SimonsVoss manual 3: practical manual

03.2017

SimonsVoss manual 3:

practical manual

Contents

SimonsVoss manual 3:

practical manual

SimonsVoss manual 3:

practical manual

1 General information

This manual uses an easy-to-understand example to show you how to use the LSM software. This manual is intended to show how individual SimonsVoss components can be programmed, combined and managed.

Other documents are available to supplement this manual:

- LSM software manual

  This manual describes the functions in the 3.3 SP1 Locking System Management software
- WaveNet manual

  Describes how to use the WaveNet radio network.
- LSM update manual

  Describes the update process for previous versions.

1.1 Safety instructions

⚠ WARNING

Access through a door may be blocked due to incorrectly fitted or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of incorrect installation, such as blocked access to injured persons or those at risk, physical damage or any other losses.

⚠ CAUTION

You must observe the warnings in the instructions for use for the individual SimonsVoss components.

⚠ CAUTION

The products/systems described in this manual may only be operated by persons who are qualified to perform the related tasks. Qualified staff are capable of identifying any risks associated with handling these products/systems and avoiding potential hazards thanks to their knowledge and skills.

NOTICE

The locking system password is an essential integral part of the security concept for the whole system. You must take care to ensure that the locking system password is kept in a safe, secure place and can be consulted at any time. Losing the locking system password may not only cause significant impairment to locking system operation, but can also lead to a greater security risk.

NOTICE

SimonsVoss Technologies GmbH reserves the right to make changes to the product without prior notification. For this reason, descriptions and illustrations in these documents may differ from the latest versions of products and software. The original German version should be taken as a reference in cases of doubt. Errors and spelling mistakes excepted. You can obtain more information about SimonsVoss products at: www.simons-voss.com

NOTICE

You should dispose of batteries in compliance with local and national regulations.

1.2 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, or 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.

1.3 Information on the manual

This manual uses an imagined example to describe how SimonsVoss locking components can be installed, used and managed.

NOTICE

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.

2 OFFLINE applications

2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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**

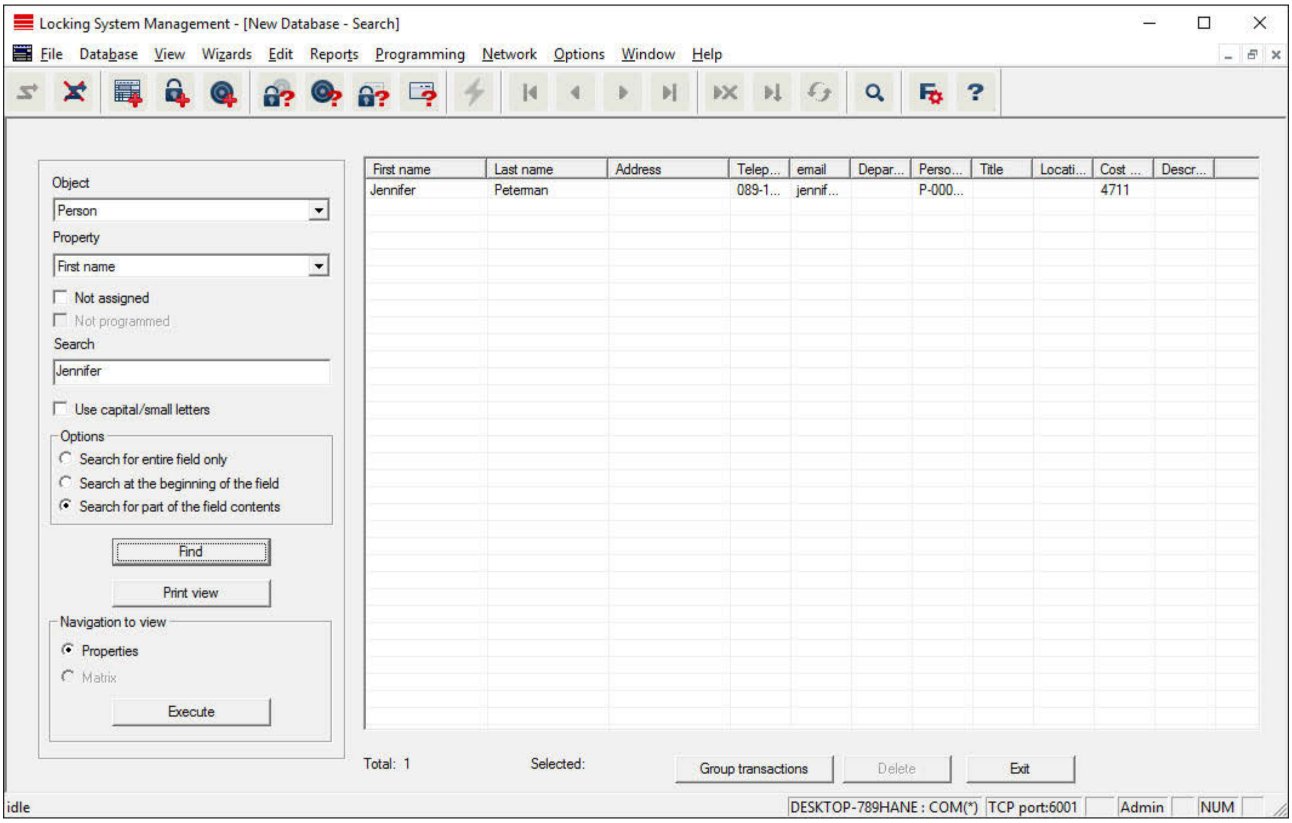
  In this view, the authorisations are changed for entire groups.

