LSM 3.5 SP3 Basic Smart User Guide

Manual

20.04.2023

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:

- *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 (ANSI Z535.6)	Possible immediate effects of non-compliance
DANGER	Death or serious injury (likely)
WARNING	Death or serious injury (possible, but unlikely)
PRUDENCE	Minor injury
IMPORTANT	Property damage or malfunction
NOTE	Low or none

WARNING

Blocked access

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

Blocked access through manipulation of the product

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

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

NOTE

Intended use

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

- Do not use SimonsVoss products for any other purposes.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

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

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

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

1.2 Product-specific safety instructions

PRUDENCE

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
- .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
  - Windows 8.1 Professional, 64-bit
  - Windows 8 Professional, 64-bit

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 [▸ 18]*.

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 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

3 Basic functions

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

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

3.1 Add new locking system

✓ Installation has been completed correctly and a backup has been created.

1. Select *Edit/New locking system* in the menu bar.
2. Define the required locking system options.
   ↳ Select a colour from "Use as common locking level" for the common locking levels. *Common locking levels act as additional levels to existing standard locking systems. See* Common locking level.
3. Click on the "Apply" button.
4. Click on the "Finish" button.

3.2 Add new transponder group

✓ A locking system has already been added.

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

3.3 Add new transponder

✓ A locking system has already been added.

1. Select *Edit/New transponder.*
2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
3. Click on the "Save & next" button.
4. Click on the "Finish" button.

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

✓ The transponder has already been created and a transponder group has been added.

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

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

3.5 Add new area

✓ A locking system has already been added.

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

3.6 Add new locking device

✓ A locking system has already been added.

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

3.7 Add PIN code Keypad

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

3.7.1 Configure PIN code Keypad

Changing the master PIN

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

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

NOTE

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

Programming a user PIN

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

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

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

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

3.7.2 Add PIN code Keypad to the locking plan

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

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

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

3.7.3 Programme PIN code Keypad

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

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

3.8 Assign locking device to an area

✓ The locking device has already been created and an area has been added.

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

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

3.9 Issue/withdraw authorisation

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

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

Observe the two views:

