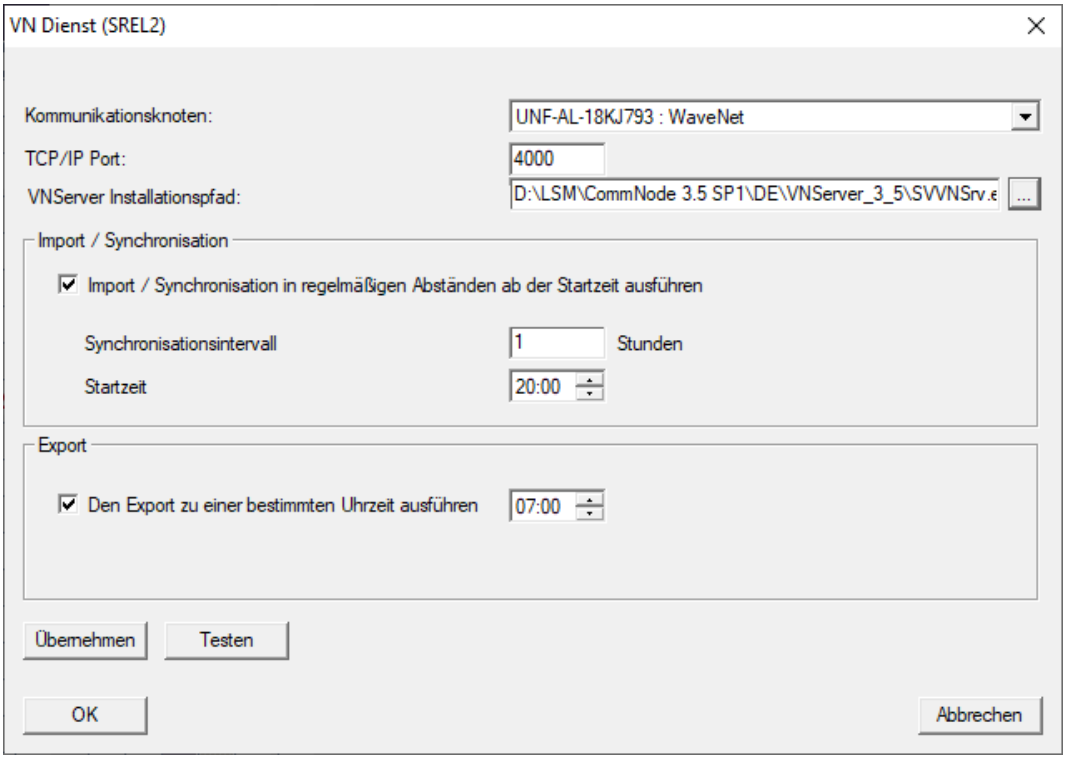
6. Click on the Open button.
   ↳ Explorer window closes.



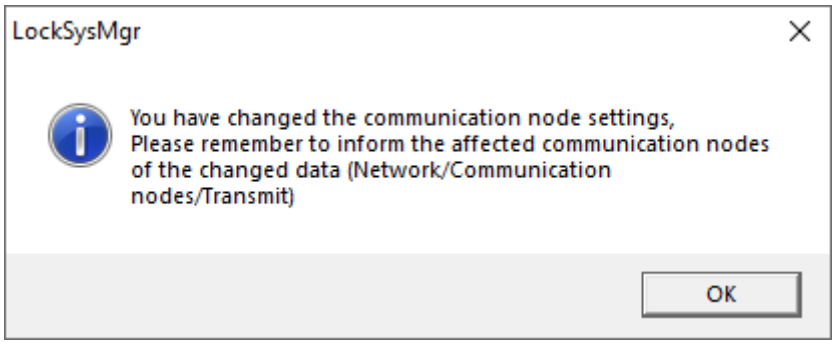
7. Optional: Go to the "Import/synchronisation" section and configure when the data from SmartRelay 2 G2 should be automatically imported back into LSM.



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



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 [▸ 201]*).

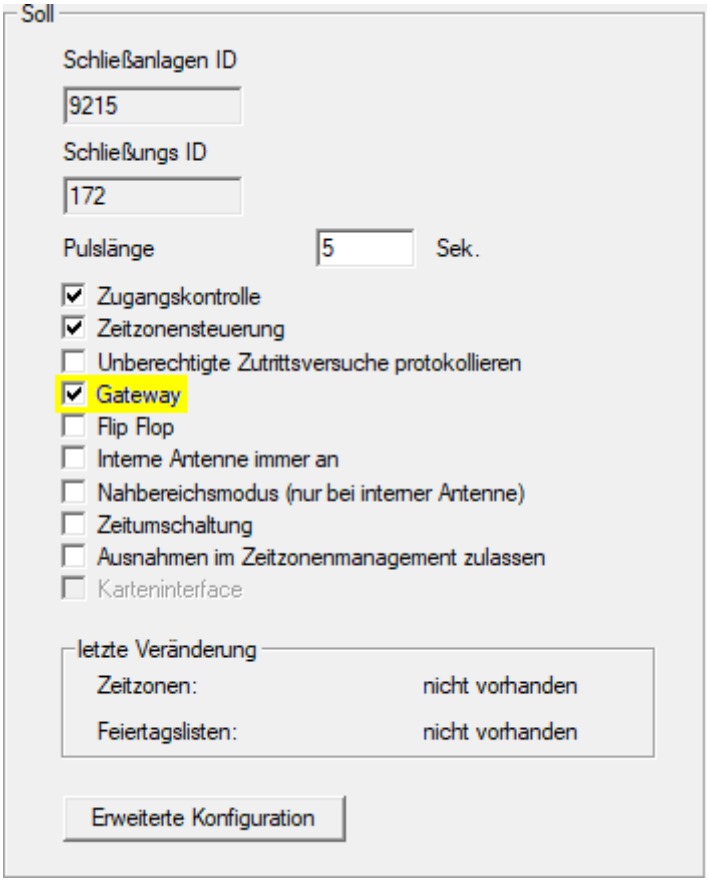
10.5.2.4 Creating components and setting up LSM

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 [▸ 190]*
- *Preparing hardware [▸ 191]*
- *Creating communication nodes [▸ 192]*
- *Setting up Task services [▸ 211]*

1. Create different identification media (e.g. *Add new transponder [▸ 133]*) and locking devices (e.g. *Add new locking device [▸ 190]*).
2. Perform initial programming of the components created (*Programme transponder [▸ 149]* and *Programme locking device [▸ 191]*).
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.



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 [▸ 192]*).
12. Assign the gateway (or SmartRelay 2 G2) to it.