2.9 Search matrix

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

SimonsVoss manual 3:

practical manual



Object: Person

Property: First name

□ Not assigned

□ Not programmed

Search: Jennifer

□ Use capital/small letters

Options

○ Search for entire field only

○ Search at the beginning of the field

● Search for part of the field contents

Navigation to view

● Properties

○ Matrix

First name	Last name	Address	Telep...	email	Depar...	Perso...	Title	Locati...	Cost ...	Descr...
Jennifer	Peterman		089-1...	jennif...		P-000...			4711	

Total: 1 Selected:

idle DESKTOP-789HANE : COM(*) TCP port:6001 Admin NUM

✓ 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.

2.10 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.

NOTICE

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

2.11 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.

2.12 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. In the case of active locking devices, only the locking device to be programmed may be in the immediate area surrounding the programming device!

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

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

✓ Locking devices (or areas) and transponders (or transponder groups) have already been created.

1. Click on *Edit/Time zone plan* in the menu bar.

⇨ An "empty time zone plan" will open up. If an existing time zone plan is displayed, click on the "New" button to create a new, empty time zone plan.

2. Fill out the "Name" and "Description" fields.
3. Select a public holiday list for your region if required. This is how to proceed if you wish to define one-time company holidays:

⇨ Click on the "... field" next to the holiday day drop-down selection.

⇨ Click on the "New holiday day" button.

⇨ Assign a name: e.g. "Company holiday 2017"

⇨ Newly defined holidays may contain a time period. The "Leave" field must be activated for this purpose. You can then enter a time period (From - To).

⇨ Select how the new holiday day should be treated: e.g. as "Sunday".

⇨ Click on the "Apply" button and then on the "Finish" button.

⇨ Click on the "Holiday administration" button.

⇨ Use the "Add" button in the holidays list *(in the right-hand column)* to add the newly created holiday *(in the left-hand column)*.

⇨ Click on the "OK" button and then on the "Finish" button to return to the main time zone plan menu.

4. Select a group in the table and edit the weekly schedule for the group.

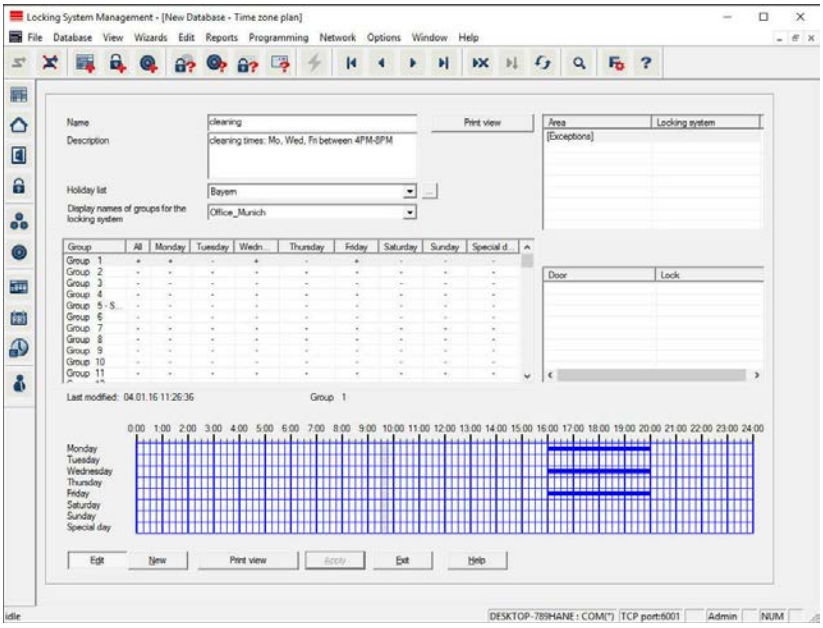
⇨ A blue bar indicates an authorisation for this time period.

⇨ You can click on fields individually or select them together.

⇨ Each time that you click on a field or area, you reverse the authorisation status.

SimonsVoss manual 3:

practical manual



Locking System Management - [New Database - Time zone plan]
File Database View Wizards Edit Reports Programming Network Options Window Help
Print view
Edit New Print view Apply Exit Help
idle DESKTOP-789HANE : COM(*) TCP port:6001 Admin NUM

Name: cleaning

Description: cleaning times: Mo, Wed, Fri between 4PM-8PM

Holiday list: Bayern

Display names of groups for the locking system: Office_Munich

Area	Locking system
[Exceptions]	

Group	All	Monday	Tuesday	Wedn...	Thursday	Friday	Saturday	Sunday	Special d...
Group 1	+	+	-	+	-	+	-	-	-
Group 2	-	-	-	-	-	-	-	-	-
Group 3	-	-	-	-	-	-	-	-	-
Group 4	-	-	-	-	-	-	-	-	-
Group 5 - S...	-	-	-	-	-	-	-	-	-
Group 6	-	-	-	-	-	-	-	-	-
Group 7	-	-	-	-	-	-	-	-	-
Group 8	-	-	-	-	-	-	-	-	-
Group 9	-	-	-	-	-	-	-	-	-
Group 10	-	-	-	-	-	-	-	-	-
Group 11	-	-	-	-	-	-	-	-	-

Door	Lock

Last modified: 04.01.16 11:26:36 Group 1

⇨

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.

2.14 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.

2.15 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.

NOTICE 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.

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

2.16 Replace defective, lost or stolen transponders

Transponders may get lost, stolen or damaged at some point. Whatever the case, the old transponder needs to be reset in the locking plan and a replacement transponder needs to be created.

