

MANUAL LSM – ADMINISTRATION

Version: May 2011

MANUAL LSM – ADMINISTRATION

Table of contents

| | | |
|------------|--|-----------|
| 1.0 | Introduction | 6 |
| 1.1. | Important note | 6 |
| 1.1. | Understanding this manual | 7 |
| 2.0 | Icons | 8 |
| 1.2. | Standard toolbar..... | 9 |
| 1.3. | Areas / transponder group view..... | 10 |
| 1.4. | Doors / Persons view | 10 |
| 1.5. | Group authorisation tree view..... | 11 |
| 1.6. | PROGRAMMING REQUIREMENT | 11 |
| 3.0 | Setting up and opening the database | 12 |
| 4.0 | User management | 13 |
| 1.7. | General..... | 13 |
| 1.8. | Introduction | 13 |
| 1.9. | logging on to the database..... | 13 |
| 5.0 | USER management (from LSM Business Edition) | 14 |
| 1.10. | READ ACCESS (LZ), Write access (SZ)..... | 14 |
| 1.11. | Assignment to transponder groups and areas | 14 |
| 1.12. | Roles..... | 14 |
| 1.12.1 | Locking system management (SV) | 14 |
| 1.12.2 | Edit locks and areas (SB)..... | 14 |
| 1.12.3 | Edit transponders and groups (TP)..... | 15 |
| 1.12.4 | Program/read locks (SP) | 16 |
| 1.12.5 | Configure network (NK)..... | 16 |
| 1.12.6 | Manage network (NV)..... | 16 |
| 1.12.7 | Administration of access lists (ZA)..... | 16 |
| 1.12.8 | Manage access lists (ZA) | 17 |
| 1.12.9 | Staff management (PV)..... | 17 |
| 1.12.10 | Use handheld (HB) | 17 |
| 1.12.11 | Time management (ZW)..... | 18 |
| 1.12.12 | Print reports (BD) | 18 |
| 1.12.13 | Read log (PL) | 18 |
| 1.12.14 | Emergency opening (NO)..... | 18 |
| 1.13. | User group | 19 |
| 1.13.1 | General information about user groups | 19 |

MANUAL LSM – ADMINISTRATION

Table of contents

| | | |
|--------|--|-----------|
| 1.13.2 | Users - Group members | 20 |
| 1.13.3 | Users - Roles | 21 |
| 1.13.4 | Roles - Responsibility..... | 22 |
| 1.13.5 | Creating a user group..... | 23 |
| 1.13.6 | Editing a user group | 23 |
| 1.13.7 | Deleting a user group | 23 |
| 1.14. | User | 24 |
| 1.14.1 | Creating users | 25 |
| 1.14.2 | Change user | 25 |
| 1.14.3 | Deleting users | 25 |
| 1.14.4 | Assigning a user group | 25 |
| 6.0 | USER MANAGEMENT (LSM Basic Edition) | 26 |
| 1.15. | Default settings..... | 26 |
| 7.0 | Inheritance principle | 27 |
| 1.16. | General | 27 |
| 1.17. | Transponder group hierarchy | 27 |
| 1.18. | Area hierarchy | 29 |
| 1.18.1 | Issuing authorisations and inheritance concept | 33 |
| 8.0 | Logging | 34 |
| 9.0 | Programming device..... | 36 |
| 1.19. | Local connections | 36 |
| 1.19.1 | General | 36 |
| 1.19.2 | Setting up SmartCD | 36 |
| 1.19.3 | Testing SmartCD | 36 |
| 10.0 | Time control..... | 37 |
| 1.20. | General | 37 |
| 1.21. | Public holidays | 38 |
| 1.21.1 | General | 38 |
| 1.21.2 | Creating a public holiday | 39 |
| 1.21.3 | Editing a public holiday..... | 39 |
| 1.22. | Public holiday list..... | 40 |
| 1.22.1 | General | 40 |
| 1.22.2 | Public holiday management..... | 41 |
| 1.22.3 | Creating a public holiday list | 42 |
| 1.23. | Time groups..... | 42 |
| 1.23.1 | General | 42 |
| 1.23.2 | Assigning a time group name..... | 43 |

MANUAL LSM – ADMINISTRATION

Table of contents

| | |
|---|-----------|
| 1.24. Time zone plan | 44 |
| 1.24.1 General | 44 |
| 1.24.2 Creating a time zone plan..... | 45 |
| 1.25. Using time management | 46 |
| 1.25.1 Time zone plans | 46 |
| 1.25.2 Time zone plans on areas | 46 |
| 1.25.3 Time groups on transponder groups..... | 48 |
| 11.0 Options..... | 50 |
| 1.26. Setting up matrix view | 50 |
| 1.27. Additional columns in label bars | 52 |
| 1.28. Automatic numbering | 53 |
| 1.29. Logging | 54 |
| 1.30. Advanced | 56 |
| 1.30.1 Optimisation / management..... | 56 |
| 1.30.2 Importing..... | 57 |
| 1.30.3 Various | 64 |
| 1.30.4 Staff photos | 64 |
| 1.30.5 Management | 64 |
| 1.30.6 Resource management..... | 65 |
| 1.31. User password security | 65 |
| 12.0 Service and Support | 66 |

NOTE:

In the explanations of the various functions of the system, the focus is on operating the software. Please refer to the individual product manuals for descriptions of the individual product features, fittings and functions.

It is important to comply with the product approvals and system requirements when installing and operating the products. SimonsVoss accepts no liability and cannot provide support for installation or operation which deviates from these instructions.

SimonsVoss Technologies AG reserves the right to make modifications to the product without notice. Consequently, descriptions and representations in this documentation may vary from the most recent product and software versions. As a general principle, the original German version shall apply in the event of any doubt. Subject to errors and misspellings.

These documents are based on the current programme status at the time of printing. The information and data they contain may be changed without advance notice and do not represent an obligation on the part of the seller. The software and hardware designations used in this manual are mainly registered trademarks and as such are subject to the legal copyright protection law regulations.

Neither the manual nor extracts of it may be reproduced or disseminated by mechanical or electronic means, photocopying or otherwise without our express written permission. The companies and other pieces of data used in the examples are fictitious, any similarities are therefore purely coincidental.

The editors of this LSM manual took great care when compiling this text. However we cannot guarantee that it is free from errors. The LSM editing team is not liable for technical or printing errors in this manual. The descriptions provided in this manual are not of a guaranteed quality in the eyes of the law.

Please send any corrections or suggestions for improvement to Info@simons-voss.de.

Thank you in advance for your support.

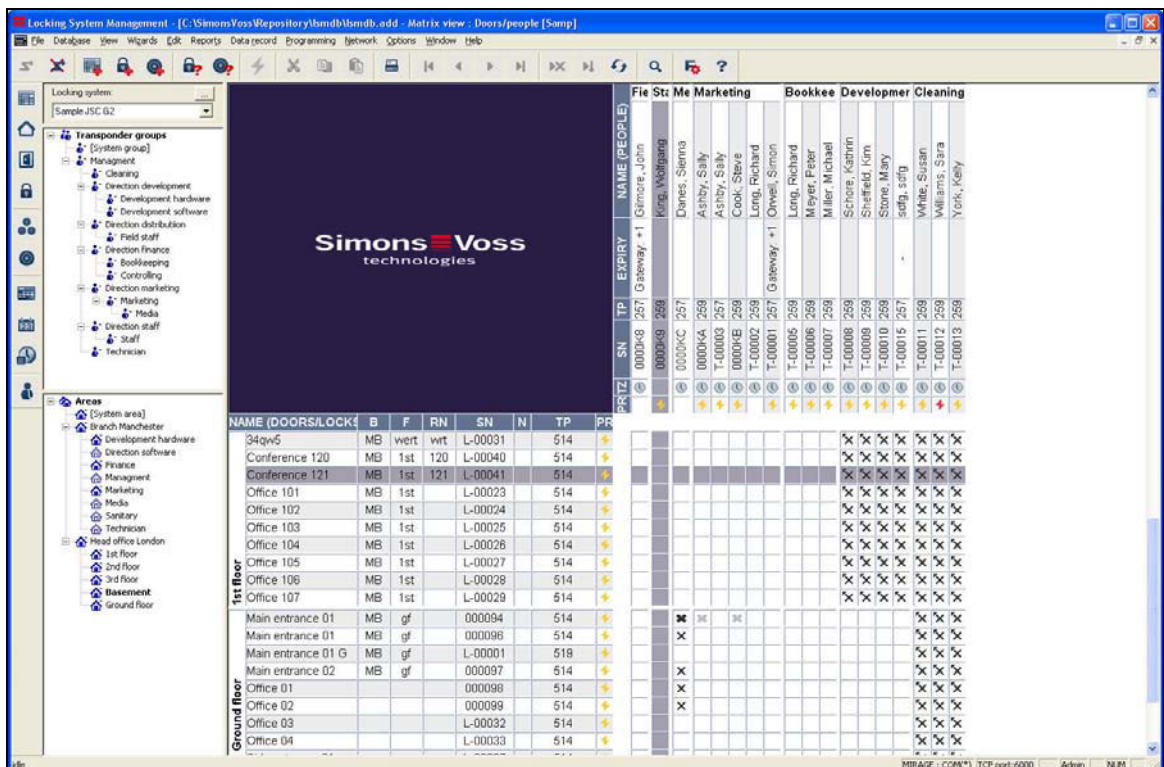
More information about SimonsVoss products can be found online at WWW.SIMONS-VOSS.DE

This manual applies to software without functional limitations. Functions or views in a customer's specific installation may deviate from these due to the software modules activated.

MANUAL LSM – ADMINISTRATION

1.0 INTRODUCTION

Locking System Management (LSM) from SimonsVoss is a database-supported software package that enables you to create, manage and control complex locking plans efficiently. This documentation serves as a guide to help you structure and configure your locking plan. It will also assist you later on when it comes to monitoring and controlling the locking system, making management of **the system** easier.



1.1. IMPORTANT NOTE

SimonsVoss Technologies AG shall assume no liability for damage caused by incorrect assembly or installation.

Access through a door may be denied if components are incorrectly assembled or programmed. SimonsVoss AG shall assume no liability for the consequences of incorrect installation, such as denied access to injured persons or persons at risk, damage to property or any other form of damage.

1.1. UNDERSTANDING THIS MANUAL

➤ MENU ITEMS

The LSM menu items are indicated in this manual by the ➤ symbol.

EXAMPLES

- Edit
- Area

HEADINGS AND CHECKBOXES

Headings and checkboxes shown in the screenshots are differentiated by the use of inverted commas.

EXAMPLES

- “User Groups”
- “Areas”

BUTTONS

Buttons shown in the screenshots are highlighted in grey.

EXAMPLES

- OK
- Apply

KEY COMBINATIONS

The key combination you can use to start the required functions is shown in bold.

Ctrl+Shift+X

PATH SPECIFICATIONS

If an instruction refers to a directory on a drive, the path is provided in italics.

EXAMPLE

C:\Program files\SimonsVoss\LockSysGui

NOTE





















The specification *[CDROM]* is a variable and describes the letter identifying the drive of the CDROM drive on the computer (e.g. “D”) on which installation is to be carried out.

2.0 ICONS















































NOTE

- Icons and entries in the menu only become active once an associated object is highlighted.
- You can use Shift or Ctrl to highlight multiple table entries at the same time.
- By double-clicking in the table you can jump to the object's properties.

EDIT TOOLBAR

| Active icon | Inactive icon | Function | Shortcut |
|---|---|--------------------------|---------------------|
|  |  | Edit locking system | Ctrl+Shift+A |
|  |  | Area | Ctrl+Shift+S |
|  |  | Edit door | Ctrl+Shift+D |
|  |  | Edit lock | Ctrl+Shift+C |
|  |  | Edit transponder group | Ctrl+Shift+G |
|  |  | Editing transponders | Ctrl+Shift+O |
|  |  | Edit public holiday list | |
|  |  | Edit public holiday | |
|  |  | Edit time zones | |
|  |  | Edit person | Ctrl+Shift+P |

1.2. STANDARD TOOLBAR

| Active icon | Inactive icon | Function | Shortcut |
|---|---|----------------------|---------------------|
|  |  | Log on | |
|  |  | Log off | |
|  |  | New locking system | |
|  |  | New lock | |
|  |  | New transponder | |
|  |  | Read lock | Ctrl+Shift+K |
|  |  | Read transponder | Ctrl+Shift+R |
|  |  | Program | |
|  |  | Cut | |
|  |  | Copy | |
|  |  | Paste | |
|  |  | Print matrix | |
|  |  | First data record | |
|  |  | Previous data record | |
|  |  | Next data record | |
|  |  | Last data record | |
|  |  | Remove | |
|  |  | Apply | |
|  |  | Update | |
|  |  | Browse | |
|  |  | Filter not active | |
|  |  | Filter active | |
|  |  | Info | |

1.3. AREAS / TRANSPONDER GROUP VIEW



A black cross with a circle inside it represents group authorisation.



A grey cross with a circle inside it stands for “inherited authorisation.

1.4. DOORS / PERSONS VIEW



Authorisation that has been enabled but not yet programmed into the lock



Authorisation that has been programmed into the lock



Authorisation that has been removed and not yet transferred to the lock



Authorisations that have not yet been programmed which comply with the group structure of the locking system, in other words that originate from the group view, are indicated by a small black triangle



Programmed authorisations that comply with the group structure of the locking system, in other words that originate from the group view, are indicated by a small black triangle



Removed authorisations that comply with the group structure of the locking system and have not yet been programmed



Authorisations that do not comply with the group structure of the locking system are indicated simply by a cross, with no black triangle (individual authorisation).



Authorisations that have been subsequently withdrawn, contrary to the group structure of the locking system, feature a black triangle but no cross indicating authorisation.



White (grey) box: authorisation can be enabled here.



Checked (greyed out) box: this field no longer belongs to the locking system and no authorisations can be enabled. You have no write permission or the locking plan blocks this box (e.g. when a transponder is deactivated).

1.5. GROUP AUTHORISATION TREE VIEW



Manually enabled (black)



Directly inherited (green)



Indirectly inherited – inherited via subordinate group (blue)



Directly and indirectly inherited (blue / green)

1.6. PROGRAMMING REQUIREMENT

EXPLANATION

There are various reasons why it may be necessary to program a transponder or lock. The programming lightning symbol is shown in different colours to indicate the different reasons why programming is required.