- **View/Doors and persons**

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

- View/Areas and transponder groups

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

3.10 Common locking level

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

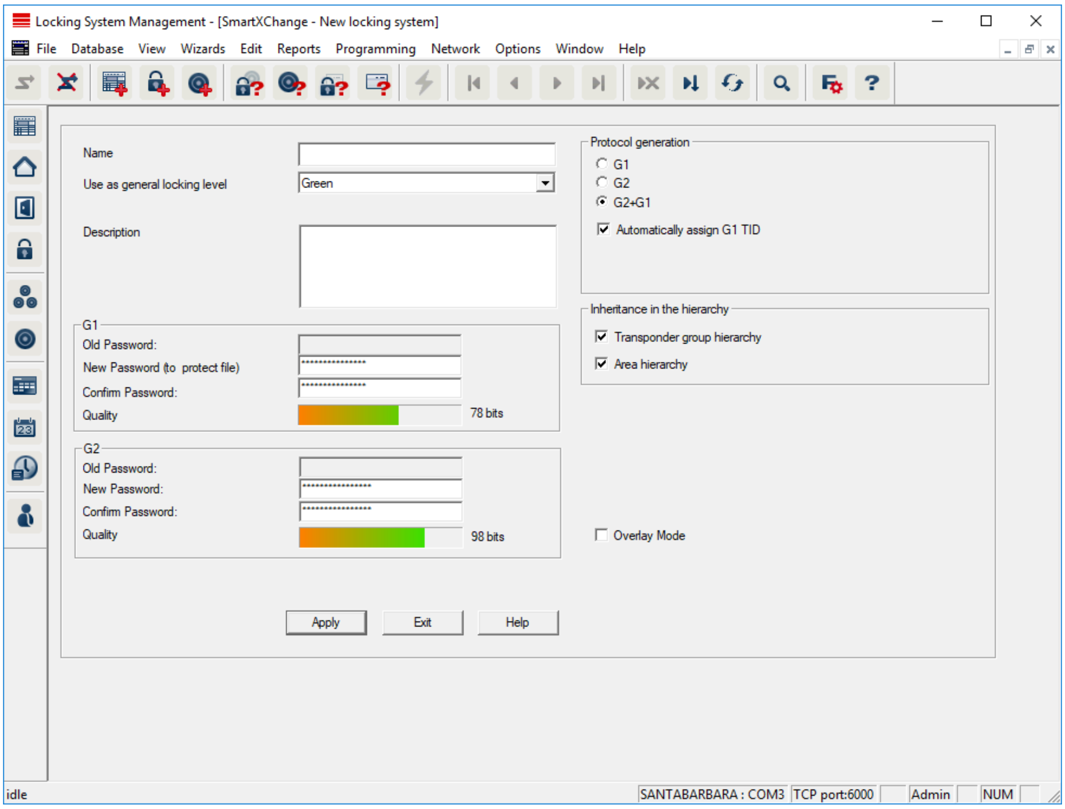
3.10.1 Add common locking level

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

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

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

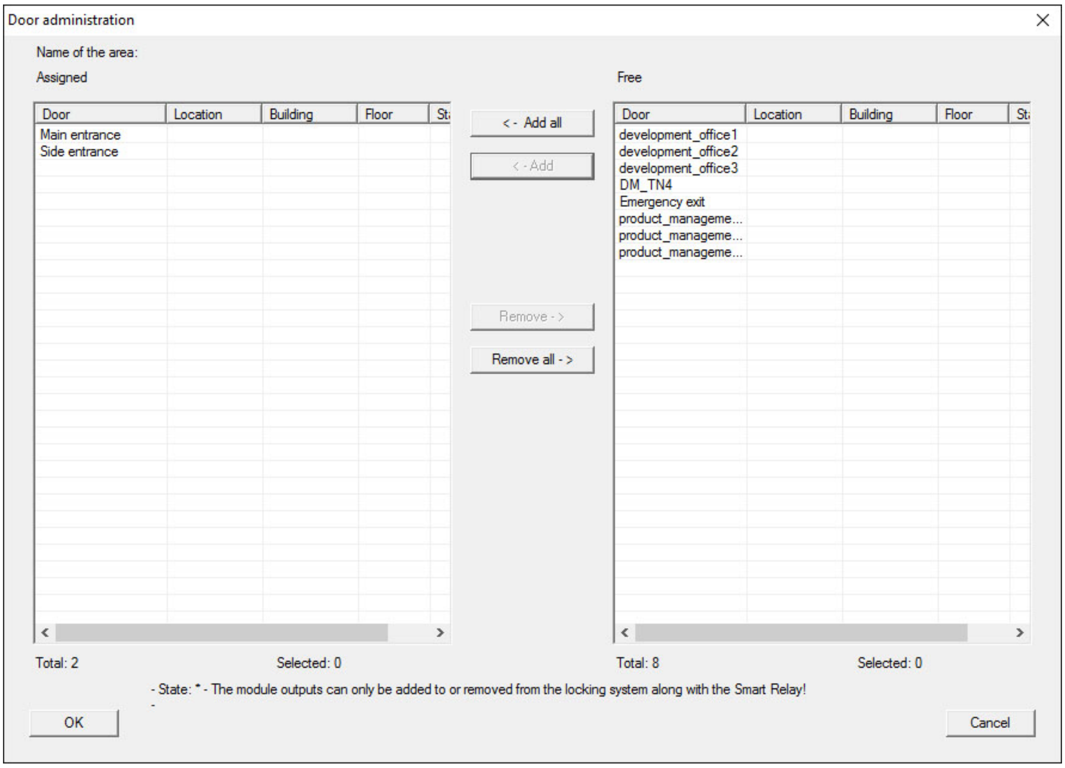
- Select any colour in "Use as common locking level".



3.10.2 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.



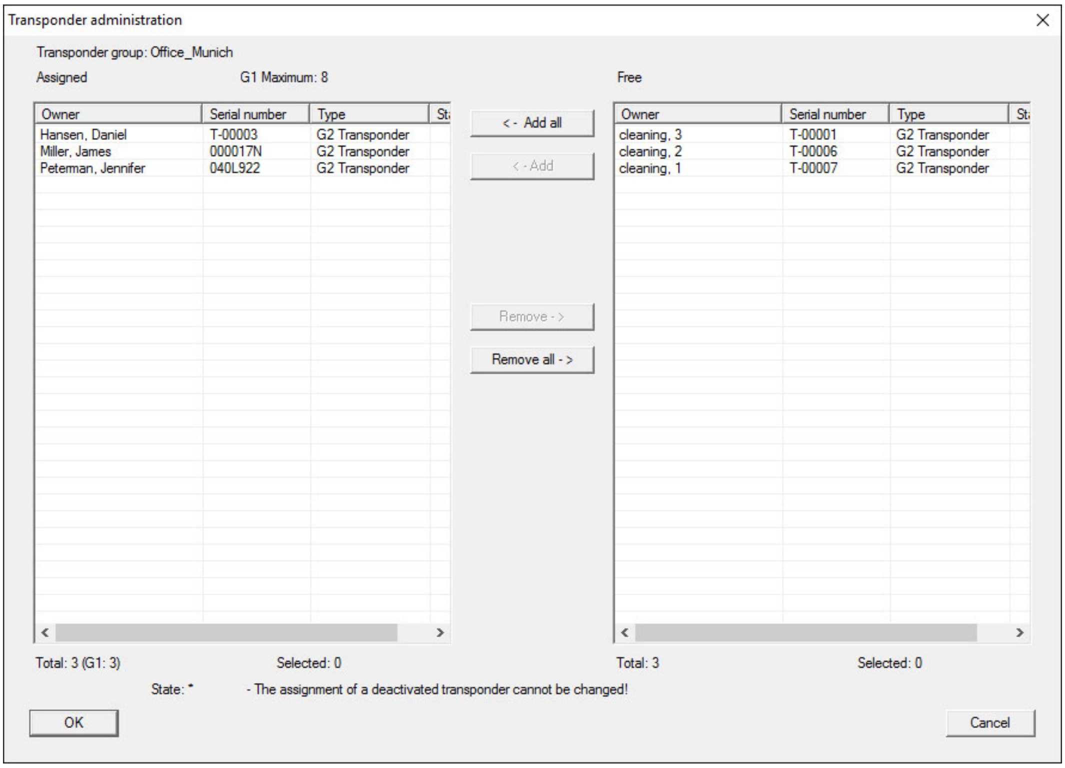
3.10.3 Link transponders

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.



3.10.4 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.

3.11 Create fire service transponders

✓ You have already created at least one locking system.