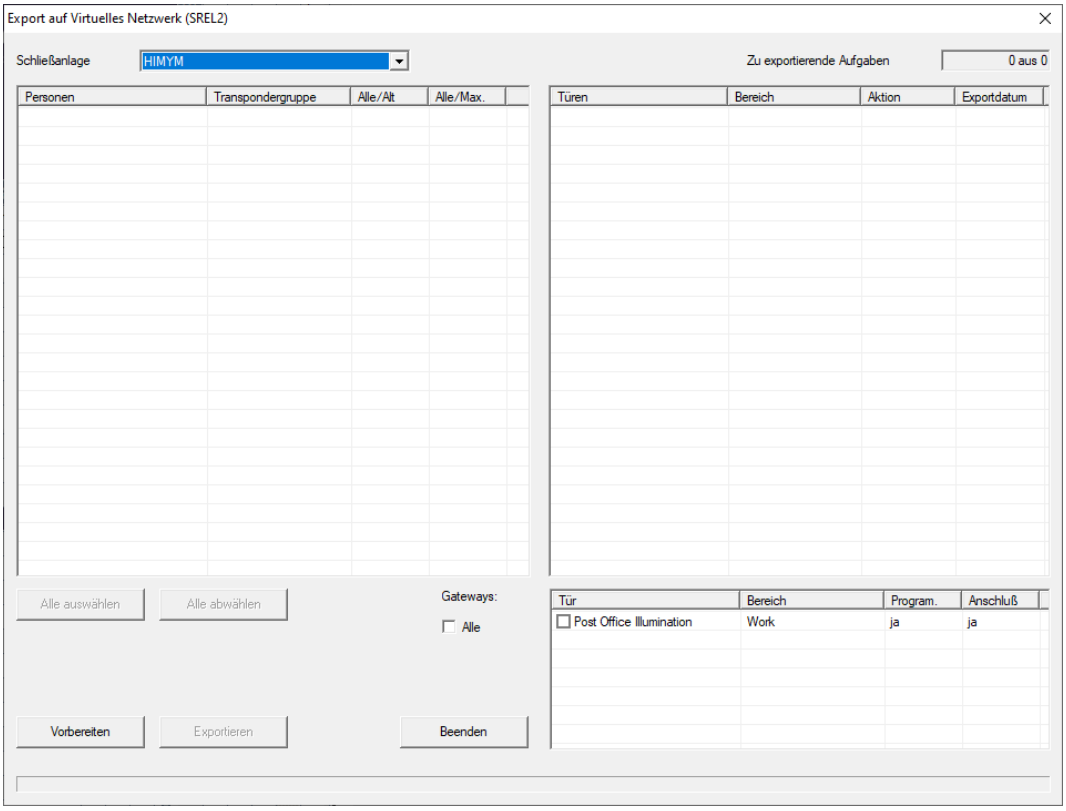
↳ The virtual network is now ready for use.

10.5.2.5 Exporting authorisation changes

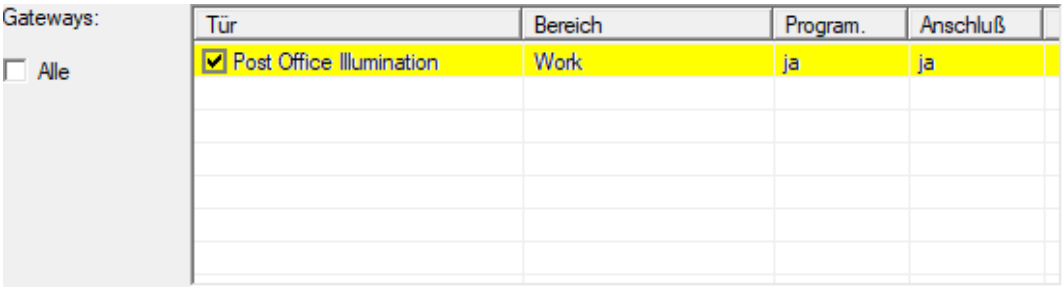
Exporting authorisation changes only works if there is at least one change. To perform the test, remove authorisation for locking cylinder 1 from transponder 1, for example.

1. Perform a reset before the first export (see *Resetting tasks in the virtual network [▸ 241]*).
2. Use | Programming | - Virtual Network to select the Export to VNetwork entry.

   ↳ The "Export to virtual network (SREL2)" window will open.