DISPLAY



Simple programming requirement for components



Transponder:

- Validity expired
- Deactivated

Lock

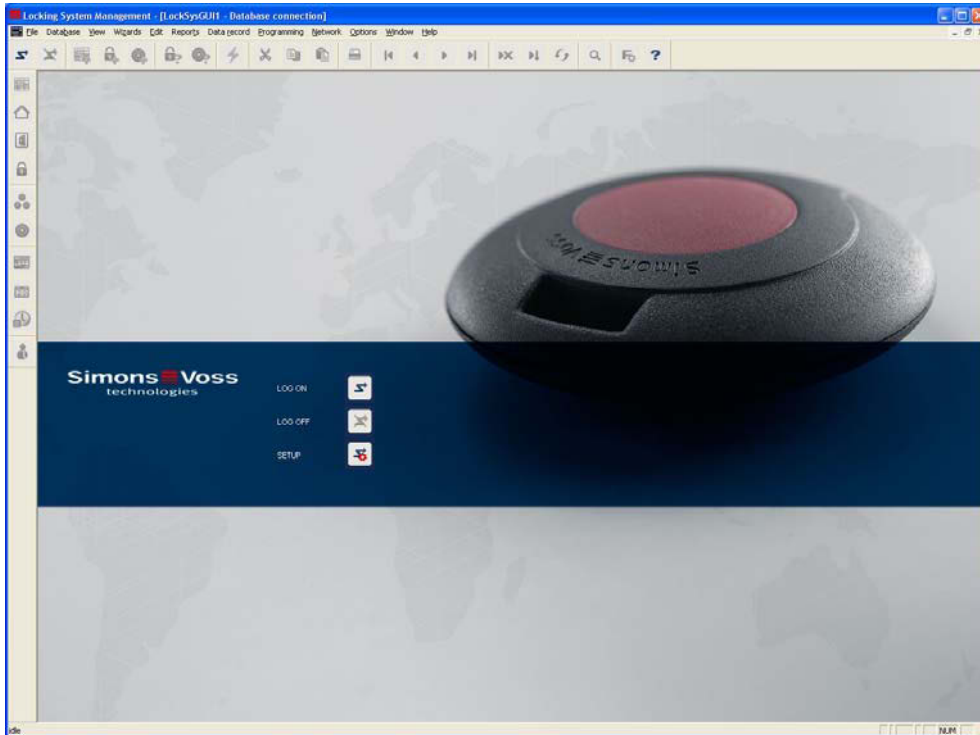
- Only overall locking level assigned
- Not assigned to any door
- Not assigned to any locking system
- Door without lock



Programming requirement on a lock after creating a replacement transponder in the overlay mode of a G1 system

MANUAL LSM – ADMINISTRATION

3.0 SETTING UP AND OPENING THE DATABASE



START SCREED



Log on to the database, authentication then takes place when user data is entered

Log off the database

Settings for the database connection

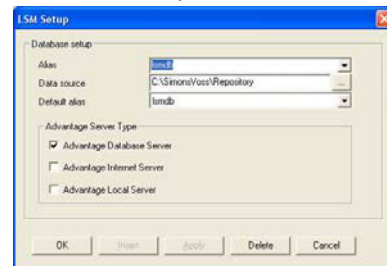
In the Setup dialogue you can set the connection to the database you want.

Your locking system administrator provides you with the necessary information.

LSM Basic



LSM Business / LSM Professional

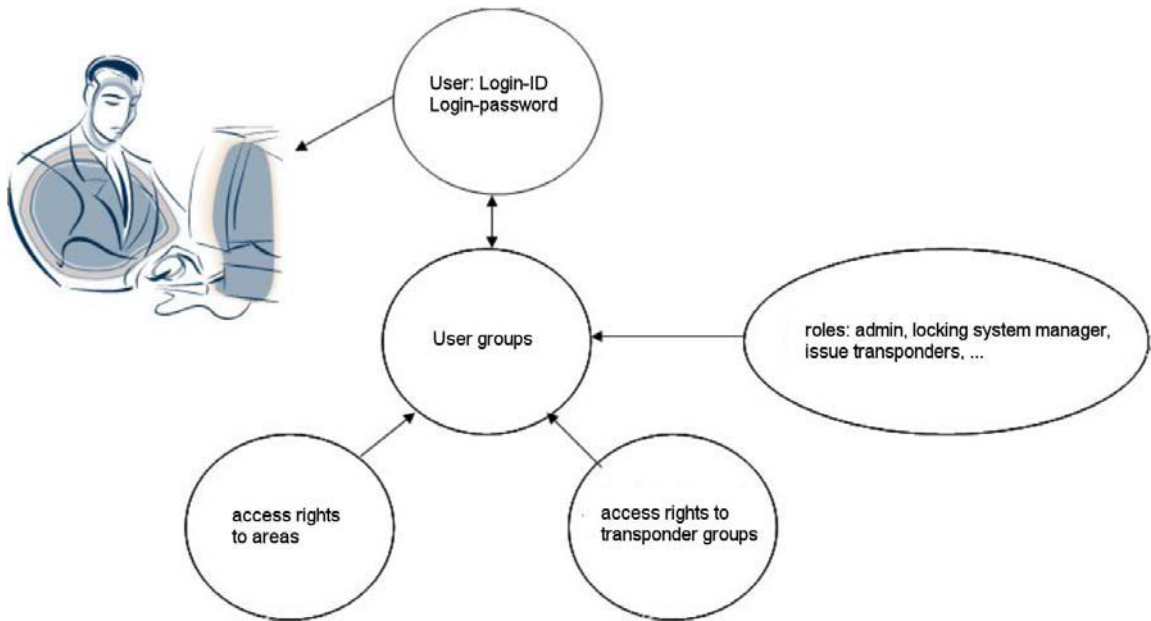


NOTE

The software access data should be kept safe according to the valid IT guidelines and not made accessible to unauthorised persons.

4.0 USER MANAGEMENT

1.7. GENERAL



LSM allows you to assign individual rights to each software user (user) in an extremely flexible manner. After logging in with their user name and password, created users can only access the database with their individual rights. Pre-defined rights are issued through user groups, which are indicated by a shared “role” (admin, locking system manager, issue transponders, etc.) and access rights to certain lock areas or transponder groups.

1.8. INTRODUCTION

All LSM users receive a login and password which they use to log into the locking plan database. Users can change their password themselves if it has been disclosed to others, for example. A user's management rights in LSM are controlled by the group(s) he or she belongs to. There is no restriction to the number of groups that a user can be in. Together, the management rights a user inherits from various groups form an effective rights profile. The management rights of each user group have three features: write access, assignment to transponder groups and areas and, lastly, roles.

1.9. LOGGING ON TO THE DATABASE

Standard log-on information

| | | |
|----------|------------|------------|
| User | Admin | Admin AL |
| Password | system3060 | system3060 |

Note:

These passwords must be changed immediately in productive systems to prevent unauthorised access to the locking system data.

5.0 USER MANAGEMENT (FROM LSM BUSINESS EDITION)

1.10. READ ACCESS (LZ), WRITE ACCESS (SZ)

If the 'write access' option is not selected, users only have read access to the roles assigned to them. In the locking plan, this means that they can view but not change the corresponding elements (select/deselect or change object properties). In terms of communication with the SV devices, this access means that users can only read data and not program or reset it. But if the 'write access' option is selected, users can perform read and write activities.

1.11. ASSIGNMENT TO TRANSPONDER GROUPS AND AREAS

Access to transponders, transponder groups, locks, doors, areas, individual authorisations, group authorisations and locking systems is enabled by assigning a user group to various transponder groups and areas.

1.12. ROLES

Each user group except the administrator group can have several roles.

1.12.1 LOCKING SYSTEM MANAGEMENT (SV)

This role allows a user to view or change the properties of a locking system. To do this, the user must at least be assigned to the system group and the system area of the locking system in question (highest level).

This role is only available in conjunction with four other roles:

1. Program/read transponders
2. Program/read locks
3. Edit transponders and groups
4. Edit locks and areas

1.12.2 EDIT LOCKS AND AREAS (SB)

This role relates to locks, doors, areas and access authorisations.

AREAS

Users can only view or change all of the area properties if they are appropriately assigned to the area.

CREATING A NEW LOCK/DOOR

All users with the 'Edit locks and areas' role with write access can create a new lock or door.

EDITING/DELETING A LOCK/DOOR

A user with the 'Edit locks and areas' role can view, edit or delete the properties of a lock or door as long as one of the following conditions is satisfied.

1. He or she is explicitly assigned to the 'black' area that the door (together with the lock) is assigned to

2. The lock has not yet been added to a door
3. The assigned door has not yet been added to a 'black' area

ACCESS AUTHORISATIONS (MATRIX VIEWS)

Groups or individual authorisations can only be viewed or changed in the matrix view if

- Both the “Edit locks and areas” and “Edit transponders and groups” roles are available
- The corresponding group and area are assigned

1.12.3 EDIT TRANSPONDERS AND GROUPS (TP)

This role relates to transponders, transponder groups and access authorisations

TRANSPONDER GROUPS

Users can only view or change all of the transponder group properties if they are appropriately assigned to the transponder group.

CREATING A NEW TRANSPONDER

All users with the 'Edit transponders and groups' role can create a new transponder

EDITING TRANSPONDERS

A user with the 'Edit transponders and groups' role can view or edit a transponder as long as one of the following conditions is satisfied

- He or she is explicitly assigned to one of the transponder groups containing the transponder
- The transponder has a free data record

To assign the transponder to a transponder group (and remove it from the group), this transponder group must always be explicitly assigned to the user group. Deleting and deactivating a transponder requires the rights to ALL of the transponder's transponder groups (data records).

ACCESS AUTHORISATIONS (MATRIX VIEWS)

See above

Program/read transponders

READING TRANSPONDERS

Irrespective of write access, a user with the 'Program/read transponder' role can read all transponders.

RESETTING TRANSPONDERS

A user with the 'Program/read transponders' role with write access to all the data records available in the transponder can reset the transponder.

PROGRAMMING TRANSPONDERS

A user with the 'Program/read transponders' role with write access to all the data records available in the target status of the transponder can program the transponder.

1.12.4 PROGRAM/READ LOCKS (SP)

READING A LOCK

Irrespective of write access, a user with the 'Program/read locks' role can read all locks.

PROGRAMMING / RESETTING A LOCK / READING A TRANSPONDER LIST / SETTING THE TIME

One of the following conditions must be satisfied

- The user has the 'Program/read locks' role and has write access to the 'black' area where the lock (or door) is located
- The lock is not assigned to the door or the door is not assigned to a 'black' area. Irrespective of write access, all users with the 'Program/read locks' role can reset this kind of lock (but not program it)

1.12.5 CONFIGURE NETWORK (NK)

Irrespective of write access and area affiliation, all users with this role can perform the following functions:

1. Configure WaveNet: manage network/WaveNet
2. Configure LON: manage network/LON network
3. Manage local connections and communication nodes: network/local connections, network/communication nodes

1.12.6 MANAGE NETWORK (NV)

Irrespective of write access and area affiliation, all users with this role can perform the following functions:

1. Manage events and responses: network/event manager
2. Manage network tasks: network/task manager
3. Perform collective tasks: network/collective tasks
4. Perform remote opening: network/activating the lock (provided that the user also has the 'Emergency opening' role)

1.12.7 ADMINISTRATION OF ACCESS LISTS (ZA)

This role is not linked to areas and transponder groups.

Only users with this role can control issuing of the 'Manage access lists' and 'Administration of access lists' roles. The administrator group has this role at first. This role can be taken away from the administrator group at a later date once a special user group has been created with the 'Administration of access lists' role. From this point, administrators can no longer issue or revoke the two roles or view, read or delete the access lists. The option of configuring the access list restrictions (Options/Access lists) is also linked to the 'Administration of access lists' role.

The 'write access' option is ignored in this role.

1.12.8 MANAGE ACCESS LISTS (ZA)

This role extends to locks as follows (either/or conditions):

1. The user must have a right to the “black” area in which the lock is located
2. The lock doesn't have a “black” area

Users with this role can perform the following functions:

- View the read access lists in the Edit/Lock Properties/Access list view. If users have write access, they can also delete the list
- The access lists can be read via 'Programming/Read lock/Access list'

ATTENTION!

The access lists can also be read via Network/Collective tasks/Locks/Access lists. All you need for this is the 'Manage network' role. The access lists themselves are however not displayed.

1.12.9 STAFF MANAGEMENT (PV)

This role is independent of area or transponder group assignment. It allows a user to open the Edit/Person view, create new persons and change or delete existing ones. In this view, users can also change assignment to transponders as long as they have the additional rights to do so.

1.12.10 USE HANDHELD (HB)

Users with this role can export tasks to the PDA or Palm and read in the results. Only the 'black' areas to which the role is assigned are available to users for exporting. This requires write access.

A user can perform the following tasks on the PDA itself:

1. Program lock (if programming is required)
2. Read transponder list (only the transponders from the assigned transponder groups are displayed by name)
3. Set time
4. Reset lock

If the user has additional roles, he or she can perform the following tasks:

| Role | Task |
|---|-----------------------|
| 'Manage access lists' | 'Read access list' |
| 'Emergency opening' | 'Open door' |
| 'Edit transponders and groups', 'Edit locks and areas' | 'Change transponders' |
| 'Edit locks and areas' | 'Change actual data' |

1.12.11 TIME MANAGEMENT (ZW)

Users with this role can manage time zones, time groups, public holidays and public holiday lists

1.12.12 PRINT REPORTS (BD)

This role allows the user to view and print out reports using the 'Reports' menu item. The reports, which are available in different views (e.g. Lock properties/Transponders/Print view) are oriented towards the rights to the corresponding object (in our example, the lock). Simply put, if the object is displayed in the view, users can also use the 'Print view'.

1.12.13 READ LOG (PL)

A user with this role can use the 'View/Log' view

1.12.14 EMERGENCY OPENING (NO)

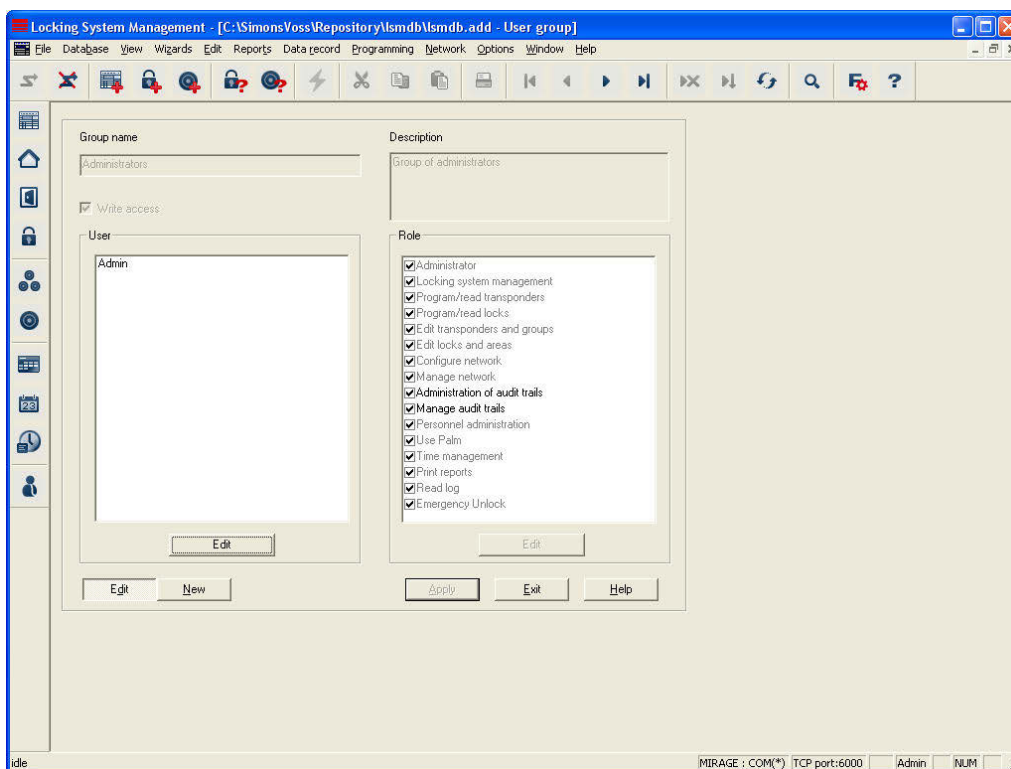
A user with this role can perform an emergency opening (Programming/Emergency opening) and remote opening (Network/Remote opening). If the user also has the 'Use handheld' role, he or she can specify an emergency opening password for the PDA and perform the 'Open door' task on the handheld device using this password.