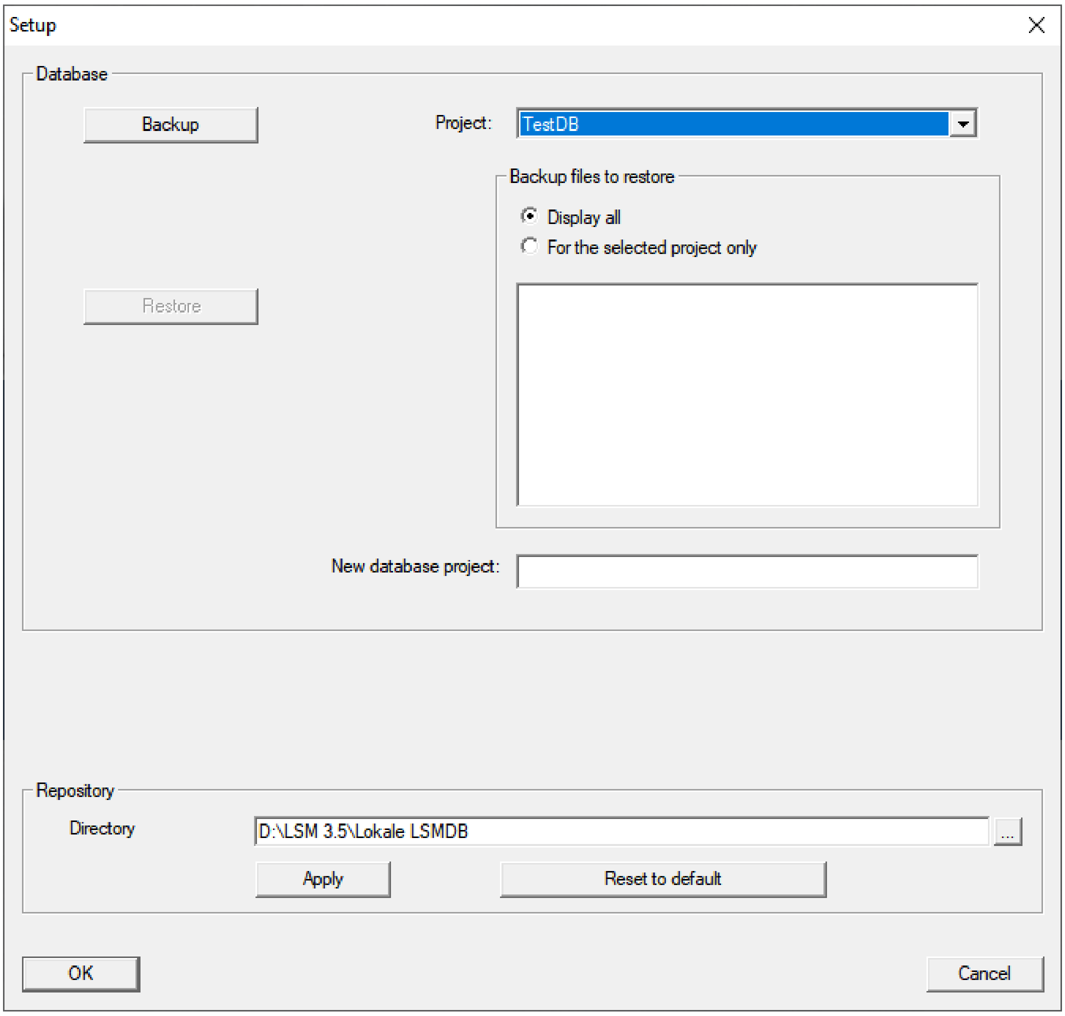
1. Create a new "red" common locking level, using *Edit/New locking system*, for example.
2. Add a new area, such as "All locking devices", and use "Door administration" to assign all the locking devices required to this area.

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.

3.12 Backing up the database manually

1. Log on as the Windows user who also manages locking system management.
2. Launch LSM.
3. Click the Setup button ( ).
   ↳ The setup opens.
4. Click the button Advanced.
   ↳ Window "Setup" opens.



5. Use the dropdown menu ▼ **Project:** to select your project.
6. Click the button Backup
   ↳ Backup is created.
7. Click on the OK button.
   ↳ Window "Setup" closes.
8. Copy the created backup (.zip) to a separate data carrier.

NOTE

The backup is saved to C:\ProgramData\SimonsVoss\Repository by default.

3.13 Working in compliance with data protection regulations GDPR

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

3.13.1 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:

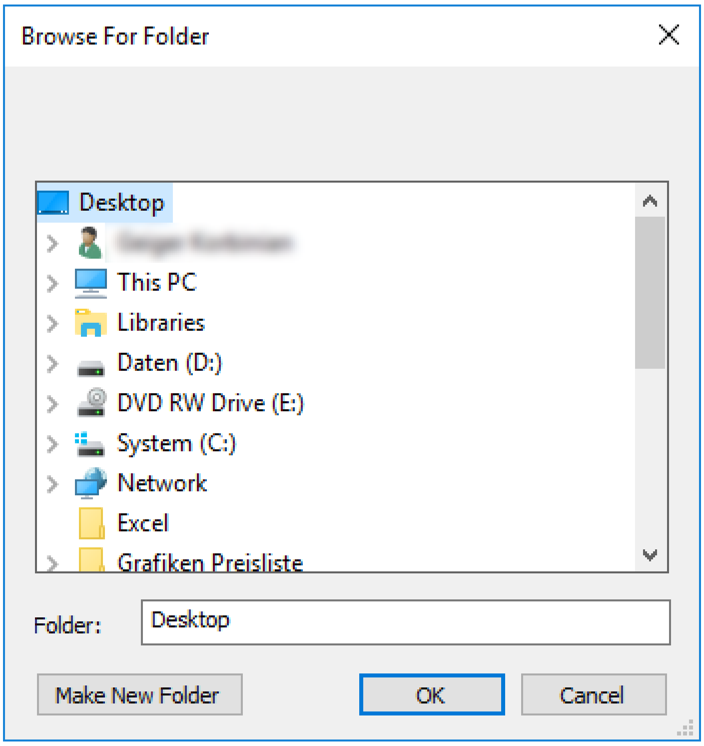
Person	This file contains personal data which can be used to identify the person (for example, surname, address or photo).
PersonHistory	This file contains the dates that the data record was created and erased.
PersonLog	This file contains different processing steps which have been performed on the person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