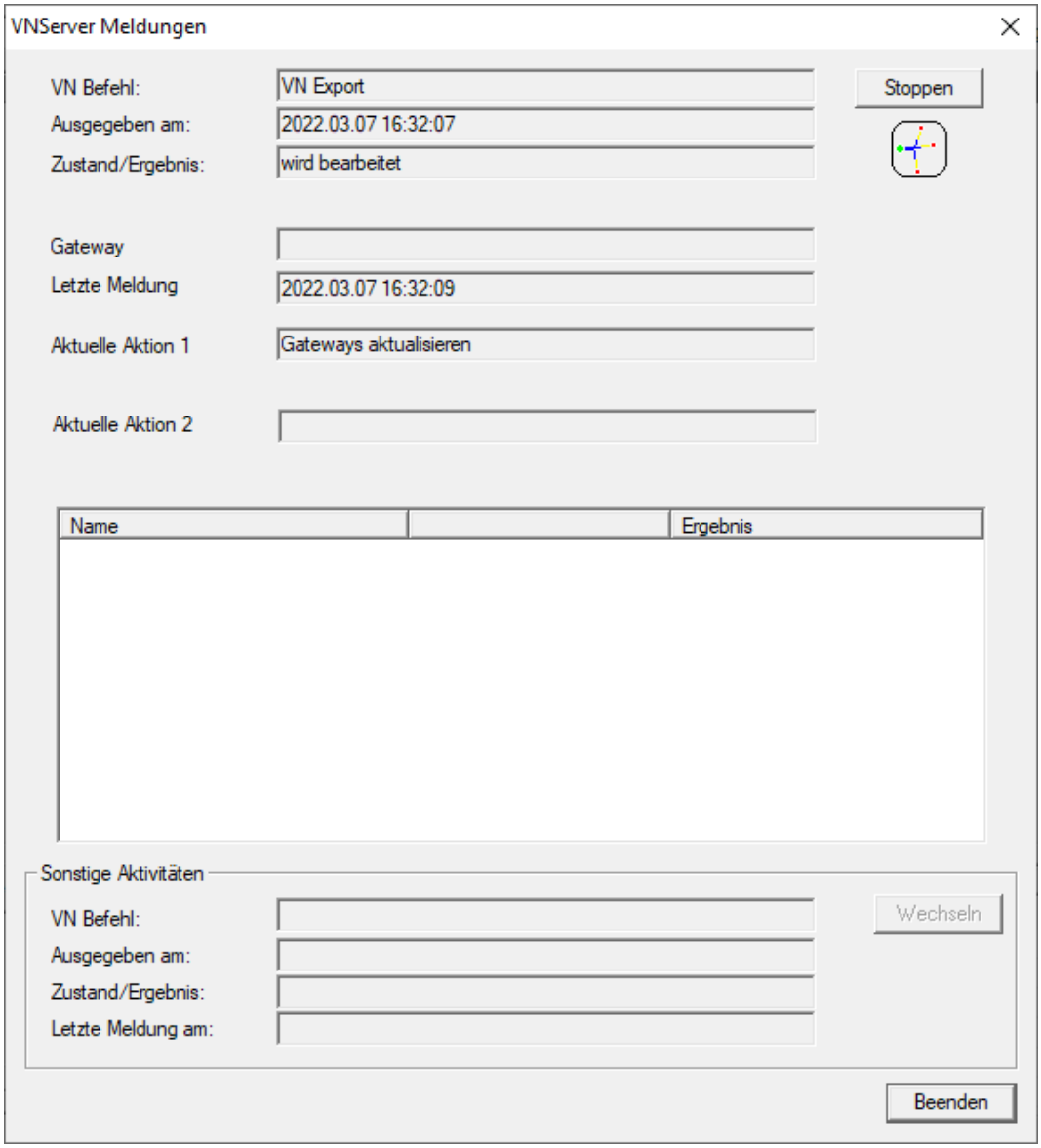


3. Select all SmartRelay 2 G2s to which you need to send/export the changes.

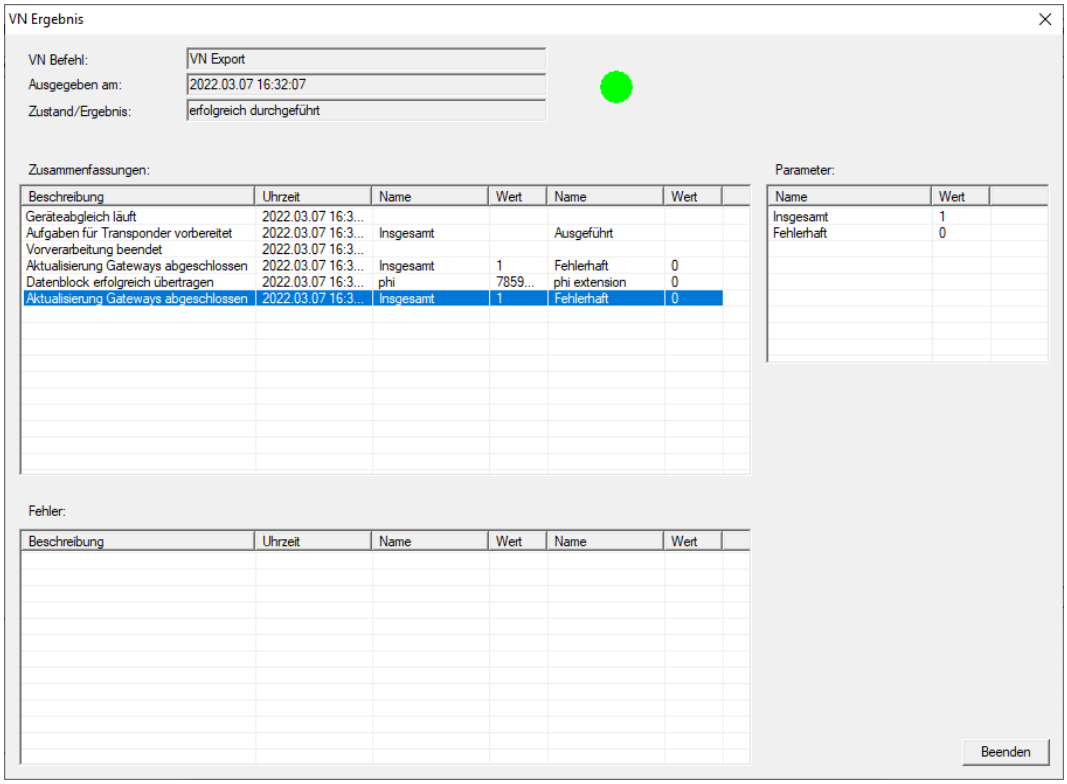


4. Check whether you have selected the correct locking system in the ▼ **Locking system** drop-down menu.
5. Click on the Prepare button.
   ↳ All exportable changes are listed in the "Persons" section.
6. Select all changes that you wish to export to the previously selected SmartRelay 2 G2.

7. Click on the Export button.
   ↳ The export process will start. The changes are sent to the gateway.



↳ A summary of the export is displayed.



You can now track the exported tasks in the overview (*Status of the tasks in the virtual network (SREL2.G2) [▸ 240]*).

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.

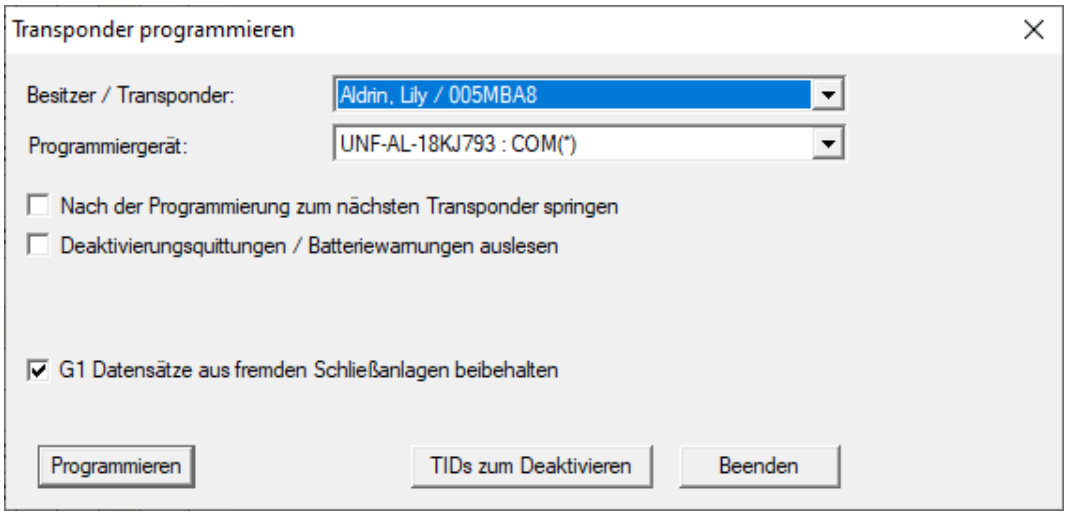
With LSM 3.5 SP3 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

Programme the TIDs to be disabled directly

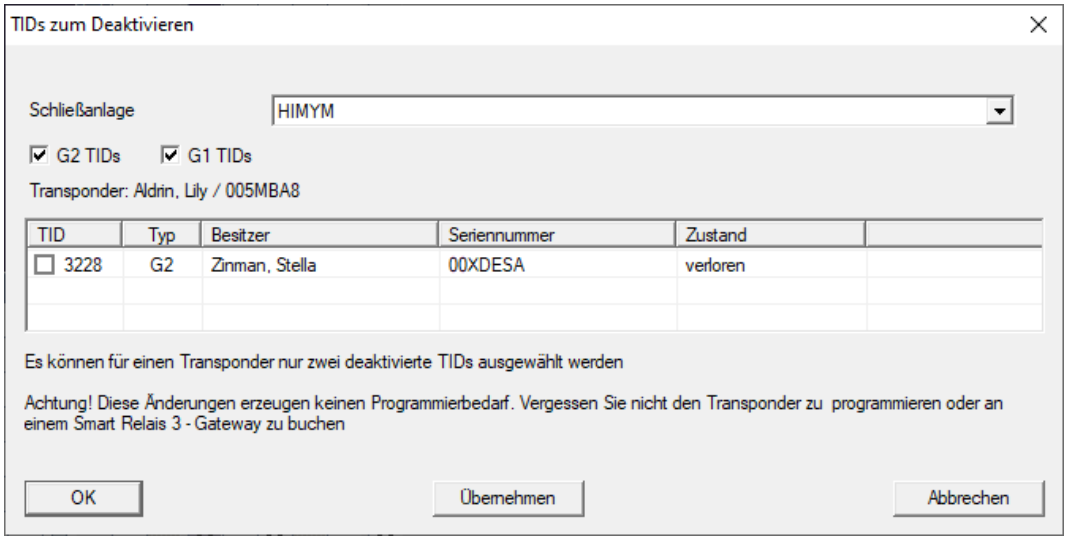
The IDs to be disabled are saved on the transponder during the programming process.

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

1. Click on the TIDs to deactivate button.



↳ The list will open.



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.

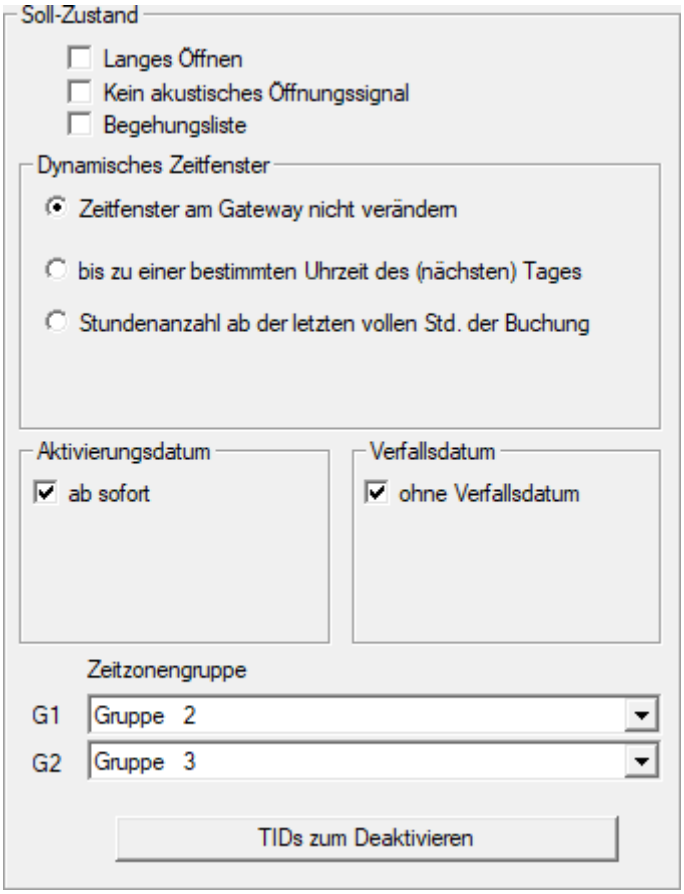
↳ The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