1.13. USER GROUP

1.13.1 GENERAL INFORMATION ABOUT USER GROUPS

PROCEDURE

- ↻ Edit
- ↻ User group



EXPLANATION

- “Group name” → Designation of user group
- “Description” → Free field for describing the user group
- “Write access” → The roles selected in the right-hand column have the right to make changes. Write access is mandatory for some roles.
- “Role” → Selects the rights that a user of the group is assigned
- Users – Edit → Manages the users in the user group
- Role – Edit → Selects the areas and transponder groups for access

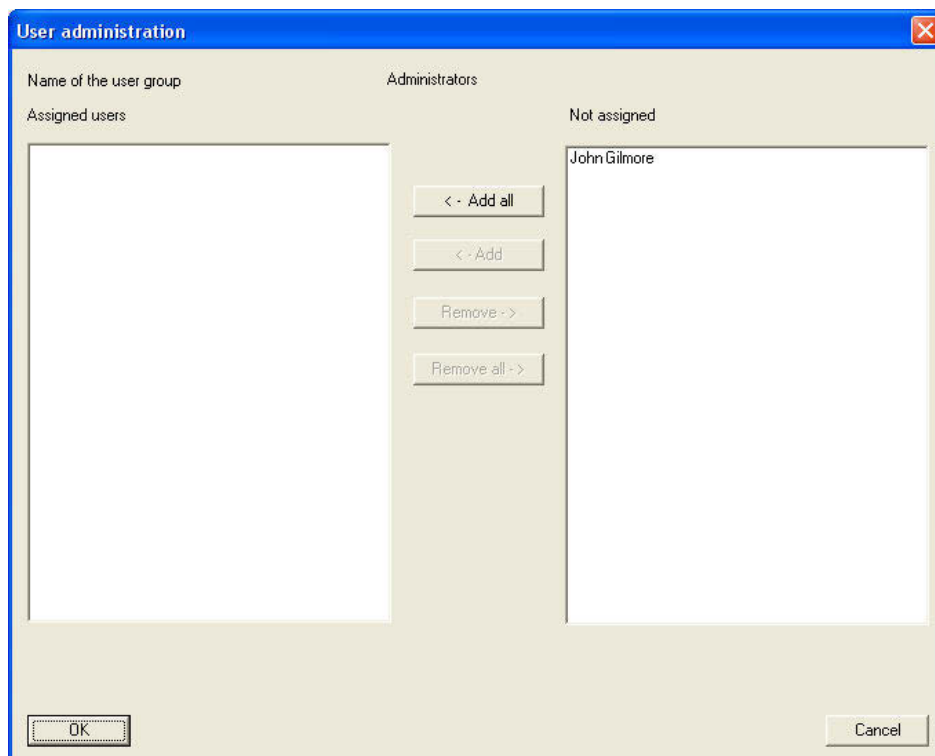
1.13.2 USERS - GROUP MEMBERS

EXPLANATION

It is possible to add individual users to certain groups

PROCEDURE

- ↻ Edit
- ↻ User group
- Edit under “User”
- Select user
- Add or Remove
- OK
- Apply
- Close



EXPLANATION

“Assigned”

→ Group members

“Unassigned”

→ Other users with no group affiliation

Add all

→ All users that have not yet been assigned are added to the group

Add

→ The highlighted user is added to the group

Remove

→ The highlighted user is removed from the group

Remove all

→ All of the assigned users are removed from the group

1.13.3 USERS - ROLES

Read access (LZ)

→ Read access in LSM

Write access (SZ)

→ Right to make changes

Locking system management (SV)

→ All the functions of relevance to managing a locking system using the software can be performed

Program/read transponders (TP)

→ Transponders can be read. Programming and resetting only possible with right (TB, SZ)

Program/read locks (SP)

→ Unknown locks can be read. Resetting possible. Programming only possible with right (SB, SZ)

Edit transponders and groups (TB)

→ Transponders and transponder groups can be created and edited. Programming only possible with right (TP, SZ)

Edit locks and areas (SB)

→ Locks and areas can only be created and edited. Programming only possible with right (SP, SZ)

Configure network (NK)

→ Network settings and local device settings can be made

Manage network (NV)

→ Events and tasks can be set up and managed

Administration of access lists (ZA)

→ Administration of access to the access lists is permitted

Manage access lists (ZV)

→ View and edit the contents of the access lists

Staff management (PV)

→ Personal details can be changed

Use handheld (HB)

→ Exporting and importing the locking plan on handheld devices is permitted

Time management (ZW)

→ The time zone plan, time groups, public holidays and public holiday lists can be edited and changed

Print reports (BD)

→ Reports can be created, printed out and exported

Read log (PL)

→ Log can be viewed

Emergency opening (NO)

→ Emergency opening can be performed

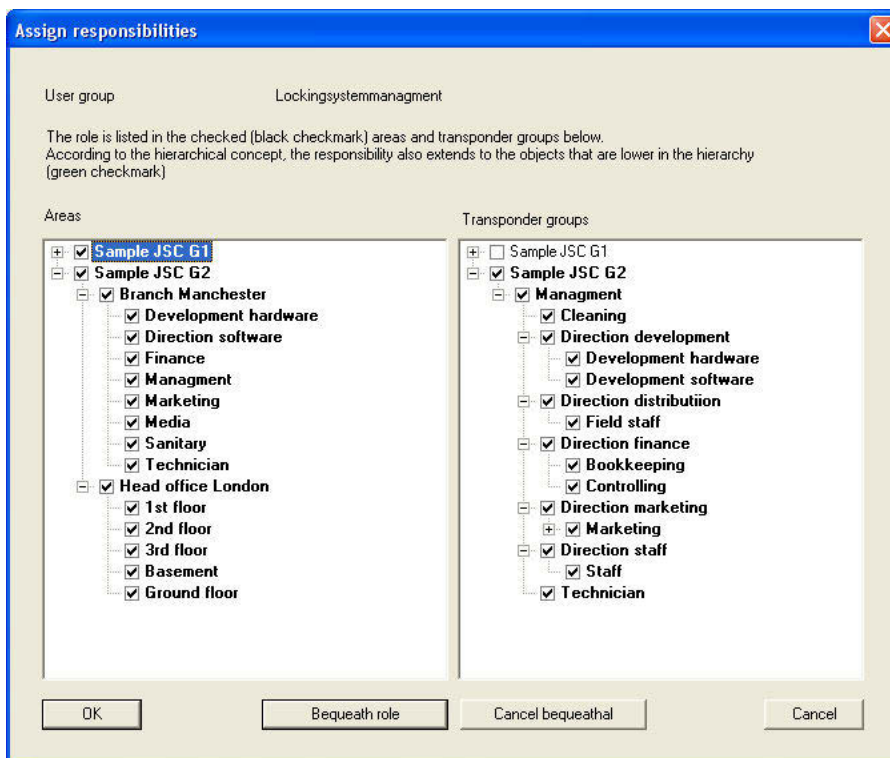
1.13.4 ROLES - RESPONSIBILITY

EXPLANATION

It is possible to restrict the user roles to certain areas and transponder groups, allowing tasks to be precisely distributed in the locking plan.

PROCEDURE

- ↻ Edit
- ↻ User group
- Edit under “Role”
- Select “Areas” and “Transponder groups”
- OK
- Apply
- Close



EXPLANATION

- “Areas” → All of the highlighted areas can be managed by the user group
- “Transponder groups” → All of the highlighted transponder groups can be managed by the user group
- Inherit role** → Subordinate areas and transponder groups are also highlighted and can therefore be

Remove inheritance → managed
Subordinate areas and transponder groups
can no longer be managed


1.13.5 CREATING A USER GROUP

PROCEDURE

- ↻ Edit
- ↻ User group
- **New**



1.13.6 EDITING A USER GROUP

PROCEDURE

- ↻ Edit
- ↻ User group
- Select user group using arrow buttons 
- Change user group
- **Apply**

1.13.7 DELETING A USER GROUP

PROCEDURE

- ↻ Edit
- ↻ User group
- Select user group using arrow buttons 
- Data record ↻ Remove or 

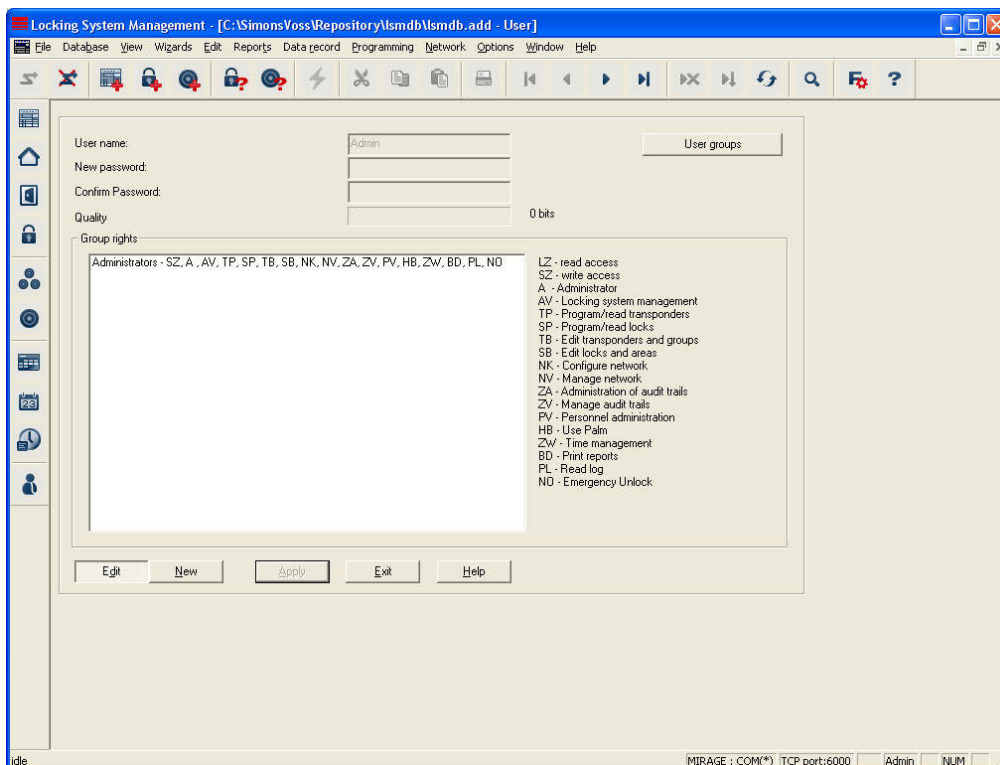
1.14. USER

EXPLANATION

Users authenticate themselves on the LSM by entering their user name and password. Users are specified in the log, making it possible to trace which user performed a certain procedure. Users receive their rights in the locking plan through the user group.

PROCEDURE

- ↻ Edit
- ↻ User



EXPLANATION

- | | | |
|--------------------|---|---|
| “User name” | → | Name with which the user logs into the LSM |
| “New password” | → | Password with which the user authenticates himself or herself on the LSM |
| “Confirmation” | → | Confirmation of the above password when creating or changing the password |
| “Quality” | → | Quality index of the entered password |
| “Group rights” | → | Displays the assigned groups and their rights |
| User groups | → | Calls up the user group management |
| New | → | Creates a new user |


1.14.1 CREATING USERS

PROCEDURE

- ↻ Edit
- ↻ User
- New



1.14.2 CHANGE USER

PROCEDURE

- ↻ Edit
- ↻ User
- Select user using arrow buttons 
- Change user
- Apply

1.14.3 DELETING USERS

PROCEDURE


- ↻ Edit
- ↻ User
- Select user using arrow buttons 
- Data record ↻ Remove or 

1.14.4 ASSIGNING A USER GROUP

EXPLANATION

- To issue a user with rights in a locking plan, the user must be assigned to a user group. A user can be a member of more than one group.

PROCEDURE

- ↻ Edit
- ↻ User group
- Select user group using arrow buttons 
- Click on Edit under “User”
- Select user
- Add
- OK
- Apply

6.0 USER MANAGEMENT (LSM BASIC EDITION)

With components from SimonsVoss it is possible to log instances of access or attempted access by transponders at locks (cylinders, SmartRelais) when corresponding fittings are installed.

Even the system administrator should not have access to this data for data protection and internal company reasons. Where necessary, this data may be accessed by the company's data protection officer or works council observing legal and company regulations.

The user concept described in chapter 2.3 is therefore also used in the LSM Basic Edition. User data and the associated roles (user groups) are predefined and cannot be modified by the user.

Any customisation or extension required can be made using the LSM Business Edition or higher.

1.15. DEFAULT SETTINGS

User groups:

1. Administrators with all roles,
however the "Administration of access lists" and "Manage access lists" roles can be removed from this group.
2. Access list administrators
with the following roles (read access only):
 - Manage access list
 - Administration of access lists
 - Program transponders
 - Program locks
 - Edit transponders and groups
 - Edit locks and areas
 - Use handheld

Users:

3. Admin
Member of "Administrators" user group
4. Admin AL (Administrator Access List)
Member of "Administration of access lists" user group

Authorisations

5. The "Administration of access lists" group has access to system groups and system areas
6. Admin is allowed to select areas and transponder groups in the "Administration of access lists" group

7.0 INHERITANCE PRINCIPLE

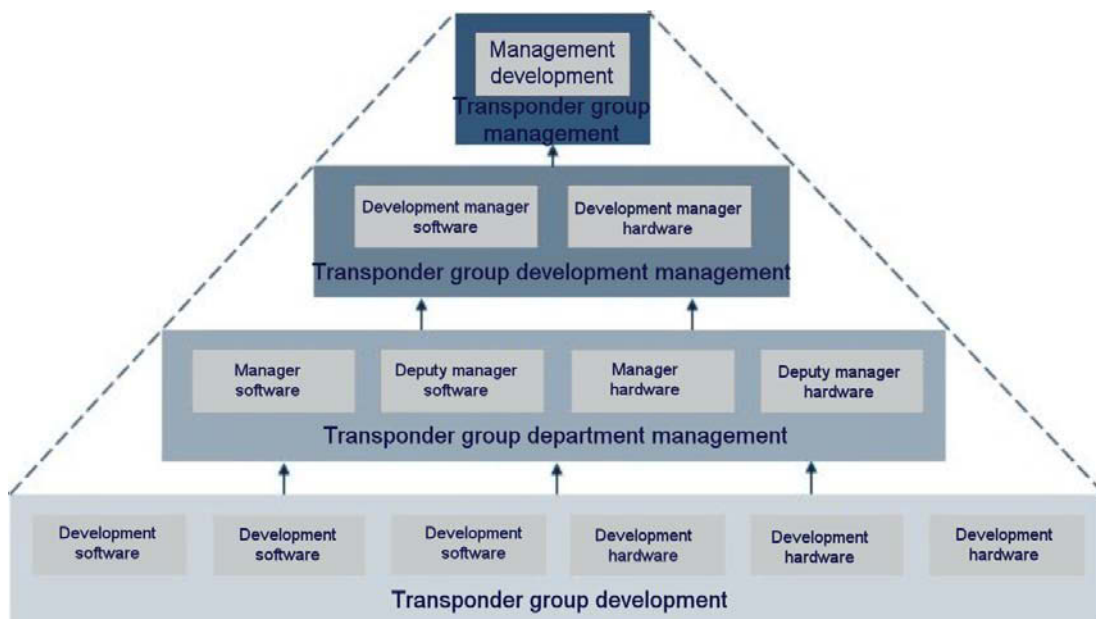
1.16. GENERAL

Inheritance is a way of representing a company's hierarchy in the locking system. When inheritance is implemented correctly, it greatly reduces the user's workload. It allows you to automate certain processes by assigning a transponder to a particular transponder group. Transponders can therefore be automatically authorised and activated in locks without the user having to perform any additional steps such as authorising in the individual locks.