NOTICE 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.

2.17 Check and evaluate battery status of locking devices

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

Transfer battery statuses to the LSM software

Fast & efficient: 'collecting' battery statuses using a transponder

1. Take a transponder which is authorised for use on all locking devices. Activate this transponder twice on each locking device.
2. Programme the transponder again. Activate the 'Deactivation resets / Read battery warnings' checkbox in the 'Programme transponders' window.

Importing battery statuses by reading the locking device

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

Using LSM Mobile to transfer battery statuses to the LSM software

You can use LSM Mobile to read battery statuses directly or transfer them to the LSM software application. Follow the instructions in the 'LSM Mobile' manual, which you can find at www.simons-voss.com.

Display battery statuses

Basic procedure for all LSM versions:

✓ The current battery warnings for the locking devices concerned have been transferred 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 status is displayed in the 'Status when last read' field.

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

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

✓ The current battery warnings for the locking devices concerned have been transferred to the LSM software.

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

Displaying battery warnings automatically in LSM Business

Generate a warning which shows battery warnings directly.

✓ The current battery warnings for the locking devices concerned have been transferred to the LSM software.

1. Select 'Reports / Manage warnings' in the menu bar
2. Use the 'New' button to create a new warning.
3. Create the warning as you require. 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. Use the 'Finish' button to quit the dialogue box.

2.18 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.

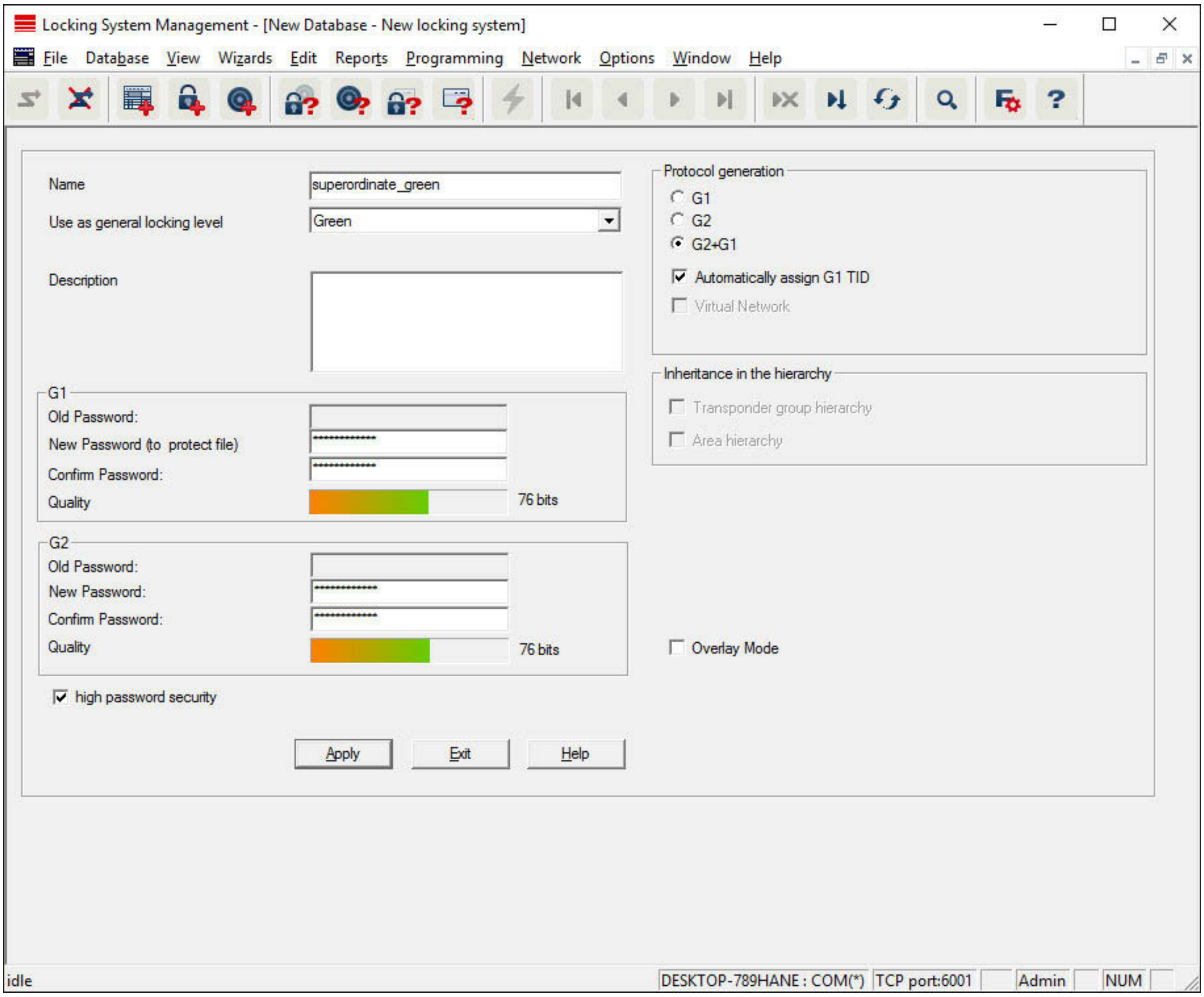
2.18.1 Add common locking level

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".