Add the TIDs to be blocked to the properties

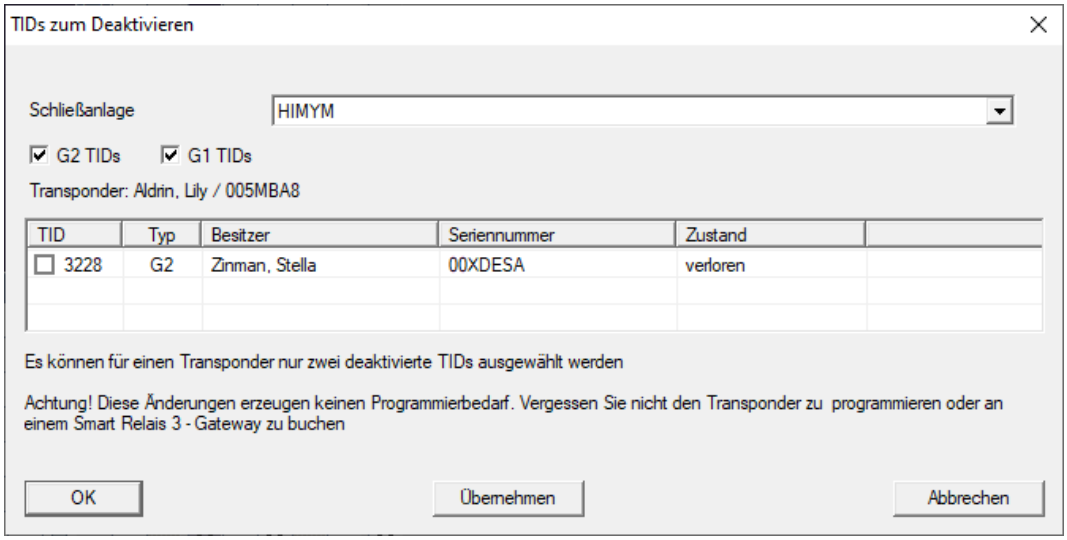
The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

✓ 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.



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

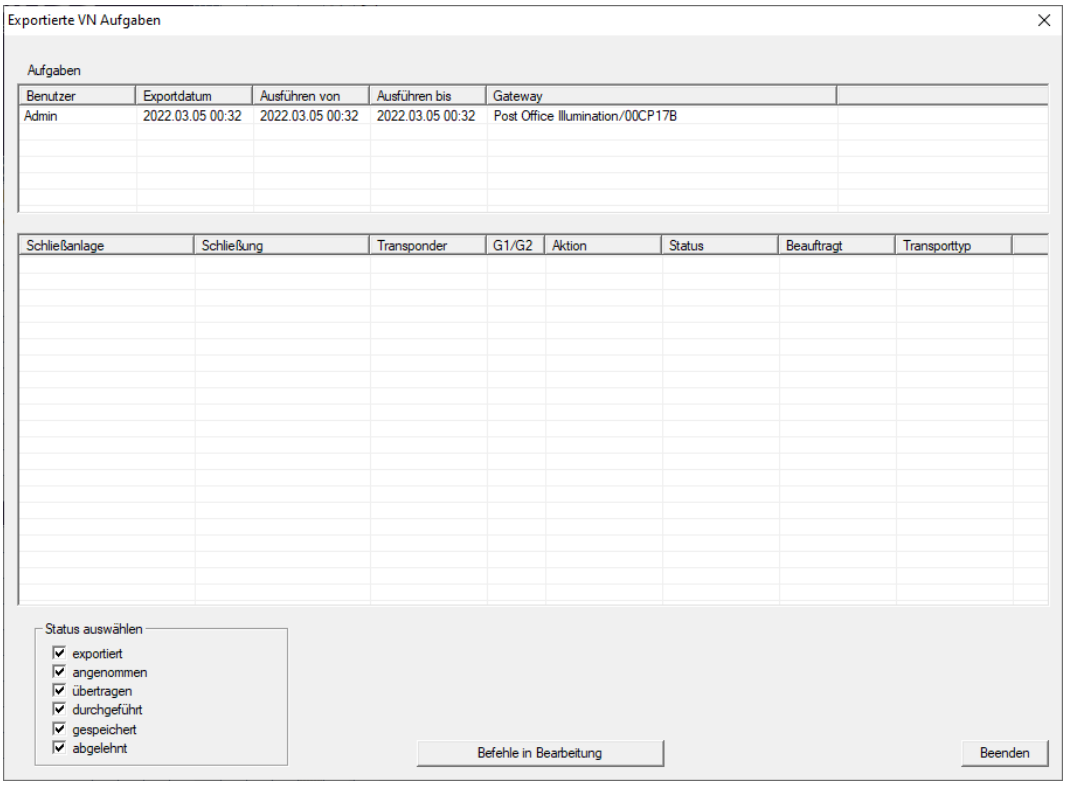
4. Click on the OK button to confirm your input.
↳ The checked TIDs are saved on the transponder either during the next programming process or the next booking on a gateway.

10.5.2.6 Status of the tasks in the virtual network (SREL2.G2)

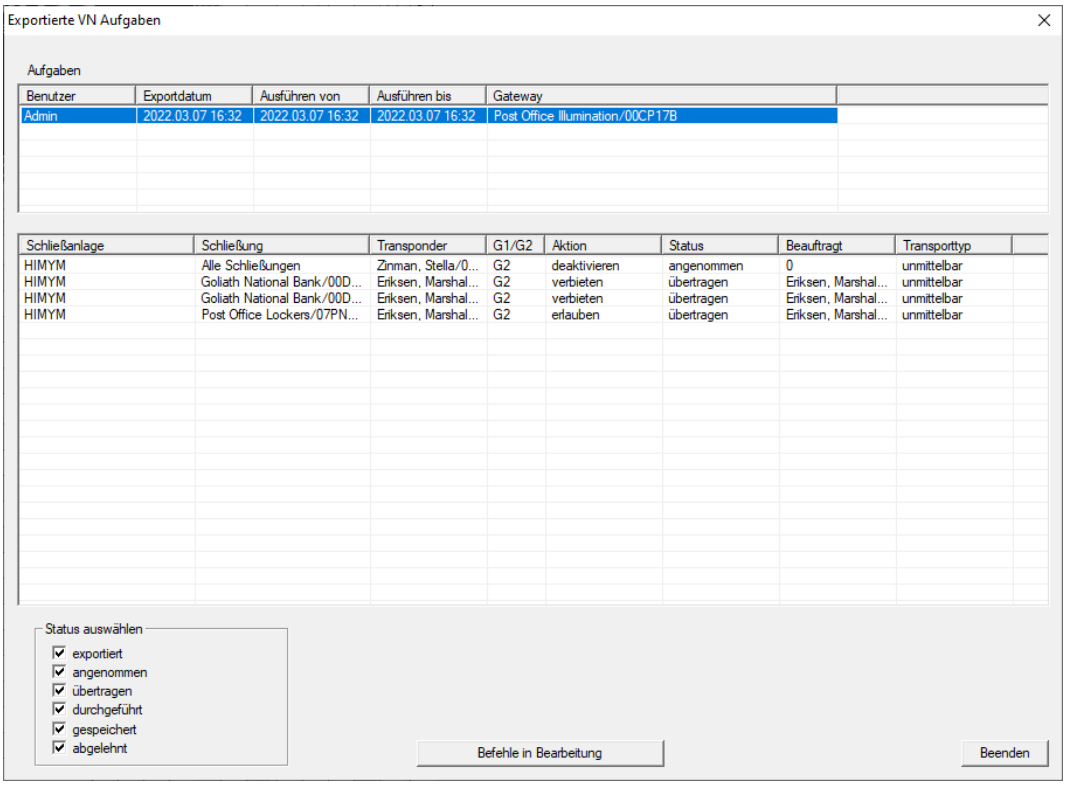
After exporting to the virtual network, you can see the tasks in an overview:

✓ Tasks exported to the virtual network (see *Exporting authorisation changes [▸ 234]*).