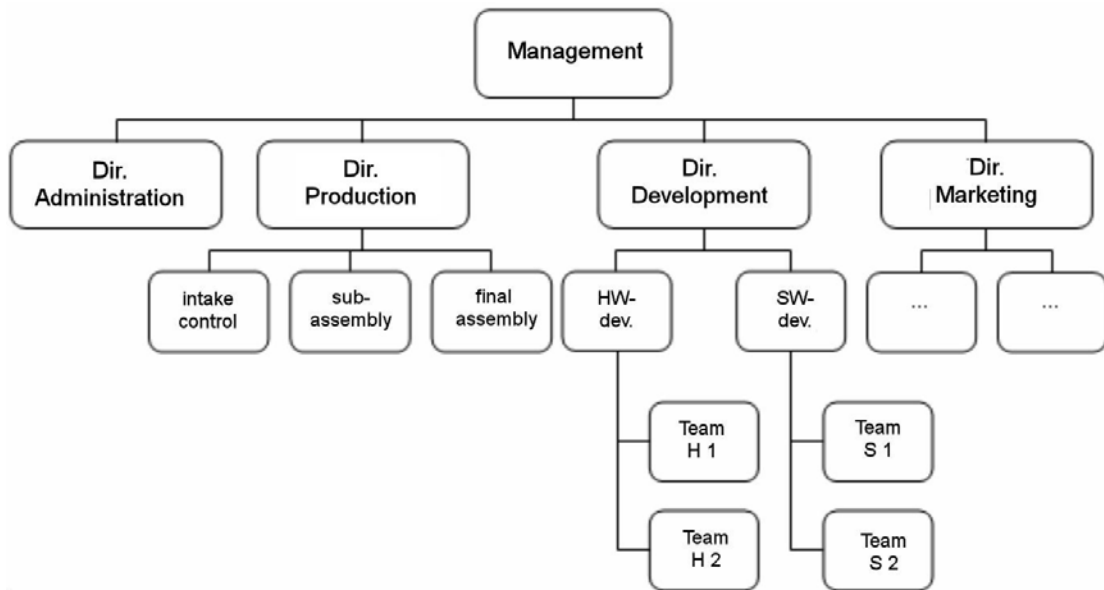
1.17. TRANSPONDER GROUP HIERARCHY

EXPLANATION

In LSM, the staff structures are mapped on transponder groups. A company's staff structure can be represented by a hierarchy in the transponder groups. The more structured a company is, the easier it is to display it in the hierarchy of transponder groups.



EXAMPLE



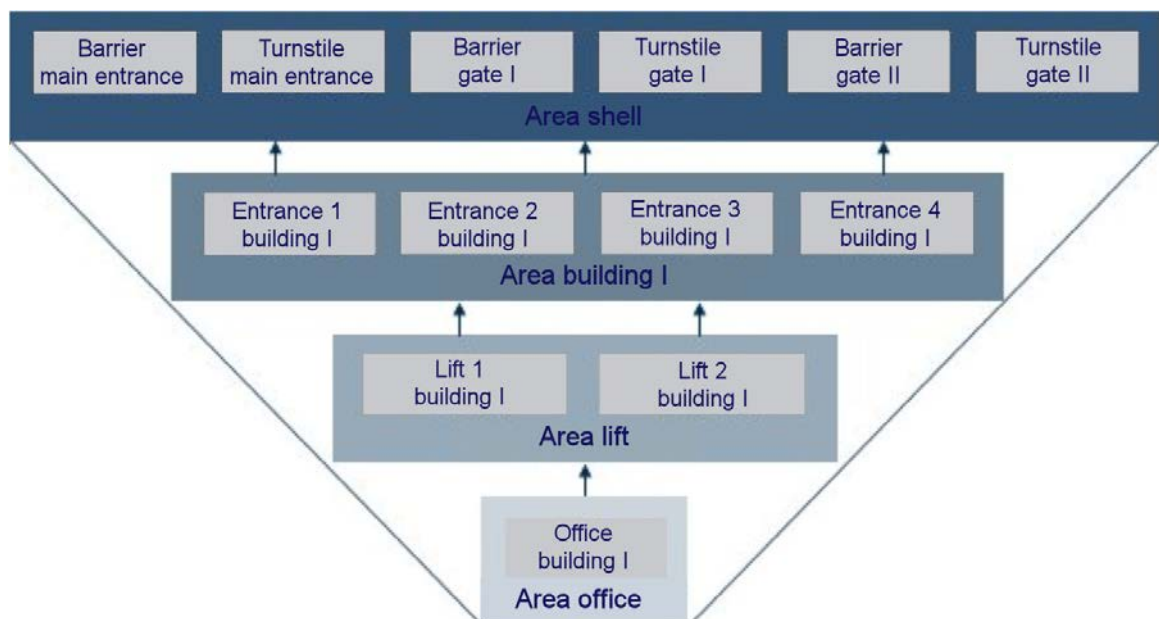
In the example above, the “S2 team” forms one transponder group. The same applies for the “Software Development” team leader, the head of the “Development” department and the management team. If a person is being added to the “S1 team” transponder group, the superordinate transponder groups are also automatically authorised if inheritance is activated. Because the transponder group for the management team is located right at the top of the hierarchy and therefore receives a multitude of locking authorisations in the locking system, it normally has very few transponders.

1.18. AREA HIERARCHY

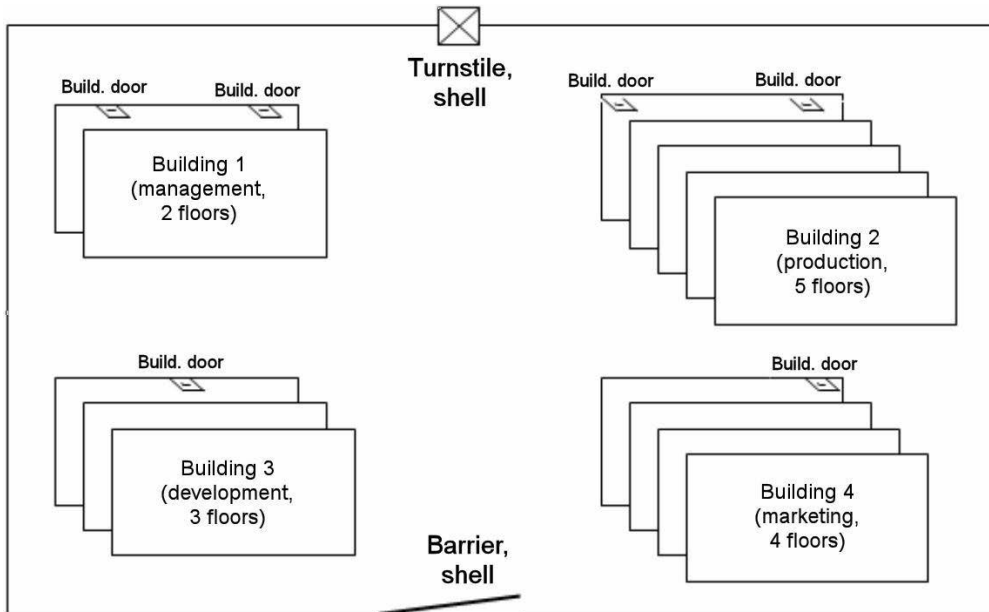
EXPLANATION

In LSM, the authorisation structure is represented by areas. A building's usage structure can be represented by a hierarchy in the areas. A superordinate area can basically have any number of subordinate areas, while a subordinate area can only have one superordinate area.

Doors that are accessed very often and by many different people should be located at the top of the structure. All of the transponders with authorisations in a specific area are automatically authorised in the areas above it.



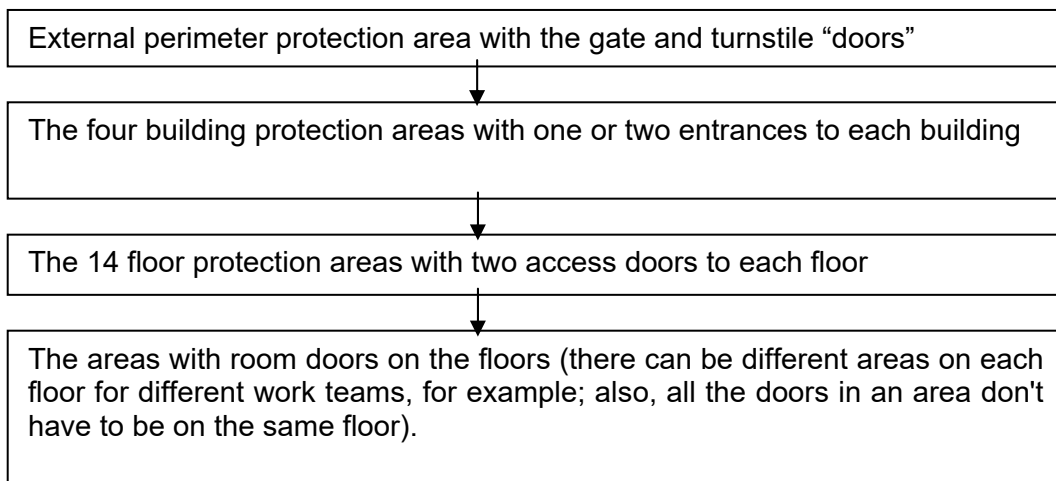
EXAMPLE

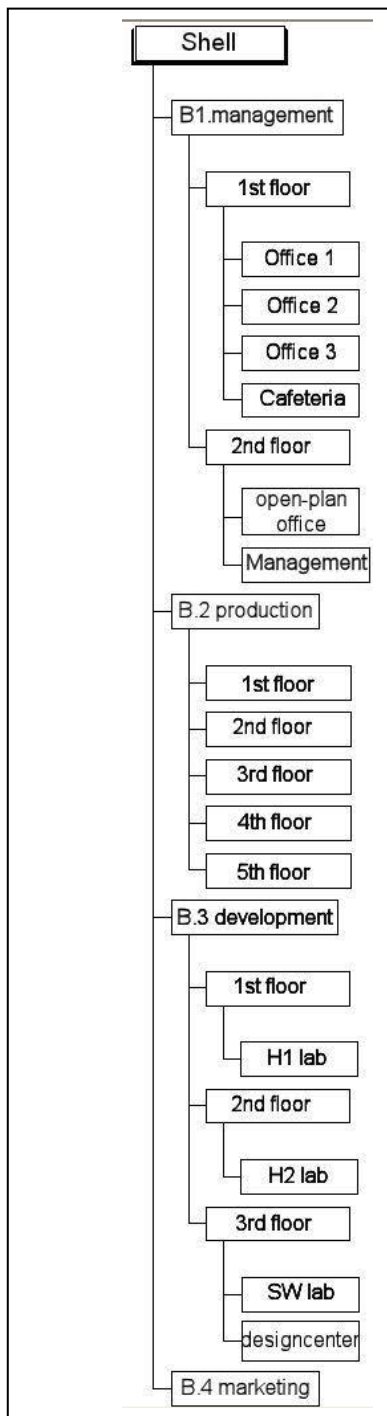


The diagram above shows a typical industrial location with 4 buildings for management, development, marketing and production.

- The external perimeter of the grounds is protected by a fence, gate, and turnstile.
- The buildings have one or two entrance doors
- The buildings also have a different number of floors, which are protected by 2 doors on each floor to the stairwell or lifts, for example.
- On the individual floors, offices and production rooms are protected by office doors and fire-retardant doors.

These basic conditions result in a simple 4-level hierarchical room structure:





The dependencies of the individual areas can be clearly represented in an organisational chart using a tree structure.

EXAMPLE:

The superordinate “external perimeter” area is made up of the 2 gate and turnstile “doors”.

This area has 4 subordinate areas:

Building 1 area: the 2 entrance doors to the management building (building 1)

Building 2 area: the 2 entrance doors to the production building (building 2)

Building 3 area: the entrance door to the development building (building 3)

Building 4 area: the entrance door to the marketing building (building 4)

The building 1 area itself has a superordinate external perimeter area and 2 subordinate areas, each consisting of 2 floor protection doors on both floors of the building, etc.

1.18.1 ISSUING AUTHORISATIONS AND INHERITANCE CONCEPT

If a transponder group is authorised to an area, the reserve for the transponder group is programmed into the lock when the locks are programmed. Normally, this means that these locks don't need to be programmed again if a new employee is added to this transponder group, because this transponder has a transponder ID from the reserve that is already authorised in the locks for the area.

If a transponder group is authorised in a certain area, this authorisation is inherited in a directly ascending line by the area one level higher, where it then continues to be inherited until it reaches the highest area, which is the external perimeter in our example.

A similar inheritance takes place in the transponder group hierarchy. If a transponder group receives an authorisation for a certain area, this authorisation is automatically inherited by the transponder group one level higher. In our example, the department managers' transponder group passes on its authorisation to the management's transponder group.

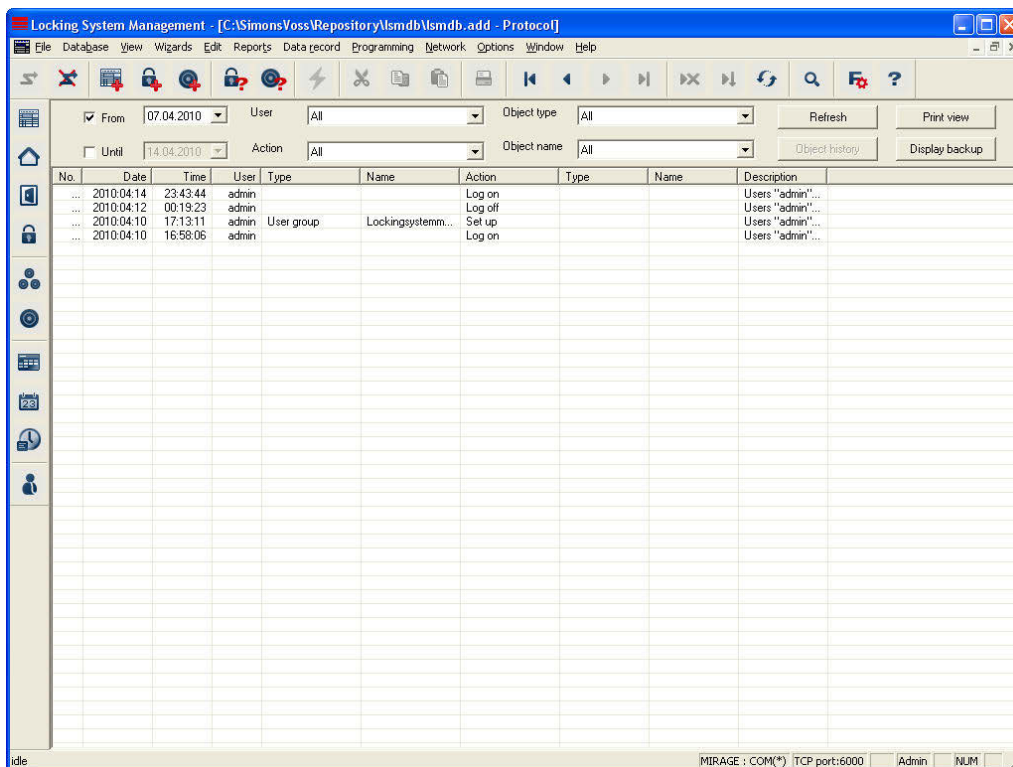
8.0 LOGGING

EXPLANATION

All of the user actions that change the status of the system are written in the log file. These records show the actions performed, who initiated them and when (thanks to date stamping and continuous numbering). The data in this file cannot be deleted individually and is stored for around half a year as standard. Complete traceability can therefore be guaranteed through the use of appropriate backup strategies. Logging in LSM is audit-compliant, in other words, individual entries cannot be changed.