Name: superordinate_green

Use as general locking level: Green

Description:

G1

Old Password:

New Password (to protect file): *************

Confirm Password: *************

Quality: 76 bits

G2

Old Password:

New Password: *************

Confirm Password: *************

Quality: 76 bits

☑ high password security

Protocol generation

○ G1

○ G2

● G2+G1

☑ Automatically assign G1 TID

□ Virtual Network

Inheritance in the hierarchy

□ Transponder group hierarchy

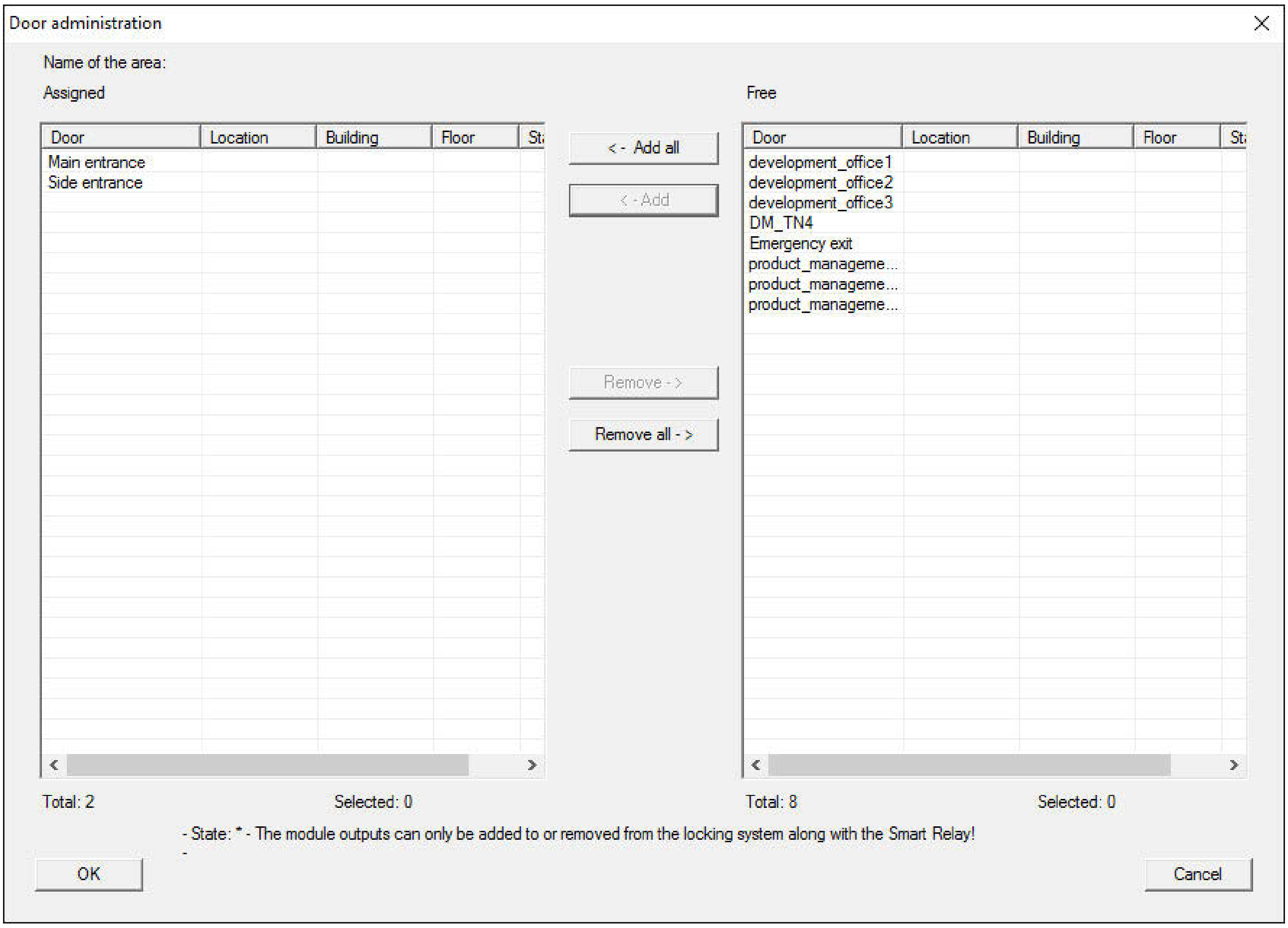
□ Area hierarchy

□ Overlay Mode

2.18.2 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.



Door administration

Name of the area:

Assigned

Door	Location	Building	Floor	St
Main entrance				
Side entrance				

Total: 2 Selected: 0

Free

Door	Location	Building	Floor	St
development_office1				
development_office2				
development_office3				
DM_TN4				
Emergency exit				
product_manageme...				
product_manageme...				
product_manageme...				

Total: 8 Selected: 0

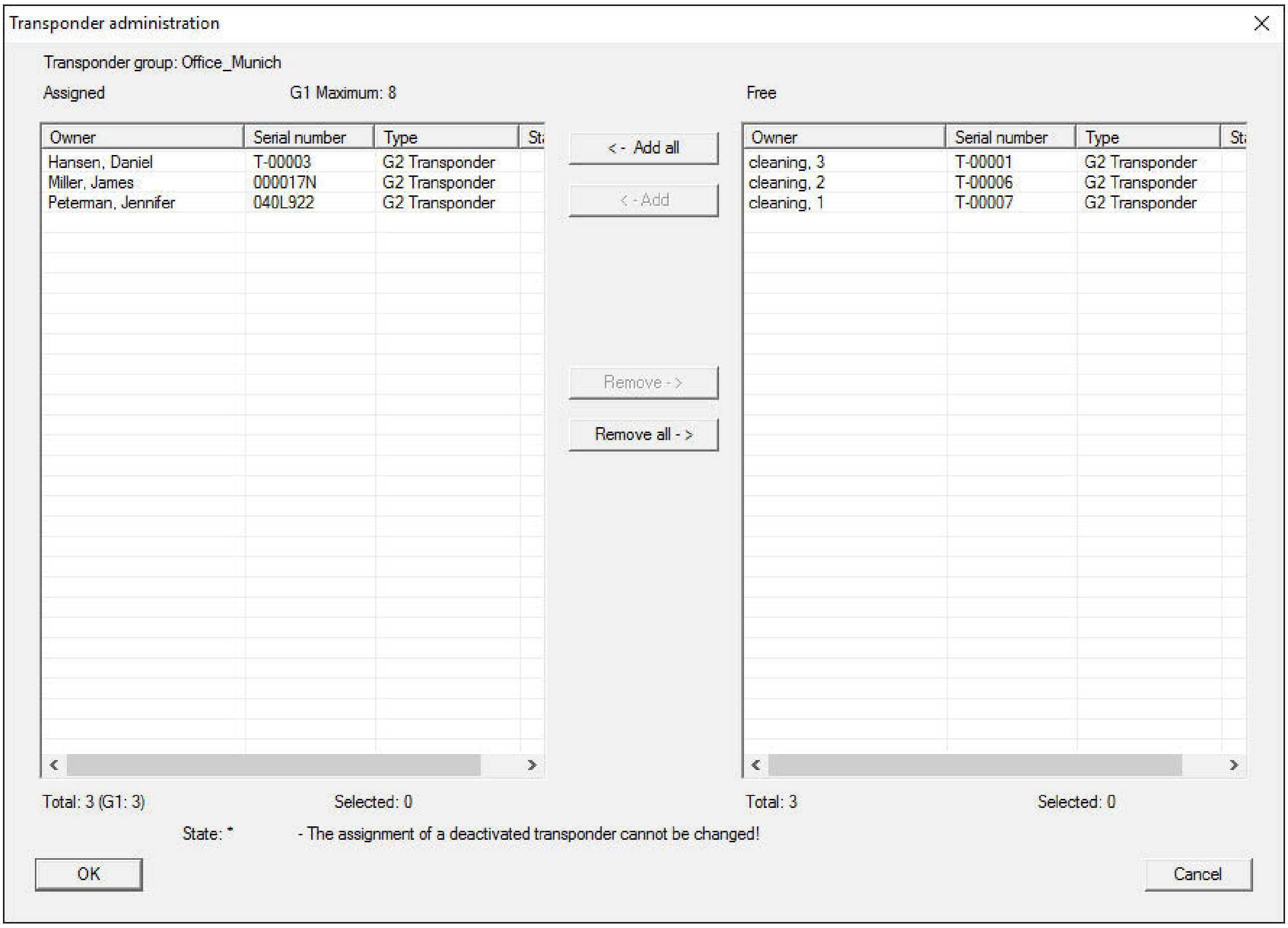
- State: * - The module outputs can only be added to or removed from the locking system along with the Smart Relay!

2.18.3 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.



Transponder administration

Transponder group: Office_Munich

Assigned G1 Maximum: 8

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

Total: 3 (G1: 3) Selected: 0

Free

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

Total: 3 Selected: 0

State: * - The assignment of a deactivated transponder cannot be changed!

2.18.4 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.

2.19 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.

2.20 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.

2.21 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 PC.*
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 is achieved using an import or synchronisation from LSM Mobile to the LSM software.

2.21.1 With pocket PC/PDA

NOTICE Programming with LSM Mobile will only work in the G1 protocol with a pocket PC or PDA.

This is 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 SMARTCD.G2 programming device is charged and connected to the PDA via Bluetooth.
- ✓ The pocket PC drivers have been correctly installed on the computer and a connection has been established.

1. Select *Programming/LSM Mobile/Export to LSM Mobile/LSM Mobile PDA*.
2. Follow the instructions in the LSM software and transfer the programming tasks to the PDA.
3. Launch LSM Mobile on the PDA and log on to the locking system concerned.
4. Use the programming device to carry out the programming processes on the components concerned.
5. Select *Programming/LSM Mobile/Import from LSM Mobile/LSM Mobile PDA*.
6. Follow the instructions in the LSM software and synchronize the programming tasks.

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

2.21.2 With laptop, netbook or tablet PC

This is 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.

2.22 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.

2.23 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. A suitable user can be added to LSM BUSINESS manually; see Administer users (LSM BUSINESS) [▸ 24].

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

NOTICE 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.

2.24 Administer users (LSM BUSINESS)

Assign user to a user group

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

Creating a new user

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

3 ONLINE applications

3.1 Creating a WaveNet radio network and incorporating a locking device

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

3.1.1 Preparing LSM software

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

1. Install the CommNode server and ensure that the service has been started.
2. Install the current version of WaveNet Manager. (See Installation of the WaveNet Manager)
3. Open the LSM software and select "Network/WaveNet Manager".
   - ⇨ Indicate the WaveNet Manager installation directory and select a directory for the output file.
   - ⇨ Use the "Start" button to launch WaveNet Manager.
4. Issue a password to increase security in your network.

⇨ WaveNet Manager will start up and the settings are then saved for the future. Exit WaveNet Manager to make more settings.

3.1.2 Initial programming of locking components

Locking devices need to be programmed before they can be incorporated into the network.

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.

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. In the case of active locking devices, only the locking device to be programmed may be in the immediate area surrounding the programming device!

3.1.3 Preparing hardware

The current RouterNode2 can be quickly and easily placed into operation. Close the RouterNode2 as per the accompanying quick guide. The RouterNode2 is configured in the factory, so that it acquires its IP address from a DHCP server. You can use the OAM tool *(available free of charge from the download center)* to detect this IP address quickly.

NOTICE

Default settings:

IP address: 192,168,100,100

User name: SimonsVoss | Password: SimonsVoss

If the locking device has not been fitted with a LockNode (LN.I) in the factory, you need to retrofit the device using corresponding accessories.

NOTICE

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

3.1.4 Creating communication nodes

The communication node forms the interface between the CommNode server and the LSM software. You must execute the LSM software as the Administrator to create the configuration XMLs.

1. Open the LSM software.
2. Select "Network/Communication nodes".
3. Add "Name", "Computer name" and "Description".
   ⇨ *e.g. WaveNet-Netzwerk_123; Computer_BS21; communication node for the WaveNet radio network 123*
4. Click on the "Config files" button.
5. Ensure that the path specifies the CommNode server's installation directory and click on the "OK" button.
6. Press "No" to accept the prompt and confirm your selection by pressing "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 query.
9. Click on the "OK" button to close the dialogue.

3.1.5 Setting up the network and importing into LSM

Add WaveNet configuration

You can start to configure the network if all requirements are met:

- ✓ LSM is installed correctly and a network module is licensed.
- ✓ The Comm Node server has been installed and the service launched.
- ✓ The CommNode server's configuration files have been created.
- ✓ WaveNet Manager has been installed in its current version.
- ✓ A communication node has been created in the LSM software.
- ✓ The initial programming of the locking device to be networked has been successful.
- ✓ The RouterNode2 can be reached via the network and you know its address.
- ✓ The programmed locking device features a fitted LockNode and you know its chip ID.

1. Select "Network/WaveNet Manager" and press the "Start" button to launch WaveNet Manager.
2. Enter the password.
3. Right-click on "WaveNet_xx_x".
4. Install the RouterNode2 first, using the "Add: IP or USB Router" option, for example.
   - ⇨ Follow the dialogue and use the RouterNode2's IP address to incorporate it into your WaveNet radio network.
5. Initialise the locking device's LockNode by right-clicking on the newly added RouterNode2 and selecting the "Search for chip ID" option.
   - ⇨ Follow the dialogue and use the locking device's chip ID to assign it or the associated LockNode to the RouterNode2.
6. Click on the buttons "Save", "Finish" and "Yes" one after another to close WaveNet Manager.
7. Import the new settings and assign them to the corresponding communication node.

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 "Transfer" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "OK" button to close the dialogue.

Assigning a LockNode to a locking device

The initialised LockNode must be linked to a locking device. The easiest way to do this is using a collective command, particularly if there are a number of LockNodes:

1. Select "Network/Collective tasks/WaveNet nodes".
2. Select all LockNodes *(WNNode_xxxx)* which have not yet been assigned. *There is no entry in the "Door" column for LockNodes which have not yet been assigned.*
3. Click on the "Configure automatically" button.

   ⇨ Auto-configuration launches immediately.
4. Click on the "OK" button to close the dialogue.

Testing the WaveNet configuration

You can reprogramme the locking device at any time by using "Right-click/Programme" in the network to test the network quickly. If programming is successful, the network is working correctly.

3.2 Putting the DoorMonitoring locking cylinder into operation

This example shows which settings need to be made to set up a DoorMonitoring locking cylinder. You will find the requirements in the Section "Creating a WaveNet radio network and incorporating a locking device [▸ 25]".

3.2.1 Adding a DoorMonitoring locking cylinder

The DM locking cylinder first needs to be added and programmed correctly in LSM:

1. Select the "Add locking device" button to launch the dialogue for a new locking device.
2. Select "G2 DoorMonitoring cylinder" as a locking device type and add all other details as you wish.
3. Exit the dialogue to add the locking device to the matrix.

4. Double-click to open the locking device's properties and select the "Configuration/Data" tab.
5. Configure the settings in the locking device's "Target area".
6. Click on the "Monitoring configuration" button and complete the following settings as a minimum:
   - ⇨ Fastening screw sampling interval: e.g. 5 seconds. The door status will be queried every 5 seconds in this case.
   - ⇨ The number of turns in the lock: e.g. one turn. This setting is important to record the bolt status correctly.
7. Save the settings and return to the matrix.
8. Use a suitable programming device to carry out initial programming.

3.2.2 Integrating a DoorMonitoring locking cylinder into the network

This is how you incorporate the DM locking cylinder into the WaveNet network:

✓ WaveNet Manager is already set up.

✓ The router to which the new locking device is to be assigned is already set up and online.

✓ A LockNode is correctly fitted to the DM locking cylinder and you know the chip ID.

1. Launch WaveNet Manager.
2. Initialise the locking device's LockNode by right-clicking on the router and selecting the "Search for chip ID" option.
   - ⇨ Follow the dialogue and use the locking device's chip ID to assign it or the associated LockNode to the RouterNode2.
3. Right-click on the newly added DM LockNode.
4. Activate the "I/O configuration" checkbox and click on the "OK" button.
5. Activate the "Send all events to the I/O configuration" checkbox and click on the "OK" button.
6. Click on the buttons "Save", "Finish" and "Yes" one after another to close WaveNet Manager.
7. Import the new settings and assign them to the corresponding communication node.

3.2.3 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 "Transfer" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "OK" button to close the dialogue.

3.2.4 Assigning a LockNode to a locking device

The initialised LockNode must be linked to a locking device. The easiest way to do this is using a collective command, particularly if there are a number of LockNodes:

1. Select "Network/Collective tasks/WaveNet nodes".
2. Select all LockNodes *(WNNode_xxxx)* which have not yet been assigned. *There is no entry in the "Door" column for LockNodes which have not yet been assigned.*
3. Click on the "Configure automatically" button.

   ⇨ Auto-configuration launches immediately.
4. Click on the "OK" button to close the dialogue.

3.2.5 Activating locking device input events

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

1. Select "Network/Collective tasks/WaveNet nodes"
2. Select the DoorMonitoring cylinder *(or any locking cylinder which is to forward events)*.
3. Click on the "Activate input events" button.

   ⇨ Programming is started immediately.
4. Click on the "Finish" button as soon as all locking devices have been programmed.

3.3 Setting up RingCast

A RingCast configuration is described below. The RingCast can be used to forward a RouterNode2 input event to other RouterNode2s in the same WaveNet radio network at the same time. This example shows how an emergency release is activated for the locking devices. When a fire alarm system activates Input 1 on a RouterNode2, all linked locking devices should be opened. Each locking device remains open until it receives the explicit command of a remote opening.

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

This example requires a configured WaveNet radio network with two RouterNode2s. Each RouterNode2 is linked to a locking device. All locking devices should be opened as soon as Input 1 has been connected to a RouterNode2 for a short interval. This allows people to gain access to all rooms, so that they can seek safety from fire or smoke.

Please note: The RingCast for RouterNode2s networked via Ethernet is first available for models which are supplied from 2017. If a RouterNode2 cannot reach another one via Ethernet, it will try to do so in a second attempt via radio. Communication by radio functions over a distance of about 30 m (this value depends heavily on the surrounding area and cannot be guaranteed).

3.3.1 Preparing the router for RingCast

First of all, the two RouterNode2s need to be pre-configured:

- ✓ Two different RouterNode2s are configured and online in the WaveNet radio network.
- ✓ Each RouterNode2 is assigned to a locking device. Both locking devices are online.

1. Launch WaveNet Manager.
2. Right-click on the first RouterNode2.
3. Activate the "I/O configuration" checkbox and click on the "OK" button.
4. Optional: Select "Input feedback static" for Input 1, for example, to activate a signalling device during deactivation.
5. Select the "Emergency release" entry for Input 1.
6. The "RingCast" entry is to be selected as a delay.
7. Use the "Select LN" button to ensure that all required LockNodes have been selected. *(All LockNodes are incorporated the first time that the router's I/O configuration is set up).*
8. Select your protocol generation and enter the locking system password.
9. Click on the "OK" button to complete the configuration.
10. Make the same settings on the second RouterNode2 as well.

3.3.2 Adding RingCast

The RingCast can be added when the RouterNode2s have been configured accordingly:

1. Right-click on the entry "WaveNet_xx_x" in WaveNet Manager.
2. Activate the "RingCast" checkbox and click on the "OK" button.
3. Select the entry "Input 1" in "Select domain".

⇨ The two RouterNode2s where you have set the I/O configurations for the RingCast appear in the "Selected router" field.

4. Highlight the two RouterNode2s where you have set the I/O configurations for the RingCast.
5. Click on the "Save" button.
6. Click on the "Finish" button.
7. Click on the "Yes" button to update the changes.

⇨ The RingCast is added and is visible in WaveNet Manager after a short interval.

The configured settings have already been written in the RouterNode2s. Save the new settings and quit WaveNet Manager.

3.3.3 Functions test

The configured settings come into effect immediately. As soon as an Input 1 is connected, the locking devices are deactivated and the Output 1 connected.

Since the input cables or other parts may have been damaged in a fire, all locking devices remain in "Emergency opening" mode. This mode is not eliminated until each locking device receives a remote opening command.

3.4 Setting up event management

Networking locking devices via RouterNode2 offers many advantages. A decisive advantage is constant communication between the RouterNode2 and the locking device.

In this example, a predefined email is to be sent by the LSM software as soon as a transponder is actuated on a specific locking device at night.

The following preconditions need to be established for this requirement:

- A WaveNet radio network is set up as in the example Creating a WaveNet radio network and incorporating a locking device [▸ 25].
- The forwarding of events to the locking device as in Activating locking device input events [▸ 30] has also been activated.

3.4.1 Setting up email server

A rudimentary email client for sending emails is implemented in the LSM software. An own email account which supports SMTP format is required to send emails.

1. Select "Network/Email notifications"

2. Click on the "Email" button.
3. Enter all your email provider's SMTP settings.
4. Click on the "OK" button.
5. Click on the "OK" button.

3.4.2 Setting task service

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

3.4.3 Forward input events via RouterNode2

Forwarding needs to be activated in the router's I/O configuration as soon as events *(e.g. a transponder is activated on a networked locking device)* need to be forwarded to the CommNode server via the RouterNode2.

1. Launch WaveNet Manager.
2. Right-click on the transponder on the router and select "I/O configuration".
3. Use the drop-down bar in "Report events to management system" to stipulate the "All LN events" option.
4. Confirm by pressing the "OK" button and quit WaveNet Manager.

3.4.4 Creating a response

Create a response first. This response can be selected later if a specific scenario arises.

1. Select "Network/Event manager".
2. Click on the "New" button under "Responses" in the right-hand section.
3. Complete a name and a description for the response.
4. Select the type "Email".
5. Click on the "Configure response" button.
6. Click on the "New" button.
7. Enter the recipient's email address, a subject matter and a message text. *You can use the "Test" button to check the email configuration immediately.*
8. Exit the dialogue box by pressing on the "OK" button three times. Press the "Finish" button to return to the matrix.

3.4.5 Creating an event

Once the response is created, you can then create the event.

1. Select "Network/Event manager".
2. Click on the "New" button under "Events" in the left-hand section.
3. Complete a name and a description for the response.
4. Select the type "Access".
5. Click on the "Configure event" button.
6. Activate the "Respond on all transponders" checkbox. *The event needs to trigger every time a transponder is activated. Alternatively, you can restrict the event to an individual transponder.*
7. You can adjust the action even 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 need to trigger when the transponder is activated and confirm your choice by pressing the "OK" button.
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 times for night time curfew. The event is only active for the time frame defined here.
15. Exit the dialogue box by pressing on the "OK" button three times. Press the "Finish" button to return to the matrix.

4 VN applications

4.1 Administering the virtual network (VN)

A virtual network (VN network) allows you to change and regulate authorisations quickly and conveniently without the need for a full network. The authorisation for locking devices (and block IDs for blocked ID media) is stored directly on the ID medium and forwarded each time the medium activates a locking device. That is why it is important to activate ID media on a gateway at regular intervals in a virtual network.

This example shows the main set-up for a virtual network.

4.1.1 Setting up a locking system

The "Virtual network" checkbox needs to be activated in a(n) (exclusively) G2 locking system. If this setting is applied to an existing locking system, it may create considerable programming requirements.

4.1.2 Setting up a VN service

1. Select "Network/VN service".
2. Select the VN server (e.g. the communication node).
3. Indicate the installation path to the VN server. *The VN server is installed in a separate folder in the main directory in an LSM Business installation.*
4. Click on the "Apply" button.
5. Click on the "Finish" button.

4.1.3 Adding components and setting up the LSM software.

Before starting with the set-up, you first need to make the key settings for operating a network in the LSM software and the RouterNode2 must be ready for use.

- Preparing LSM software [▸ 25]
- Preparing hardware [▸ 26]
- Creating communication nodes [▸ 26]
- Setting task service [▸ 33]

1. Add the different ID media (e.g. transponders) and locking devices (e.g. active locking cylinders).
2. Carry out initial programming for the added components.
3. Add a SmartRelay2 and authorise all ID media which are to receive new authorisations from it at a later stage.

⇨ The "Gateway" checkbox **must** be activated in the tab in the SREL2's locking device properties.

4. Carry out initial programming of the SREL2 and ensure that it features a correctly connected LockNode.
5. Use WaveNet Manager to set up the RouterNode2 and assign the gateway (or the SREL2) to it.

   ⇨ See Setting up the network and importing into LSM [▸ 27].

4.1.4 Exporting changes to authorisations

Exporting changes to authorisations will only work if there is at least one change. Withdraw authorisation for Locking Cylinder 1 from Transponder 1, for example, to test the export.

1. Select "Programming/Virtual network/Export to VN network".
2. Select all SREL2s to which the changes need to be sent/exported.
3. Check that you have selected the right locking system.
4. Click on the "Prepare" button

   ⇨ The "Persons" list contains all the changes which are being exported.
5. Click on the "Export" button

   ⇨ The export process will now start. The changes are transmitted to the gateway.

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

– Transponder 1 books on the gateway. Locking Device 1 then detects that Transponder 1 is no longer authorised and refuses entry.

– Another transponder (not Transponder 1) first books on the gateway and authorises itself on Locking Device 1. Locking Cylinder 1 is informed of the block ID for Transponder 1.

4.1.5 Importing changes to authorisations

When the changes have been exported to the gateway, you are not able to see which changes have already been collected from the gateway in LSM software at first. Only an import will reveal this.

1. Select "Programming/Virtual network/Import synchronisation".

   ⇨ The import process starts immediately.
2. Click on the "Finish" button

4.1.6 Tips on VN

- It is important to use all transponders in the system at short, regular intervals to distribute the changes quickly offline throughout the locking system. This is where you can use time budgets:

  The "Dynamic time frames" options in the locking system properties offer the option of imposing a time budget on transponders. This obliges a person to reload their ID medium at the gateway on a regular basis. If they do not, the ID medium is blocked for this locking system.
- You can automate the import and export of changes for a gateway. You can make the settings directly under "Network/VN service". *Note that importing and exporting many changes will take up the WaveNet's full capacity for a time.*

SimonsVoss manual 3:

practical manual

5 Smart user guide for beginners

This section offers helpful tips on different processes.

5.1 Use ID media correctly

Different ID media must be used in different ways on locking devices.

5.1.1 Active transponders

This is how you identify yourself with a transponder on an active locking device:

1. Hold the transponder at a distance of about 10 cm from the active locking device.
2. Press the transponder button.
   ⇨ An audible signal is emitted:
   ⇨ 2 beeps = Authorised has been issued.
   ⇨ Beep = no authorisation.
3. Activate the locking device.
   ⇨ Locking cylinder: turn the door thumb-turn in the required direction to open or close the door.
   ⇨ SmartHandle: Turn the handle and gain entry.

5.1.2 Passive cards & tags

This is how you identify yourself with a card or a smart tag on an active locking device:

1. hold the passive ID medium directly on the middle of the locking device.
   ⇨ An audible signal is emitted:
   ⇨ 2 beeps = Authorised has been issued.
   ⇨ Beep = no authorisation.
2. Activate the locking device.
   ⇨ Locking cylinder: turn the door thumb-turn in the required direction to open or close the door.
   ⇨ SmartHandle: Turn the handle and gain entry.