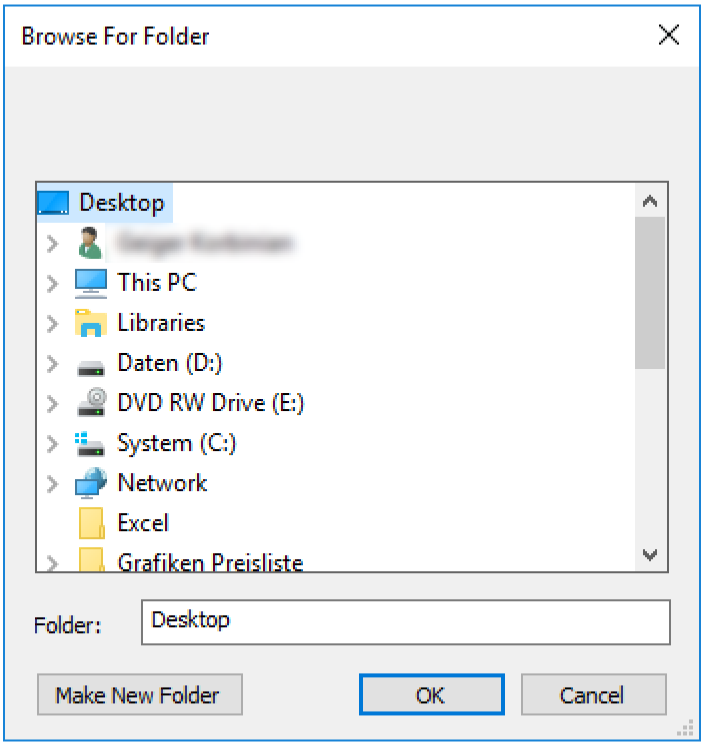
You can export the users' saved personal data as CSV files in the LSM software. Two files are generated during this process:

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.

3.13.2 Deleting Data

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

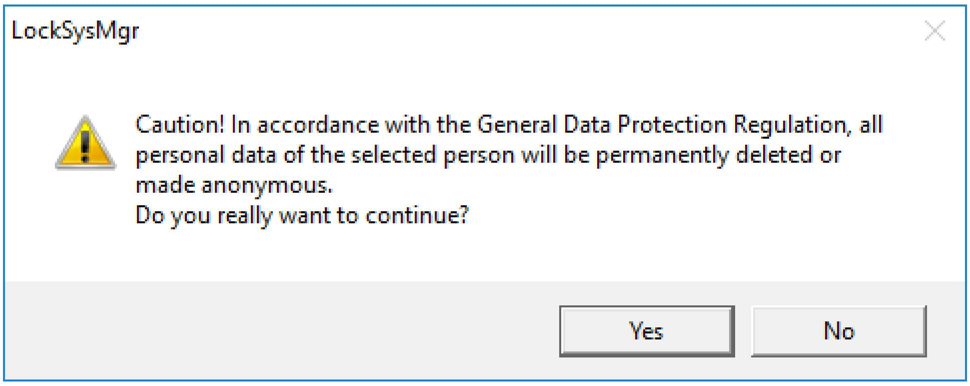
Persons

NOTE

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

✓ LSM open.

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



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

NOTE

Erasure of remaining data from previous deletions

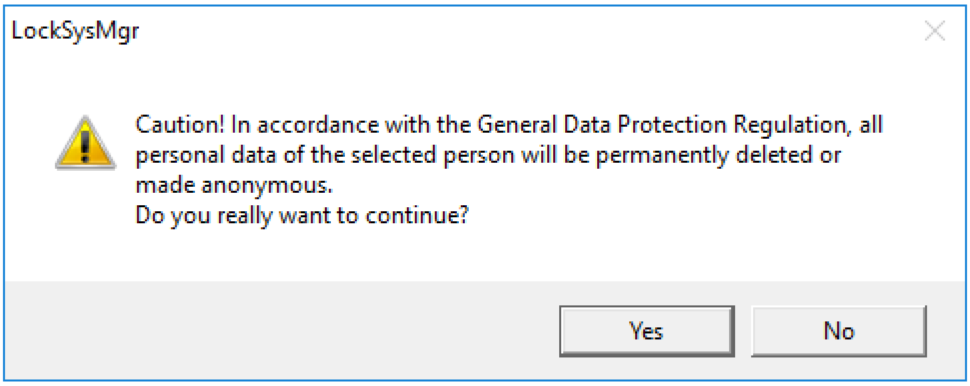
You can also use the button in the [Name] tab in the assigned identification media to erase personal data. Unlike erasure using the GDPR module, this button does not delete logs, which will remain in the system. This means that only a part of personal data is erased. People who are deleted in this way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

Users

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

✓ LSM open.

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



4. Click on the Yes button.

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

3.13.3 What personal data is stored in the software?

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

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

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

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

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

3.13.5 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, can be changed at will by the locking system administrator.