PROCEDURE

- ➡ View
- ➡ Log

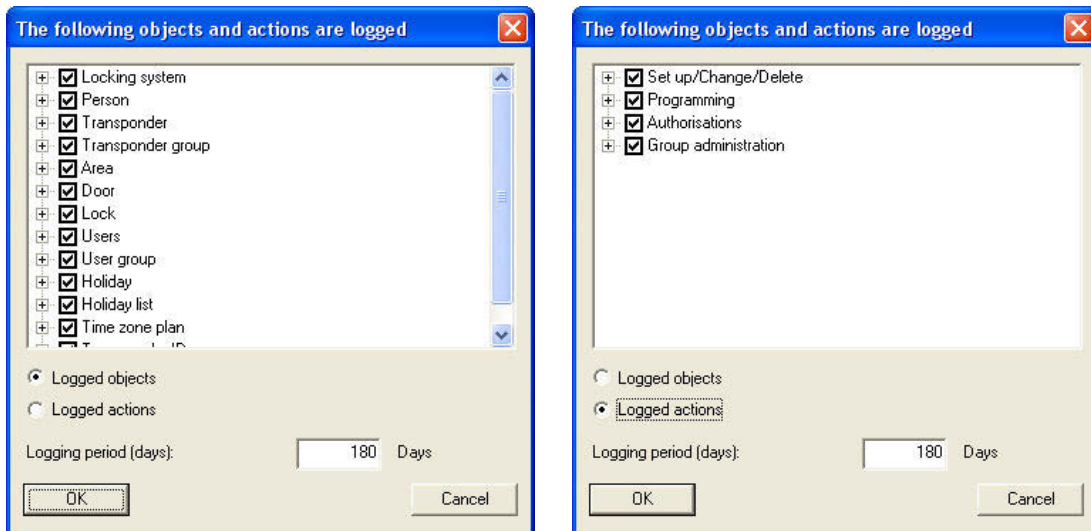


The volume of data displayed can be filtered by various criteria using the selection boxes, which increases clarity. For example, information can be accurately filtered for certain time periods, such as actions for certain locking system objects (doors, locks, transponders, persons, etc.).

NOTE

You will find checkboxes for the objects and actions to be logged under ➡ Options ➡ Logging.

MANUAL LSM – ADMINISTRATION



The logging options can either be viewed by the individual objects in the locking plan or by the activities in the locking plan management and can be set according to requirements. You can also set logging periods here. Older entries are deleted accordingly.

9.0 PROGRAMMING DEVICE

All of the settings for an attached programming device, (ConfigDevice), the configuration of the network and for tasks are made under the ↻ Network menu item.

1.19. LOCAL CONNECTIONS


1.19.1 GENERAL

EXPLANATION

The programming devices that are connected to the computer, for example, the SmartCD , are configured using the item ↻ Network ↻ Local connections. Please refer to the device descriptions for the interface required for connection.


1.19.2 SETTING UP SMARTCD

PROCEDURE

- ↻ Network
- ↻ Local connections
- Check computer name
- Select computer using arrow buttons 
- Add
- Search for SmartCD
- OK
- Apply

1.19.3 TESTING SMARTCD

PROCEDURE

- ↻ Network
- ↻ Local connections
- Check computer name
- Select computer using arrow buttons 
- Highlight device in list
- Test

10.0 TIME CONTROL

1.20. GENERAL

The time zone control for the system 3060 enables transponders to be authorised for certain locks in a time-dependent manner. So-called time zone plans, which can save different authorisation times for various groups with access authorisation (the time groups), are the key element for this. It isn't just different weekdays that are taken into account for this process, the program also recognises Sundays and public holidays, individual public holidays and holiday periods. Each time zone plan can manage several time groups with different authorisation times and is assigned one or more areas. Transponder groups are assigned one of the possible time groups, so that an area can accept different, time-dependent authorisation groups with its time zone plan. Internally, each lock manages an additional time group (group 0), which contains all of the transponders that were not assigned to a time group and therefore have access authorisation at all times.

NOTE

Please take care when using time zone control. You should incorporate tolerance times and take into account possible exceptional situations in which access may be necessary outwith plan times.

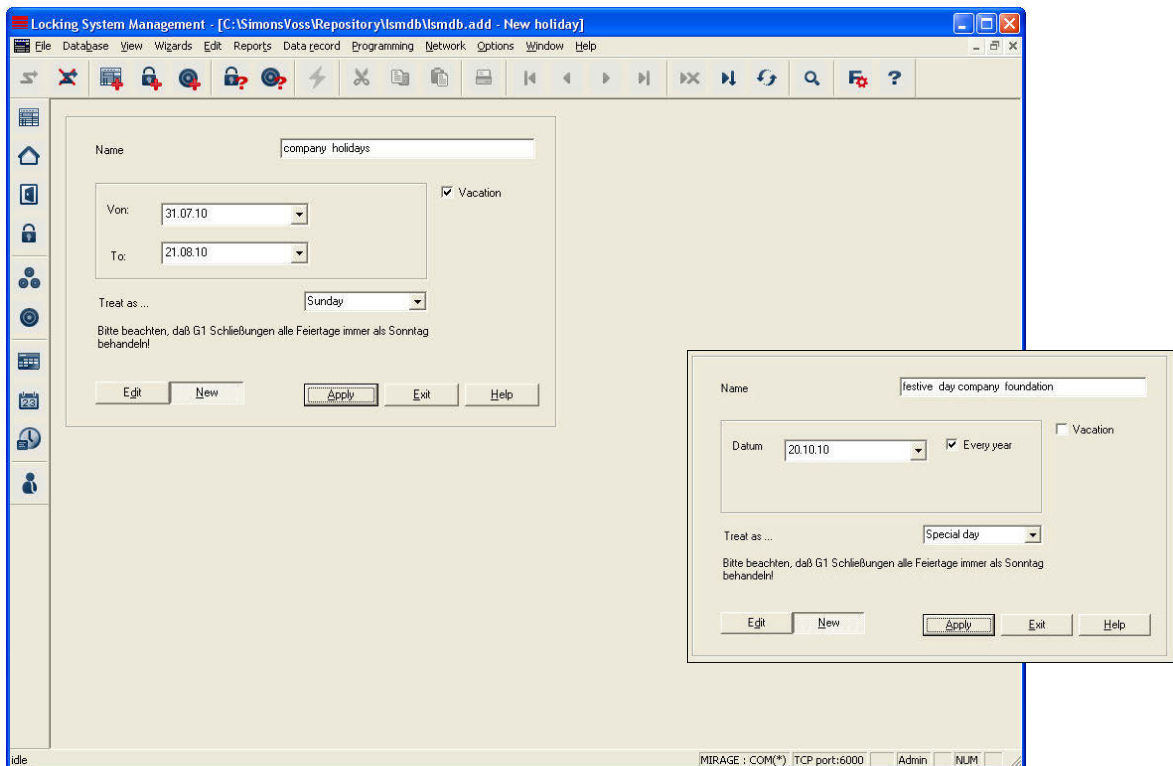
PROCEDURE

- Select / create public holiday list
- Create time zone plans
- Assign a time zone plan to areas
- Assign a time zone group to transponder groups

1.21. PUBLIC HOLIDAYS

1.21.1 GENERAL

In LSM, you can create your own public holidays or holiday periods regardless of the public holiday lists that already exist. You can also edit existing public holidays, add new ones and delete them. These public holiday lists and the associated public holidays are used in conjunction with the time zone plans to control access of person groups to areas.



EXPLANATION

- | | |
|----------------|--|
| “Name” | → Designation of public holiday |
| “Holiday” | → A time period may only be entered if this option is selected |
| “From” | → Start of time period |
| “Until” | → End of time period |
| “Date” | → Calendar day entry |
| “Every year” | → Determines whether entry should be repeated every year |
| “Treat as ...” | → Used daily profile (only possible with G2) |


1.21.2 CREATING A PUBLIC HOLIDAY

PROCEDURE

- ↻ Edit
- ↻ Public holiday
- New
- Enter data
- Apply

1.21.3 EDITING A PUBLIC HOLIDAY

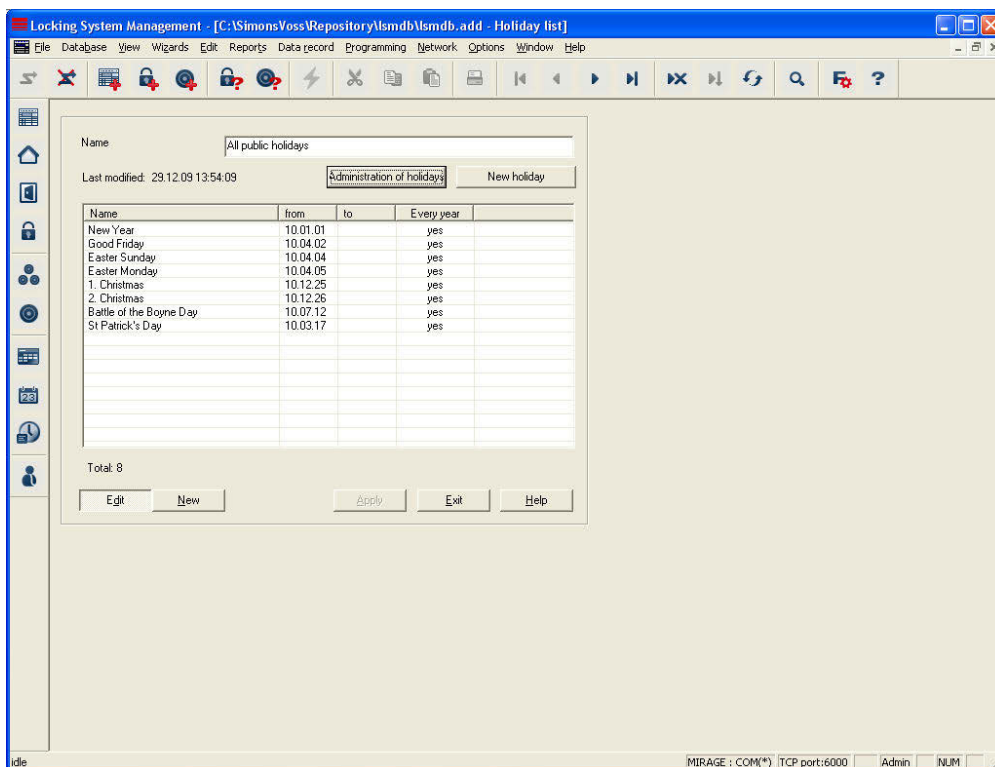
PROCEDURE

- ↻ Edit
- ↻ Public holiday
- Select public holiday using arrow buttons 
- Change settings
- Apply

1.22. PUBLIC HOLIDAY LIST

1.22.1 GENERAL

A public holiday list manages all of the days which should be treated as deviating from normal days. It makes a distinction between weekdays and weekends, public holidays and holiday periods. These days apply to all users assigned to a time group.



“Name”

→ Name of public holiday list (e.g. Region)
The key public holiday lists are already saved here, you can add your own at any time.

Last change

→ Date of last revision
If you change public holiday lists, editing of the public holidays means that programming is required in all areas with time zone plans in which this public holiday list is used.

Public holiday management

→ Add a public holiday or remove one from the list displayed

New public holiday

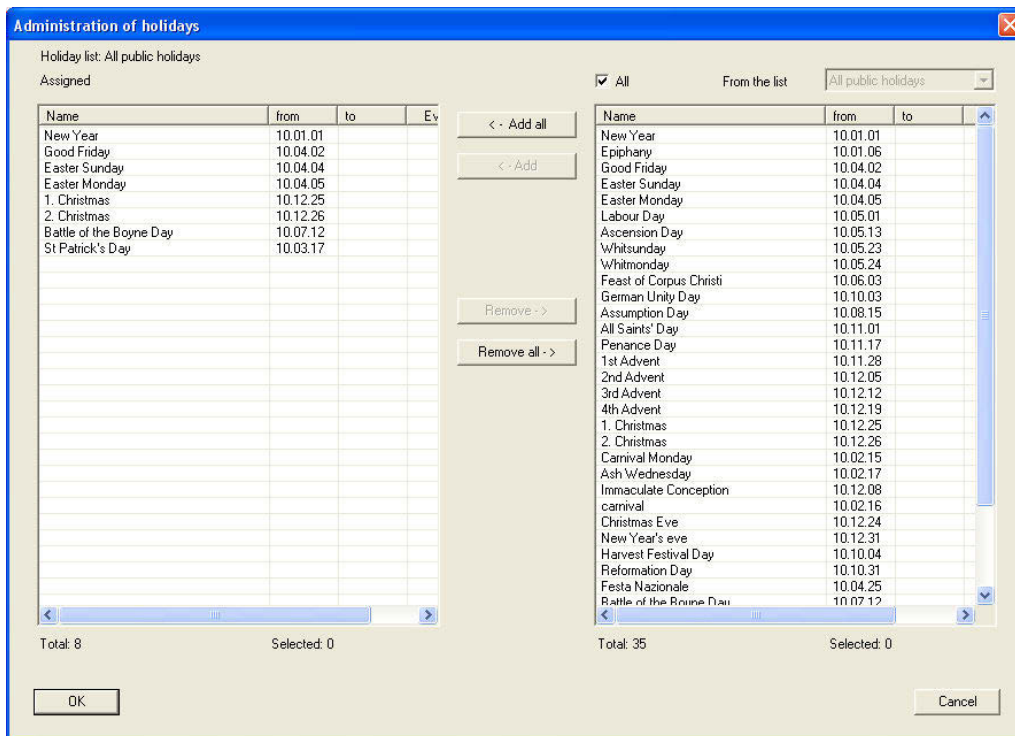
→ Creates your own public holiday

Table

→ List of public holidays

1.22.2 PUBLIC HOLIDAY MANAGEMENT

Depending on your region, you can assign various public holidays from prepared lists to your own public holiday list. You can also set your own public holidays, such as bridging days and holiday periods and assign them to the public holiday list. If you want to set time plans at a later date, the public holidays from the public holiday lists are given time authorisations that are set for the individual days.



EXPLANATION

“Public holiday list xyz”
Table “Assigned”
“All”

“From the list”

Add all

Add

Remove

Remove all

- Name of public holiday list (e.g. region)
- List of public holidays already used
- All of the entered public holidays are displayed
- Only public holidays from the list selected (e.g. Bavaria) are displayed
- All of the public holidays on the right are added.
- All of the public holidays highlighted on the right are added.
- All of the public holidays highlighted on the left are removed.
- All of the public holidays on the left are removed.