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



2. Select a user to view their exported tasks.

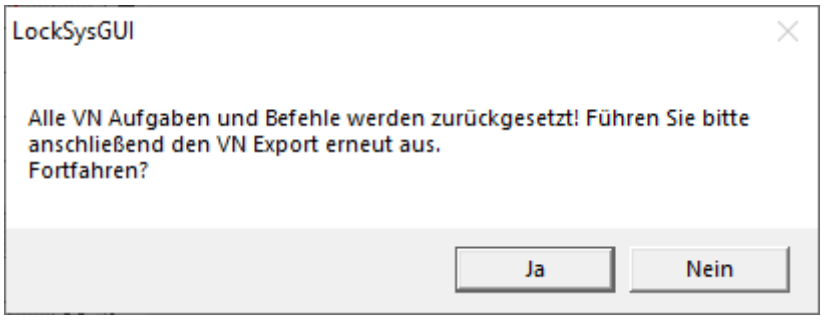


↳ Exported tasks are displayed.

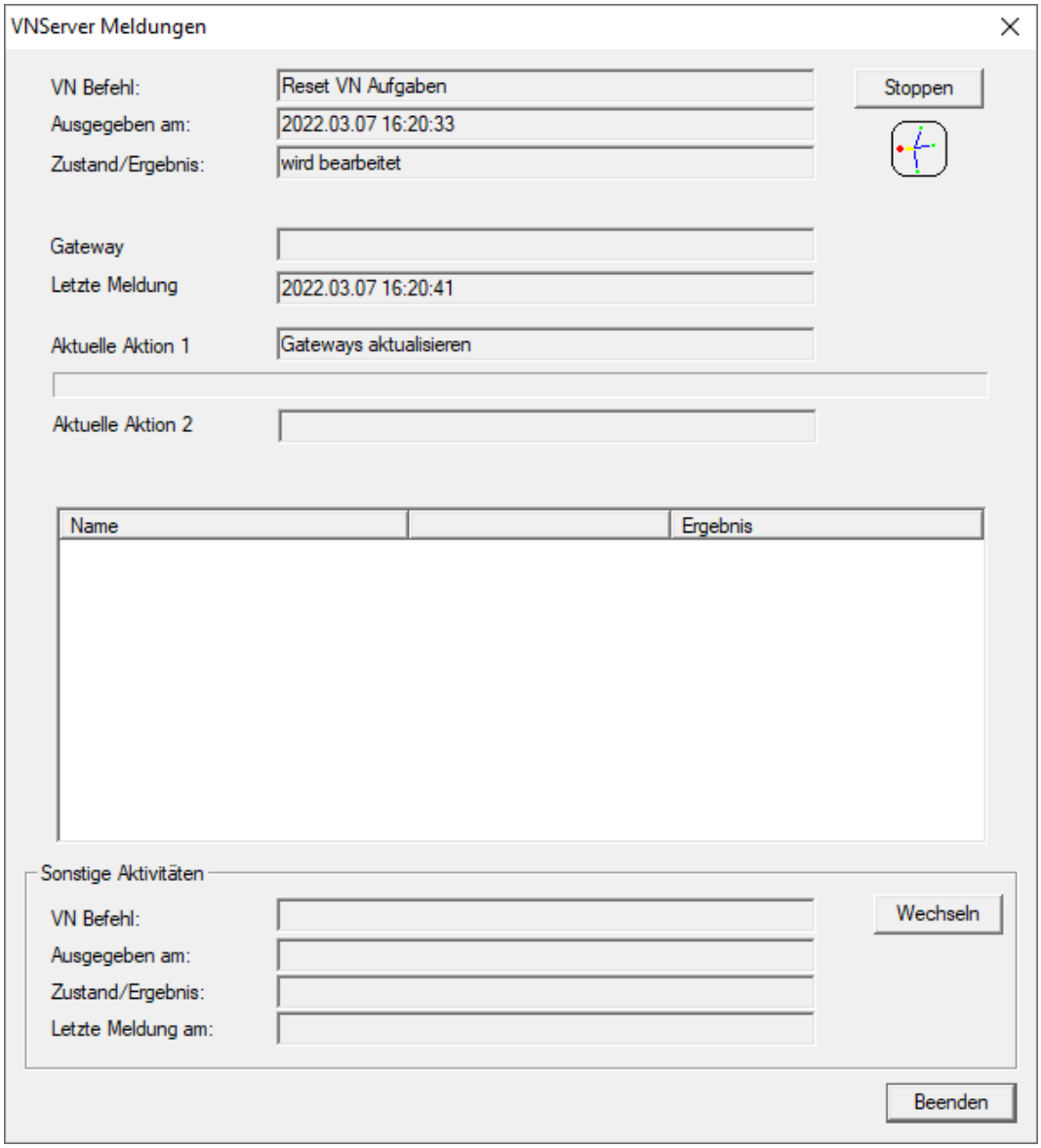
10.5.2.7 Resetting tasks in the virtual network

You can also reset tasks that you have exported to the virtual network.

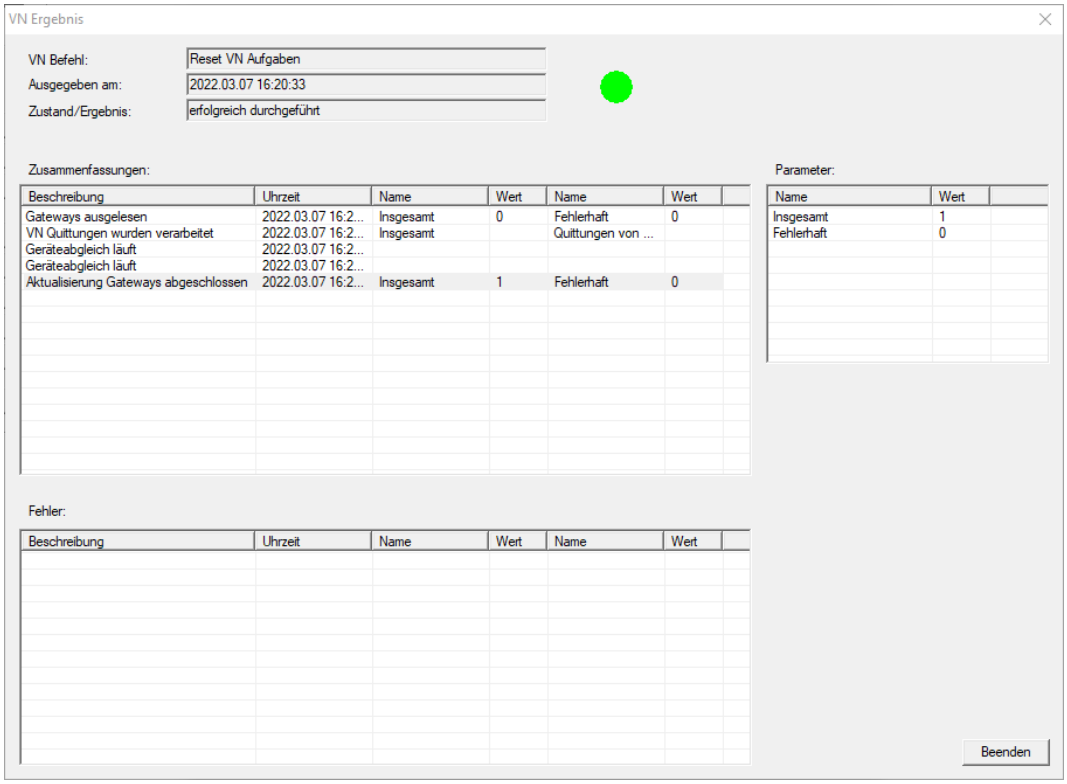
1. Use | Programming | - Virtual Network to select the Reset VN tasks entry.
   ↳ Reset prompt will open.