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

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

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

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

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

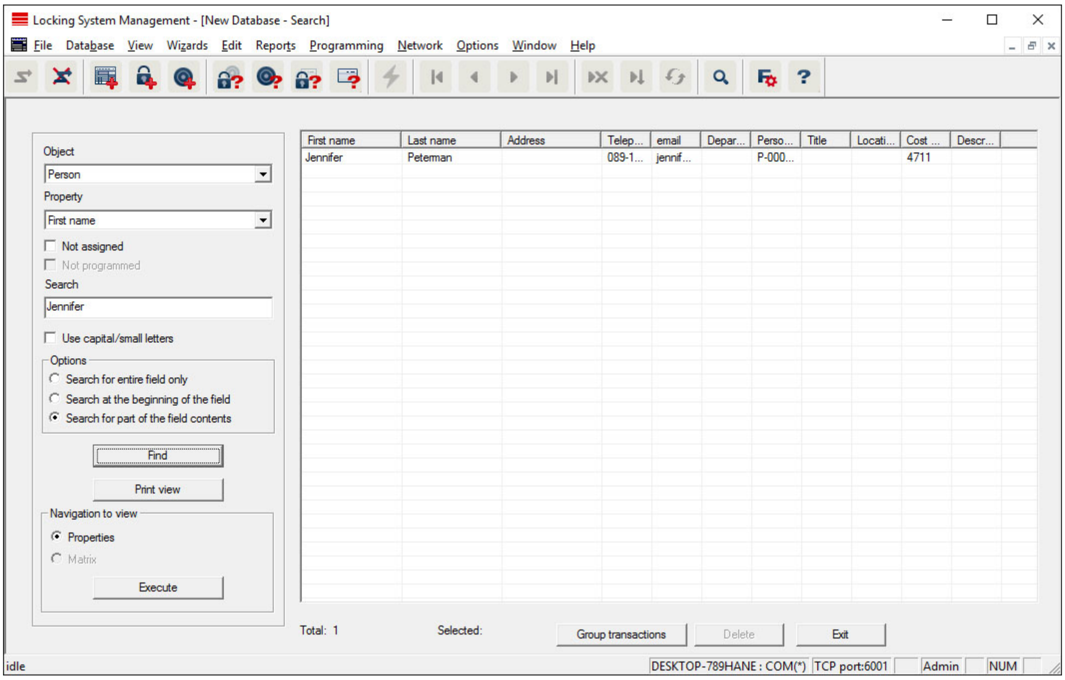
All collected data on a data subject can be made available as a copy by means of an export function (Art. 15 GDPR).

3.13.8 Can personal data be deleted from the software?

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

3.14 Search matrix

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



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

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

3.15 Execute group actions

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

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

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

NOTE

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

3.16 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 [▸ 29]*).

NOTE

Automatically recognise G2 cards

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

3.17 Programme locking device

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

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

Ensure that you select the right programming device.

NOTE

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

First transponder activation rejected after initial programming of AX products

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

3.18 Programme using LSM Mobile

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

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

3.18.1 With laptop, netbook or tablet PC

This how you programme with the help of LSM Mobile:

- ✓ There are components in the LSM software which require programming.
- ✓ Initial programming has already been completed on the components requiring programming.
- ✓ LSM Mobile has been correctly installed on the mobile device. The version numbers are identical.
- ✓ The drivers have been correctly installed in the SMARTCD.G2 and SMARTCD.MP programming devices (depending on requirements).

1. Select *Programming/LSM Mobile/Export to LSM Mobile/LSM Mobile PC*.
2. Follow the instructions in the LSM software and export the programming tasks in a file.
3. Launch LSM Mobile on the mobile PC and import the file with the programming tasks into LSM Mobile.
4. Follow the instructions in LSM Mobile.

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

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

3.19 Resetting components

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

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

1. Use *Programming/Read components* to read the components concerned.
2. Select the "Reset" button to start the reset process.
3. Follow the instructions in the LSM software.
   ↳ If necessary, you will be requested to enter the locking system password or select the dataset to be deleted.

3.20 Replace defective locking device

Locking devices may become damaged or contain a defect.

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

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

4. Carry out a programming process on the replacement locking device.
5. Fit the replacement locking device into the door and check that it functions correctly.

NOTE

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

NOTE

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

3.21 Block transponders

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

- *Block transponder permanently and create replacement transponder [▸ 29]*
- *Block transponder temporarily [▸ 33]*

NOTE

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

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

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

3.21.1 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.

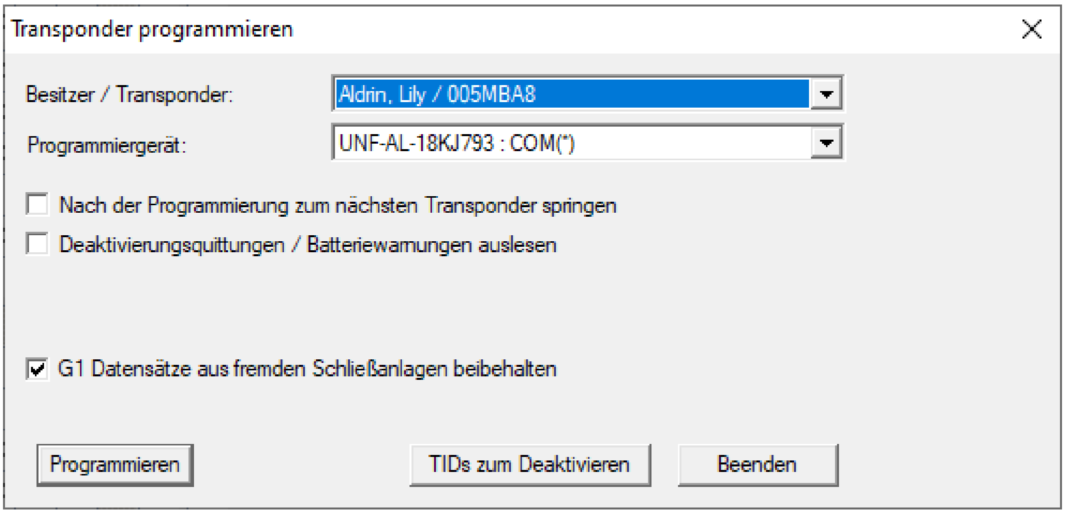
Programme the TIDs to be disabled directly