1.22.3 CREATING A PUBLIC HOLIDAY LIST

PROCEDURE

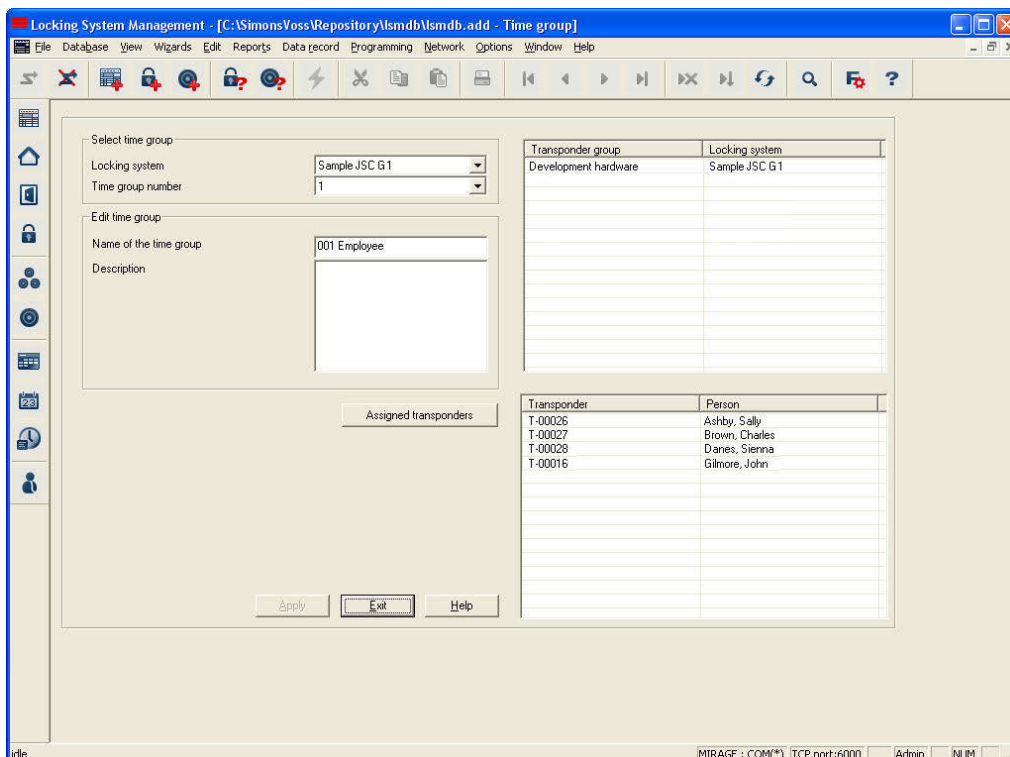
- ↻ Edit
- ↻ Public holiday list
- New
- Make entries
- Apply

1.23. TIME GROUPS

1.23.1 GENERAL

To simplify the process of assigning groups to the areas in question when creating time zone plans, you can assign the time zone groups names that are easy to understand instead of numbers. These designations apply to the entire locking system. But you must remember that these named time groups may have different authorisation times in the individual time zone plans. They are always oriented towards the settings in the corresponding time zone plan for the area in which they were set up. You can therefore create your own time zone plan with up to five different time zone groups for each area in your locking system. Each transponder group can be assigned one of these groups. This makes time zone control very complex.

The names created here are used to assign time groups to transponder groups later on.



EXPLANATION

| | | |
|-----------------------|---|---|
| “Locking system” | → | Locking system for which the settings are to be used |
| “Time group number” | → | Number of time group (G1 1-5, G2 1-100) |
| “Name of time group” | → | Name that can be freely issued |
| “Description” | → | Free field for describing the time group |
| List, top | → | Overview of the transponder groups assigned to the time group |
| List, bottom | → | If a transponder group is highlighted at the top, the associated transponders are displayed at the bottom |
| Assigned transponders | → | A report is created with an overview of the transponders for the time group selected |

1.23.2 ASSIGNING A TIME GROUP NAME

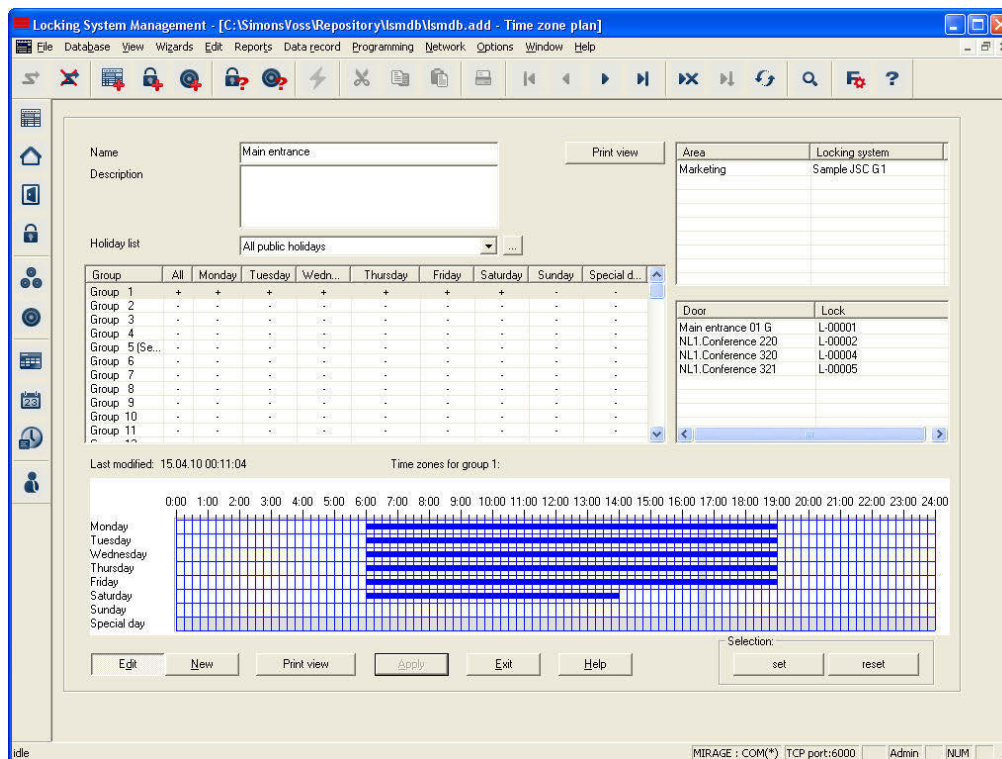
PROCEDURE

- ↻ Edit
- ↻ Time group
- Select “Locking system”
- Select “Time group number”
- Change “Name of time group”
- Apply

1.24. TIME ZONE PLAN

1.24.1 GENERAL

Once you have created your own public holidays and public holiday lists, you can now create so-called time zone plans, which record different authorisation times for each day of the week and later assign them to one or more areas. Each plan can manage different time groups, which are then assigned to transponder groups.



EXPLANATION

- “Name” → Name of time zone plan
- “Description” → Free field for describing the time zone plan
- “Public holiday list” → Public holiday list which is saved in the time zone plan
- ... → Jumps to properties for the public holiday list
- Table → Overview of assignment of the individual days for the individual time groups
- Last change → Date of last revision
If you change the time windows, you need to program all of the areas in which this time zone plan is used.
- Time window → Time window to highlight the time period in which the time groups can open the assigned locks. Each block is 15 minutes

- | | | |
|--------------|---|--|
| List, top | → | long. Overview of the areas assigned to the time zone plan |
| List, bottom | → | If an area is highlighted at the top, the associated doors are displayed at the bottom |
| Set | → | The highlighted time period is entered |
| Reset | → | The highlighted time period is removed |

1.24.2 CREATING A TIME ZONE PLAN

PROCEDURE

- ↻ Edit
- ↻ Time zone
- New
- Issue “Name” and brief “Description”
- Select “Public holiday list”
- Highlight the desired group
- Highlight the desired time window
- Assign the permitted access times (e.g. 5.30 am to 4.45 pm); each box stands for a quarter of an hour. Individual blocks can be highlighted, associated time periods can be set or reset by right-clicking and then dragging
- Apply
- Close

NOTE

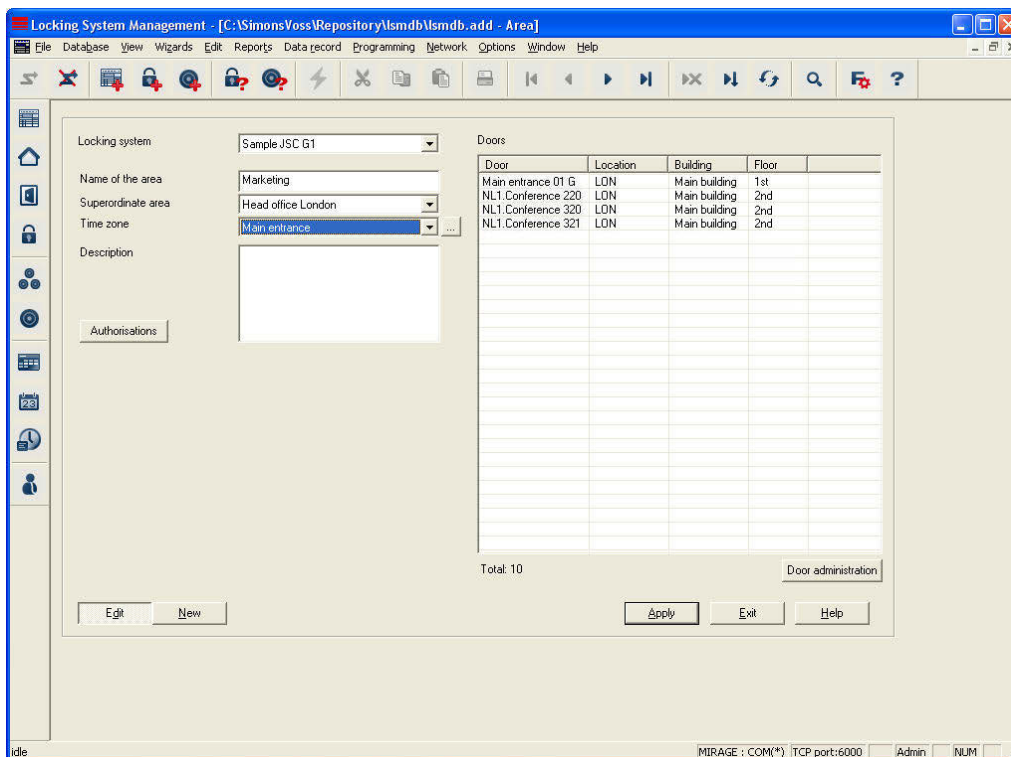
Proceed as outlined above to create more time zone plans or edit other time groups in a time zone plan.

1.25. USING TIME MANAGEMENT

1.25.1 TIME ZONE PLANS

If time zone plans were created before the rest of the database objects, you can immediately assign the valid time zone plan when you create a new area, for example. But it is of course possible to assign it later on. But you should remember that you will then have to program the locks in the area.

1.25.2 TIME ZONE PLANS ON AREAS



EXPLANATION

- “Locking system” → Area’s locking system
- “Name of area” → Designation of area
- “Superordinate area” → Details of the area one level higher in the hierarchy
- “Time zone” → Details about the time zone of the area
- ... → Displays properties for the selected time zone
- “Description” → Free field for describing the area
- Door management → Displays and adds doors
- Authorisations → Authorised transponder groups can be set

PROCEDURE

- ↻ Edit
- ↻ Area

or

- Right-click on Area
- Left-click on Properties

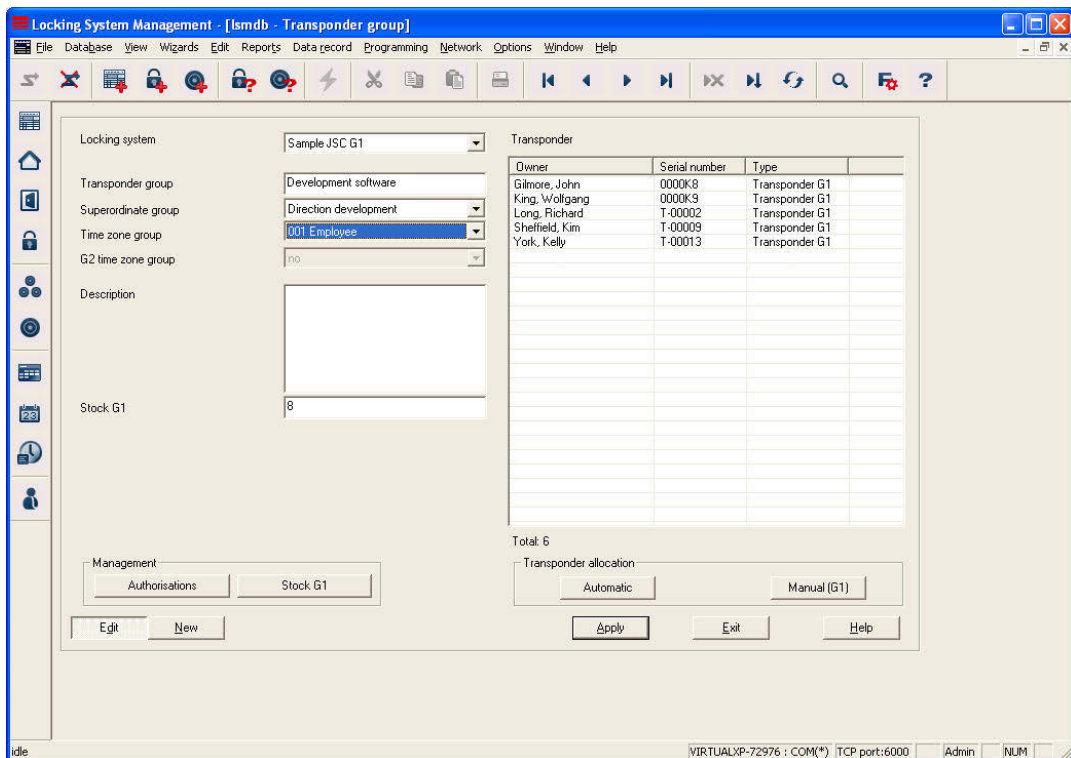
then

- Select “time zone”
- Apply
- Close

MANUAL LSM – ADMINISTRATION

1.25.3 TIME GROUPS ON TRANSPONDER GROUPS

Please remember that if you assign a time group to a transponder group later on, you will have to program all of the transponders in the transponder group!



EXPLANATION

- "Locking system" → Select the created locking system
- "Transponder group" → Name of transponder group
- "Superordinate group" → Transponder group assigned to a higher position in the hierarchy
- "Time zone group" → Specifies the time group for the transponder group
- "G2 time zone group" → Specifies the time group for G2 components in the transponder group
- "Description" → Free field for describing the transponder group
- "Reserve G1" → Total number of transponder IDs (G1) available in the transponder group
- Authorisations → Option of issuing group authorisations
- Reserve (G1) → Option of managing the transponder IDs (G1 only)
- Automatic → Option of automatically assigning a free transponder to the transponder group
- Manual → Option of manually assigning a particular transponder to a particular transponder ID

PROCEDURE

- ↻ Edit
- ↻ Transponder group

or

- Right-click on a transponder group
- Left-click on “Properties”

or

- Double-click on the transponder group designation in the matrix

then

- Select “Time zone group”
- Apply
- Close

11.0 OPTIONS

You can call up settings and functions that support working with the locking system under the Options menu item.