2. Click on the Yes button.
   ↳ Gateways are programmed to reset the exported tasks.



↳ Exported tasks are reset.

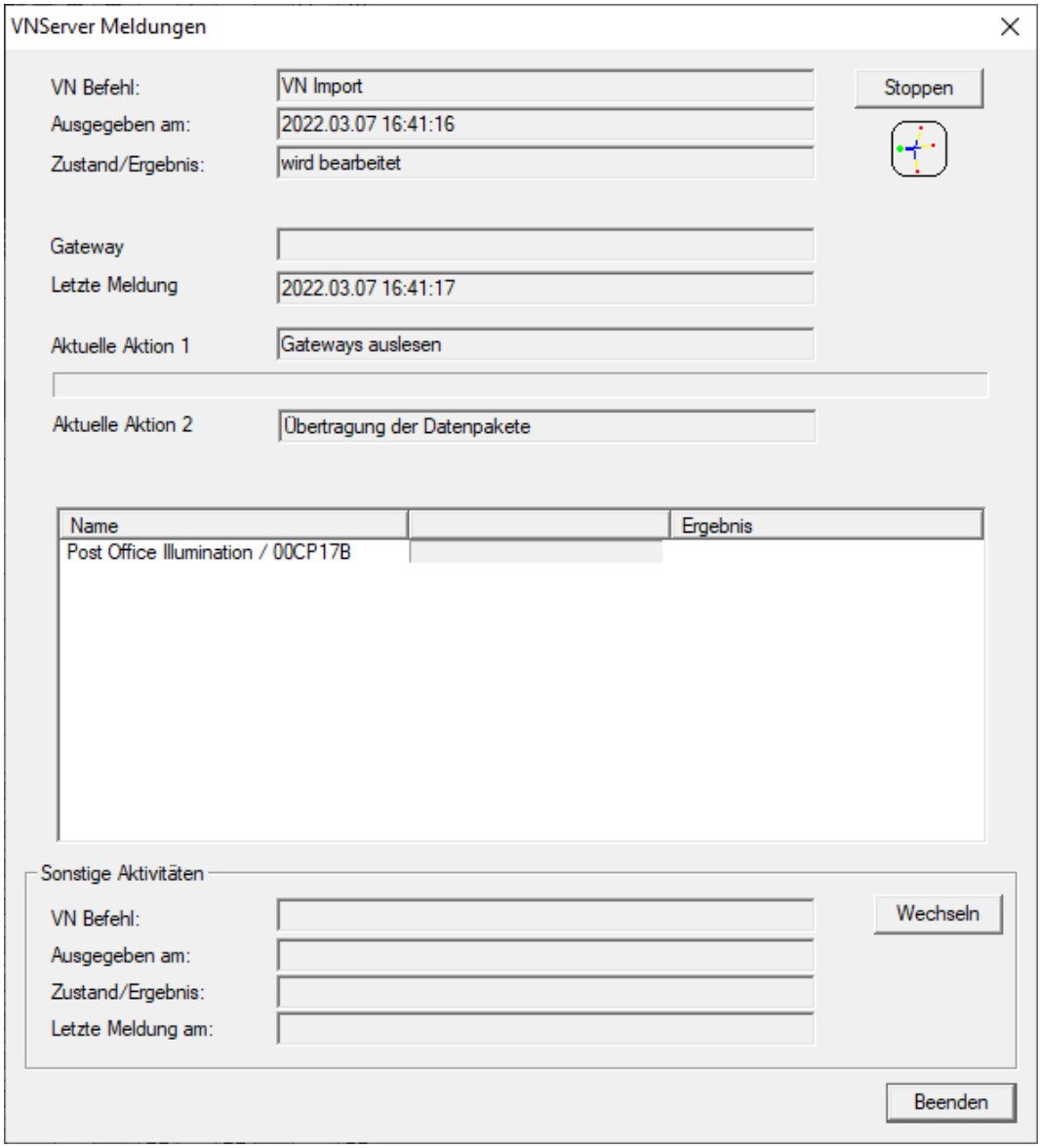


You can export the required tasks to the virtual network again (see *Exporting authorisation changes [▸ 234]*).

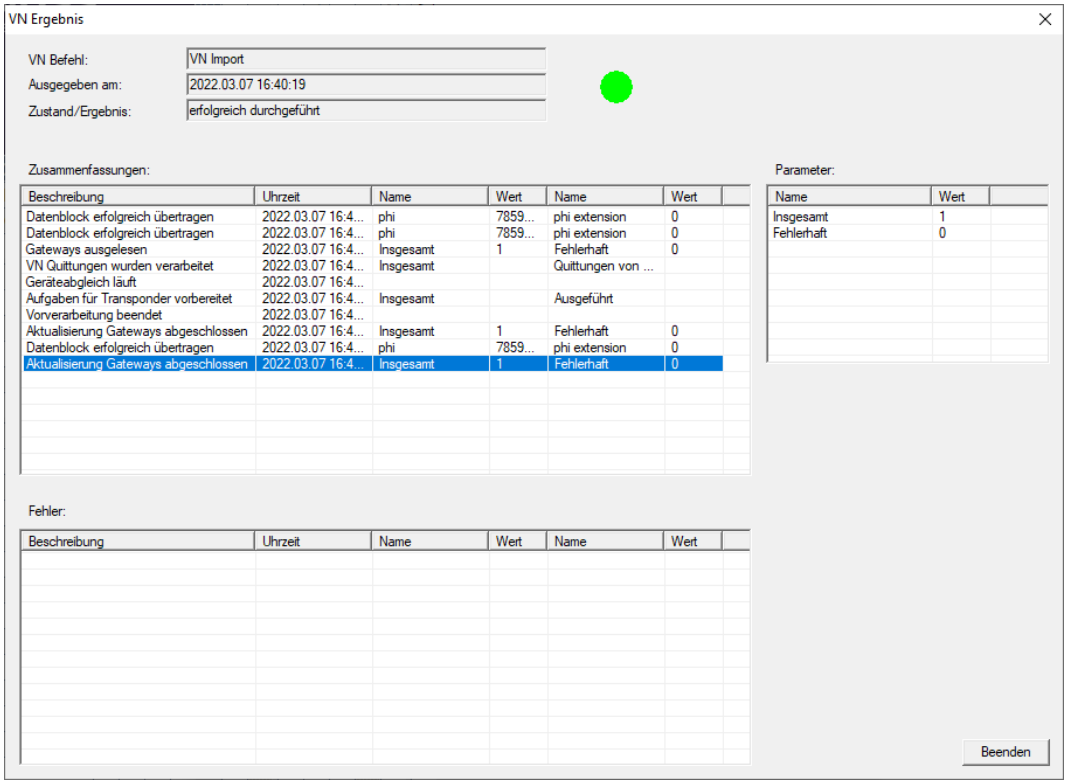
10.5.2.8 Importing authorisation changes

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.