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

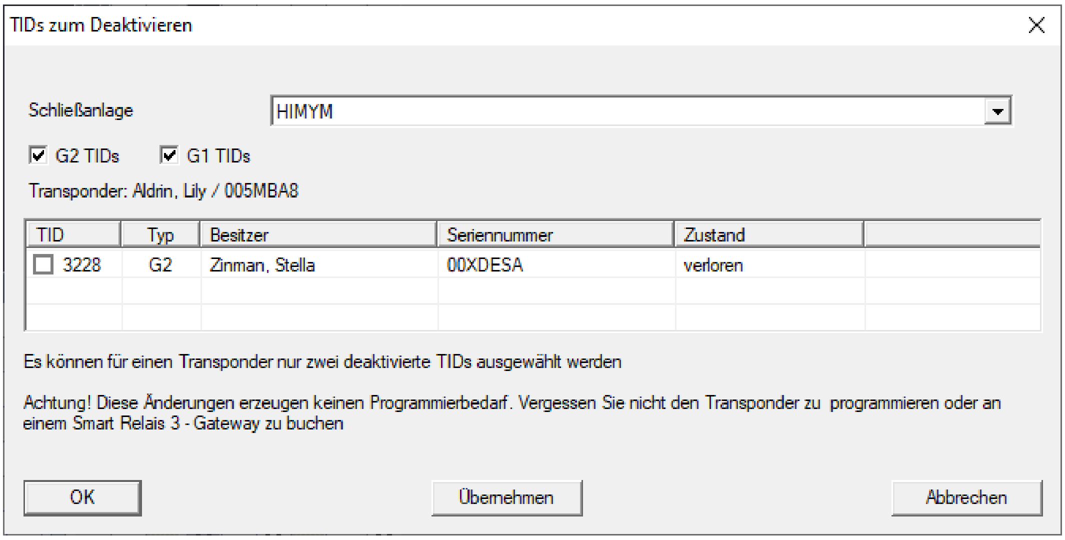
✓ The transponder is physically available.

✓ 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.

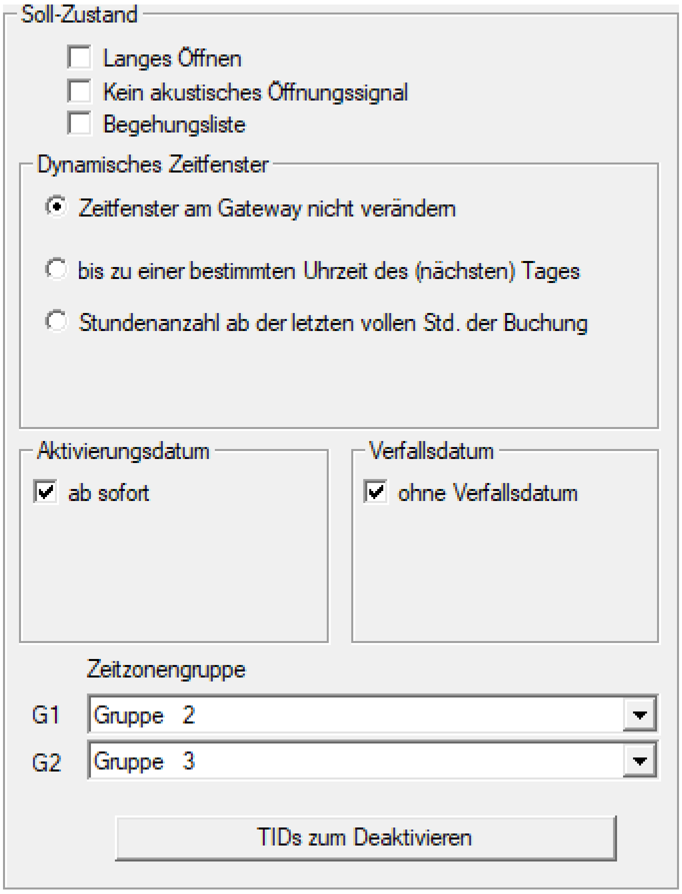
↳ The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

Add the TIDs to be blocked to the properties

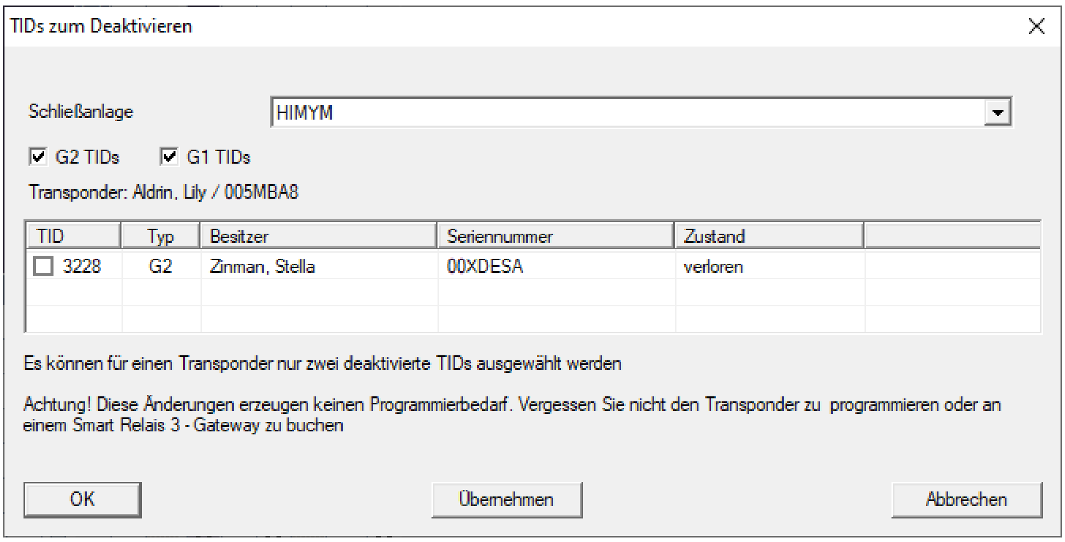
The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

✓ 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.