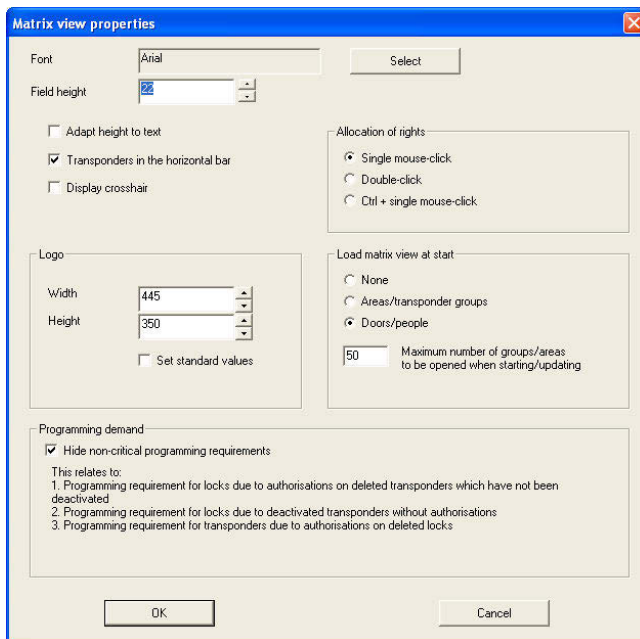
1.26. SETTING UP MATRIX VIEW

EXPLANATION

Each user can configure their preferred view as the standard view. This view is displayed once the user logs on. Various basic settings can also be activated here.

PROCEDURE

- ➔ Options
- ➔ Matrix view



EXPLANATION

- “Font” → Standard font and font size
- “Field height” → Adjust the height of rows and columns
- “Adapt height to font” → When this option is selected, the font size and row height are automatically optimised.
- “Transponders to horizontal bar” → When this option is selected, transponders / persons are positioned (horizontally) as column headings. Horizontal is standard.
- “Show crosshair” → The crosshair, which aids orientation in large matrices, is displayed.
- “Logo” → This enables you to change the size of the logo in the top left-hand corner of the matrix. This can also be done in the matrix itself by dragging the mouse. By changing the size of the logo you define the height or width of the column and row names.
- “Issue authorisations” → To avoid issuing an authorisation accidentally you can choose from 3 options as to when an authorisation cross should be set
- “Load matrix view on start-up” → Select your preferred start view and the number of groups / areas which are automatically opened. The more groups and areas displayed in the matrix, the longer it takes to structure them. You can limit the number of groups / areas to be opened to enable quicker matrix updating and starting.
- Hide non-critical programming requirements → So-called non-critical programming requirements (i.e. no direct need for action on behalf of the administrator) can be hidden in order to improve clarity in large locking systems. The effects are described immediately.

1.27. ADDITIONAL COLUMNS IN LABEL BARS

EXPLANATION

Extra columns can be added to both the horizontal and vertical bars to provide the user with useful additional information. The settings made only apply to the particular view where they are made. So different information will be available depending on the view being used.

The order of the data shown can also be set individually.

PROCEDURE

- ➡ Options
- ➡ Extra columns
- Make selection, e.g. transponders / persons

POSSIBLE EXTENSIONS FOR TRANSPONDERS / PERSONS

- Name NAME
- Department AB
- Number of data records ND
- E-mail EM
- Period of validity EXPIRY
- Location ORT
- Employee number PN
- Programming requirement PB
- Serial number SN
- Phone number TN
- Title TITEL
- Type TP
- Time group (image) ZB
- Time group name ZN
- G2 time group name ZN G2
- Time group number ZG

POSSIBLE EXTENSIONS FOR LOCKS / DOORS

- Name NAME
- Outer dimensions AM
- Outer dimensions of door AT
- Inner dimensions IM
- Inner dimensions of door IT
- Expanded data ED
- Floor E
- Building G
- Configure N
- Network address ADDRESS
- PinCode Terminal PIN

- Programming requirement PB
- Room number RN
- Serial number SN
- SmartReader SR
- Type TP
- Time zone (image) ZB
- Time zone names ZN

POSSIBLE EXTENSIONS FOR TRANSPONDER GROUPS

- Name NAME
- Time group (image) ZB
- Time group name ZN
- Time group name ZN G2
- Time group number ZG

POSSIBLE EXTENSIONS FOR AREAS

- Name NAME
- Time zone (image) ZB
- Time zone names ZN

1.28. AUTOMATIC NUMBERING

EXPLANATION

This option allows you to specify the default used by the system to name new components when they are created.

PROCEDURE

- ➡ Options
- ➡ Automatic numbering

The screenshot shows a dialog box titled "Automatic numbering" with a close button (X) in the top right corner. It contains three sections, each with a label and a "Template" text input field:

- Personnel number**: Template field contains "P-00001".
- Serial number for transponder**: Template field contains "T-00001".
- Serial number for lock**: Template field contains "L-00001".

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

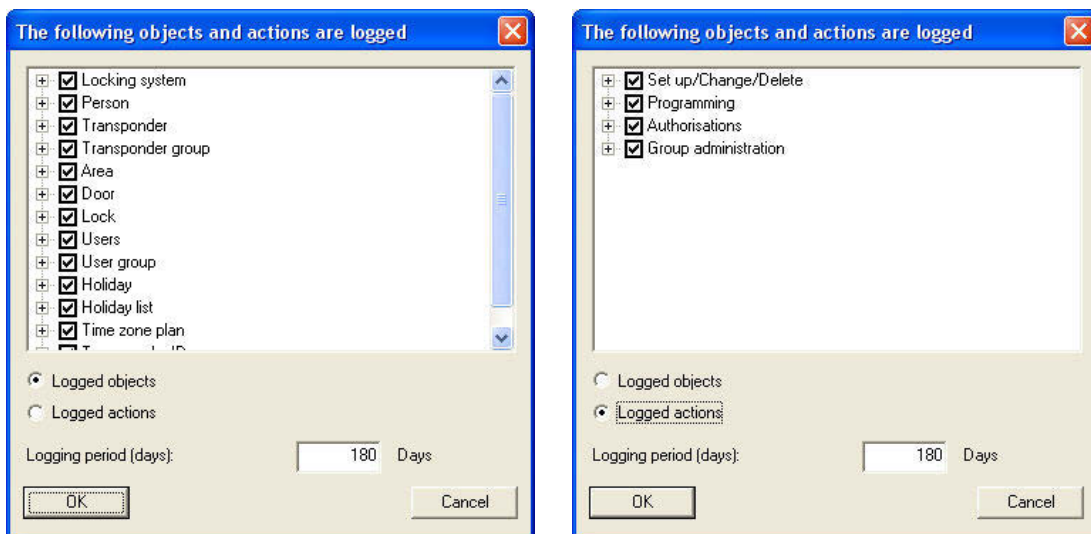
1.29. LOGGING

EXPLANATION

All of the user actions that change the status of the system are written in the log file. These records show the actions performed, who initiated them and when (thanks to date stamping and continuous numbering). The data in this file cannot be deleted individually and is stored for around half a year as standard. Complete traceability can therefore be guaranteed through the use of appropriate backup strategies. Logging in LSM is audit-compliant, in other words, individual entries cannot be changed.

PROCEDURE

- ➔ Options
- ➔ Logging



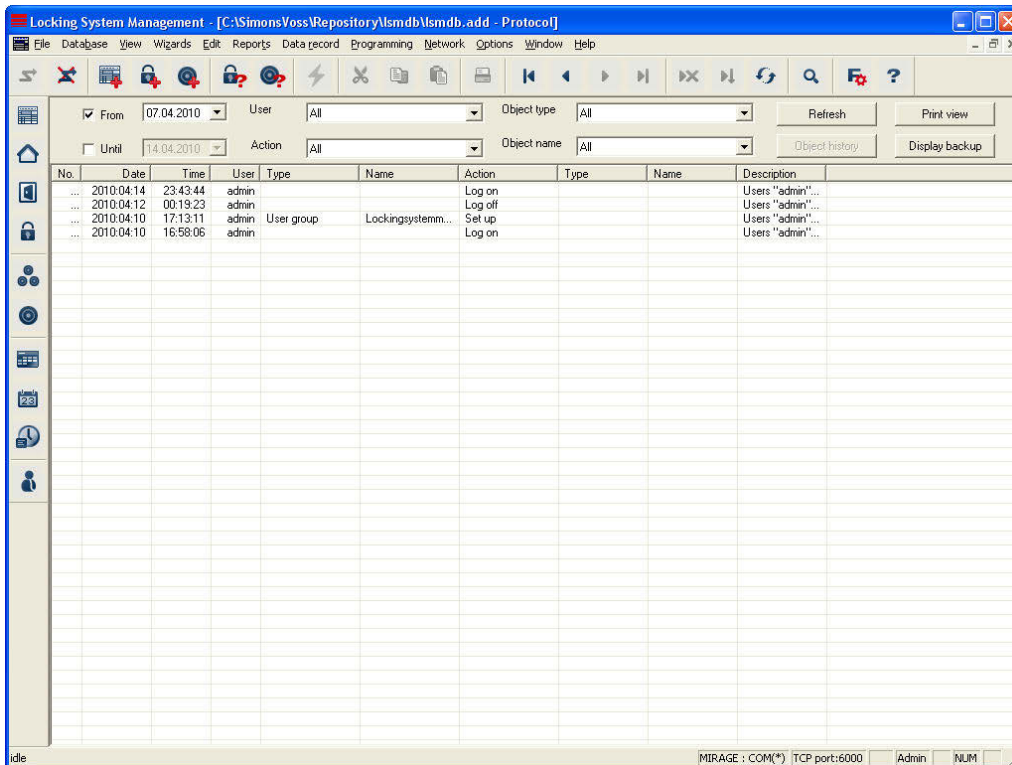
The logging options can either be viewed by the individual objects in the locking plan or by the activities in the locking plan management and can be set according to requirements. You can also set logging periods here. Older entries are deleted accordingly.

MANUAL LSM – ADMINISTRATION

Page 55

PROCEDURE

- ↻ View
- ↻ Log



The filter options allow the contents of the view to be filtered:

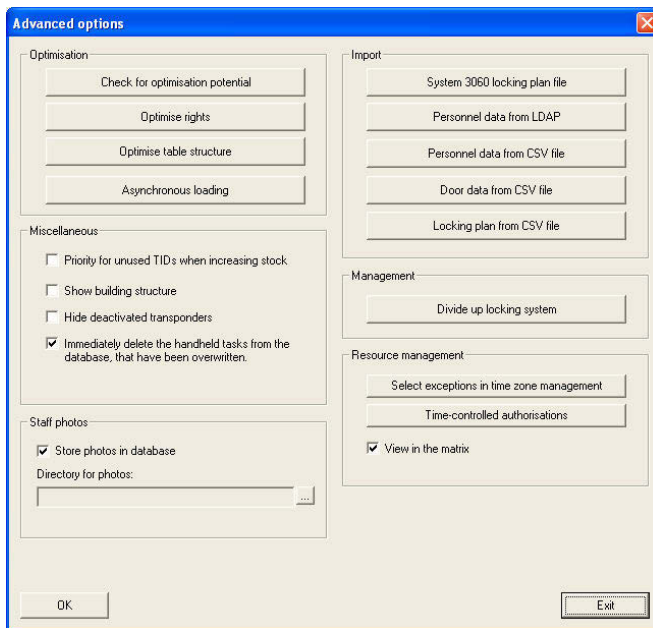
- “From”, “To” → Restriction on the period displayed
- “User” → Displays the activities of the selected user
- “Action” → Displays selected activities such as “Programming” or “Log on”
- “Object type” → Displays only certain objects such as “Locks” or “Transponders”
- “Object name” → Selection depends on the selected object type and restricts the display further.

Note:

The log can only be displayed if the Monitor module is available.

1.30. ADVANCED

Additional functions that are especially helpful when initially setting up and extending locking systems are summarised in the ➔ Advanced menu.



1.30.1 OPTIMISATION / MANAGEMENT

These functions optimise and structure the locking system structure.

Note

Only perform these functions after explicitly prompted to do so by the SimonsVoss software support team

1.30.2 IMPORTING

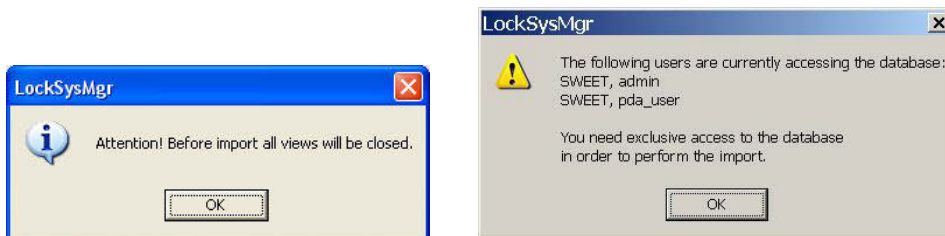
The options described below allow you to rapidly and easily create the components you need to be able to efficiently commission the locking system. These range from lists for doors and persons to using IT infrastructures. You can also import locking plan files in LDB software (locking database) from existing systems. The information the files contain about the components and programming statuses is retained, but programming may be required if you use other functions. You should comply with the data protection regulations when transferring personal data.

Note

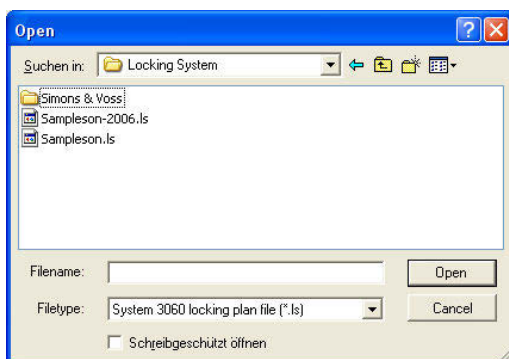
Before importing, you must contact the dealer or a SimonsVoss employee to clarify the procedure. You must also ensure that you have a working data backup of all of the relevant components (software and data) before starting the work. SimonsVoss Technologies AG accepts no liability for data transfer carried out independently or incorrectly. You should comply with the data protection regulations when transferring personal data.

1.30.2.1 SYSTEM 3060 LOCKING PLAN FILE

Before importing an LDB file, all views must be closed and in a multi-user environment, all other users/services must be logged out.



Once the views that are still open have been closed and other users have logged out, the import is performed once the LDB file has been selected. Only use copies of the original file for this import.



Select the locking plan file to be imported. Confirm with **Open**.

MANUAL LSM – ADMINISTRATION

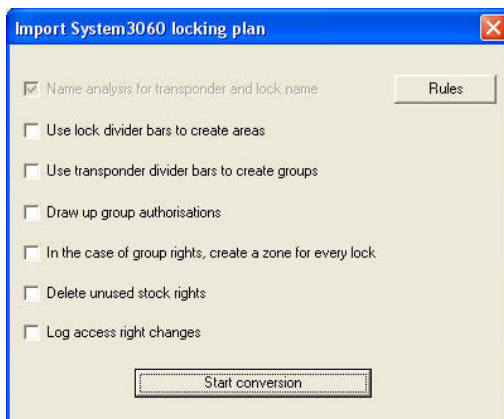
Page 58



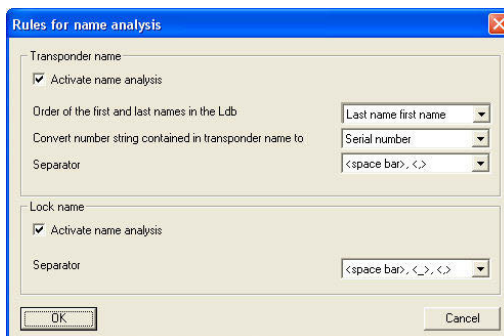
Importing is protected by the file password and locking system password so that only authorised persons can access the locking plan data. Confirm with **OK**.