↳ Import report is now displayed.



2. Click on the Exit button.

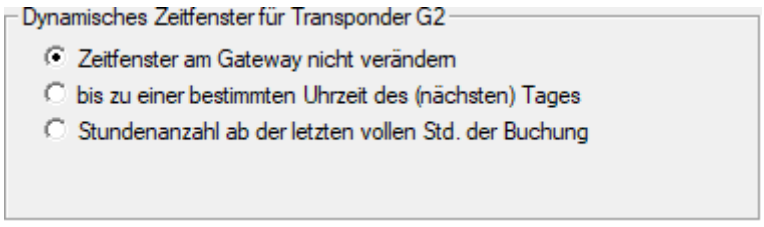
You can now check the status of the tasks (see *Status of the tasks in the virtual network (SREL2.G2) [▸ 240]*).

10.5.2.9 Tips on VN

Time budgets

It is important to have all transponders book at short, regular intervals so that changes are quickly distributed offline in the locking system. Time budgets can be used for this purpose.

The "Dynamic time window for G2 transponder" section in the locking system properties offers you the option of imposing a time budget on transponders. This means that a person can be required to load the identification medium regularly at the gateway. If they do not, the identification medium is blocked for this locking system.



Automatic import/export

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.

10.6 Read locking device

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

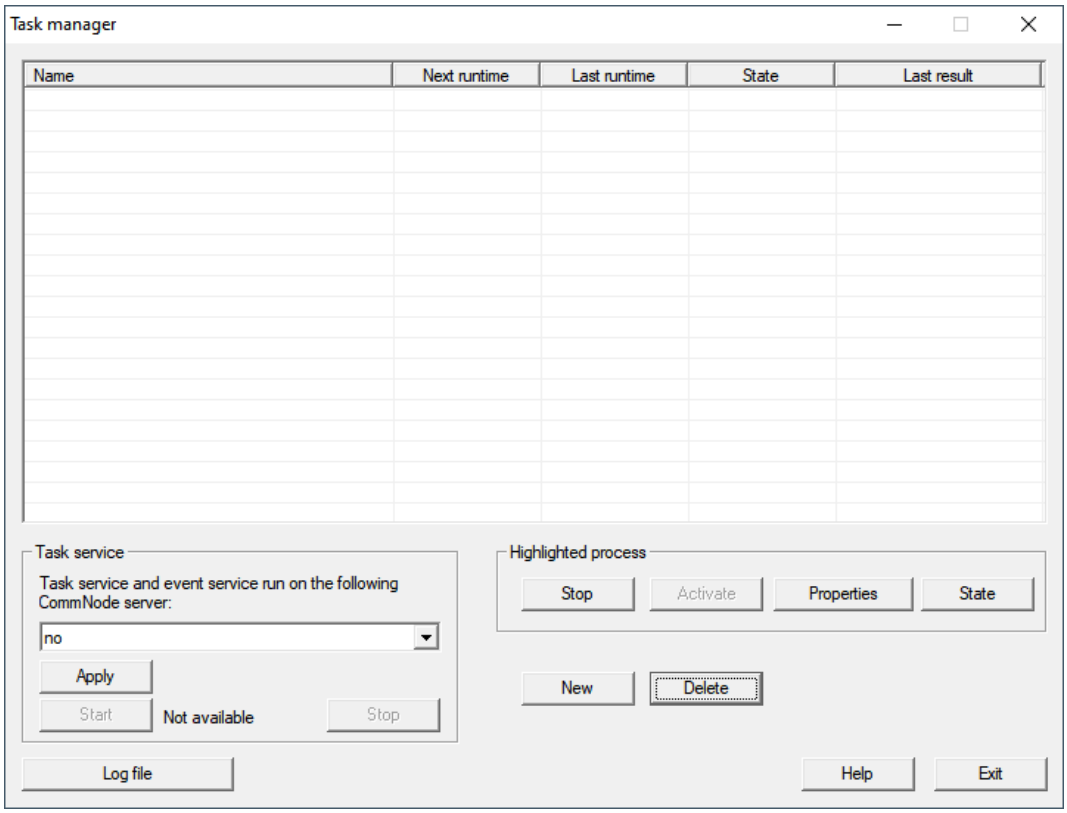
You can even automate this with the Task Manager.

You can then further process the information in LSM, for example by means of warnings and messages (see *Warning monitor [▸ 111]* and *Manage warnings [▸ 108]*).

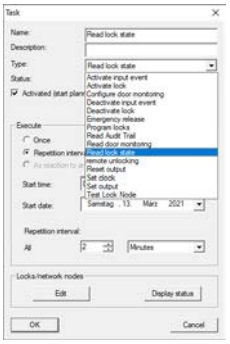
✓ LSM open.

✓ Locking devices to be read out programmed and networked (see *Creating a WaveNet radio network and incorporating a locking device [▸ 190]*).

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.