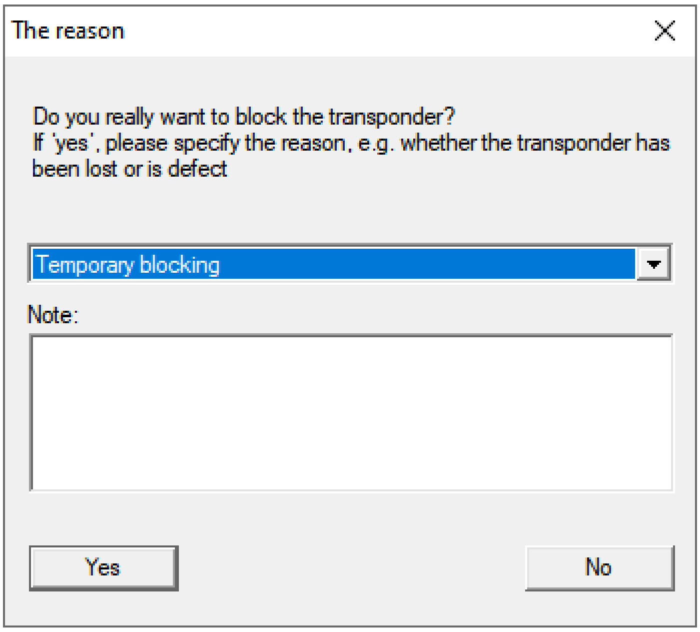
3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.

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.

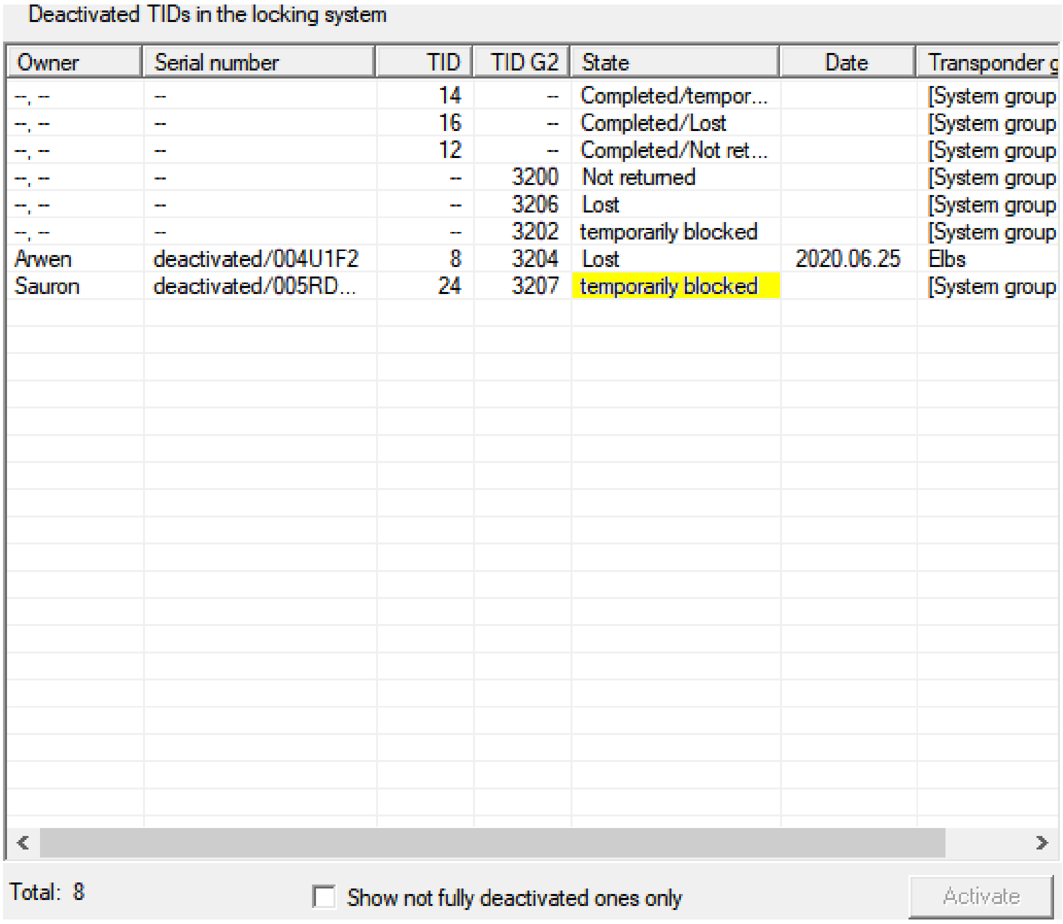
3.21.2 Block transponder temporarily

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].


Deactivated TIDs in the locking system

Owner	Serial number	TID	TID G2	State	Date	Transponder g
--, --	--	14	--	Completed/tempor...		[System group
--, --	--	16	--	Completed/Lost		[System group
--, --	--	12	--	Completed/Not ret...		[System group
--, --	--	--	3200	Not returned		[System group
--, --	--	--	3206	Lost		[System group
--, --	--	--	3202	temporarily blocked		[System group
Arwen	deactivated/004U1F2	8	3204	Lost	2020.06.25	Elbs
Sauron	deactivated/005RD...	24	3207	temporarily blocked		[System group

Total: 8 Show not fully deactivated ones only Activate

3.22 Check and evaluate the battery level in the locking devices

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

Transmitting battery levels to the LSM software

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

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

Importing battery levels by reading the locking device

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

Transmitting battery levels to the LSM software using LSM Mobile

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

Displaying battery levels

Basic procedure for all LSM versions:

✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.

1. Double-click on a locking device to display the locking device properties.
2. Select the "Status" tab.
3. The battery level will be displayed in the "Status at last readout".

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

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

✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.

1. Select from the "Reports/Building structure" menu bar.
2. Select the "Locking devices with battery warnings".
3. Click on the "Display" button.

Displaying battery warnings automatically in LSM Business

Create a warning which displays battery warnings directly.

✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.

1. Selecting from the "Reports/Warnings" menu bar
2. Create a new warning using the "New" button.
3. Create the warning as you wish. Select "Locking device battery warning" as the type.
4. Do not forget to assign the locking devices concerned to this warning. The "Locking devices" field should not be empty.
5. Click on the "OK" button to confirm the new warning.
6. Click on the "Exit" button to close the dialogue.

3.23 Reset storage mode in G1 locking devices

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

3.24 Reset freeze mode in G2 locking devices

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

✓ Battery replacement identification medium added (see Special functions/G2 battery replacement transponder).

✓ Battery replacement identification medium programmed.

1. Activate the Battery replacement identification medium on the locking device.
   ↳ Freeze mode is deactivated.
2. Activate any authorised identification medium.
   ↳ Locking device opens.
3. Change the battery.
4. Activate the Battery replacement identification medium on the locking device.
   ↳ Freeze mode is deactivated.
5. Use any authorised identification medium to verify whether the locking device functions correctly.

↳ Freeze mode is reset.

IMPORTANT

Locking device failure due to misuse

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

3.25 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.

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

Configure AdminAL and permit reading of access lists

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

Remove rights to read access lists from Admin

NOTE

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

1. Use the "AdminAl" user name to log on to the project.
   - ↳ The default password in LSM BASIC is "system3060".
   - ↳ Change this password immediately.
2. Select "Edit/User group" to open user group administration.
3. Use the navigation arrow to scroll to the "Admin" user group.
4. Deactivate the "Access lists administration" and "Administer access lists" roles.
5. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.
   - ↳ Configuration is now complete. Only the "AdminAL" user account may read or view access lists and physical access lists from now on.

3.25.1 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

3.26 Card management

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

IMPORTANT

MIFARE DESFire recommended

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

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

NOTE

Different templates for AX products

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

3.26.1 Change configuration

You have two options for using cards.

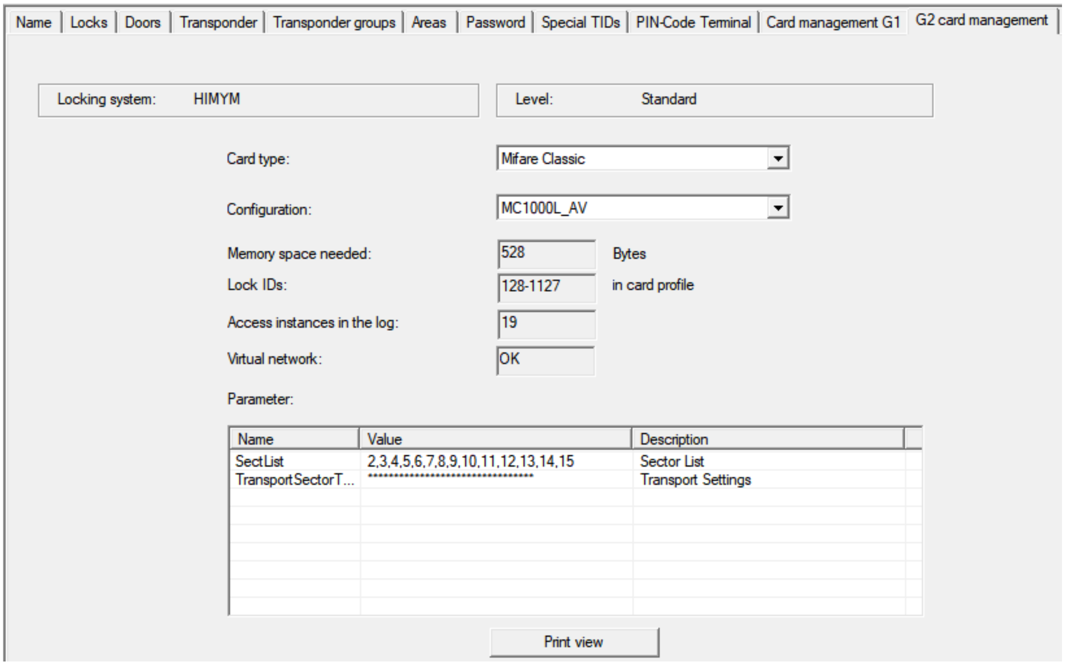
- You can use cards that have already been used.
- You can use new cards.

In both cases, enter the card type, the configuration and, if necessary, the sectors to be described (see *Overview [▸ 40]*).

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).

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

7. Click on the Apply button.

↳ You have changed the configuration.

3.26.2 Overview

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

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

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MD1000 L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	✓
MD3200 L_AV	G2	128-3212 7	32000	470	n.a. (DES-Fire)	7000	✓
MD2400 L_AV	G2	128-2527	2400	34	n.a. (DES-Fire)	830	✓
MD3650 L_AV	G2	128-3777	3650	2	n.a. (DES-Fire)	830	✓

4 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