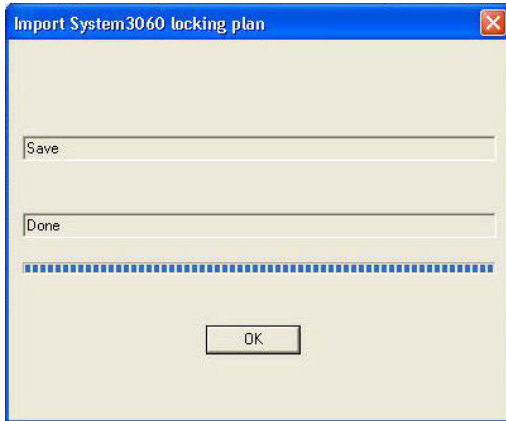
If the locking plan file contains expired public holiday plans, programming is required. Confirm with **OK**.



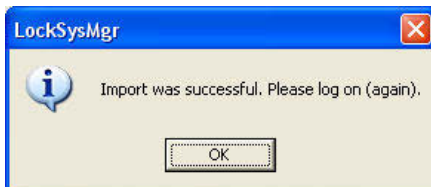
This screen determines how the locking plan data is processed. Please contact your dealer or SimonsVoss Technologies AG for the exact procedure. To adapt the import, see the next screen. Then confirm with **Start conversion**.



The conversion of available designations is determined under **Rules**. Confirm with **OK**.



The progress bar indicates the status and whether the process is complete. Confirm with **OK**.



Confirm with **OK**.

1.30.2.2 PERSONAL DATA FROM LDAP

You can use this function to query a directory service using LDAP and import personal data. You should observe the corresponding data protection guidelines.

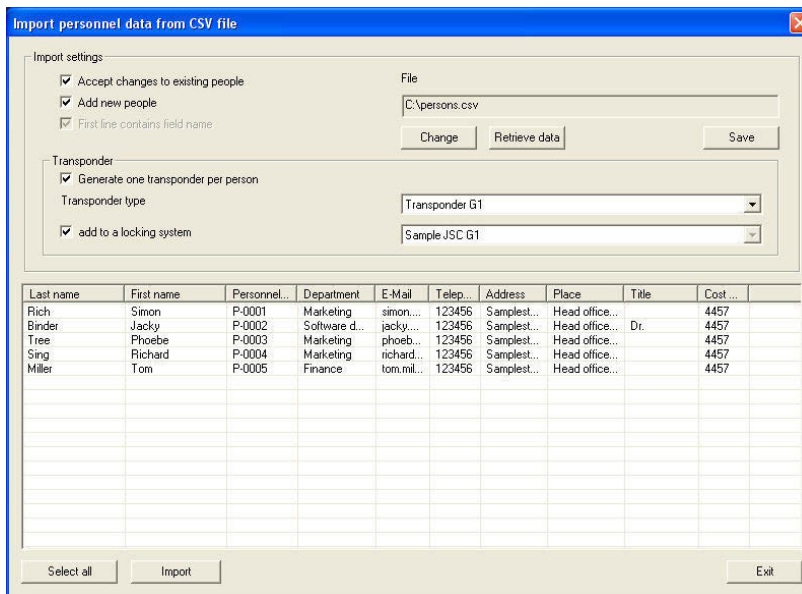
The screenshot shows a dialog box titled "Import personnel data from LDAP". It contains the following sections:

- Source:** Radio buttons for "Windows NT domain" (selected) and "Active Directory". A "Retrieve data" button is next to the "Windows NT domain" option. Below is a "Domain:" field containing "SIMONSSVOSS".
- Import settings:** Checkboxes for "Accept changes to existing people" (checked) and "Add new people" (checked).
- Transponders:** Checkboxes for "Generate one transponder per person" (checked) and "add to a locking system" (checked). Below are two dropdown menus: "Transponder type" set to "Transponder G1" and "add to a locking system" set to "Sample JSC G1".
- Name extraction options:** Radio buttons for "Do not extract" (selected), "Complete name = first name last name", and "Complete name = last name first name". A note above states: "If first name and last name do not exist, extract from the complete name:".
- Table:** A table with columns: Login, Complete name, First name, Last name, Telefon, email, Department. The table is currently empty.
- Buttons:** "Import" and "Cancel" buttons at the bottom.

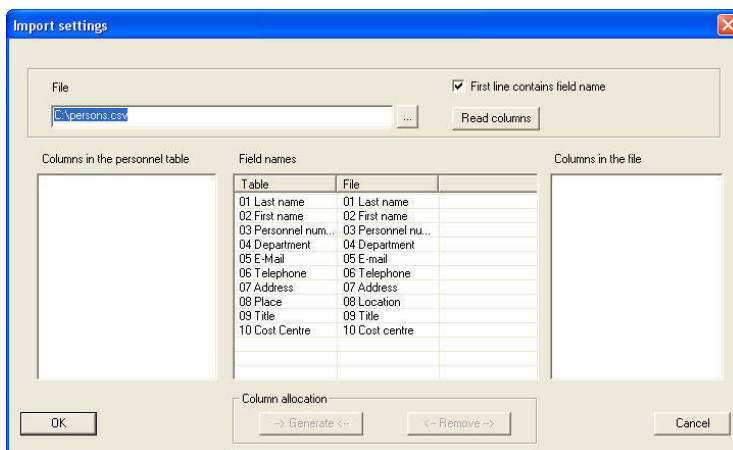
This screen determines how the data is processed. Please contact your dealer or SimonsVoss Technologies AG for the exact procedure and the required settings. Then confirm with **Import**.

1.30.2.3 PERSONAL DATA FROM A CSV FILE

You can use this function to adopt personal data from existing files in CSV format. You should observe the corresponding data protection guidelines.



The “Read” function reads in data and displays them in the lower table. The desired data records can be selected using “Select all” or by marking them individually and inserted in accordance with the settings via “Import”. You can use the “Change” function to select the desired file and perform the field assignments.

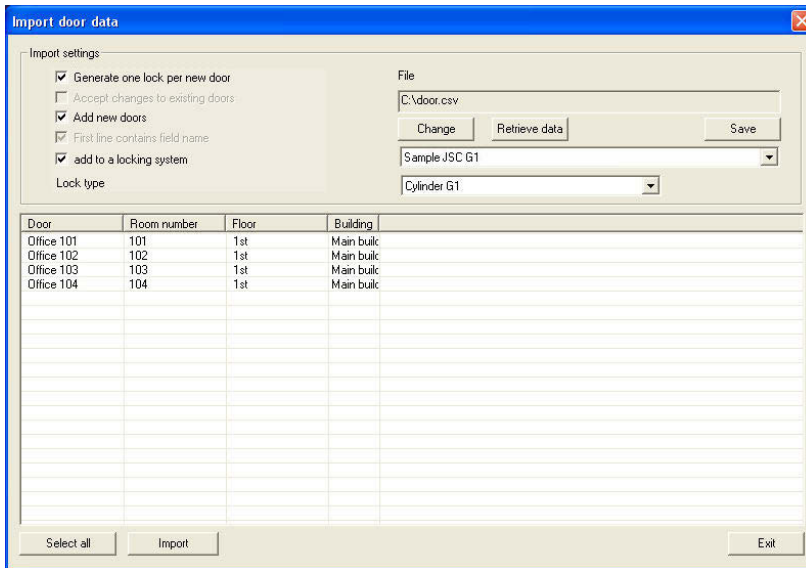


MANUAL LSM – ADMINISTRATION

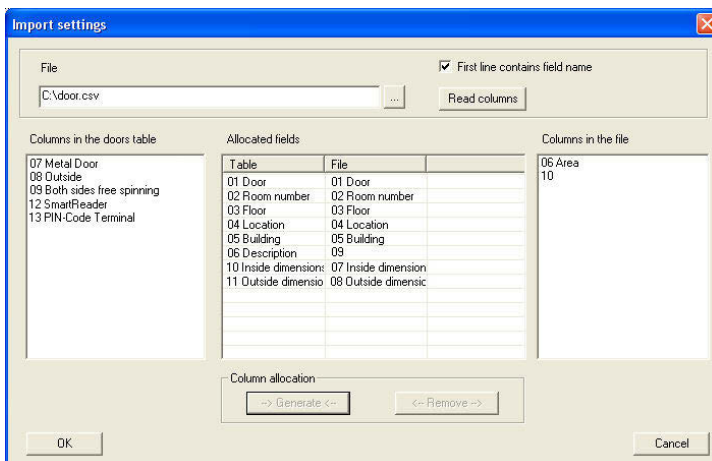
Page 62

1.30.2.4 DOOR DATA FROM A CSV FILE

You can use this function to adopt door data from existing files in CSV format. You should observe the corresponding data protection guidelines.

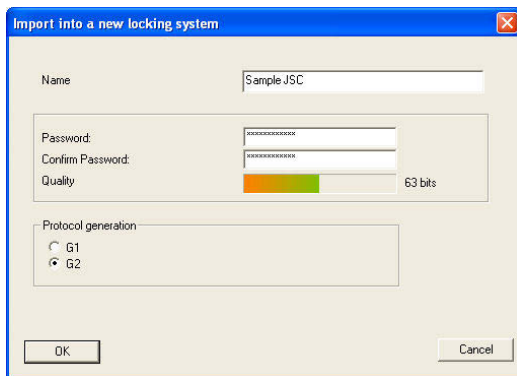


The “**Read**” function reads in data and displays them in the lower table. The desired data records can be selected using “**Select all**” or by marking them individually and inserted in accordance with the settings via “**Import**”. You can use the “**Change**” function to select the desired file and perform the field assignments.

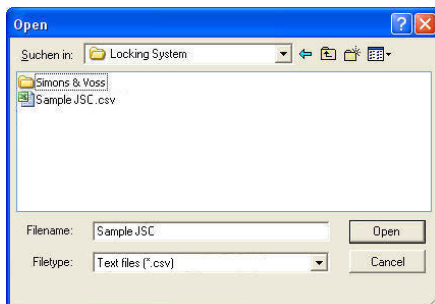


1.30.2.5 LOCKING PLAN FROM CSV FILE

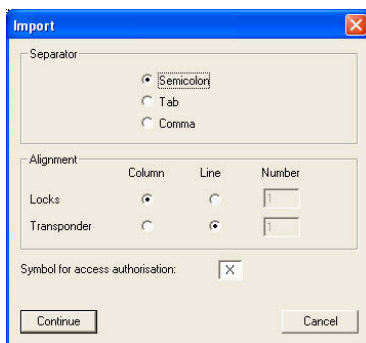
This function allows a locking plan matrix that exists in table form (e.g. created in Excel) to be imported into a new locking system. Doors with a lock and persons with a transponder are created during this operation. Authorisations are imported as individual authorisations. Group authorisations cannot be imported.



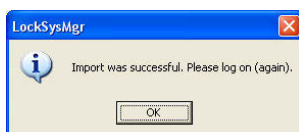
After the locking system being created has been given a name, the locking system password in compliance with the quality index and the log generation must be entered.



The template file in CSV format is then selected.



After the data field delimiters for the file, the arrangement of locks and transponders and the authorisation character have been selected, the locking plan will be created.



Once created, the new locking plan will be available after a new log on is performed.

1.30.3 VARIOUS

- “Increase reserve” → TIDs that have already been used and then reset will be used last.
- “Building structure” → The stored building structure will be used in various displays (export to LSM Mobile Edition).
- “deactivated transponders” → Deactivated transponders will not be displayed in the matrix for the sake of clarity.
- “Tasks for handheld” → Overwritten tasks will be deleted and no longer displayed.

1.30.4 STAFF PHOTOS

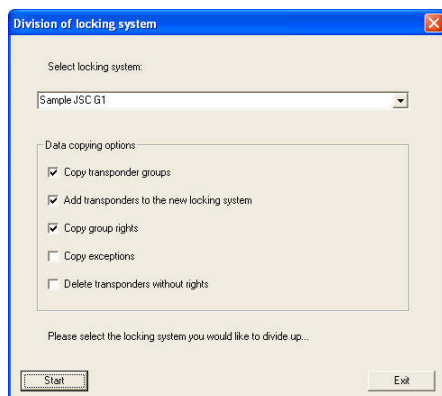
It is possible to store a photograph with a person’s master data. This option allows you to specify how the system should handle the photos.

Note:

- Storing photographs in a directory:
Access to the directory must be ensured and the file with the name stored must exist in order for the photographs to be displayed
- Storing photos in the database
Photos are stored 1:1 in the database, thus increasing the amount of storage space required

1.30.5 MANAGEMENT

Due to certain circumstances (organisational, technical) it may be necessary to split the existing database.



Note:

Before splitting the locking system, you must contact the dealer or a SimonsVoss employee to clarify the procedure. You must also ensure that you have a working data backup of all of the relevant components (software and data) before starting the work. SimonsVoss Technologies AG accepts no liability for database splitting carried out independently or incorrectly.

1.30.6 RESOURCE MANAGEMENT

Managing the timed control of authorisations.

Please refer to the separate manual dealing with the “Resource management” module for further details.

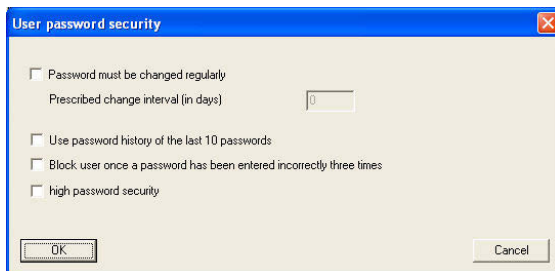
1.31. USER PASSWORD SECURITY

EXPLANATION

This option allows you to specify how user passwords are to be handled.

PROCEDURE

- ➔ Options
- ➔ User password security



- “Password must be changed regularly” → Users must change their password after the number of days entered.
- “Use password history ... ” → When a password is changed, the last 10 passwords will not be accepted as valid.
- “Block user ... ” → The user will be deactivated after entering an incorrect password three times and must then be reactivated by the administrator in user management. The block will also be recorded in the log.
- “High password security” → Activating this option will cause the same requirements relating to complexity to be applied to user passwords as for locking system passwords.

12.0 SERVICE AND SUPPORT

PRODUCT SUPPORT

If customers have any questions relating to products from SimonsVoss Technologies AG, the general support team will be happy to help:

Telephone +49 (0) 1805 78 3060

The product hotline does not offer support for the LSM Business and Professional software.

SOFTWARE SUPPORT

SUPPORT STANDARD

For customers with a chargeable Support Standard software agreement, the following support options are also available:

E-mail ism-support@simons-voss.de
Telephone +49 (0) 1805 57 3060

SUPPORT PREMIUM

For customers with a chargeable Support Premium software agreement, the following support options are also available:

E-mail ism-support@simons-voss.de
Telephone +49 (0) 1805 57 3060

Online support tool

- Short call to LSM hotline
- Launch LSM
- ↻ areas,
- ↻ SimonsVoss Online Support