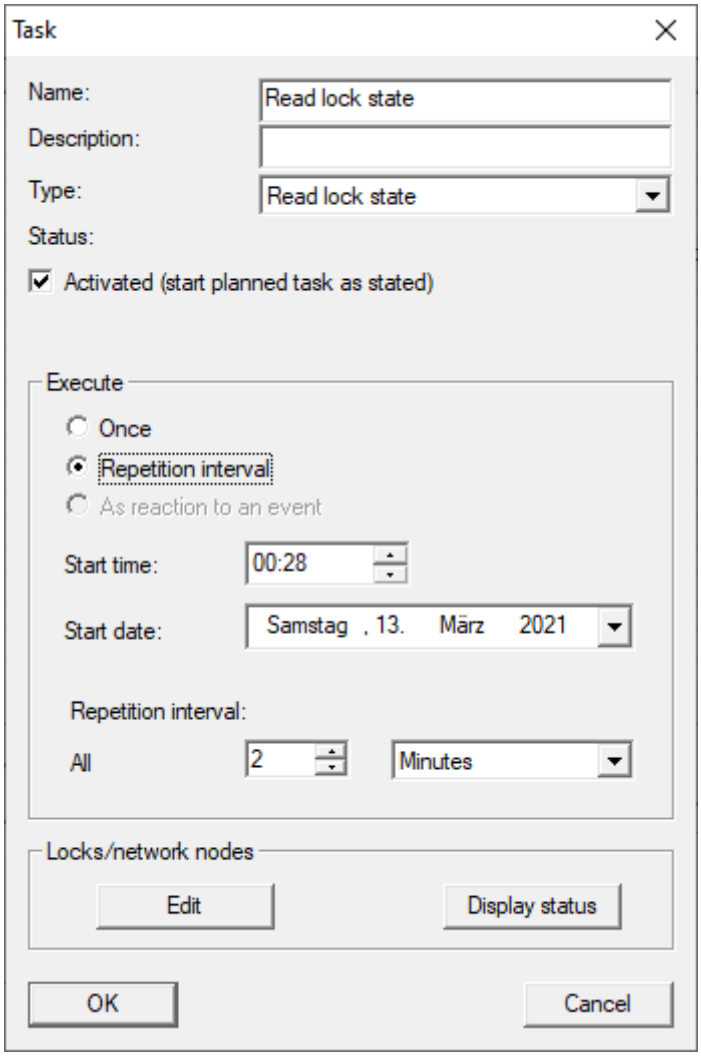


5. Select in the area "Execute" the option ◉ Repeat interval off.
6. Set the desired interval.

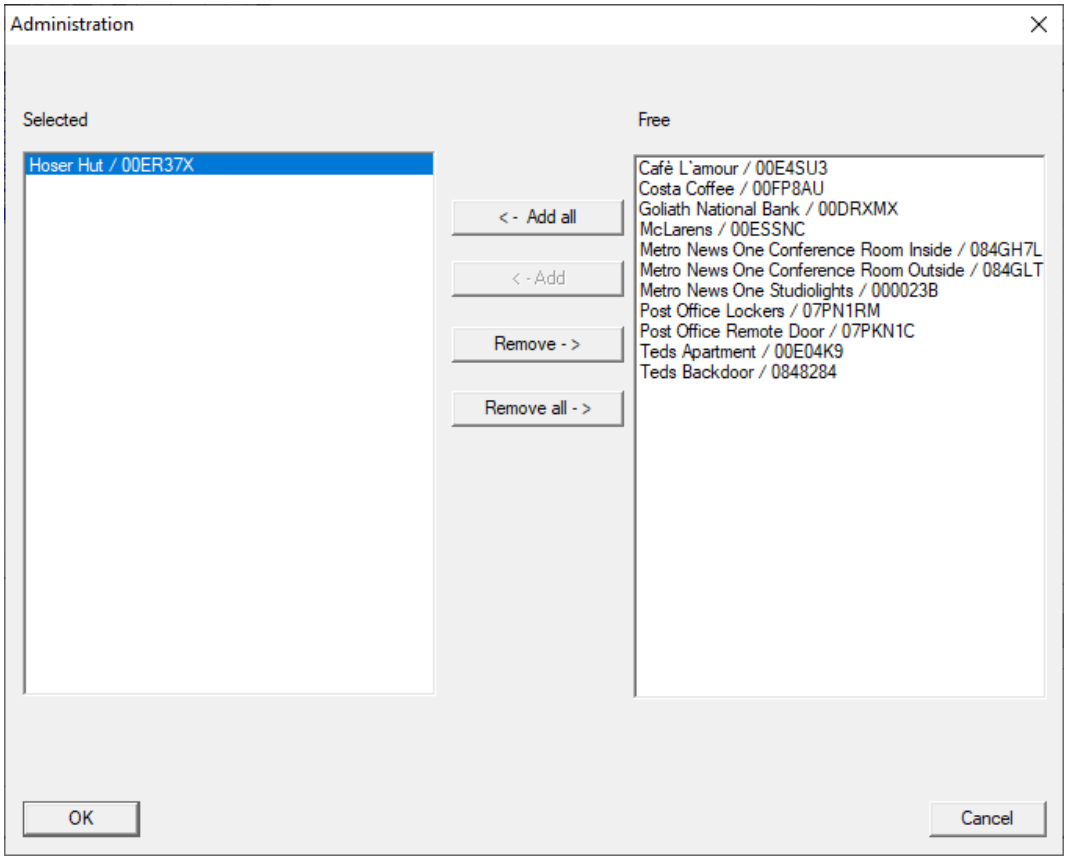
NOTE

Effect of the repeat interval on the battery run time

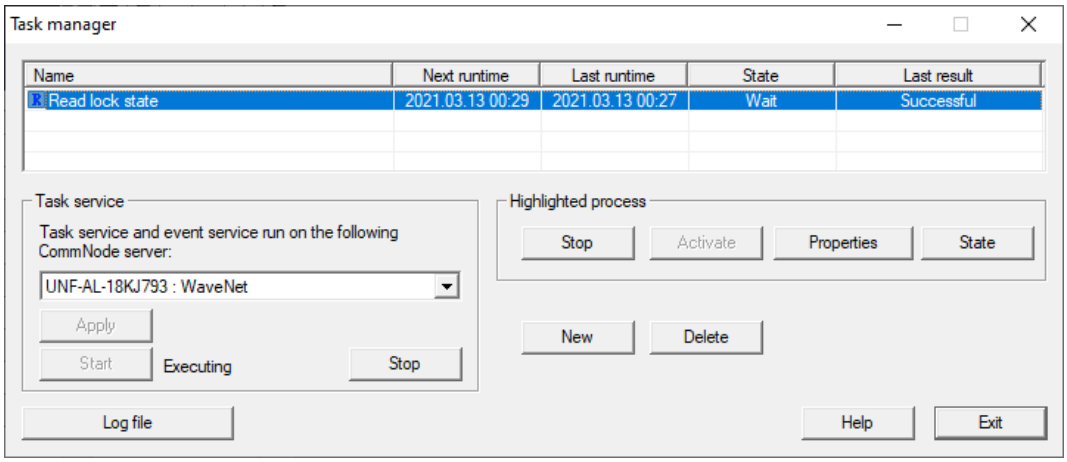
The more often you read the locking device, the more often the locking device is woken up from the energy-saving standby mode. Battery life may therefore be shorter.



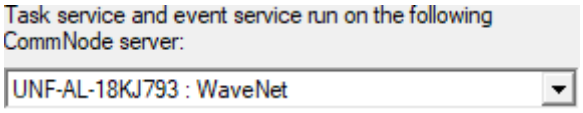
7. Click in the area "Locks/network nodes" on the button Edit .
   ↳ Windows "Administration" launches.



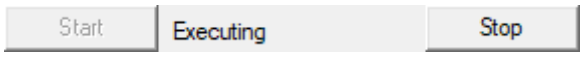
8. Select the locking devices you want to read.
9. Then move the locking devices using the button Add into the left column.
10. Click on the OK button.
    ↳ Windows "Administration" closes.
11. Click on the OK button.
    ↳ Windows "Task" closes.
    ↳ Task is listed in the Task Manager.



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.

11. Glossary & abbreviations

Individual terms are explained in more detail below. The explanations are easy to understand, but may not contain all details.

Term	Abbreviation	Explanation
Advantage Database Server	ADS server	Essential server service required to operate LSM Business and Professional.
CSV file		Standard file format for importing and exporting data, such as employee lists and locking systems.
DoorMonitoring	DM	Option for locking components which reports key door status properties, such as 'door closed' and 'double locked', to the LSM software.
Freeze mode		When batteries reach a critical level, locking devices switch to freeze mode to allow the door to be opened one more time.
Protocol generation G1	G1	First protocol generation allowing locking devices and ID media to communicate.
Protocol generation G2	G2	Second protocol generation, which adds a number of convenience functions.
Lightweight Directory Access Protocol	LDAP	Network protocol to access and change information. LDAP can be used to upload employee data directly into the LSM software, for example.
Locking Data Base Software	LDB	The preceding version of the LSM software.
Lock ID	LID	Identifies the locking device within the locking system. (Can be compared to a car registration)
Local Operating Network	LON network	Local Operating Network (LON) is an older standard, which is/was mainly used for building automation.

Term	Abbreviation	Explanation
Locking System Management	LSM	Current software allowing flexible management of SimonsVoss locking components.
Matrix		The matrix offers a clearly arranged view, showing which particular ID media are entitled to use specific locking devices.
MIFARE		MIFARE is a world standard for one of the most widely used card systems. (Locking device is activated with 'passive cards')
Personal Digital Assistant	PDA	Small computer roughly the size of a smartphone. A PDA can be used as a portable device to programme active G1 locking components.
Physical Hardware Identifier	PHI	The PHI number is imprinted on SimonsVoss components and stored in its internal memory. This number is fixed and cannot be changed.
Profile cylinder	PC	A profile cylinder is the most widely used variety of security lock and a type of locking cylinder.
Router (Central-Node)		Special routers are used to address suitably equipped locking devices over the network.
SMART.SURVEIL		SMART.SURVEIL is an independent monitoring program. It can be run on computers without LSM software and requires a free user client. (From LSM 3.4 SP1)
Transponder ID	TID	Identifies the transponder within the locking system. (Can be compared to a car registration)
Virtual network	VN	A 'virtual network' can be used to enjoy a variety of advantages offered by networks without special routers.

Term	Abbreviation	Explanation
Access Control	ZK	SimonsVoss components with an AC function log all accesses (or 'bookings') in the locking system.

12. 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.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION