User Guide

for LEHMANN Management Software

For LEHMANN RFID systems in offline or online operation

LEHMANN®

1 Chapter 1: General Information

1.1 General description

LEHMANN Management Software (hereafter referred to as LMS) is a software based on Microsoft Windows® for the assignment and administration of user rights as well as for the configuration of LEHMANN RFID systems. You can efficiently create and manage access rights with the software LMS. This document supports you in using the software. The manual provides you with information to configure and operate the LMS software and RFID systems.

Please read the respective operating instructions (e.g. M410 L033-A02) for the installation of the RFID systems and for basic information about the RFID systems including the safety instructions. The operating instructions for your system can be found on the Internet at www.lehmann-locks.com. Please read the safety and installation guidelines in the operating instructions of the respective RFID systems. Furthermore, you will find instructions for commissioning and battery replacement in the respective operating instructions. Read the respective operating instructions and this user guide carefully before installation and commissioning.

Text and graphics have been prepared with care. For nevertheless occurring errors no liability is taken over. We reserve the right to make technical changes.

1.2 Online and offline mode

All Lehmann RFID locks can be used in offline mode. In offline mode, the locks are configured either with master and programming cards or with the LEHMANN Management Software LMS. If the locks are configured with the LMS in offline mode, the locks are not directly connected to the LMS via the customer's network. In offline mode, configuration and authorization changes are manually transferred from the LMS to the individual locks by using the LEHMANN Data Transfer app.

The networked LEHMANN RFID systems CAPTOS and CAPTOS iCharge can be used either offline or online. In online mode, the CAPTOS and CAPTOS iCharge locks are connected directly to the customer's network and thus to the LMS via a primary controller. Configurations, authorizations and status information are updated in real time between the LMS and the online locks. Mixed operation of online and offline locks is possible without restrictions.

1.3 Components of a LMS project

To operate an RFID system with the LMS software, the following components are required:

- MIFARE® RFID system
  - Captura MIFARE
  - RFID lock M300, M400, M500, M410 or M610 with RFID reader L033 with firmware 0.1.79 or higher
  - CAPTOS / CAPTOS iCharge
- LEGIC RFID system
  - Captura LEGIC
  - RFID lock M300, M500, M410 or M610 with RFID reader L043 with firmware 1.0.10 or higher
- Transponder (requirements about supported transponders can be found in 1.2.2)

- LMS incl. corresponding license key (the LMS Online license key is required for online operation with CAPTOS and CAPTOS iCharge locks)
- App LEHMANN Data Transfer for Android-based and NFC-enabled smartphones or tablets for data exchange between the software and the RFID systems
- USB deasktop reader (Elatec TWN4) for LEHMANN Management Software

The following components are also required for online operation with CAPTOS and CAPTOS iCharge locks:

- Primary controller and, if applicable, secondary controller
- Power unit including power plug for controller
- Connecting cables
- Connection of the primary controller to the customer's local area network (LAN). Ethernet cable is not included.

1.3.1 RFID-System

The RFID system is a compact, battery-operated furniture lock. There are two modes of operation available:

Operating mode	**Description**
Assigned use	There is a fixed assignment between the transponders and the locks. The transponders receive authorizations for the respective lock. At the same time, a transponder can be granted access authorization for several locks in the operating mode "assigned use".
Shared use	The user can use with his transponder a lock of his choice. If a lock is closed with the transponder, the transponder and the lock are coupled to each other. The transponder cannot be used at any other lock in the operating mode "shared use". This coupling is only canceled when the user reopens the lock with his transponder. The transponder can now be used for another lock in operating mode “shared use”. The transponder can be used in parallel on locks in “assigned use” mode. When operating the RFID systems with the LMS software, transponders can also be permanently assigned to the locks in the operating mode “shared use” (see “assigned use”). This is necessary, for example, for an emergency opening. Note: RFID systems operating in “shared use” mode are represented by an asterisk in front of the name in the matrix.

ATTENTION: Please note the instructions regarding the transponders in the operating instructions of the RFID systems!

1.3.2 Supported transponders

The LMS software supports MIFARE® DESFire® EV1 / EV2 transponders. The LEHMANN transponders (user cards) correspond to this type and have 4K storage capacity. Third-party transponders with the above-mentioned specifications might be supported. It is recommended to use transponders with at least 4K or more.

LEGIC advent transponders with LEGIC stamp are also supported in the software LMS. LEGIC Access and a LEGIC data segment with 832 bytes for the use of LMS must be available on the transponders.

For security reasons, MIFARE® Classic and LEGIC prime transponders are not supported.

Depending on the available storage space, up to 250 authorizations can be programmed to a transponder. If more than 250 authorizations are required on a transponder (e.g. card for facility management), a special transponder type (see point 4.2.3) must be configured.

Third-party transponders (transponders not purchased from LEHMANN) must be checked for compatibility and RFID reading range in advance.

1.3.3 LEHMANN Management Software

The LMS software is available for download free of charge from the website https://lms.lehmann-locks.com. To activate the software, a licence key is required, which must be purchased from LEHMANN.

The software is operated and managed by the customer on the customer's own IT infrastructure. With the licence keys "LMS" and "LMS Online" one administrator workplace is activated in the LMS software. In addition to the basic version, additional modules for the software can be activated via further licence keys. The software can be used as a standalone solution (for example on a laptop) or as a server-client configuration in a network solution. In the network solution, several authorized persons can access the database at the same time. This function can be activated via a licence extension. It is not possible to register as an LMS user at several workstations at the same time. When operating CAPTOS / CAPTOS iCharge locks in online mode, a client- / server-configuration is recommended.

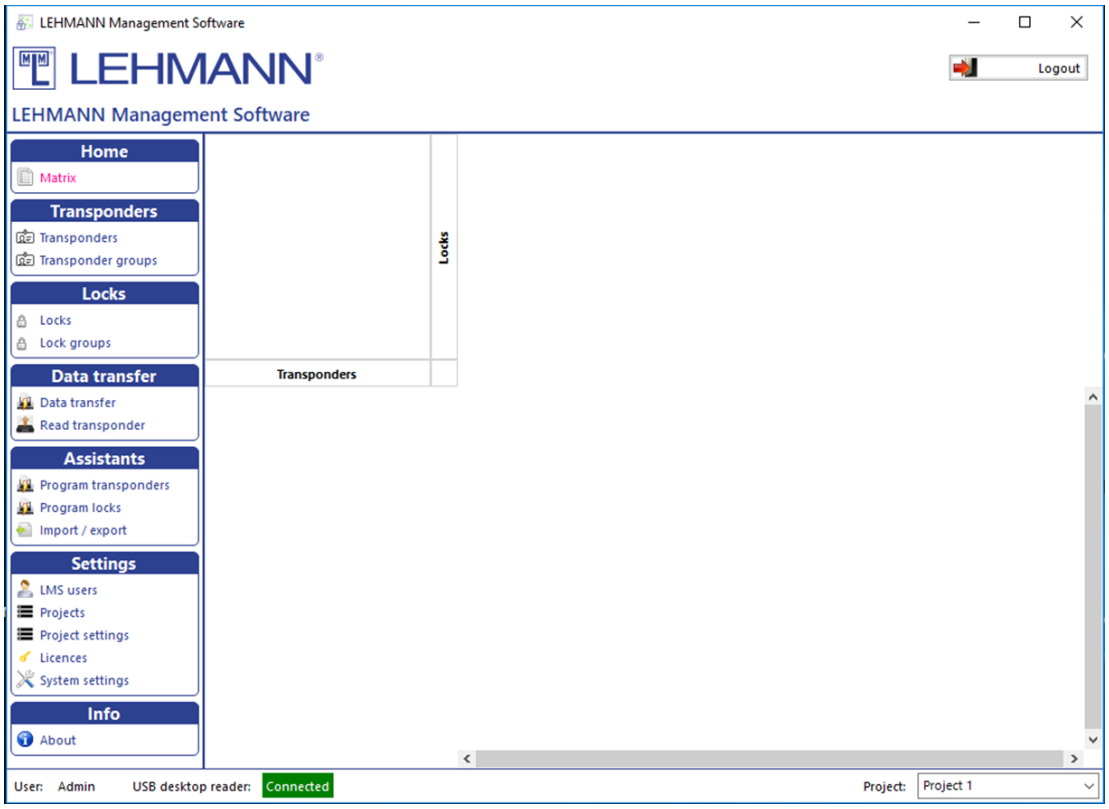


Figure: LMS GUI

1.3.4 App LEHMANN Data Transfer

LEHMANN Data Transfer is an app for data exchange between the software LMS and the LEHMANN RFID systems (e.g. programming locks in offline and online mode). An Android-based and NFC-enabled smartphone or tablet is required. Install the LEHMANN Data Transfer app from the Google PlayStore on the smartphone or tablet. Further information about the operation of the App LEHMANN Data Transfer can be found in the menu of the app under the item “Help”. Below is the QR code for the app LEHMANN Data Transfer in Google PlayStore.

1.3.5 USB desktop reader for LEHMANN Management Software

Connect the USB desktop reader to the laptop / PC. The Elatec firmware version 3.06 (TWN4_CCx306_PRS104_Core_CDC_Simple_Protocol.bix) must be installed on the USB desktop reader. The USB desktop reader connects automatically when you start the software for the first time.

1.4 Software vs. using Master Cards and Programming Cards

With the use of the LMS software there are many advantages and new functions in the context of user administration and the configuration of the RFID systems compared to the programming with

master and programming cards (see operating instructions of the RFID systems). In addition to new functions, there are also new processes for some existing functions. Please pay your attention to the following points:

- Operating mode “shared use“
  When operating the RFID systems with master and programming cards, only one transponder can be paired with the respective lock in operating mode “shared use”. When using the LMS software, further transponders can also be permanently assigned to locks in mode “shared use” (see “Assigned use” operating mode). This is necessary for an emergency opening in the offline mode. Even when using the LMS software, only one transponder can be coupled with a lock in operating mode “shared use”. This transponder is blocked for further RFID systems in the operating mode “shared use” until the coupling is canceled.
- Configuration of RFID systems
  The entire configuration of the RFID systems takes place in the LMS software. Functions such as activation / deactivation of acoustic signals, resetting to factory settings, change of operating mode etc. are carried out without master and programming cards. The settings of the RFID systems are configured in the LMS software and transmitted online in real-time to the RFID systems or with the app LEHMANN Data Transfer on a smartphone in the offline mode. Simultaneous use of LMS and master and programming cards is not possible!
- Automatic Opening
  This is a new feature for LEHMANN RFID systems that allows automatic opening after a period of time or at a fixed time. This function can be activated for RFID systems in both operating modes. The function is deactivated in the factory settings.
- Automatic Closing
  A new feature for LEHMANN RFID systems that allows automatic locking after a period of time or at a fixed time. This function can only be activated for RFID systems in “assigned use” operating mode. Note that this feature is only suitable for locks with a spring-loaded bolt.
- Activity logging

  Activities at the RFID systems can be logged and displayed online in real-time or in offline operations by using the smartphone with the app LEHMANN Data Transfer. This function is deactivated in the factory settings. If required, the log files can only be displayed with a 2-factor authentication. Furthermore, you can set how long the data should be stored in the software (factory settings: 14 days). The display of the data is only possible for LMS users with “admin rights”.
- Replace transponders
  If a transponder is not available any more, the authorizations can easily and quickly be transferred to a new transponder.
- Emergency opening
  The emergency opening is possible with standard transponders. For this purpose, the authorization for the respective RFID system is given to a transponder in the LMS software.

ATTENTION:
Deleting or losing the LMS database or losing all administrator passwords means that all locks programmed in the LMS database become unusable if the RFID systems were not reset to the factory

delivery status. Losing all administrator passwords means that no configuration or authorization changes are possible for all locks.

It is therefore strongly recommended to carry out regular backups (see point 4.5.1) or to install the database on a suitably secured drive.

2 Chapter 2: Operation of the LEHMANN Management Software in offline mode

All Lehmann RFID systems can be used in offline mode. In offline mode, the locks are configured either with master and programming cards or with the LEHMANN Management Software LMS. In offline mode, configuration and authorization changes are manually transferred from the LMS to the individual locks by using the LEHMANN Data Transfer app. If you want to manage locks in offline mode with the LMS, follow the instructions in this chapter. If you want to manage CAPTOS or CAPTOS iCharge locks in online mode with the LMS, follow the instructions in Chapter 3.

2.1 Commissioning and first steps

2.1.1 First start of the software

- Connect the USB desktop reader to the laptop / PC
- Download the latest version of the LMS from the Lehmann website https://lms.lehmann-locks.com
- Start the installation of the software LMS and follow the instructions during the installation.
- Select the installation type. For more information about the installation, please refer to the separate installation manual.
- After completing the installation, start the LMS software. Double-click the icon for the LEHMANN Management Software on your desktop. Alternatively, you can search and start the LEHMANN Management Software under the Windows Start button (“Search programs / files”).
- Select the language. You can change the language at any time.

- Enter the licence key “LMS” or “LMS Online” to activate the software. Additional licenses (e.g. “+5 LMS Users) are entered later in the software and must not be entered at this point. Place the card with the licence key on the USB desktop reader and click on “Read card with licence key”. Alternatively, you can enter the licence key on the keyboard. Click on “Continue”.
- Assign a username and secure password. The first LMS-user automatically has admin rights.
- Assign a project name and click on “Save”.

2.1.2 Login

- Enter username and password.
- Select in the drop-down list the project that should be opened. Note that the required authorizations for the respective project must be assigned to the LMS user (see 4.1).
- Click on “Login”.

2.2 Selection of the RFID technology per project

LEHMANN MIFARE® RFID systems and LEHMANN LEGIC RFID systems can be managed and configured in the LMS software. When creating a new project, the standard setting is always set to MIFARE® DESFire®.

If you are using MIFARE® RFID systems in the project, you do not have to make any changes to the RFID technology in the settings. **Please continue with point 2.3 in this manual when using LEHMANN MIFARE® RFID systems.**

If you are using **LEHMANN LEGIC RFID systems** in the project, you must first make a change in the project settings with regard to the supported RFID technology. To do this, proceed as follows:

- Click on "Project Settings" in the main menu.
- Activate the "LEGIC advant" type in the "General Settings" tab.
- Click on "Save".

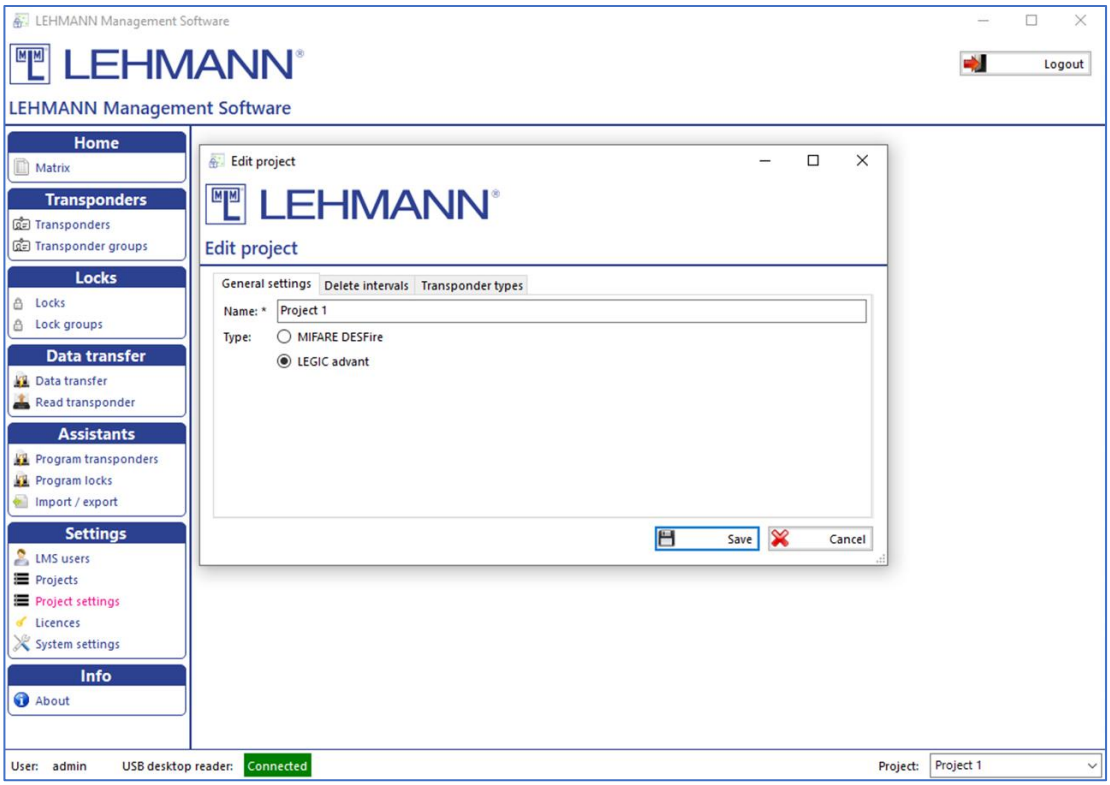


Figure: Selection of the RFID technology per project

Only one RFID technology is supported within a project. Please note the supported transponder types (see point 1.3.2). It is possible to use LEHMANN MIFARE® RFID systems in the first project and LEHMANN LEGIC RFID systems in other projects.

After activating LEGIC advant under the project settings, the additional item "LEGIC" appears in the main menu. Before LEHMANN LEGIC RFID systems or the corresponding transponders can be programmed, the USB desktop reader must first be launched with a LEGIC SAM. To do this, proceed as follows:

- Click on "Launch data wizard" in the main menu under “LEGIC”.
- Place your LEGIC SAM transponder on the USB desktop reader and leave it there until the data has been transferred.

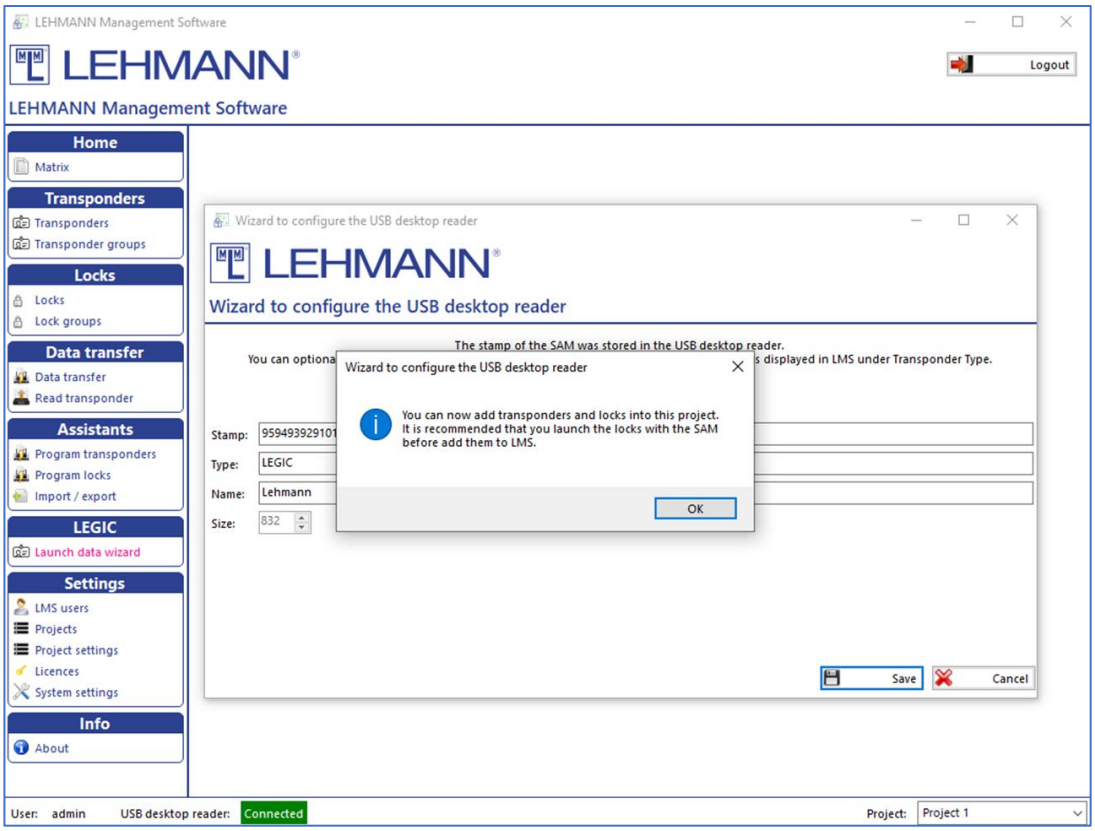


Figure: Configuration of USB desktop reader with LEGIC SAM

If LEGIC RFID systems should be used in LMS, the RFID systems must be configured with your LEGIC SAM63 before they can be programmed in LMS. Further information on the LEGIC-specific functions in the LMS software can be found under point 4.6.

2.3 Assistence functions

With the assistance functions, RFID systems and transponders can easily be added to the LMS software. If you are using LEHMANN LEGIC RFID systems, the RFID systems must be launched with a LEGIC SAM before programming. Further information can be found in point 4.6.

2.3.1 Programming RFID systems

The RFID systems must be in factory settings. Click in the main menu under assistants on “Program locks”. Follow the instructions in the assistant to initialize and configure the RFID systems.

Alternatively, without wizard:

- Open the app LEHMANN Data Transfer on your smartphone.
- Hold the smartphone with the NFC antenna centered on the RFID readers of the locks.The initial information of the lock is transferred to the app.
- It is recommended that you give in the app a clear and understandable name for the lock so that you can easily identify the lock.
- Click on ”Add” in the app to confirm the name of the lock.
- If required, repeat the process for further locks.
- Click on “Data transfer” in the LMS software.

- Place the smartphone with the open app on the USB desktop reader and leave it there during the entire data transfer.
- The lock information is now transmitted. For each lock, a configuration window opens in succession. Configure the locks. Pay attention to the correct time zone. For more information about the configuration options, see 2.9.2. Then click on “Save”.

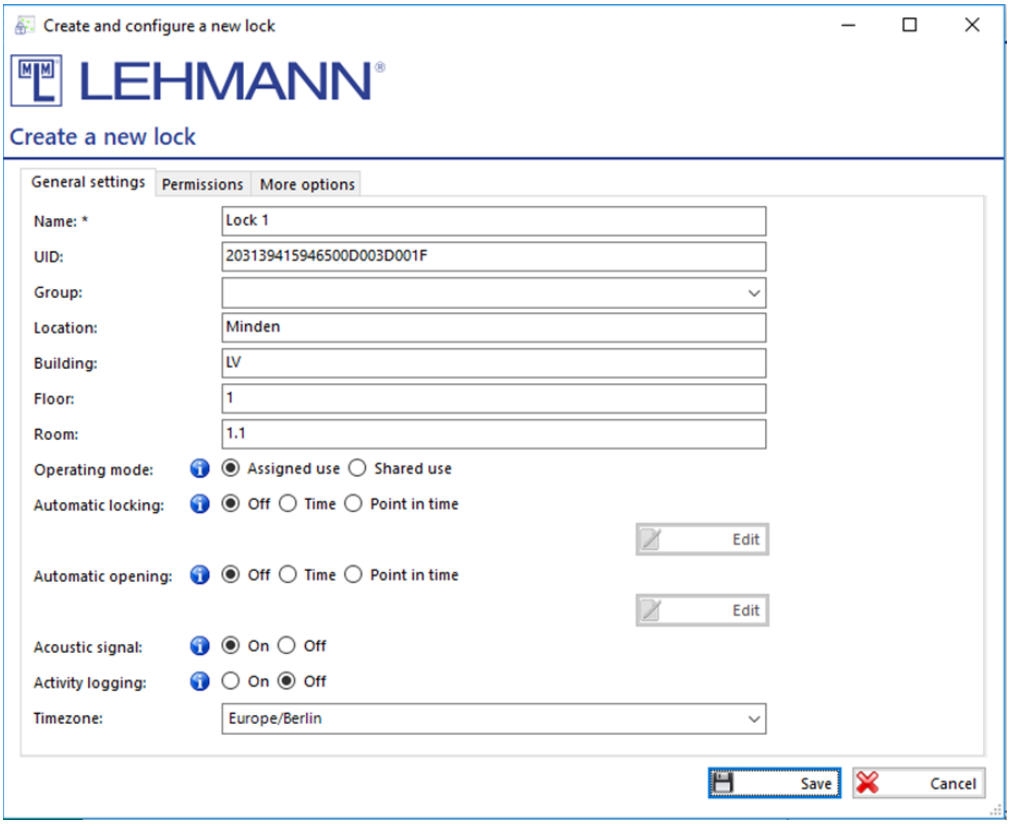


Figure: Create a new lock

- The new configuration data for the locks will be transferred back to the smartphone.
- Hold the smartphone with the app in front of the RFID readers of the locks, until the data transfer is confirmed with a green tick. The new configuration data and encryption information are transmitted to the individual locks.
- The assigning of new RFID systems is completed by placing the smartphone with the open app again on the USB desktop reader and by clicking on “Data transfer” in the LMS software. With this step, the software receives confirmation that the RFID systems are now configured and ready for use.

2.3.2 Programming transponders

- Click in the main menu on “Program transponders” and follow the instructions in the software.
- Place a transponder on the USB desktop reader and leave it there during the process of adding the transponder to the LMS software.
- Enter the name of the transponder in the pop-up window.

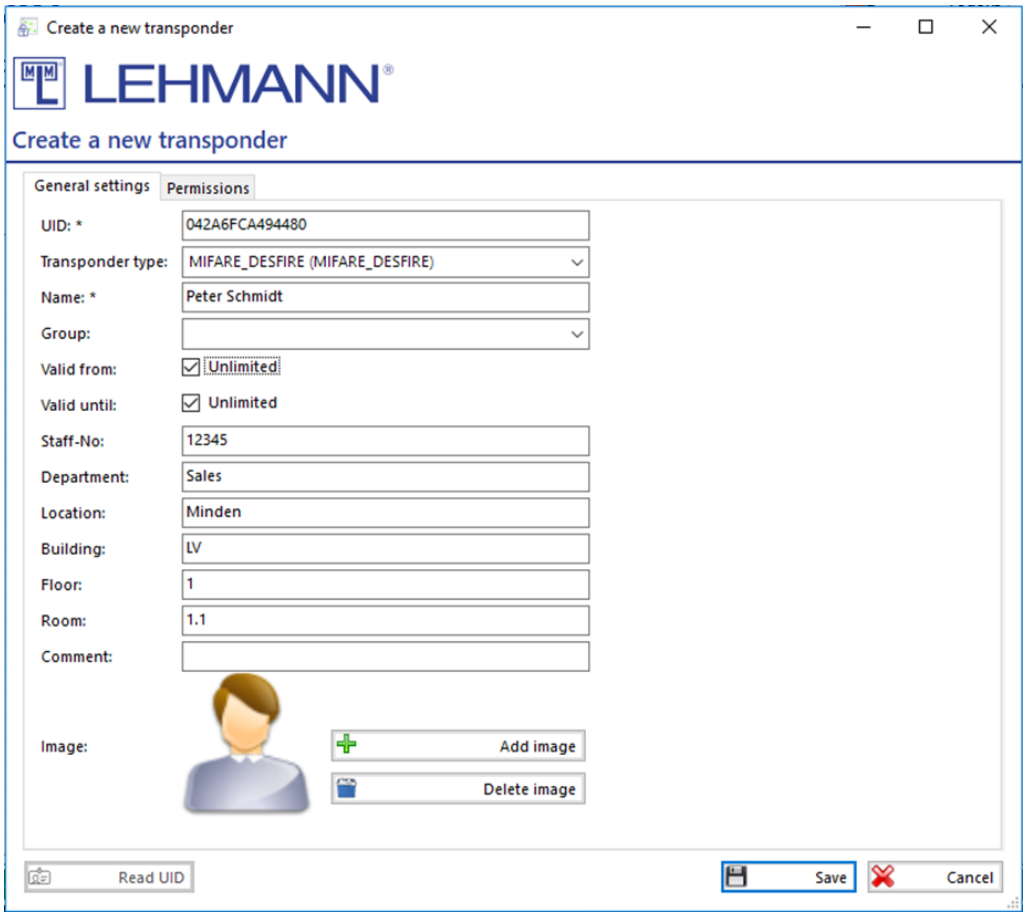


Figure: Create a new transponder

- You can enter additional information in the pop-up window to simplify the administration.
- If the transponder should not be valid immediately and / or not indefinitely, uncheck the box “Valid from” or “Valid to” and enter the corresponding date.
- Click on “Save”.
- The data is transferred to the transponder.
- After the process has been completed, you can place another transponder on the USB desktop reader and repeat the process.

2.4 Assign authorisations / delete authorisations

Depending on the available storage space, up to 250 authorizations can be programmed to a transponder. If more than 250 authorizations are required on a transponder (e.g. card for facility management), a special transponder type (see point 4.2.3) must be configured.

- Click on “Matrix” in the main menu.
- Assign permissions for transponders for the required RFID systems by ticking in the matrix with a mouse click.
- To delete an authorization, remove the check mark in the matrix with a mouse click.
- The blue dot next to the transponder and next to the RFID system means that a data transfer to the transponder or to the RFID system has to be carried out.
- Click on “Data transfer“ in the main menu.

- The lists show the transponders and RFID systems that require programming.

Distribute permissions with transponders:

- Place the transponder on the USB desktop reader for which you have created or changed authorizations.
- The data transfer is done automatically.
- If required, place further transponders with pending programming on the USB desktop reader one after the other.
- The transponders are now programmed and can be used for the RFID systems.
- The blue dot next to the transponder and next to the RFID systems in the matrix has now disappeared.
- Hold the transponder in front of the RFID reader and check the open / close functions when the furniture door is open.

Alternatively, permissions can be distributed to the locks with the smartphone:

- Place the smartphone with the open app LEHMANN Data Transfer on the USB desktop reader and leave it there during the process of data transfer.
- The data transfer is done automatically.
- Hold the smartphone with the app in front of the RFID readers of the locks, until the data transfer is confirmed with a green tick. Hold the NFC antenna on your smartphone centered in front of the RFID reader on the lock.
- The new permissions are transferred to the individual locks.
- The process is completed by placing the smartphone with the open app on the USB desktop reader and by clicking on “Data transfer” in the LMS software. With this step, the software receives the confirmation that the RFID system has received the new authorizations.

2.5 Data transfer

After each adding of new transponders or locks as well as after authorization and configuration changes in the software there is a need for programming on the transponders or on the locks. The programming requirement is shown in the matrix and in the lock / transponder overviews by a blue dot next to the transponders or locks.

- Click on “Data transfer” in the main menu.
- In the lists for “Transponders” and “Locks” there are all components with programming requirements.
- Data transfer to transponders:
    - Place the transponders with programming requirement one at a time on the USB desktop reader.
    - The data is transferred automatically
    - The transponders are now programmed and can be used for the RFID systems.
    - The blue dot next to the transponder and next to the RFID systems in the matrix has now disappeared.

- Hold the transponder in front of the RFID reader and check the open / close functions when the furniture door is open.
- After successful data transfer, the transponders are automatically removed from the list.

- Data transfer to smartphones:
  - Open the app LEHMANN Data Transfer on your smartphone.
  - Place the smartphone with the open app on the USB desktop reader and leave it there during data transfer.
  - The data is transferred automatically.
  - Hold the smartphone with the app in front of the RFID readers of the locks, until the data transfer is confirmed with a green tick. Hold the NFC antenna of your smartphone centered in front of the RFID reader of the lock.
  - The new permissions are transferred to the individual locks.
  - The process is completed by placing the smartphone with the open app on the USB desktop reader and by clicking on “Data transfer” in the LMS software. With this step, the software receives the confirmation that the RFID system has received the new authorizations.
  - After successful data transfer, the transponders are automatically removed from the list.

2.6 Groups

For easier management, transponders and RFID systems can be grouped. It is possible to create up to ten group levels. The groups are displayed in the matrix next to the associated transponders or the associated RFID systems. Note that groups are not displayed in the matrix until transponders or RFID systems have been assigned to these groups.

2.6.1 Transponder groups

- Click on “Transponder groups”. You receive an overview of the transponder groups. Transponder groups are displayed under the “Main group”. The following actions are possible:

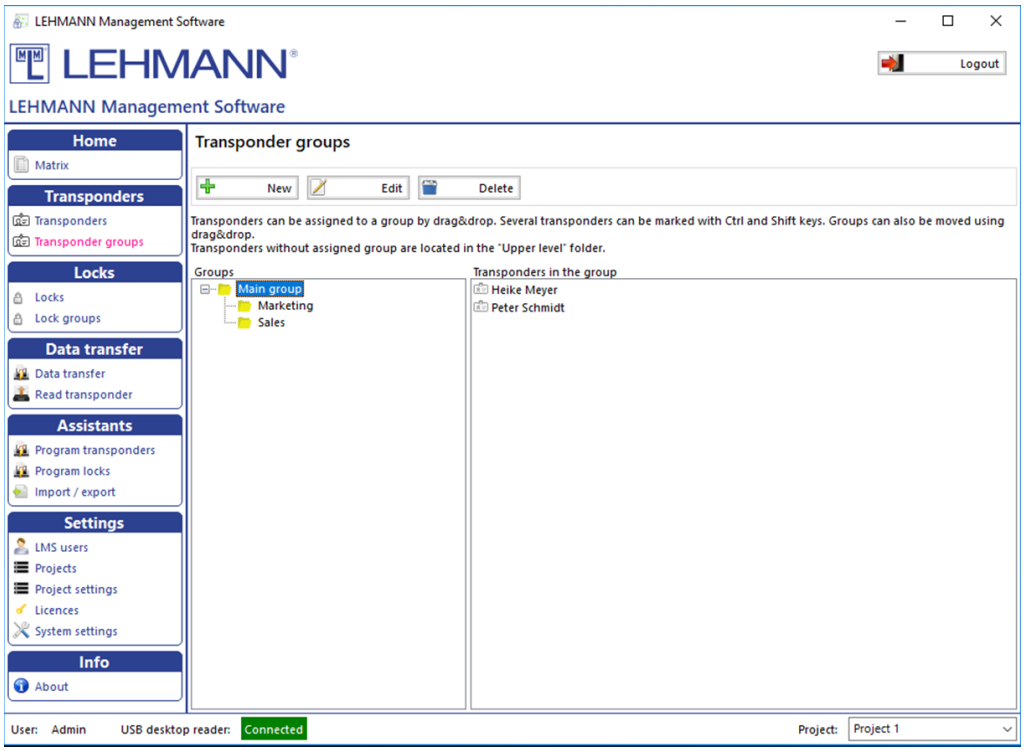


Figure: Transponder groups

- New: Add new groups
- Edit: Change existing group names and hierarchy levels
- Delete: Delete groups

2.6.1.1 Add transponder group

- Click on “New“.
- Assign a name to the new group and, if necessary, select a previously created group as the superior group.
- You can assign colours to each group displayed in the matrix.
- Click on “Save“.

2.6.1.2 Assign or move a transponder to a group

- All transponders that are not assigned to a group are located in the folder “Main group” (see figure “transponder groups”).
- Select one or more transponders to be assigned or moved to a group.
- Then drag & drop the transponders into the required group.

2.6.1.3 Edit transponder groups

- Select the group to be changed in the list with a mouse click and click on “Edit”.
- Change the name of the group, the parent group or the colour representation in the matrix.
- Click on “Save“.

- To move groups, select a group and drag & drop the group to the required location. Any sub-groups are moved as well.

2.6.1.4 Delete transponder groups

- Select the group to be deleted in the list with a mouse click and click on “Delete”.
- Confirm the deletion.
- If transponders are still in the group that should be deleted, the transponders are retained and are moved to the next higher group.

2.6.2 Lock groups

- Click on “Lock groups” in the main menu and you will get an overview of the lock groups. You can also assign a superior group to a lock group. Lock groups are displayed under the “Main group”. The following actions are possible:

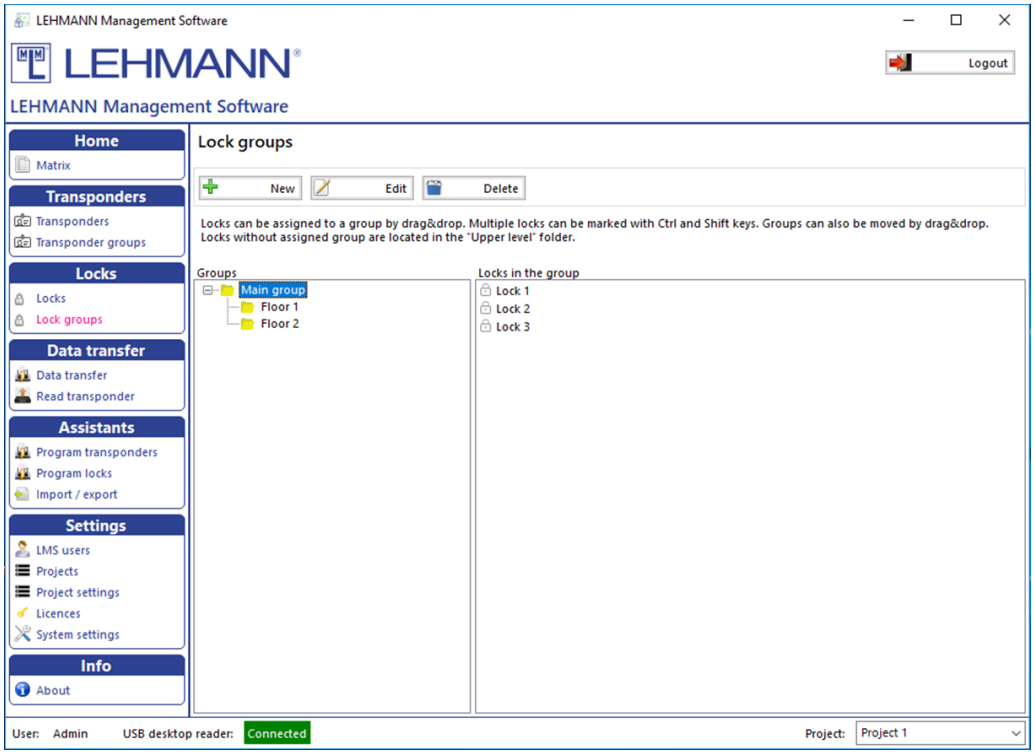


Figure: Lock groups

- New: Add new groups
- Edit: Change existing group names and hierarchy levels
- Delete: Delete groups

2.6.2.1 Add lock groups

- Click on “New“.
- Assign a name to the new group and, if necessary, select a previously created group as the superior group.
- You can assign colours to each group displayed in the matrix.

- Click on “Save“.

2.6.2.2 Assign or move a lock to a group

- All locks that are not assigned to a group are located in the folder “Main group” (see figure “Lock groups”). Please click on “Main group”.
- Select one or more locks to be assigned or moved to a group.
- Then drag & drop the locks into the required group.

2.6.2.3 Edit lock groups

- Select the group to be changed in the list with a mouse click and click on “Edit”.
- Change the name of the group, the superior group or the colour representation in the matrix.
- Click on “Save“.
- To move groups, select a group and drag & drop the group to the required location. Any sub-groups are moved as well.

2.6.2.4 Delete lock groups

- Select the group to be deleted in the list with a mouse click and click on “Delete”.
- Confirm the deletion.
- If locks are contained in the group to be deleted, the locks are retained and may be moved to the next higher group.

2.7 Authorisation of groups

- Click on “Matrix“ in the main menu.
- Click on the group name (transponder / lock) within the matrix. The associated transponders or locks are hidden, so that only the group name is displayed (see figure: Groups (2)).

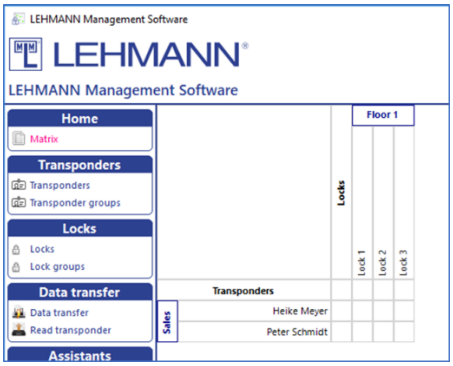


Figure: Groups (1)

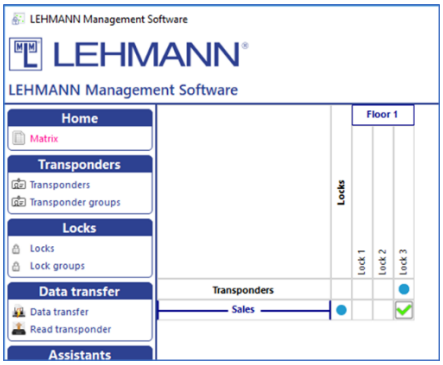


Figure: Groups (2)

- Authorise the entire group on the respective RFID system by ticking in the matrix with a mouse click.
- The blue dot next to the transponder group and next to the RFID system means that data must be transferred to all transponders in the group or to the RFID system.

- Click on “Data transfer” in the main menu and carry out the data transfer as described in 2.5.

If not all transponders or locks of a group have the same authorizations, this is indicated in the matrix by a gray tick.

CAUTION: If there are a large number of concurrent permission changes, such as those that occur when permission changes are made to groups, the software LMS may need much more time to process the changes.

2.8 Add, configure and delete transponders

To add, configure and delete transponders, you need the appropriate authorization (see 4.1).

- Click on “Transponders” in the main menu and you get an overview of the transponders.
- The following actions are possible
  - New: Add new transponders
  - Edit: The settings for one or more selected transponders can be changed.
- Several transponders can be marked and selected at the same time (Ctrl or shift key). In this way, configurations (e.g. validity) or actions (e.g. deleting lost transponders) can be carried out for several transponders at the same time. To configure several transponders at the same time, click on "Edit" after selecting the transponders. Please note that not all actions or configuration changes for transponders can take place at the same time. Certain changes must be made separately for each transponder.

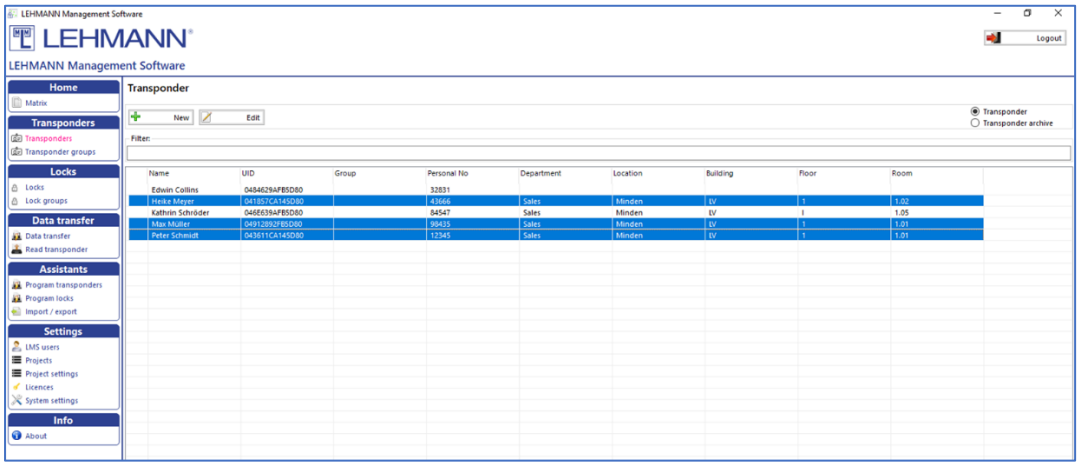


Figure: Selection of several transponders

2.8.1 Add new transponders

- Click on “New” to create a transponder.
- Place a transponder on the USB desktop reader and click on “Read UID”. The transponder's UID is automatically written to the required UID field.
- The Transponder Type field is automatically filled.
- The following settings are possible in the “Common Settings” tab:

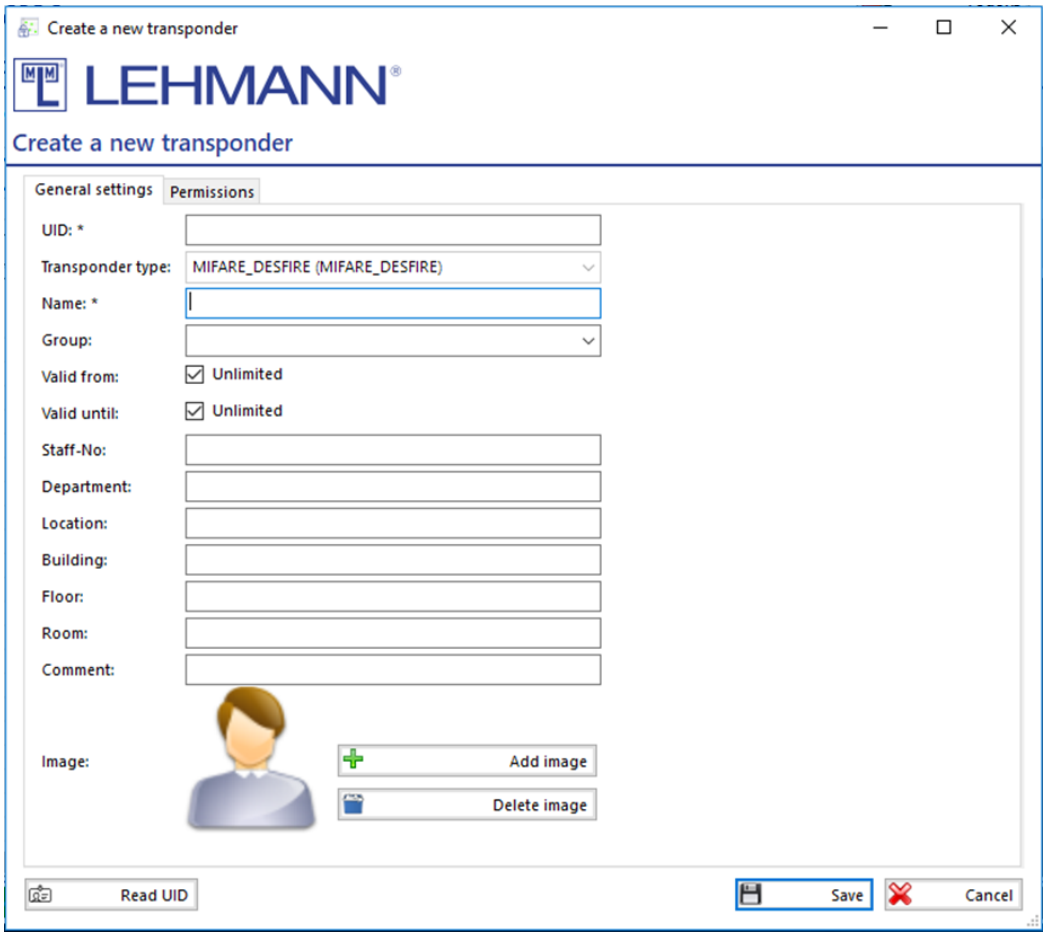


Figure: Create a new transponder

- Assign a unique name for the transponder.
- If necessary, assign the transponder to a previously created group.
- If the transponder is not to be valid immediately and / or not indefinitely, uncheck the box “Valid from” or “Valid to” and enter the corresponding date.
- If required, enter additional information about the person using the transponder, such as employee number, department, etc.
- You can add a picture of the transponder holder by clicking on “Add image” or delete an existing picture by clicking on “Delete image”.

- Click on “Save”.
- Click on “Data transfer” in the main menu and transfer the changes to the transponder (see 2.5).

2.8.2 Settings for the transponders

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- You can use the filter function to search for specific transponders. To do this, enter a part of the transponder name in the filter, then you will see all transponders that contain the text in the name.
- The information and settings in this screen can be changed at any time, except for the UID and Transponder Type.

- Click on “Save“.
- Check whether the changes require any programming. Click on “Data transfer” in the main menu and transfer the changes to the transponder if required (see 2.5).

2.8.3 Permissions

In addition to the authorization management in the matrix, permissions can also be managed in the main menu under “Transponders”. Depending on the available storage space, up to 250 authorizations can be programmed to a transponder. If more than 250 authorizations are required on a transponder (e.g. card for facility management), a special transponder type (see point 4.2.3) must be configured.

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- Click on the “Permissions” tab.

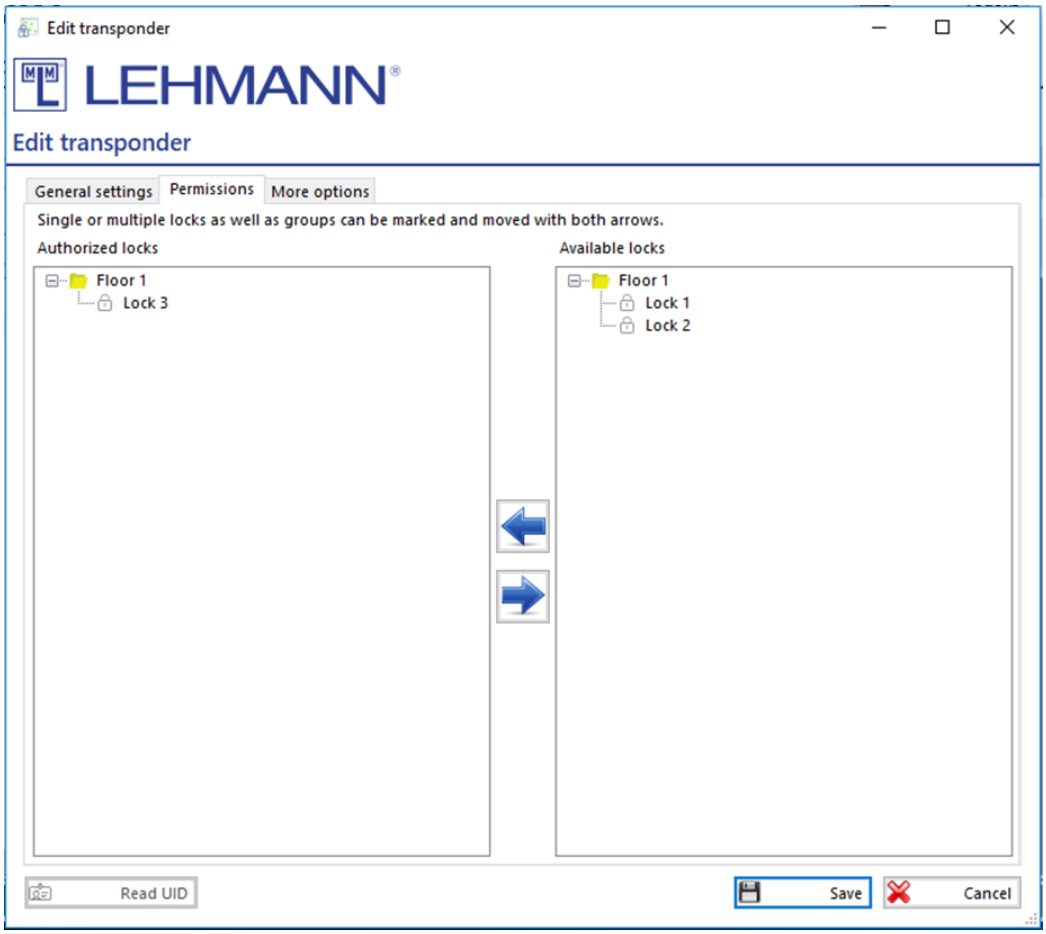


Figure: Edit transponders - Permissions

- In the right table (Available locks) you will find all the locks that are already available in the project and for which the transponder has no authorisation. Furthermore, the groups in which the locks are located are displayed here.
- In the left table (Authorized locks) are the locks for which the transponder is already authorized. Furthermore, the groups in which the locks are located are displayed here.

- Select and mark any number of locks and drag the locks from one side to the other in order to edit permissions. Before the data transfer is done, changes in permissions are marked in this view with a blue dot (new authorization) or with a red cross (authorization revoked).
- You can also move entire groups including all locks.
- Programming requirement is indicated by a blue dot.
- Click on “Save”.
- Click on “Data transfer” in the main menu and transfer the changes to the transponder or to the locks by using the smartphone (see 2.5).

2.8.4 Replacing and deleting transponders and more options

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- Click on the tab “More options”.
- In the tab “More options” the following settings can be made:

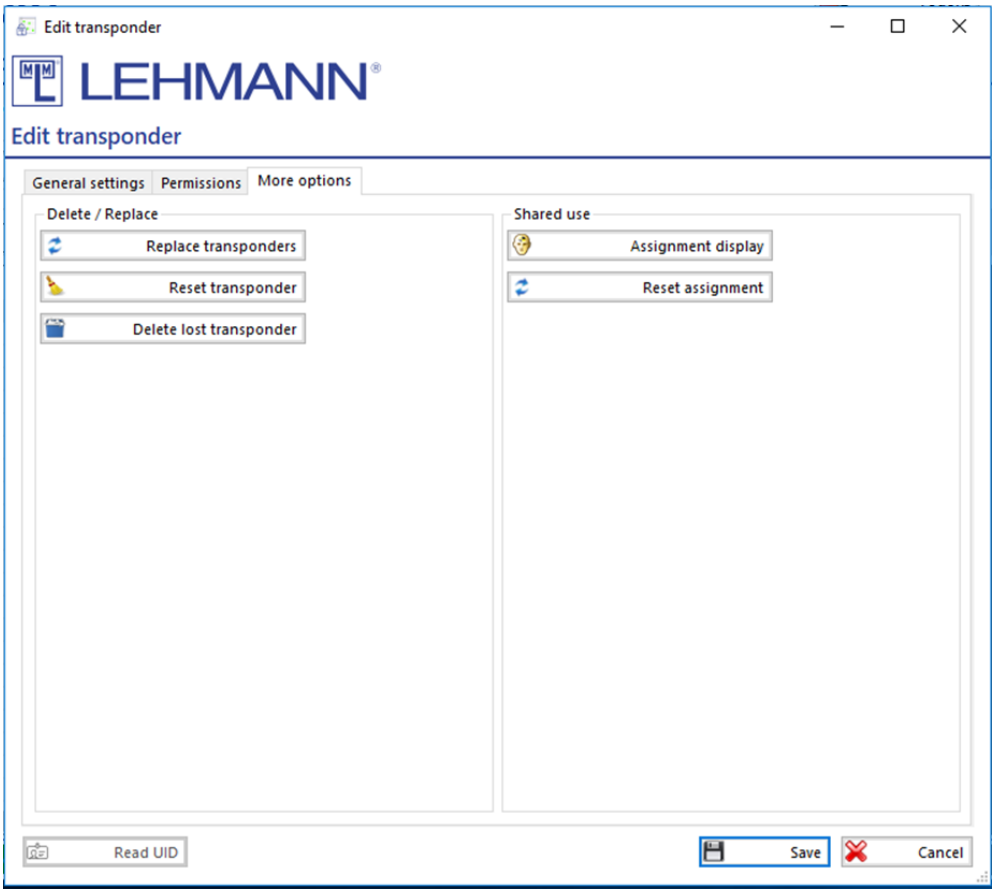


Figure: Edit transponder – More options

- Replace transponders: The transponder can be replaced e.g. after loss.
  - Click on “Replace transponders”.
  - Place the new transponder on the USB desktop reader and click on “Read UID”.

- All previous authorizations and blocking remarks are automatically transferred to the new transponder. The previous transponder loses its validity for locks in „assigned use" mode.
- Click on "Save". The data transfer to the new transponder starts automatically.

  ATTENTION: Click on "Data transfer" in the main menu. Transfer the data to the RFID systems immediately with a smartphone as described under point 2.5.

  The temporary authorisation for a lock in "shared use" mode is not transferred to the new transponder. In this case, an emergency opening must be carried out on the lock (see point 5.5).

- Reset transponder: The transponder will be reset. The transponder does not appear in the matrix any more. The transponder can then be programmed again.
  - Place the transponder that should be reset on the USB desktop reader.
  - Click on "Reset transponder".
  - The transponder is reset immediately and removed from the matrix. There is no further need for programming under "Data transfer".

- Delete lost transponder: All information on the transponder will be deleted. The transponder does not appear any longer in the matrix. The transponder can then be used again.
  - Click on "Delete lost transponder".
  - The transponder will be deleted immediately and removed from the matrix.

  ATTENTION: Click on "Data transfer" in the main menu. Transfer the changes to the RFID systems with the smartphone as described in 2.5. The authorization in the locks in "assigned use" mode is deleted after performing the data transfer to the RFID systems. Otherwise, the old transponder retains access rights.

- Assignment display: If an RFID lock in the operating mode "shared use" has been locked with the transponder, the name of the corresponding RFID lock is displayed.
  - Place the transponder on the USB desktop reader.
  - Click on "Assignment display".
- Reset assignment: After an emergency opening in operating mode "shared use", the transponder is blocked for parallel use on other RFID systems in operating mode "shared use". In order to un-block the transponder, use this function:
  - Place the transponder on the USB desktop reader.
  - Click on "Reset assignment".
  - The occupancy settings on the transponder are automatically deleted. There is then no further need for programming under "Data transfer".

2.9 Add, configure and delete RFID systems

To add, configure and delete RFID systems, you need the appropriate authorization (see 4.1). If you are using LEHMANN LEGIC RFID systems, the RFID systems must be launched with a LEGIC SAM before programming. Further information can be found in point 4.6.

- Click on "Locks" in the main menu and you will get an overview of the RFID systems. In this overview you will see all the RFID systems added to this project as well as further

information such as groups, operation mode and battery status. Further information about the battery status can be found in section 5.6 of this manual.

- Several locks can be marked and selected at the same time (Ctrl or shift key). In this way, configurations (e.g. operating mode) or actions (e.g. resetting locks) can be carried out for several locks simultaneously. To configure several locks at the same time, click on "Edit" after selecting the locks. Please note that not all actions or configuration changes for locks can take place at the same time. Certain changes must be made separately for each lock.

2.9.1 Add RFID systems

- The RFID systems must be in factory settings.
- Click in the main menu on “Program locks” and follow the instructions in the software.

Alternatively, proceed as follows:

- Open the app LEHMANN Data Transfer on your smartphone.
- Hold the smartphone with the opened app in front of the RFID readers of the locks. Hold the NFC antenna of your smartphone centered in front of the RFID reader of the lock.
- The initial information of the lock is transferred to the app.
- It is recommended that you give a new and clear name for the lock in the app with which you can identify the lock.
- Click on “Add” in the app to confirm the (new) name.
- If necessary, repeat the process for further locks.
- Click on “Data transfer” in the LMS software.
- Place the smartphone with the open app on the USB desktop reader and leave it there during the entire data transfer.
- The lock information is now transmitted. For each lock, a configuration window opens in succession. Configure the locks. Pay attention to the correct time zone. For more information about the configuration options, see 2.9.2. Then click on “Save”.

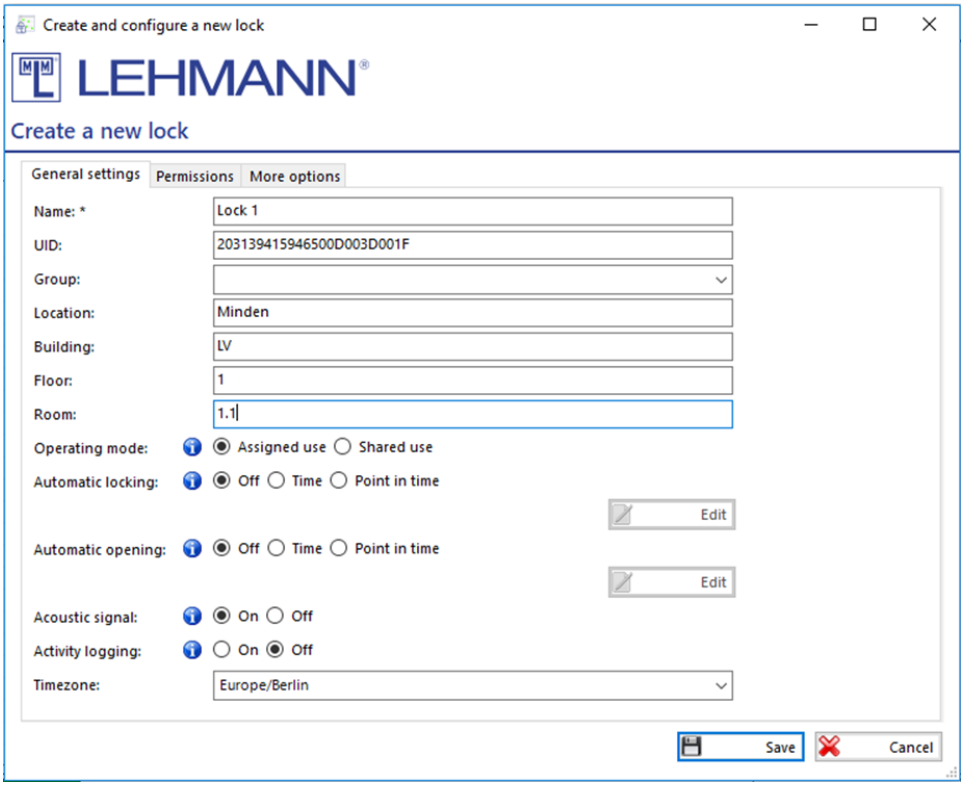


Figure: Create a new lock – General settings

- The new configuration data for the locks will be transferred back to the smartphone.
- Hold the smartphone with the opened app in front of the RFID readers of the locks, until the data transfer is confirmed by a green tick. Hold the NFC antenna of your smartphone centered in front of the RFID reader of the lock.
- The process is completed by placing the smartphone with the open app on the USB desktop reader and clicking on "Data transfer" in the LMS software. Leave the smartphone on the USB desktop reader during the data transfer. With this step, the software receives the confirmation that the RFID system is now configured and ready for use

Hold the smartphone with the opened app of the RFID readers of the locks, in order to update the time in the RFID systems. Make sure that the correct time is set on the smartphone. This is necessary, for example, after a battery change. Otherwise, a trouble-free operation is not possible for RFID systems with time-dependent functions.

2.9.2 Settings of the RFID systems

- Click on “Locks“ in the main menu.
- Select one or more locks in the overview for which the configuration should be changed and click on “Edit”.
- You can use the filter function to search for specific locks. To do this, enter a part of the lock name in the filter, then you will see all locks that contain the text in the name.
- In the tab “General settings”, the following settings for the respective RFID system can be made both directly when the lock is added and during operation:

- Operating mode: Selection of the operating mode (Note: RFID systems in the operating mode “shared use” are shown in the matrix with an asterisk in front of the lock name). Further information about the operating modes can be found in 1.3.1.
- Automatic locking: In addition to the default setting (Off), a time period or a fixed time can be selected when the locks close automatically. This function is available in “assigned use” mode. NOTE: Please note that this function is only suitable for locks with a spring-loaded bolt!
- Automatic opening: In addition to the default setting (Off), the locks can be configured to open automatically after a period of time or at a fixed time.
- Acoustic signal: In addition to the default setting (On), the acoustic signal can be deactivated.
- Activity logging: Activities on the RFID systems can be logged and transferred using the LEHMANN Data Transfer app and then displayed in the software. This function is deactivated in the factory settings. When you first click on “On” within a project, you must make a decision whether you want a 2-factor authentication.

Figure: Two-factor authentication

With a 2-factor authentication (enter of a second password) the log files are additionally secured. Furthermore, in the main menu under Project settings (see 2.11.2) you can set how long the data should be stored in the software (factory setting: 14 days). The display of the data is only possible for users with “admin rights”.
After activating the “Activity logging”, the tab “Lock activities” appears.

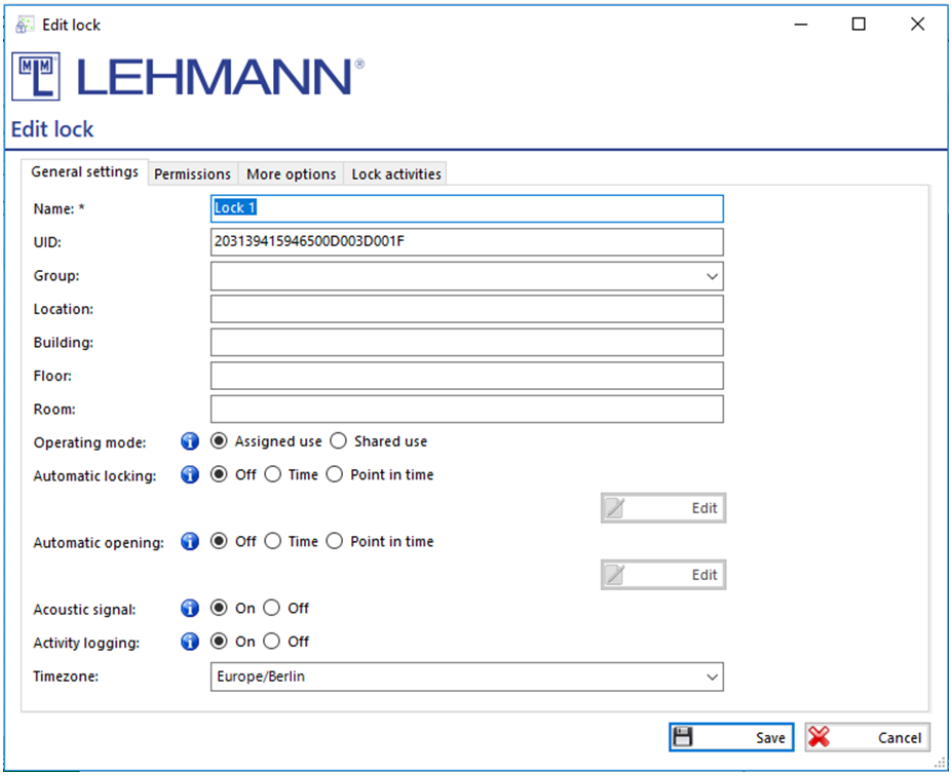


Figure: Edit lock – General settings

- Time zone: If the time zone for the RFID system is not set correctly, please set the correct time zone. The correct time is necessary for time-dependent functions. Also make sure that the time on your smartphone is set correctly.

- Enter your required settings for the RFID lock.
- Click on “Save“.
- Click on “Data Transfer” in the main menu and transfer the changes to the smartphone. Execute the data transfer to the RFID systems as described under 2.5.

2.9.3 Permissions

- Click on “Locks“ in the main menu.
- In the locks overview, select one or more locks for which the permissions should be changed and click on “Edit”.
- In addition to the authorization management in the matrix, permissions can also be managed in the tab “Permissions”:

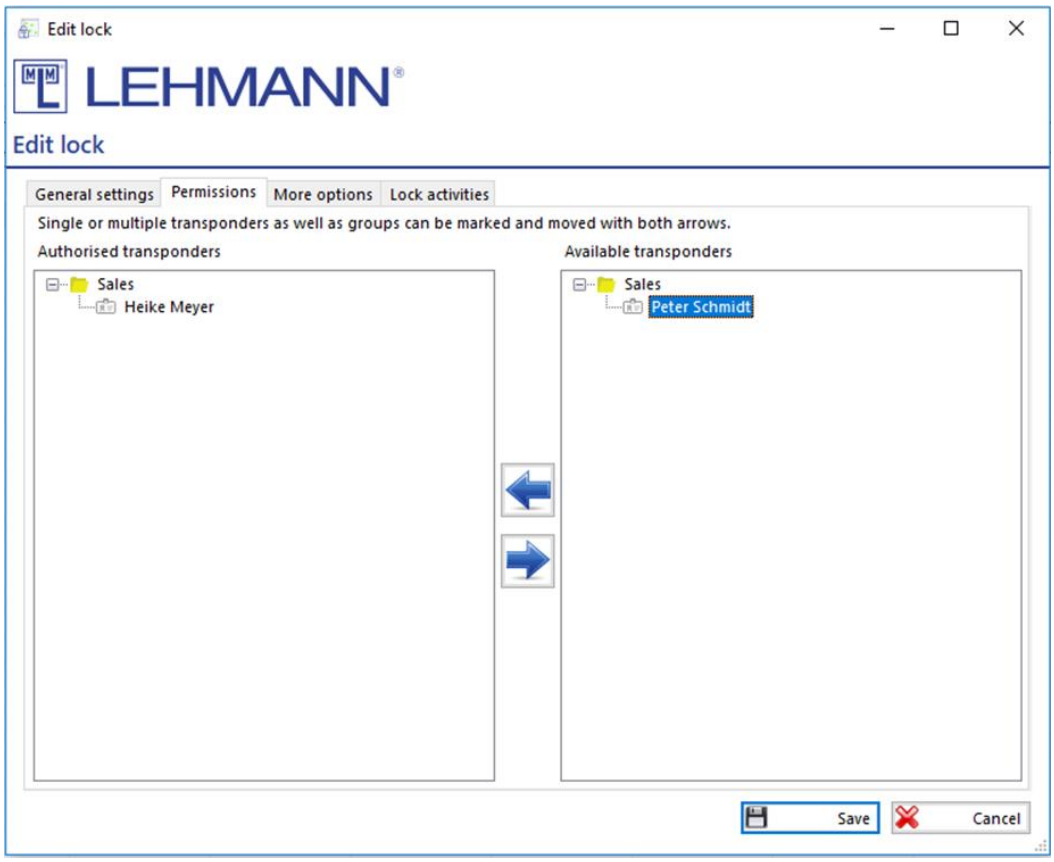


Figure: Edit lock - Permissions

- In the right table (Available transponders) you will find all the transponders that are already available in the project and that have no permission at this lock. Furthermore, the groups in which the transponders are located are displayed here.
- In the left table (Authorised transponders) are the transponders that have a permission for this lock. Furthermore, the groups in which the transponders are located are displayed here.
- Select and mark any number of transponders and drag the transponders from one side to the other in order to edit permissions. Before the data transfer is done, changes in permissions are marked in this view with a blue dot (new authorization) or with a red cross (authorization revoked).
- You can also move entire groups including all transponders.
- The authorization change is indicated by a blue dot.
- Click on “Save”.
- Click on “Data transfer” in the main menu. Execute the data transfer as described in 2.5.

2.9.4 Reset lock, delete lock and firmware updates

- Click on “Locks” in the main menu.
- In the overview of locks, select the required lock(s) and click on “Edit”.
- In the tab “More options” the following settings can be made:

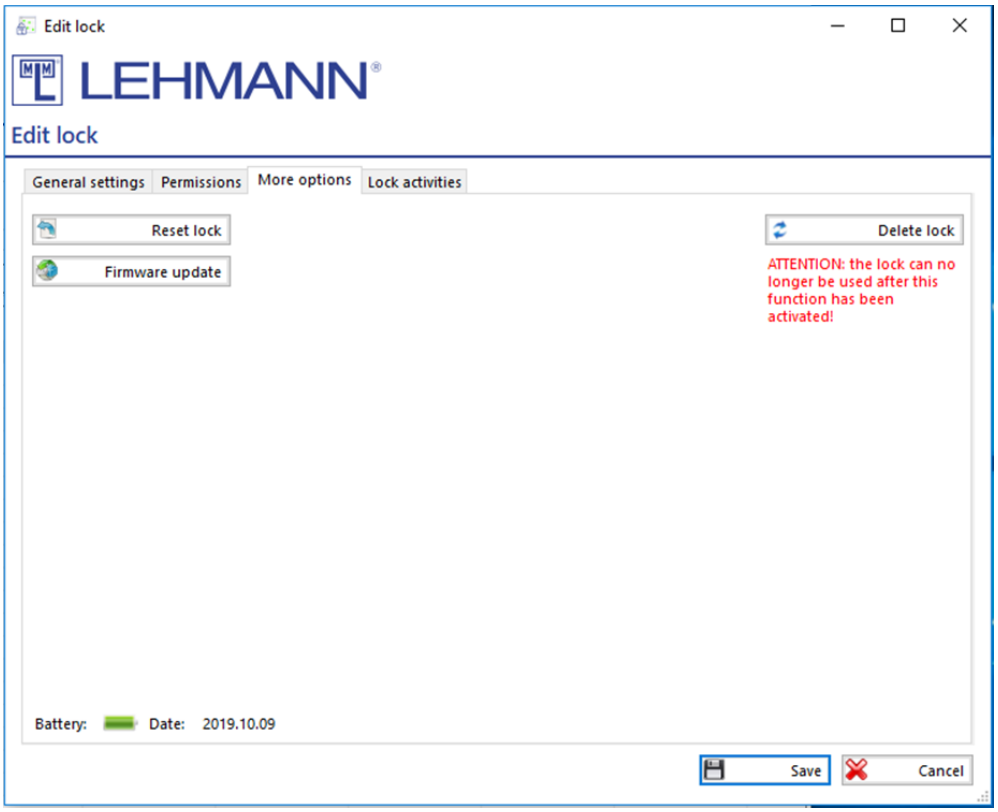


Figure: Edit lock – More options

- Reset lock: The lock will be set to the factory settings. Confirm the reset in the pop-up window.
  - Click on “Save“.
  - Click on “Data transfer” in the main menu. Execute the data transfer to the RFID systems with the smartphone as described in 2.5.
- Delete lock: The lock can be deleted from the software e.g. in the event of a defect without further programming possibilities. Confirm the operation after clicking “Delete lock” in the dialog box. **IMPORTANT: The lock cannot be used any more after this process!**
- Firmware update: The RFID reader at the lock is set in a special mode to update the firmware.
  - Click on “Firmware update”.
  - Click on “Data transfer” in the main menu. Execute the data transfer to the RFID systems with the smartphone as described in 2.5. To update the firmware, use the software LEHMANN Firmware Updater at www.lehmann-locks.com.
- Battery: The last transferred battery status is displayed for battery operated locks. For an updated battery status, the data must be collected from the lock by using the app.
  - Hold the smartphone with the opend app in front of the RFID reader of the lock. Transfer the data into the software.
  - Click on “Data transfer“ in the main menu.
  - Place the smartphone with the opened app on the USB desktop reader and transfer the data to LMS.

ATTENTION: If a programming requirement for the lock continues to be listed under Data transfer after resetting a lock, the lock must be marked under “Lock archive” and then deleted with the button “Delete lock data” (see 4.2.2).

2.9.5 Activity logging (only with admin rights)

- This function must be activated for all relevant locks (see 2.9.2).
- The lock saves the last 640 activities. The oldest entry is overwritten in the lock when new events are added. Administrators can decide how long the collected data will be stored in the LMS.
- Use the smartphone to collect the data at the respective locks. Hold the smartphone with the opened app LEHMANN Data Transfer in front of the RFID reader of the lock.
- Click in the software on “Data transfer”.
- Place the smartphone with the opened app on the USB desktop reader and transfer the data to LMS.
- Click on “Locks” in the main menu.
- In the overview of locks, select the required lock and click on “Edit”. The activity logs are only displayed for one lock. It is not possible to display the activity logs of several locks at the same time.
- The following operations can be done in the tab “Lock activities”:

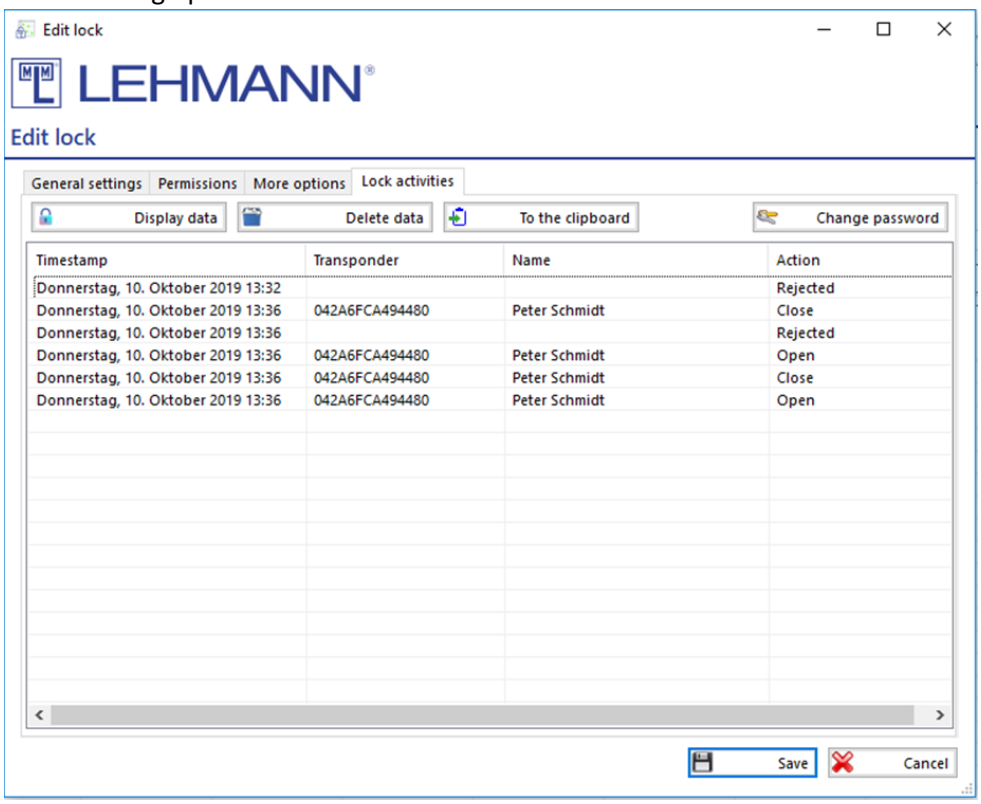


Figure: Edit lock – Lock activities

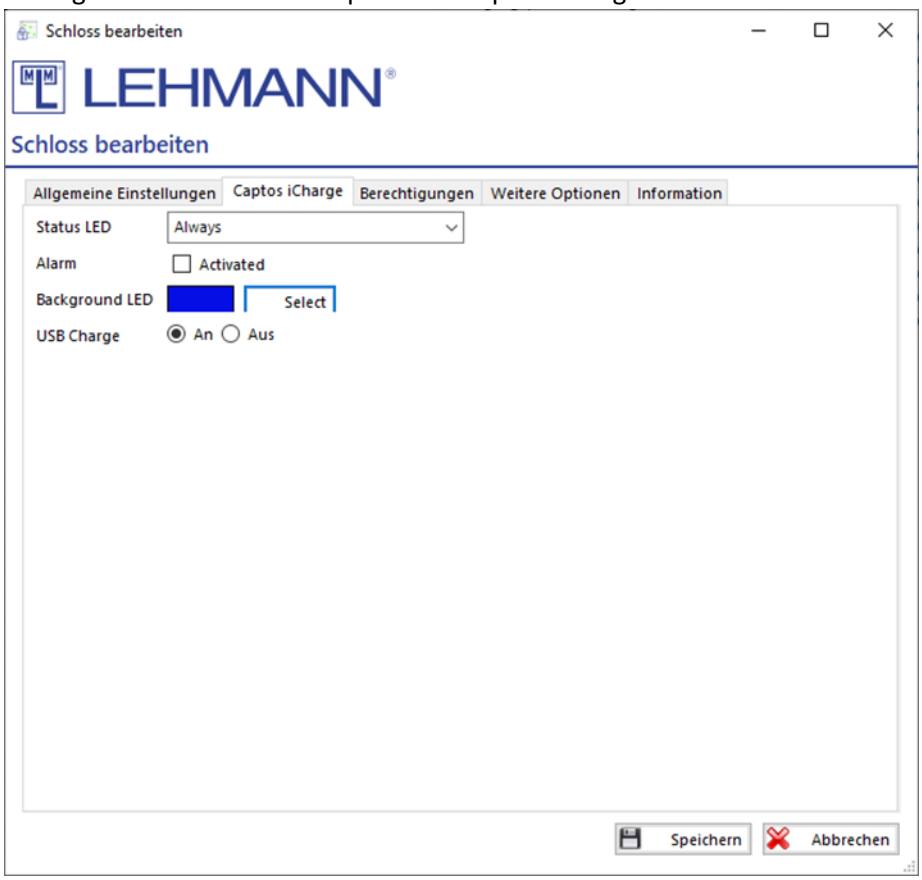
  - Display data: If data is available, this button can be selected. If the 2-factor-authentication has been activated, enter your password and click on “Save”. Available data will be displayed.
  - Delete data: The available data will be deleted.

- To the clipboard: The data is copied to the clipboard so that you can paste this data into other file formats such as Excel.
- Change password: If the 2-factor-authentication has been activated, you can change the password here. For security purpose, all previous activity logs are deleted when changing the password.

2.9.6 Additional functions for CAPTOS and CAPTOS iCharge locks in offline mode

Additional functions are available to you with CAPTOS and CAPTOS iCharge locks:

- Click on "Locks" in the main menu.
- In the overview of locks, select one or more CAPTOS or CAPTOS iCharge locks and click on "Edit".
- If you have selected a CAPTOS or CAPTOS iCharge lock, you can make the following settings in the additional "Captos" or "Captos iCharge" tab:



- Status LED: The status LED signals to the user whether the lock and thus the locker is open or closed. This function is particularly suitable for locks in the shared use operating mode. Green stands for open (available), red for closed (occupied). The following settings are possible in the drop-down menu:
  - Off: The status LED never lights up, apart from optical signals when opening or closing the lock.
  - Only when open: The status LED only lights up when the lock is unlocked.
  - Only when closed: The status LED only lights up when the lock is closed.

        - Always: The status LED is always on.
    - Alarm: By ticking the box, the alarm function of the lock can be activated or deactivated. When the lock is locked, the locking pin is detected by a sensor in the lock. If the lock is locked and the locking pin is removed without opening having taken place, a manipulative opening can be assumed and an audible alarm is triggered.
    - Background LED (only with CAPTOS iCharge): Clicking on “Select” opens a dialog window in which the colour of the background LED can be set. Click on the color scales to select the required colour, or RGB values can be set. The LED can also be deactivated by setting the colour to black (All RGB values = 0).
    - USB charge (only with Captos iCharge): The USB charging socket can be activated or deactivated.
- Click on "Save".
- Click on "Data transfer" in the main menu. Carry out the data transfer as described under point 2.5.

2.10 RFID systems in offline mode with a virtual locking plan

The LMS offers the possibility to prepare lock profiles in the software without having an existing real lock, and to transfer the configuration to the real lock at a later point in time. These virtual locks are marked with a blue star as long as they are virtual. These locks can then be assigned to real locks. Configuration settings and permissions can be assigned to a virtual lock. This procedure can significantly accelerate the commissioning of complex locking systems. It is also possible to create virtual locks from a data import.

To create a virtual lock, proceed as follows:

- Click on "Locks" in the main menu.
- Click on "New". The "Edit lock" configuration window opens.
- You can now create a virtual lock. Enter at least the name for the virtual lock and add further information if necessary. Permissions can be assigned to the virtual lock in the "Permissions" tab.
- Click on "Save" to confirm the entries and create the virtual lock.
- The virtual lock appears in the lock list with a blue star in front of the name.
- You can now also assign authorizations for the virtual lock in the matrix.
- You can create any number of virtual locks in the same way.

For a later assign of real locks to the virtual lock profiles, proceed as follows:

- Open the LEHMANN Data Transfer app on your smartphone.
- In the main menu of the LMS, click on "Data transfer".
  ATTENTION: The virtual locks are not displayed as programming requirements under "Data transfer".
- Place the smartphone on the USB desktop reader and wait until the green tick appears and the data transfer is complete.
- The data of the virtual lock profiles are transferred to the LEHMANN Data Transfer app.
- Go to the first lock for which you have created a virtual lock profile.
- Hold the smartphone with the LEHMANN Data Transfer app open in front of the lock.

- An input field appears for the name of the lock. Below this is a list with the names of the virtual locks that were previously created in the LMS.
- Select the appropriate name including configuration data from the list for the lock.
- Click on "Add".
- Repeat the process for the other locks.
- To transfer the locks to the LMS, place the smartphone on the RFID desktop reader and click on "Data transfer".
- The virtual lock profiles are now assigned to the real locks and all settings are adopted accordingly. The locks no longer appear with a blue star in front of the name.
- Click on "Locks" in the main menu.
- Here you find the new locks, which are marked with a blue dot.
- If you do not want to make any more changes to the lock configurations, mark the locks, click on "Edit" and then on "Save".
- The locks are now ready to use and visible in the matrix.

3 Chapter 3: Operation of the LEHMANN Management Software in online mode

The networked LEHMANN RFID systems CAPTOS and CAPTOS iCharge can be used either offline or online. In online operation, the CAPTOS and CAPTOS iCharge locks are connected directly to the customer's network and thus to the LMS via a primary controller. Configurations, authorizations and status information are updated in real time between the LMS and the online locks. The LEHMANN management software is operated online in the customer's IT infrastructure. The customer is responsible for operating the LEHMANN management software.

3.1 Commissioning and first steps

3.1.1 Commissioning and first steps

- Connect the USB desktop reader to the laptop / PC
- Download the latest version of the LMS from the Lehmann website https://lms.lehmann-locks.com
- Start the installation of the software LMS and follow the instructions during the installation.
- Select the installation type. For more information about the installation, please refer to the separate installation manual.
- After completing the installation, start the LMS software. Double-click the icon for the LEHMANN Management Software on your desktop. Alternatively, you can search and start the LEHMANN Management Software under the Windows Start button (“Search programs / files”).
- Select the language. You can change the language at any time.
- Enter the licence key “LMS Online” to activate the software. Additional licenses (e.g. “+5 LMS Users) are entered later in the software and must not be entered at this point. Place the card with the licence key on the USB desktop reader and click on “Read card with licence key”. Alternatively, you can enter the licence key on the keyboard. Click on “Continue”.
- Assign a username and secure password. The first LMS-user automatically has admin rights.
- Assign a project name and click on “Save”.

3.1.2 Login

- Enter username and password.
- Select in the drop-down list the project that should be opened. Note that the required authorizations for the respective project must be assigned to the LMS user (see 4.1).
- Click on “Login”.

3.2 Selection of the supported RFID technology per project

LEHMANN MIFARE® RFID systems and LEHMANN LEGIC RFID systems can be managed and configured in the LMS software. Online operation is currently supported with the LEHMANN MIFARE® DESFire® standard. Therefore, no changes under "Project Settings / General Settings" are necessary.

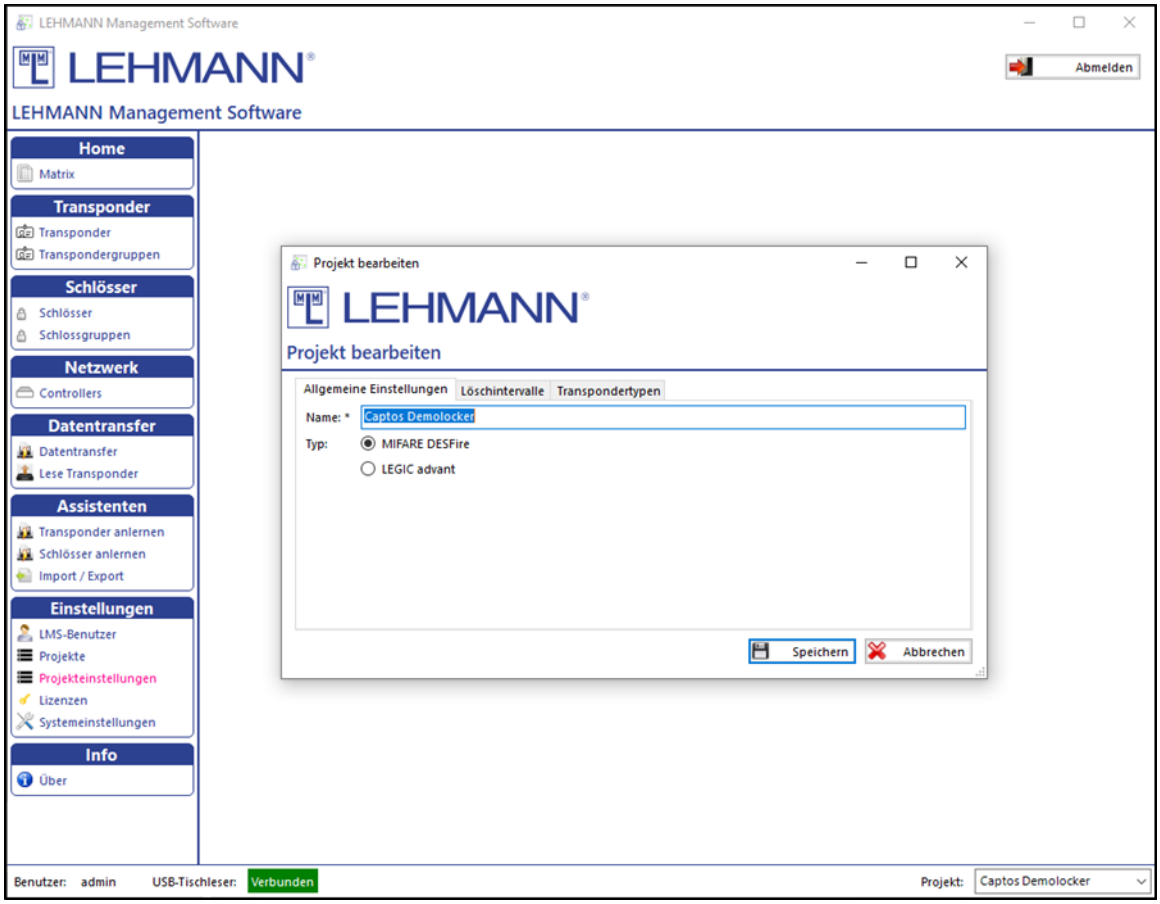


Figure: Selection of the RFID technology per project

3.3 Controller

When you activate the "LMS Online" license key, the "Network" menu item appears on the left-hand side of the LMS menu. All primary and secondary controllers are managed under the Network menu item.

3.3.1 Programming a Primary Controller

Before new locks or secondary controllers can be programmed, a primary controller must first be programmed in and configured. In order to be accessible in the network, the network settings of the Primary Controller must be set according to the customer's network properties.

- Make sure that the primary controller is connected to the LAN and the power supply.
- Open the app LEHMANN Data-Transfer on your smartphone.
- Hold the smartphone with the NFC antenna in front of the RFID antenna of the Primary Controller.

- The UID of the controller appears as the name.
- Enter a suitable name for the controller.
- Enter the IP settings according to your network requirements. Under certain circumstances, TCP releases must also be made in your network or firewall for the primary controller. The server URL is the address under which your LMS database is installed (server for server/client configuration or the corresponding single-user PC for single-user installation).
- Click on "Direct" in the app and then hold the smartphone with the NFC antenna in front of the RFID antenna of the primary controller.
- Click on "Controller" in the main menu.
- Mark the primary controller and click on "Edit".

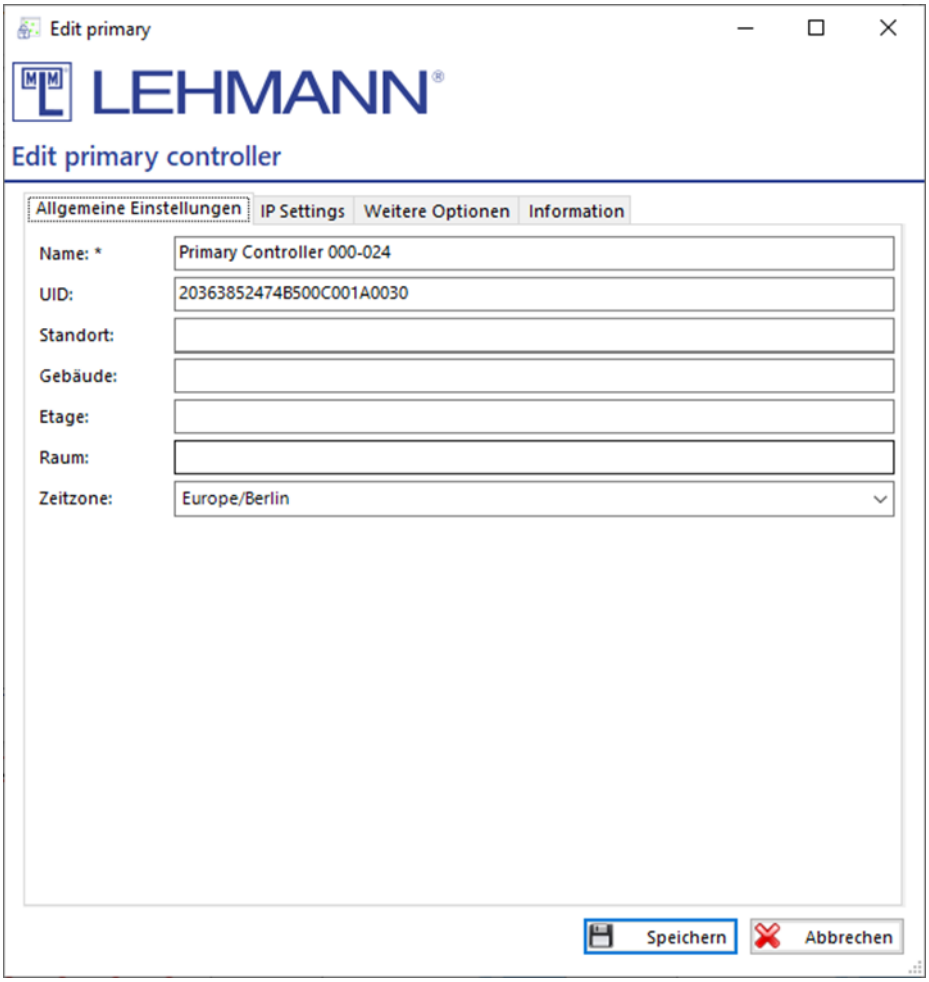


Figure: Primary Controller configuration window

- Complete the required information and click on the tab “IP Settings”. The IP settings for the controller open.

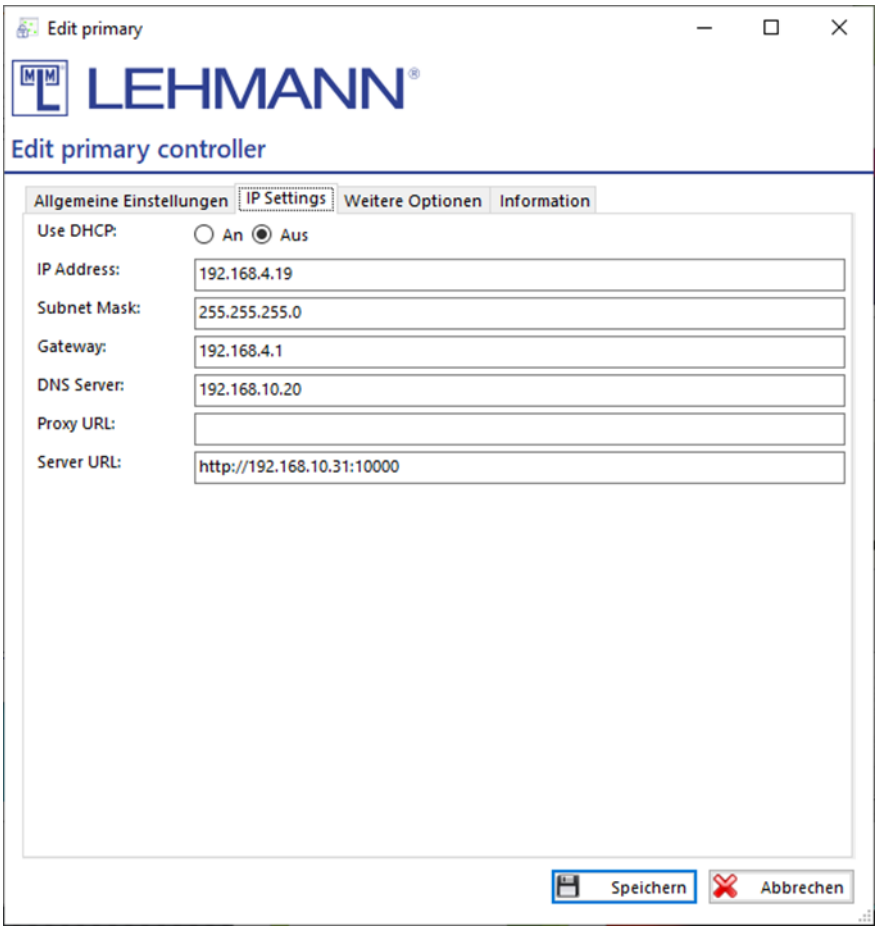


Figure: IP settings view

- Click on "Save".
- The blue dot next to the controller name disappears and the primary controller now appears under its name in the overview under "Controller".
- If the transferred IP settings are correct, the primary controller can now be reached from the LMS.
- This completes the configuration of the primary controller.
- The locks connected to the primary controller and the connected secondary controllers are also visible in the LMS (initially only with the respective UID as a name).
- If the blue dot does not disappear, the IP configuration is incorrect or the wiring of the LAN is incorrect. In this case, check the cabling or change the IP settings of the primary controller.

3.3.2 Changing the IP settings of the Primary Controller

It may be necessary to change the IP settings of a Primary Controller. This can become necessary after incorrect settings were entered when learning the controller or after changes in the LAN. Note that incorrect changes to the IP settings mean that the controller can no longer communicate with the LMS and that the locks connected to the controller can no longer be reached online. For correct IP settings, contact your network administrator. To change the IP settings of a primary controller, proceed as follows:

- Click on “Controller” under the item “Network” in the LMS menu.
- Mark the primary controller to be changed and click on "Edit".
- Open the "IP Settings" tab and make the appropriate changes. Then click on "Save".
- Now click on "Data transfer" and place your smartphone with the LEHMANN Data Transfer app open on the USB desktop reader. A green arrow will appear with the name of the controller.
- Now go to the relevant controller and hold your smartphone in front of the RFID antenna until a green tick appears.
- If the settings are correct, the LMS can now connect to the primary controller. This will then be visible under "Network / Controller" with its name without status symbols (blue dot, red X), as well as the secondary controllers and locks connected to it.

3.3.3 Programming a Secondary Controller

In order to program the locks that are connected to a secondary controller in the LMS, the secondary controller must first be programmed. To do this, make sure that the secondary controller is connected to a primary controller that has already been programmed and can be reached by the LMS and that it is also supplied with power.

- Click on “Controller” under the item “Network” in the LMS menu.
- Expand the structure tree of the primary controller under which the secondary controller is connected. The Secondary Controller should appear under its UID with a blue star. If not, check the connection cables to the primary controller and make sure it is connected to the network and to the power supply.
- Double-click on the UID of the Secondary Controller.
- Enter a name for the Secondary Controller under "General settings", add further details if necessary and then click on "Save".
- The Secondary Controller is now programmed and ready for operation. If you now open the structure tree of the controller (on +), the locks connected to this controller become visible.

3.3.4 Reset of a controller

Proceed as follows to reset a primary or secondary controller to the factory delivery status. Make sure that locks that may have been connected to the respective controller have either already been reset to the factory delivery status or that the locks can now be accessed via another controller.

- Click on “Controller” under the item “Network” in the LMS menu.
- Mark the controller to be reset and click on "Edit".
- Open the "More options" tab.
- Click on "Reset device" and confirm your selection.
- The controller is reset.

3.3.5 Firmware update for a controller

Proceed as follows to update the firmware on a primary or secondary controller.

- Click on “Controller” under the item “Network” in the LMS menu.

- Mark the controller that is to receive a firmware update and click on "Edit".
- Open the "More options" tab.
- Click on “Firmware update”.
- If new firmware is available, it will be displayed to you. Click Firmware Update.
- The update process starts and you can monitor the progress under "Information".
- If you have received individual firmware from Lehmann, select the firmware on the drive or folder where you previously saved it.
- Click on "Open". The update process starts automatically and you can monitor the progress under "Information.

3.4 Assistance functions

With the assistance function, RFID systems and transponders can be programmed in the LMS by using a guided process. In order to program new locks, at least one primary controller and then, if necessary, the secondary controllers connected to it must first be programmed (see point 3.3). All controllers and locks to be programmed must be in the factory delivery status, otherwise the programming procedure is not possible. Locks that have already been programmed in in other projects or that have been programmed with a master card must first be reset to the factory delivery status.

3.4.1 Programming transponders

- Click in the main menu on “Program transponders” and follow the instructions in the software.
- Place a transponder on the USB desktop reader and leave it there during the process of adding the transponder to the LMS software.
- Enter the name of the transponder in the pop-up window.

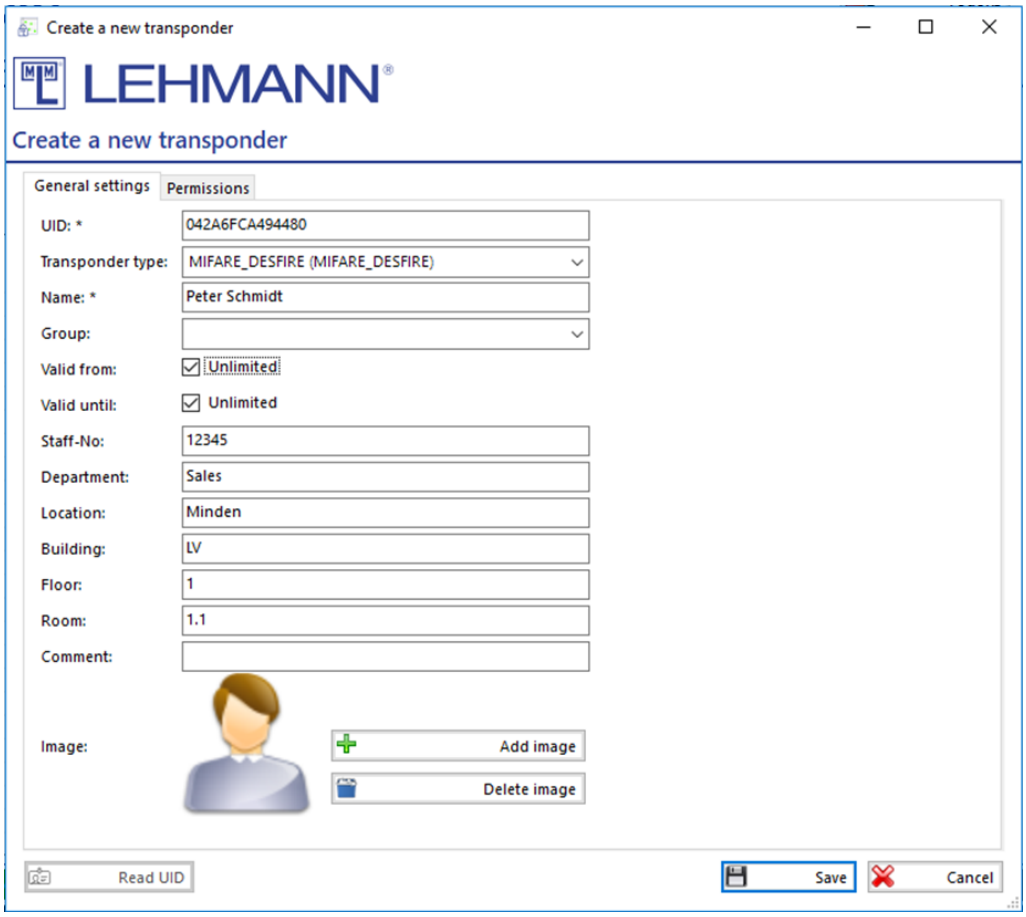


Figure: Create a new transponder

- You can enter additional information in the pop-up window to simplify the administration.
- If the transponder should not be valid immediately and / or not indefinitely, uncheck the box “Valid from” or “Valid to” and enter the corresponding date.
- Click on “Save”.
- The data is transferred to the transponder.
- After the process has been completed, you can place another transponder on the USB desktop reader and repeat the process.

3.4.2 Programming RFID systems (CAPTOS / CAPTOS iCharge)

The CAPTOS and CAPTOS iCharge locks must be in the factory delivery status and must not have already been programmed with a master card or in another LMS project. Make sure that the lock is connected to a controller that has already been programmed and that it is supplied with power. Under Assistants, click on "Program locks". Follow the instructions in the wizard to initialize and configure the RFID systems. Programming without an assistant and the configuration options are described in detail under point 3.5.

3.5 Programming and configuring RFID systems

There are different ways of programming CAPTOS and CAPTOS iCharge locks in the LMS. It must be ensured that the lock is correctly connected to a controller and that both the corresponding primary controller and, if applicable, the secondary controller are correctly programmed in the LMS and connected to a power supply.

3.5.1 Programming RFID-Systems with the app LEHMANN Data Transfer

- Open the app LEHMANN Data Transfer on your smartphone.
- Hold the smartphone with the NFC antenna in the middle of the RFID reader of the lock.
- The initial information from the RFID system is transferred to the app.
- It is recommended that you give the lock a clear and understandable name in the app, with which you can identify the lock.
- Click **"Add"** in the app to confirm the name.
- Repeat the process for further RFID systems.
- The name for the next lock is logically generated, so if the previous lock was named “113”, then “114” would be suggested as the name for the next lock. Clicking “Add” will add that name for the selected lock. A name can also be entered manually by writing in the text field and confirmed with "Add".
- Click on "Data transfer" in the LMS software.
- Place the smartphone with the open app on the USB desktop reader and leave it there during the entire data transfer.
- The information from the RFID systems is now being transmitted. A configuration window opens one after the other for each RFID system. Configure the locks. Make sure to use the correct time zone. For more information about the configuration options, see point 3.11. Then click on "Save".

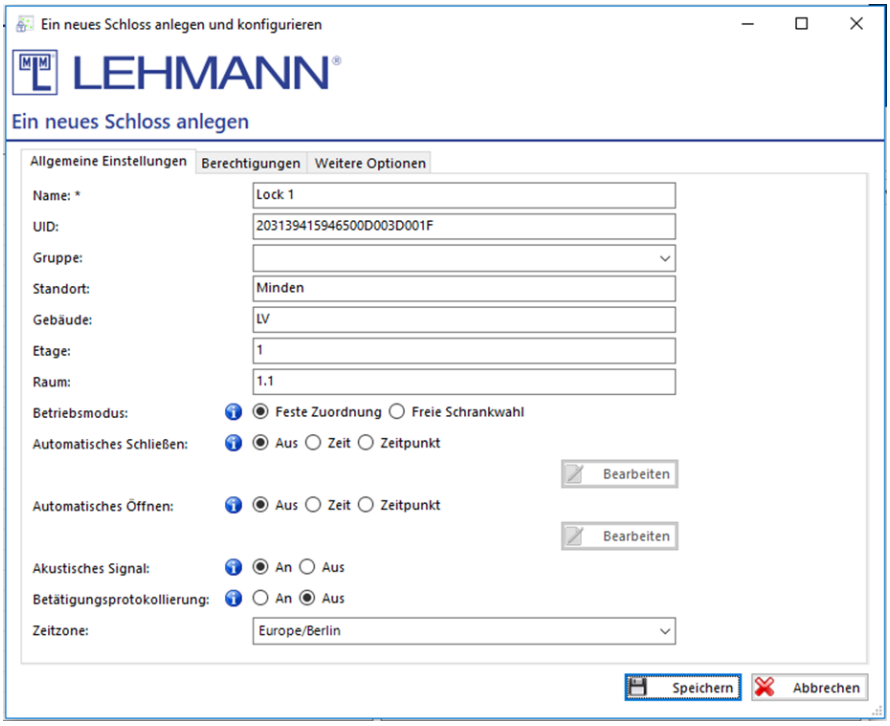


Figure: Create a new lock

- The new configuration data for the RFID systems are transferred back to the smartphone.
- Hold the smartphone with the open app in front of the RFID readers of the locks one after the other until the data transfer is confirmed with a green tick. The new configuration data is transmitted to the individual RFID systems.
- The initial programming of the RFID systems is completed by placing the smartphone with the open app on the USB desktop reader again and clicking on "Data transfer" in the LMS software. With this step, the software receives confirmation that the RFID systems are now configured and ready for use.

3.5.2 Programming RFID systems with LEHMANN Data Transfer via the LAN

This way of programming new locks is particularly suitable if the locks and the LMS installation are located separately from each other. The RFID systems must be in the factory delivery state and be connected to the network via a programmed controller.

- Open the app LEHMANN Data Transfer on your smartphone.
- Hold the smartphone with the NFC antenna in the middle of the RFID reader of the lock.
- The initial information from the RFID system is transferred to the app.
- It is recommended that you give the lock a clear and understandable name in the app, with which you can identify the lock.
- Click **"Direct"** in the app to confirm the name.
- Hold the smartphone with the NFC antenna in the middle of the RFID reader of the lock.
- Repeat the process for further RFID systems.
- The name for the next lock is logically generated, so if the previous lock was named “113”, then “114” would be suggested as the name for the next lock. Clicking “Direct” will then add that name for the selected lock. A name can also be entered manually by writing in the text field and confirmed with "Transfer". After selecting the name in the app, hold the smartphone with the NFC antenna in the middle of the RFID reader of each lock.
- Under "Network" in the LMS menu click on "Controller".
- Expand the structure tree of the controller to which the locks are connected.
- Click on the individual locks and complete the corresponding configurations. Then click on "Save".
- After saving, the lock is programmed and can be used.

3.5.3 Programming RFID systems via LAN without LEHMANN Data Transfer

It must be ensured that the lock is correctly connected to a controller and that both the corresponding primary controller and, if applicable, the secondary controller are correctly programmed in the LMS and connected to a power supply.

- Click on “Controller” under "Network" in the LMS menu.
- Select the controller to which the lock is connected, that should be is programmed. To do this, unfold the structure tree of the controller.
- Locks that have not yet been programmed are marked with a blue star and with the UID in the overview.

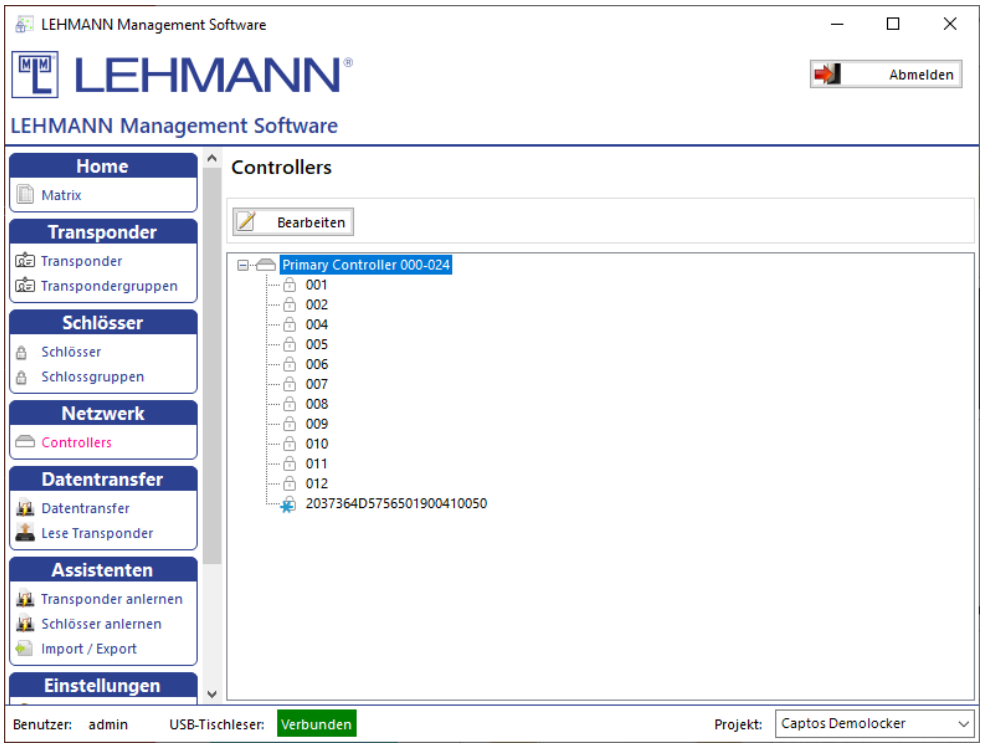


Figure: Programming an RFID lock

- Select the lock with a double-click, that should be programmed. The configuration window opens.

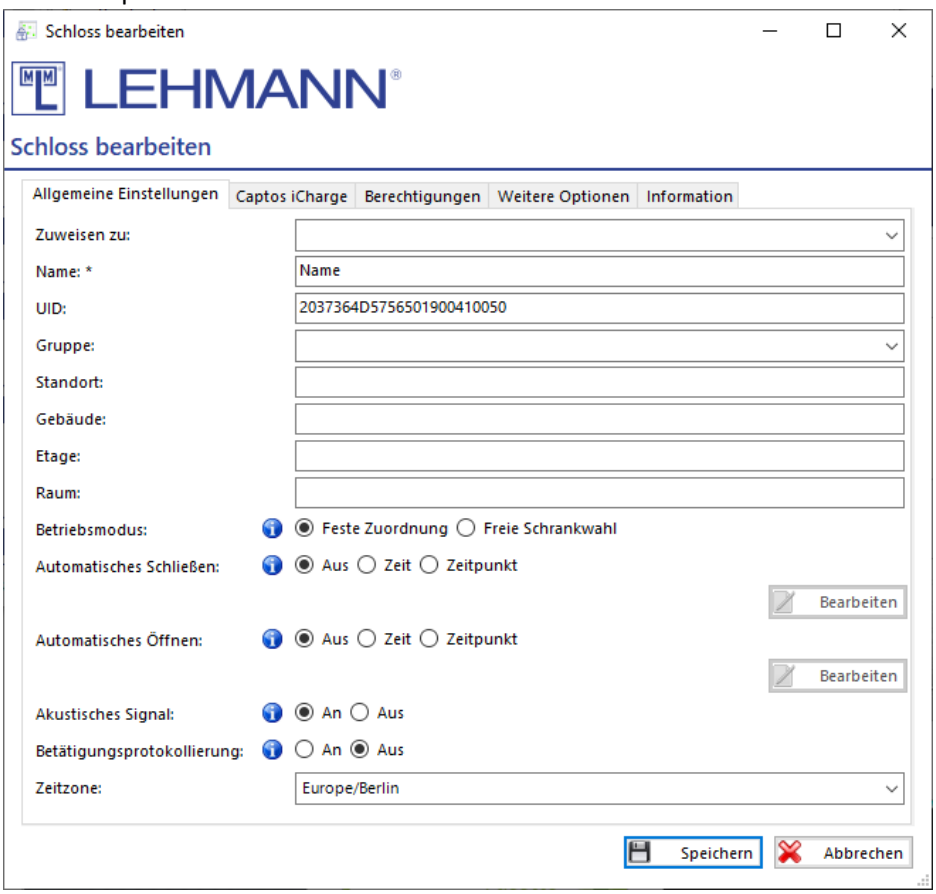


Figure: Configuration window RFID lock

- If you cannot clearly identify the lock, click on "Identifier" under "Further options". The lock starts beeping and flashing white with the status LEDs. A clear identification of the lock is possible in this way.
- Enter a name for the lock, carry out further configurations if necessary and click on "Save".
- The lock is now displayed with its name and a blue dot. As soon as the data has been automatically transferred to the lock via the network, the blue dot disappears and the lock is programmed.

3.6 Data Transfer

After each adding of new transponders or locks to the LMS as well as after authorization and configuration changes in the software there is a need for programming on the transponders or on the locks. The programming requirement is shown in the matrix and in the lock / transponder overviews by a blue dot next to the transponders or locks.

In online mode, all authorization and configuration changes are transmitted to the locks in real time. The blue dots then usually disappear after a few seconds. An exception to this is the change of the validity of a transponder. This must be updated via "Data Transfer" after the change.

In the event of network disruptions, changes may not be able to be transferred directly to the locks. In this case, or in the case of mixed operation with offline locks, the data transfer function can be used. To do this, proceed as follows:

- Click on “Data transfer” in the main menu.
- In the lists for “Transponders” and “Locks” there are all components with programming requirements.
- Data transfer to transponders:
  - Place the transponders with programming requirement one at a time on the USB desktop reader.
  - The data is transferred automatically
  - The transponders are now programmed and can be used for the RFID systems.
  - The blue dot next to the transponder and next to the RFID systems in the matrix has now disappeared.
  - Hold the transponder in front of the RFID reader and check the open / close functions when the furniture door is open.
  - After successful data transfer, the transponders are automatically removed from the list.
- Data transfer to smartphones:
  - Open the app LEHMANN Data Transfer on your smartphone.
  - Place the smartphone with the open app on the USB desktop reader and leave it there during data transfer.
  - The data is transferred automatically.
  - Hold the smartphone with the app in front of the RFID readers of the locks, until the data transfer is confirmed with a green tick. Hold the NFC antenna of your smartphone centered in front of the RFID reader of the lock.
  - The new permissions are transferred to the individual locks.

- The process is completed by placing the smartphone with the open app on the USB desktop reader and by clicking on “Data transfer” in the LMS software. With this step, the software receives the confirmation that the RFID system has received the new authorizations.
- After successful data transfer, the transponders are automatically removed from the list.

3.7 Assign authrisations / delete authorisations

Depending on the available storage space, up to 250 authorizations can be programmed to a transponder. If more than 250 authorizations are required on a transponder (e.g. card for facility management), a special transponder type (see point 4.2.3) must be configured.

- Click on “Matrix” in the main menu.
- Assign permissions for transponders for the required RFID systems by ticking in the matrix with a mouse click.
- To delete an authorization, remove the check mark in the matrix with a mouse click.
- The blue dot next to the transponder and next to the RFID system means that a data transfer to the transponder or to the RFID system has to be carried out.
- As soon as the data transfer is completed and the new authorizations have been automatically transferred to the lock, the blue dot will disappear.

- If the blue dot does not disappear, the connection between the LMS and the lock is (temporarily) interrupted. In this case, the pending data transfer can be carried out manually using the LEHMANN Data Transfer app (see point 3.6).

3.8 Gruppen

For easier management, transponders and RFID systems can be grouped. It is possible to create up to ten group levels. The groups are displayed in the matrix next to the associated transponders or the associated RFID systems. Note that groups are not displayed in the matrix until transponders or RFID systems have been assigned to these groups.

3.8.1 Transponder groups

- Click on “Transponder groups”. You receive an overview of the transponder groups. Transponder groups are displayed under the “Main group”. The following actions are possible:

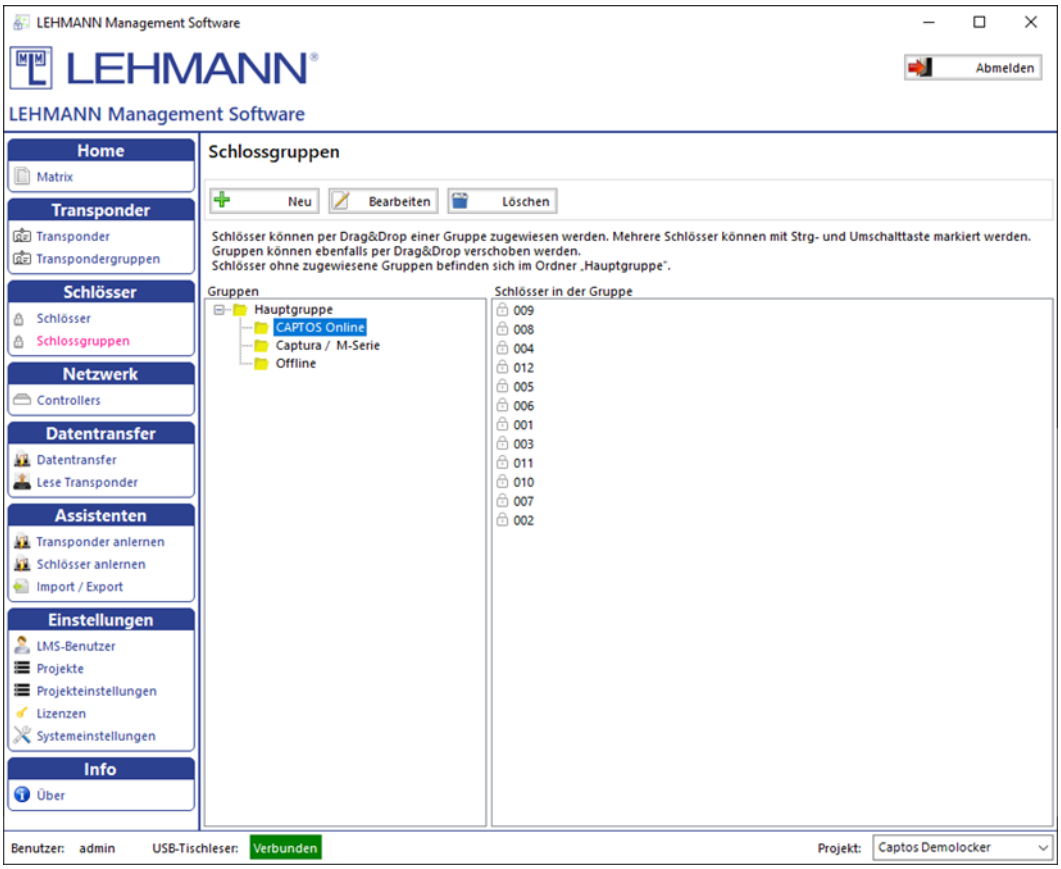


Figure: Transponder groups

- New: Add new groups
- Edit: Change existing group names and hierarchy levels
- Delete: Delete groups

3.8.1.1 Add transponder groups

- Click on “New“.
- Assign a name to the new group and, if necessary, select a previously created group as the superior group.
- You can assign colours to each group displayed in the matrix.
- Click on “Save“.

3.8.1.2 Assign or move a transponder to a group

- All transponders that are not assigned to a group are located in the folder “Main group”.
- Select one or more transponders to be assigned or moved to a group.
- Then drag & drop the transponders into the required group.

3.8.1.3 Edit transponder groups

- Select the group to be changed in the list with a mouse click and click on “Edit”.
- Change the name of the group, the parent group or the colour representation in the matrix.
- Click on “Save“.

- To move groups, select a group and drag & drop the group to the required location. Any sub-groups are moved as well.

3.8.1.4 Delete transponder groups

- Select the group to be deleted in the list with a mouse click and click on “Delete”.
- Confirm the deletion.
- If transponders are still in the group that should be deleted, the transponders are retained and are moved to the next higher group.

3.8.2 Lock groups

- Click on “Lock groups” in the main menu and you will get an overview of the lock groups. You can also assign a superior group to a lock group. Lock groups are displayed under the “Main group”. The following actions are possible:

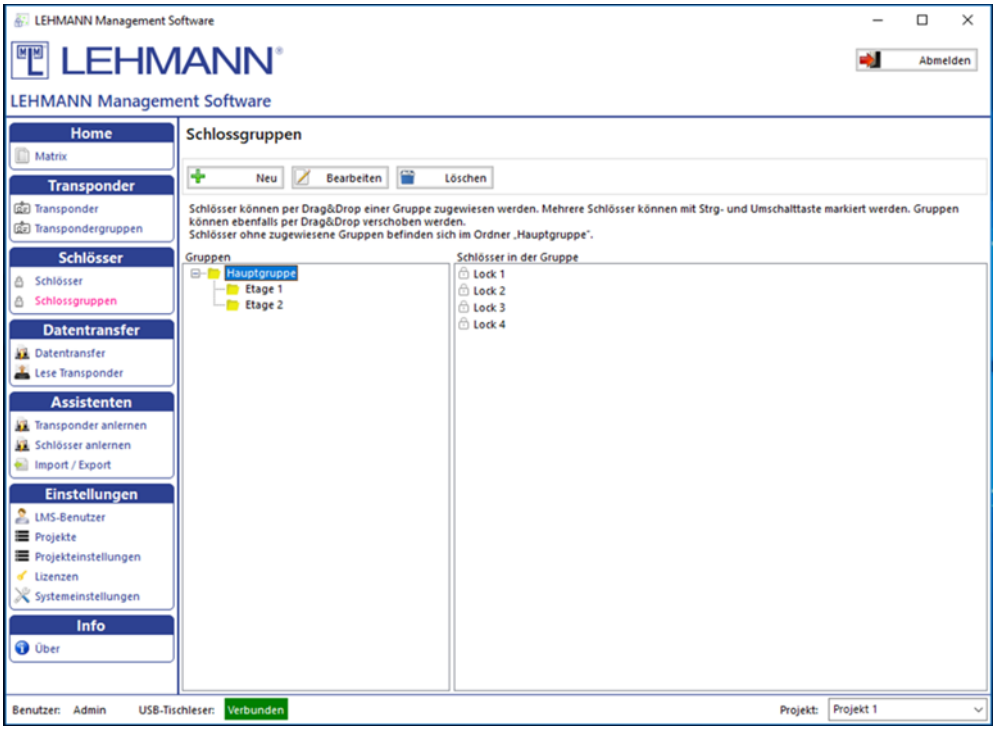


Figure: Lock groups

- New: Add new groups
- Edit: Change existing group names and hierarchy levels
- Delete: Delete groups

3.8.2.1 Add lock groups

- Click on “New“.
- Assign a name to the new group and, if necessary, select a previously created group as the superior group.
- You can assign colours to each group displayed in the matrix.
- Click on “Save“.

3.8.2.2 Assign or move a lock to a group

- All locks that are not assigned to a group are located in the folder “Main group” (see figure “Lock groups”). Please click on “Main group”.
- Select one or more locks to be assigned or moved to a group.
- Then drag & drop the locks into the required group.

3.8.2.3 Edit lock groups

- Select the group to be changed in the list with a mouse click and click on “Edit”.
- Change the name of the group, the superior group or the colour representation in the matrix.
- Click on “Save“.
- To move groups, select a group and drag & drop the group to the required location. Any sub-groups are moved as well.

3.8.2.4 Delete lock groups

- Select the group to be deleted in the list with a mouse click and click on “Delete”.
- Confirm the deletion.
- If locks are contained in the group to be deleted, the locks are retained and may be moved to the next higher group.

3.9 Berechtigungsvergabe von Gruppen

- Click on “Matrix“ in the main menu.
- Click on the group name (transponder / lock) within the matrix. The associated transponders or locks are hidden, so that only the group name is displayed (see figure: Groups (2)).

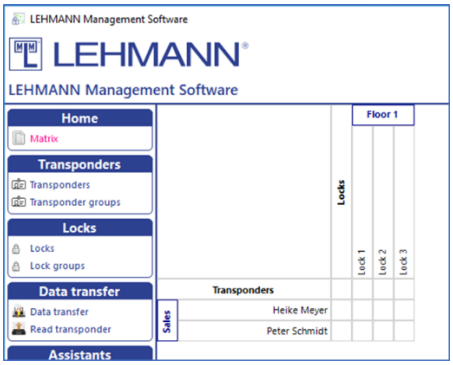


Figure: Groups (1)

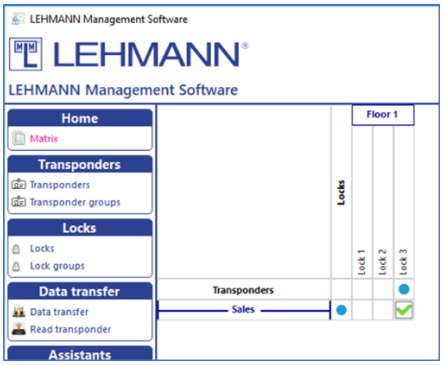


Figure: Groups (2)

- Authorise the entire group on the respective RFID system by ticking in the matrix with a mouse click.
- The blue dot next to the transponder group and next to the RFID system means that data must be transferred to all transponders in the group or to the RFID system.
- In online mode, the blue dots usually disappear within a few seconds. If this is not the case, for example due to a network problem, you can carry out the data transfer manually (see point 3.6).

If not all transponders or locks of a group have the same authorizations, this is indicated in the matrix by a gray tick.

CAUTION: If there are a large number of concurrent permission changes, such as those that occur when permission changes are made to groups, the software LMS may need much more time to process the changes.

3.10 Add, configure and delete transponders

To add, configure and delete transponders, you need the appropriate authorization (see 4.1).

- Click on “Transponders” in the main menu and you get an overview of the transponders.
- The following actions are possible:
  - New: Add new transponders
  - Edit: The settings for one or more selected transponders can be changed.
- Several transponders can be marked and selected at the same time (Ctrl or shift key). In this way, configurations (e.g. validity) or actions (e.g. deleting lost transponders) can be carried out for several transponders at the same time. To configure several transponders at the same time, click on "Edit" after selecting the transponders. Please note that not all actions or configuration changes for transponders can take place at the same time. Certain changes must be made separately for each transponder.

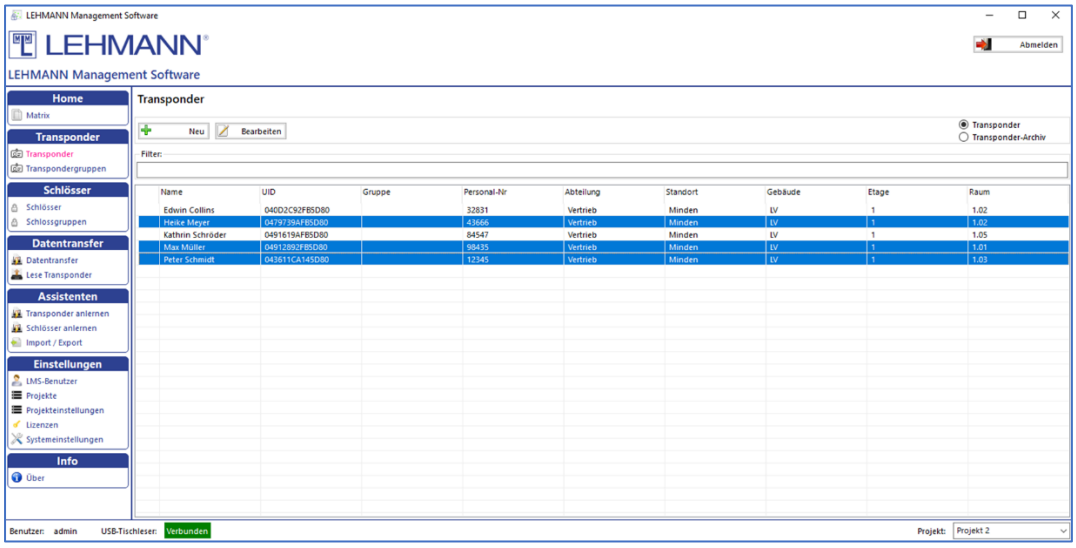


Figure: Selection of several transponders

3.10.1 Add new transponders

- Click on “New” to create a transponder.
- Place a transponder on the USB desktop reader and click on “Read UID”. The transponder's UID is automatically written to the required UID field.
- The Transponder Type field is automatically filled.
- The following settings are possible in the “Common Settings” tab:

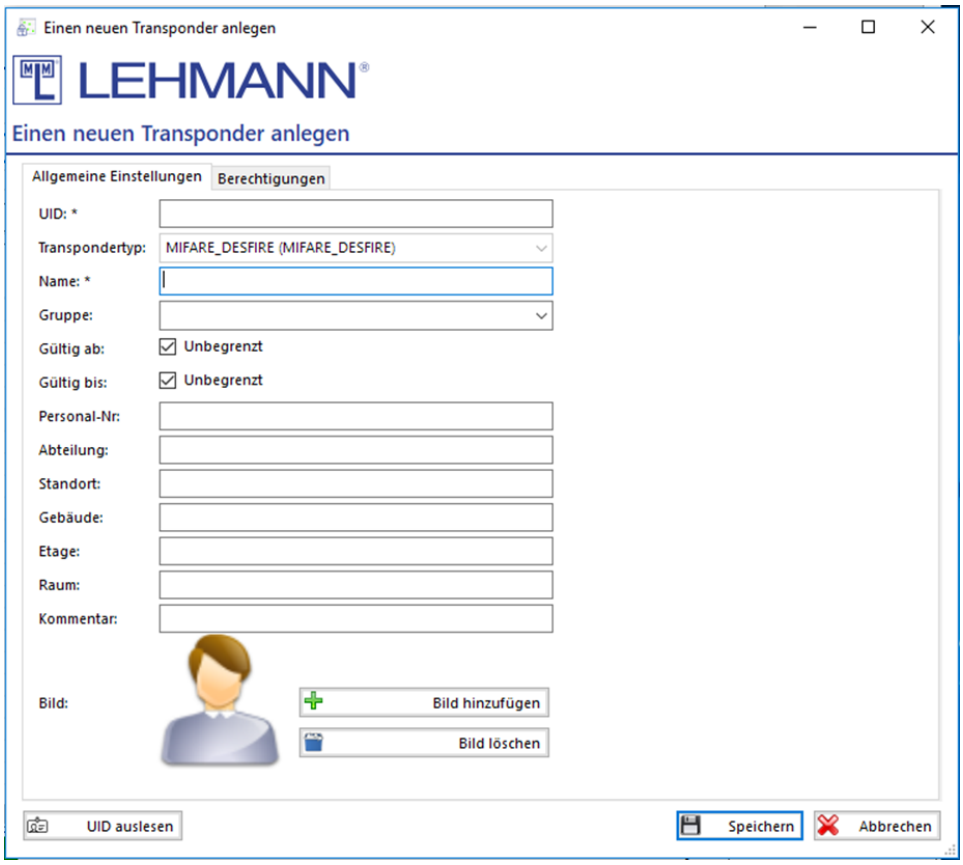


Figure: Create a new transponder

- Assign a unique name for the transponder.
- If necessary, assign the transponder to a previously created group.
- If the transponder is not to be valid immediately and / or not indefinitely, uncheck the box “Valid from” or “Valid to” and enter the corresponding date.
- If required, enter additional information about the person using the transponder, such as employee number, department, etc.
- You can add a picture of the transponder holder by clicking on “Add image” or delete an existing picture by clicking on “Delete image”.

- Click on “Save”.
- Click on “Data transfer” in the main menu and transfer the changes to the transponder (see 2.5).

3.10.2 Settings for the transponders

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- You can use the filter function to search for specific transponders. To do this, enter a part of the transponder name in the filter, then you will see all transponders that contain the text in the name.
- The information and settings in this screen can be changed at any time, except for the UID and Transponder Type.

- Click on “Save“.
- In exceptional cases (e.g. when changing the period of validity) there is also a need for programming the transponders in online operation. This is indicated by a blue dot next to the name of the transponder in the transponder list or under data transfer. In this case, click on "Data transfer" in the main menu and, if necessary, transfer the changes to the transponder (see point 3.6).

3.10.3 Permissions

In addition to the authorization management in the matrix, permissions can also be managed in the main menu under “Transponders”. Depending on the available storage space, up to 250 authorizations can be programmed to a transponder. If more than 250 authorizations are required on a transponder (e.g. card for facility management), a special transponder type (see point 4.2.3) must be configured.

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- Click on the “Permissions” tab.

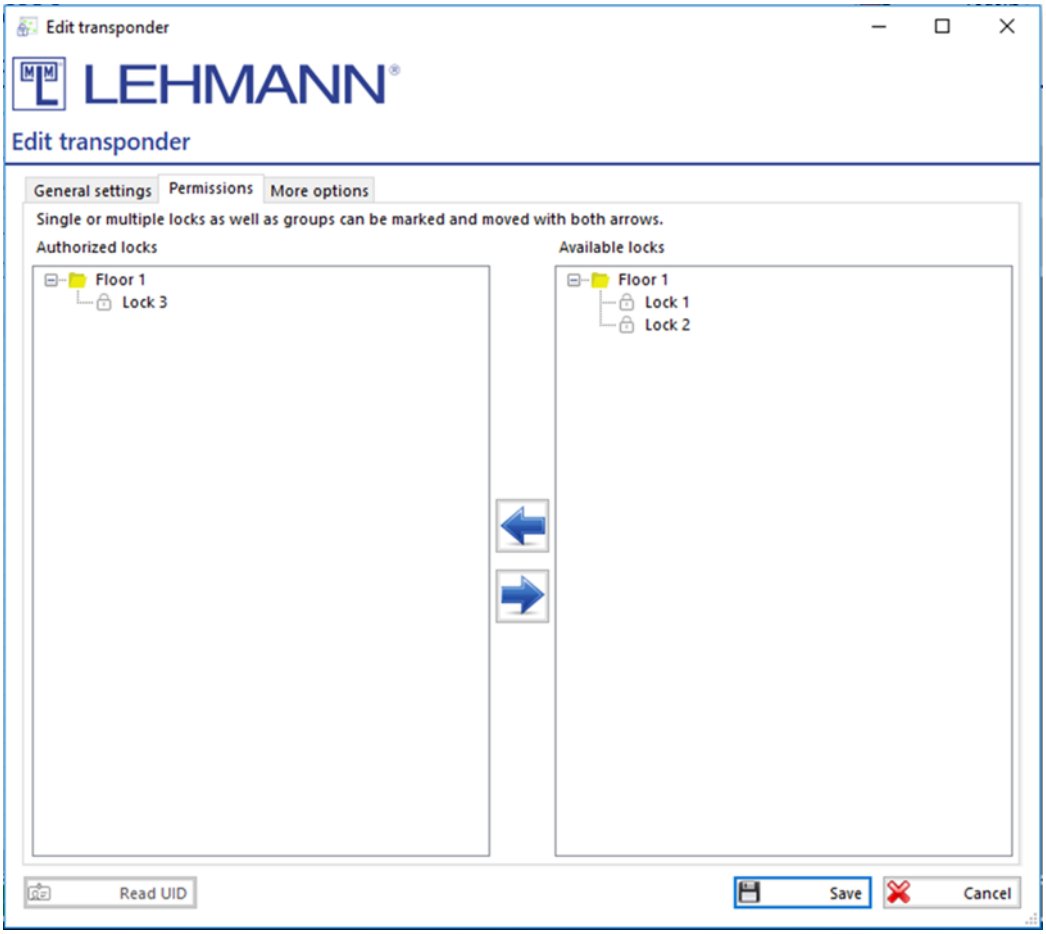


Figure: Edit transponders – Permissions

- In the right table (Available locks) you will find all the locks that are already available in the project and for which the transponder has no authorisation. Furthermore, the groups in which the locks are located are displayed here.

- In the left table (Authorized locks) are the locks for which the transponder is already authorized. Furthermore, the groups in which the locks are located are displayed here.
- Select and mark any number of locks and drag the locks from one side to the other in order to edit permissions. Before the data transfer is done, changes in permissions are marked in this view with a blue dot (new authorization) or with a red cross (authorization revoked).
- You can also move entire groups including all locks.
- Programming requirement is indicated by a blue dot.
- Click on “Save”.
- The data is transferred to the locks automatically. In exceptional cases, there is also a need for programming in online operation. This is indicated by a blue dot next to the name of the transponder in the transponder list or under data transfer. In this case, click on "Data transfer" in the main menu and, if necessary, transfer the changes to the transponder (see point 3.6).

3.10.4 Replacing and deleting transponders and more options

- Click on “Transponders“ in the main menu.
- Select one or more transponder in the overview of all transponders and click on “Edit”.
- Click on the tab “More options”.
- In the tab “More options” the following settings can be made:

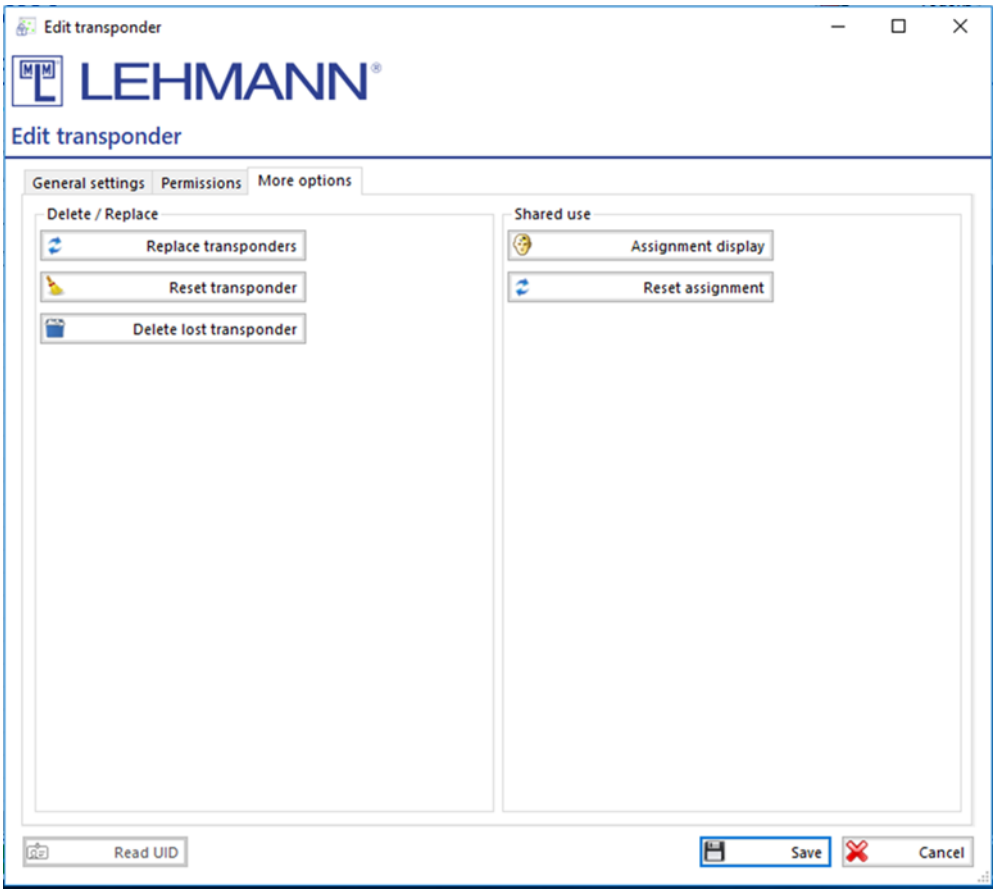


Figure: Edit transponder – More options

- Replace transponders: The transponder can be replaced e.g. after loss.
  - Click on “Replace transponders”.
  - Place the new transponder on the USB desktop reader and click on “Read UID”.
  - All previous authorizations and blocking remarks are automatically transferred to the new transponder. The previous transponder loses its validity for locks in „assigned use” mode.
  - Click on “Save”. The data transfer to the new transponder starts automatically.

ATTENTION: Click on "Data transfer" in the main menu and check whether there is a need for programming. Usually this is not the case. However, especially in the event of network disruptions, it may happen that the authorizations for the corresponding locks cannot be updated automatically. In order to prevent unauthorized access with the replaced transponder, you should immediately carry out the data transfer to the RFID systems with the smartphone as described in point 3.6.

The temporary authorisation for a lock in “shared use” mode is not transferred to the new transponder. In this case, an emergency opening must be carried out on the lock (see point 5.5).

- Reset transponder: The transponder will be reset. The transponder does not appear in the matrix any more. The transponder can then be programmed again.
  - Place the transponder that should be reset on the USB desktop reader.
  - Click on “Reset transponder“.
  - The transponder is reset immediately and removed from the matrix. There is no further need for programming under “Data transfer”.

- Delete lost transponder: All information on the transponder will be deleted. The transponder does not appear any longer in the matrix. The transponder can then be used again.
  - Click on “Delete lost transponder“.
  - The transponder will be deleted immediately and removed from the matrix.

ATTENTION: Click on "Data transfer" in the main menu and check whether there is a need for programming. Usually this is not the case. However, especially in the event of network disruptions, it may happen that the authorizations for the corresponding locks cannot be updated automatically. In order to prevent unauthorized access with the replaced transponder, you should immediately carry out the data transfer to the RFID systems with the smartphone as described in point 3.6. Only then is the authorization in the locks in "fixed assignment" mode deleted. Otherwise, the old transponder retains access authorizations until the authorizations have been updated and there is no longer any need for programming.

- Assignment display: If an RFID lock in the operating mode “shared use” has been locked with the transponder, the name of the corresponding RFID lock is displayed.
  - Place the transponder on the USB desktop reader.
  - Click on “Assignment display“.
- Reset assignment: After an emergency opening in operating mode “shared use”, the transponder is blocked for parallel use on other RFID systems in operating mode “shared use”. In order to un-block the transponder, use this function:
  - Place the transponder on the USB desktop reader.
  - Click on “Reset assignment”.
  - The occupancy settings on the transponder are automatically deleted. There is then no further need for programming under “Data transfer”.

3.11 Configure and delete RFID systems

You need the appropriate authorization to add, configure and delete RFID systems (see point 4.1).

- Click on "Locks" in the main menu and you will get an overview of the RFID systems. In this overview you can see all the available RFID systems in this project as well as further information such as groups, operating mode, status displays, network faults, etc.
- Several locks can be marked and selected at the same time (Ctrl or shift key). In this way, configurations (e.g. operating mode) or actions (e.g. resetting locks) can be carried out for several locks simultaneously. To configure several locks at the same time, click on "Edit" after selecting the locks. Please note that not all actions or configuration changes for locks can take place at the same time. Certain changes must be made separately for each lock.

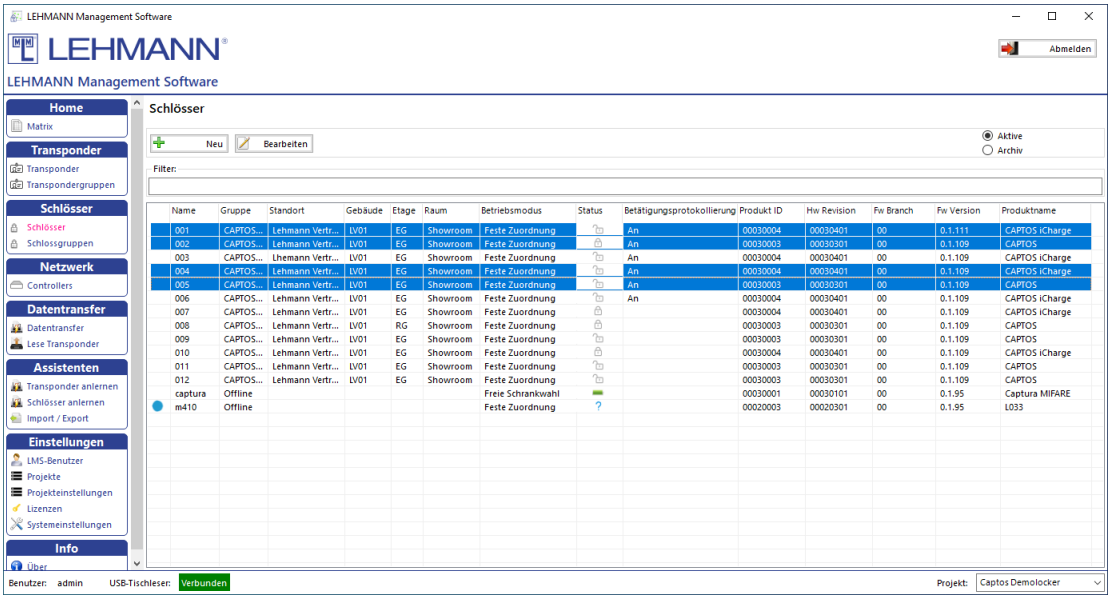


Figure: Selecting multiple locks

3.11.1 Configuration of RFID systems

- Click on “Locks“ in the main menu.
- Select one or more locks in the overview for which the configuration should be changed and click on “Edit”.
- You can use the filter function to search for specific locks. To do this, enter a part of the lock name in the filter, then you will see all locks that contain the text in the name.
- In the tab “General settings”, the following settings for the respective RFID system can be made both directly when the lock is added and during operation:
    - Operating mode: Selection of the operating mode (Note: RFID systems in the operating mode “shared use” are shown in the matrix with an asterisk in front of the lock name). Further information about the operating modes can be found in 1.3.1.
    - Automatic locking: In addition to the default setting (Off), a time period or a fixed time can be selected when the locks close automatically. This function is available in “assigned use” mode. NOTE: Please note that this function is only suitable for locks with a spring-loaded bolt!
    - Automatic opening: In addition to the default setting (Off), the locks can be configured to open automatically after a period of time or at a fixed time.
    - Acoustic signal: In addition to the default setting (On), the acoustic signal can be deactivated.
    - Activity logging: Activities on the RFID systems can be logged and transferred using the LEHMANN Data Transfer app and then displayed in the software. This function is deactivated in the factory settings. When you first click on “On” within a project, you must make a decision whether you want a 2-factor authentication.

Figure: Two-factor authentication

With a 2-factor authentication (enter of a second password) the log files are additionally secured. Furthermore, in the main menu under Project settings (see 2.11.2) you can set how long the data should be stored in the software (factory setting: 14 days). The display of the data is only possible for users with “admin rights”.
After activating the “Activity logging”, the tab “Lock activities” appears.

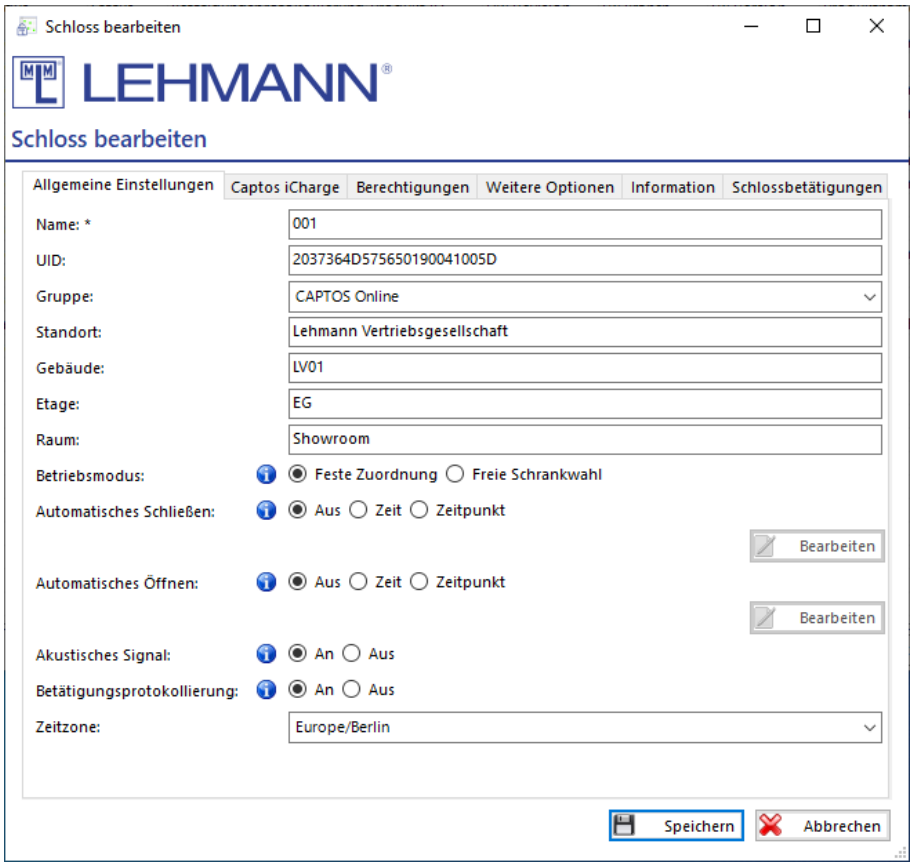


Figure: Edit lock – General settings

- Time zone: If the time zone for the RFID system is not set correctly, please set the correct time zone. The correct time is necessary for time-dependent functions. Also make sure that the time on your smartphone is set correctly.

- Enter your required settings for the RFID lock.
- Click on “Save“.
- The data is automatically sent to the respective lock.
- In exceptional cases, there is also a need for programming in online mode (see point 3.5).

3.11.2 Additional functions for CAPTOS and CAPTOS iCharge locks

- Click on “Locks“ in the main menu.
- Select one or more CAPTOS or CAPTOS iCharge locks in the overview for which the configuration should be changed and click on “Edit”.
- If you have selected a CAPTOS or CAPTOS iCharge lock, you can make the following settings in the additional tab "Captos" or "Captos iCharge":

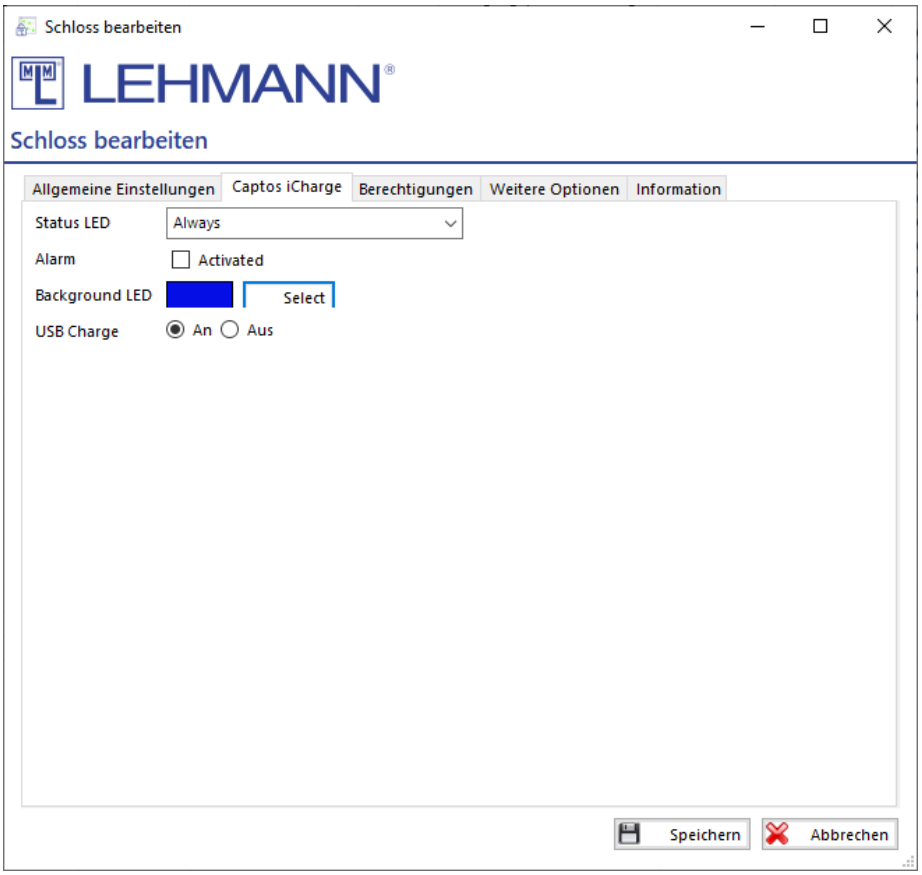


Figure: CAPTOS and CAPTOS iCharge settings

- Status LED: The status LED signals to the user whether the lock and thus the locker is open or closed. This function is particularly suitable for locks in the shared use operating mode. Green stands for open (available), red for closed (occupied). The following settings are possible in the drop-down menu:
  - Off: The status LED never lights up, apart from optical signals when opening or closing the lock.
  - Only when open: The status LED only lights up when the lock is unlocked.
  - Only when closed: The status LED only lights up when the lock is closed.
  - Always: The status LED is always on.
- Alarm: By ticking the box, the alarm function of the lock can be activated or deactivated. When the lock is locked, the locking pin is detected by a sensor in the lock. If the lock is locked and the locking pin is removed without opening having taken place, a forced opening can be assumed and an audible alarm is triggered. If the logging function is activated, the time of the alarm is logged.
- Background LED (only with CAPTOS iCharge): Clicking on “Select” opens a dialog window in which the colour of the background LED can be set. Click on the color scales to select the required colour, or RGB values can be set. The LED can also be deactivated by setting the colour to black (All RGB values = 0).

- USB charge (only with Captos iCharge): The USB charging socket can be activated or deactivated.

- Click on "Save".
- The data is automatically sent to the respective lock.
- In exceptional cases, there is also a need for programming in online mode (see point 3.5).

3.11.3 Permissions

- Click on “Locks“ in the main menu.
- In the locks overview, select one or more locks for which the permissions should be changed and click on “Edit”.
- In addition to the authorization management in the matrix, permissions can also be managed in the tab “Permissions”:

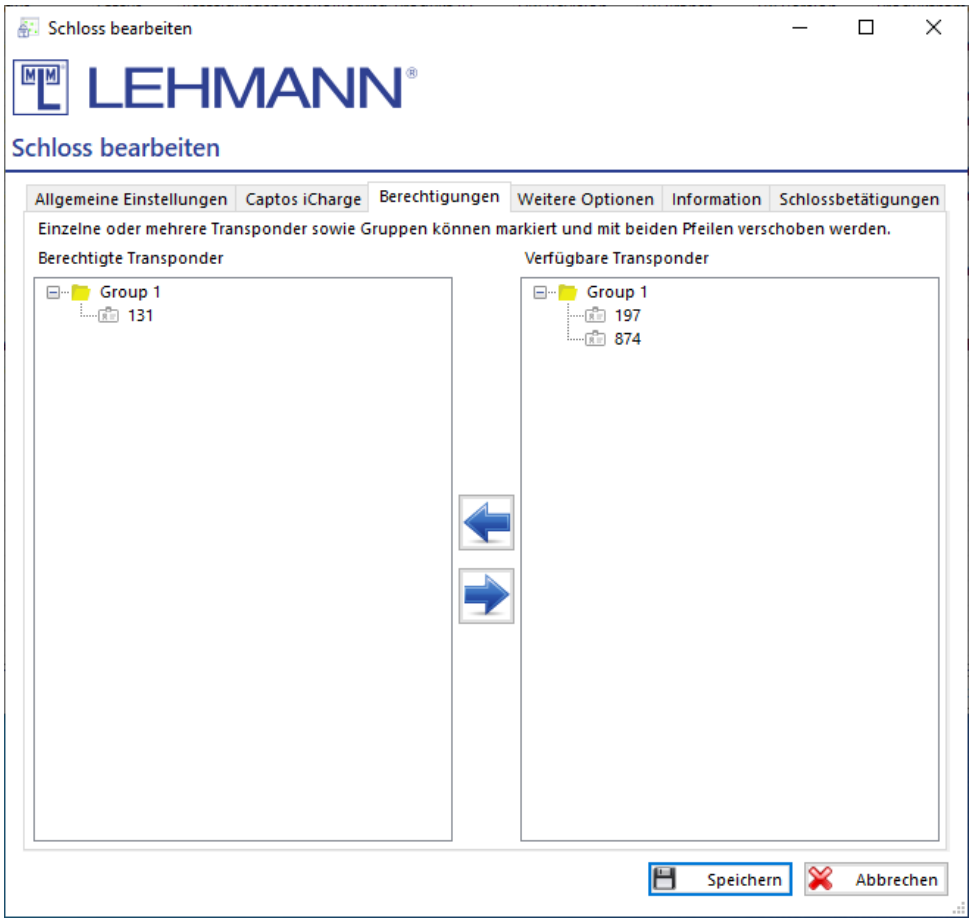


Figure: Edit lock – Permissions

- In the right table (Available transponders) you will find all the transponders that are already available in the project and that have no permission at this lock. Furthermore, the groups in which the transponders are located are displayed here.
- In the left table (Authorised transponders) are the transponders that have a permission for this lock. Furthermore, the groups in which the transponders are located are displayed here.
- Select and mark any number of transponders and drag the transponders from one side to the other in order to edit permissions. Before the data transfer is done,

changes in permissions are marked in this view with a blue dot (new authorization) or with a red cross (authorization revoked).

- You can also move entire groups including all transponders.
- Click on “Save”.
- The data is automatically sent to the respective lock.
- In exceptional cases, there is also a need for programming in online mode (see point 3.5).

3.11.4 Reset lock, delete lock, remote openings, firmware updates and further funtions

- Click on “Locks” in the main menu.
- In the overview of locks, select the required lock(s) and click on “Edit”.
- In the tab “More options” the following settings can be made:

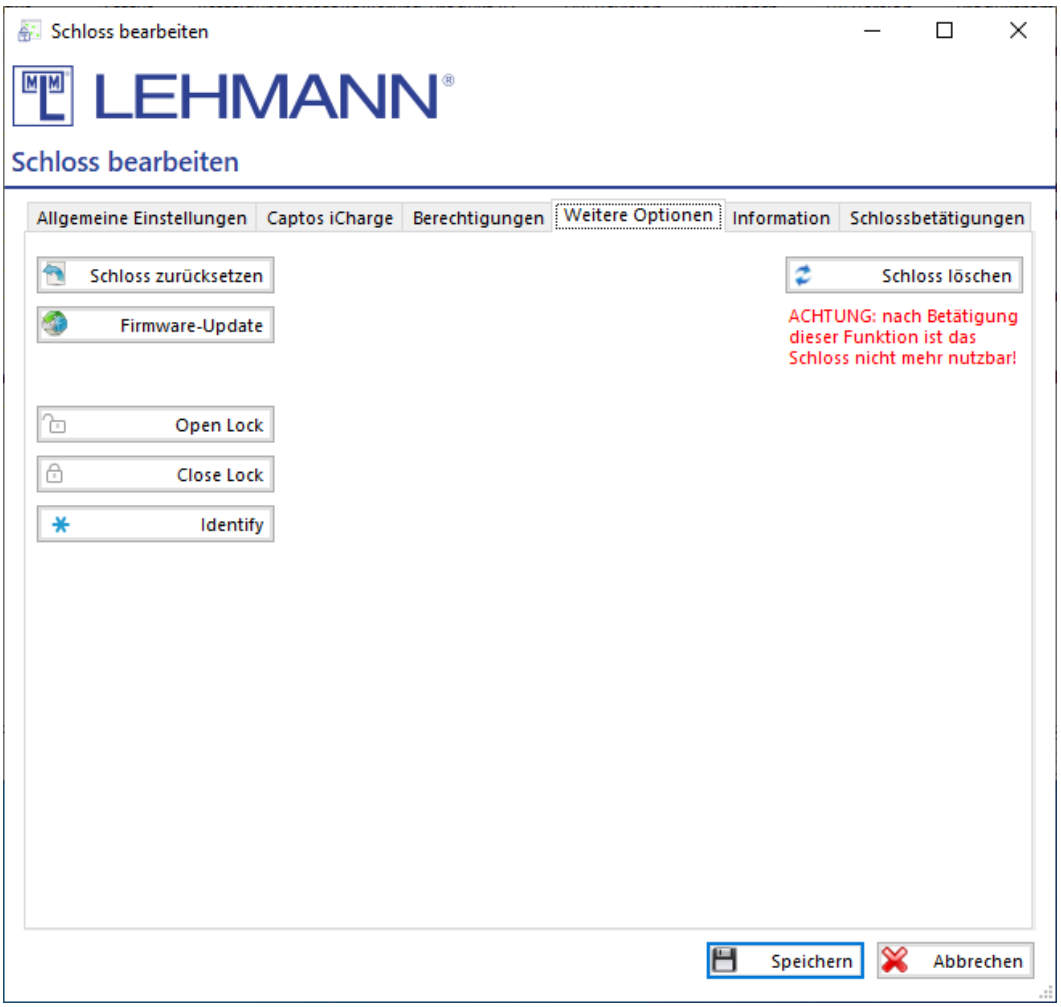


Figure: Edit lock – More options

- Reset lock: The lock will be set to the factory settings. Confirm the reset in the pop-up window.
  - Click on „Save“.

- The lock is reset via the network. After a successful reset, it appears like a new lock and is marked with a blue star under the menu item “Network” and "Controller".
- If the lock cannot be reached online, it can also be reset offline (see point 2.9.4).

- Delete lock: The lock can be deleted from the software e.g. in the event of a defect without further programming possibilities. Confirm the operation after clicking “Delete lock” in the dialog box. **IMPORTANT: The lock cannot be used any more after this process.**
- Firmware update: The lock is put into the mode for firmware updates. The firmware update is transferred over the network to the lock. After a successful update, it appears under "Locks" and has the new firmware revision in the column FW version.
- Open Lock: Clicking “Open Lock” will remotely open the respective lock, if it is online.
- Close Lock: Clicking “Close Lock” will remotely lock the respective lock, if it is online.
- Identifier: In order to check which lock is currently being processed in the LMS, you can click on "Identifier". If the lock is online, the lock's status LED flashes white for approx. 20 seconds and the lock gives an acoustic signal during this time.

ATTENTION: If a programming requirement for the lock continues to be listed under Data transfer after resetting a lock, the lock must be marked under “Lock archive” and then deleted with the button “Delete lock data” (see 4.2.2).

3.11.5 Activity logging (only with admin rights)

- This function must be activated for all relevant locks (see 2.9.2).
- The lock saves the last 640 activities. The oldest entry is overwritten in the lock when new events are added. Administrators can decide how long the collected data will be stored in the LMS.
- The data is transmitted online from the locks to the LMS.
- Click on “Locks” in the main menu.
- In the overview of locks, select the required lock and click on “Edit”. The activity logs are only displayed for one lock. It is not possible to display the activity logs of several locks at the same time.
- The following operations can be done in the tab “Lock activities”:

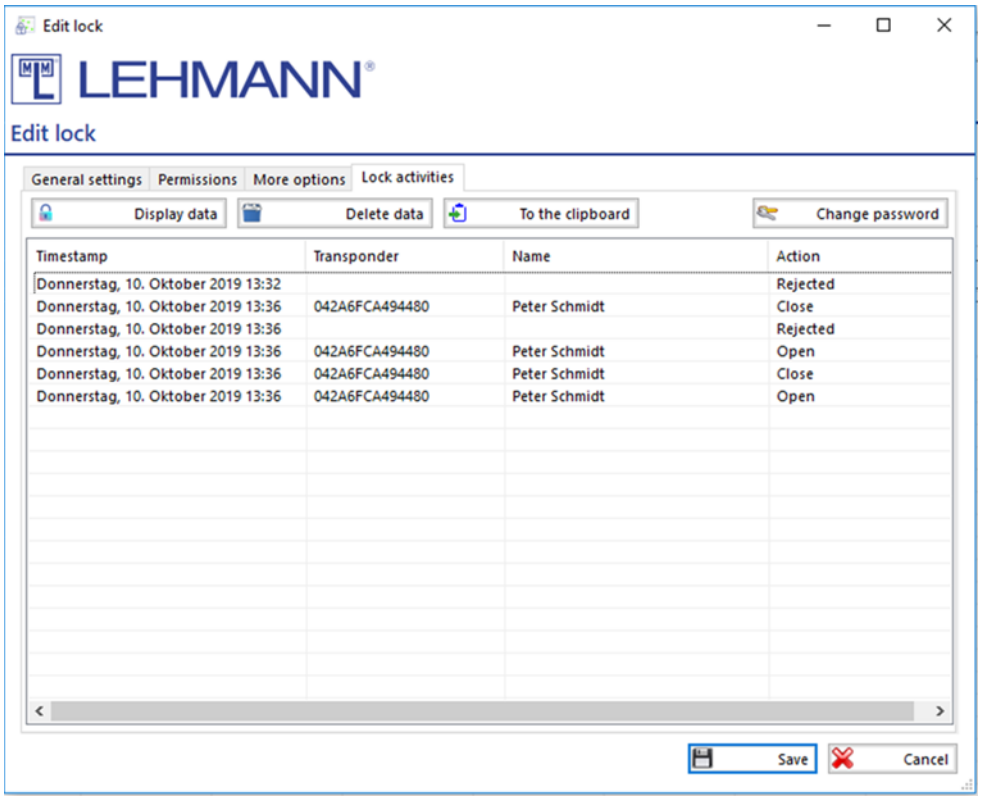


Figure: Edit lock – Lock activities

- Display data: If data is available, this button can be selected. If the 2-factor-authentication has been activated, enter your password and click on “Save”. Available data will be displayed.
- Delete data: The available data will be deleted.
- To the clipboard: The data is copied to the clipboard so that you can paste this data into other file formats such as Excel.
- Change password: If the 2-factor-authentication has been activated, you can change the password here. For security purpose, all previous activity logs are deleted when changing the password.

3.12 Creation of RFID systems in online operation with a virtual locking plan

The LMS offers the possibility to prepare lock profiles in the software without having an existing real lock, and to transfer the configuration to the real lock at a later point in time. These virtual locks are marked with a blue star as long as they are virtual. These locks can then be assigned to real locks. Configuration settings and permissions can be assigned to a virtual lock. This procedure can significantly accelerate the commissioning of complex locking systems. It is also possible to create virtual locks from a data import.

To create a virtual lock, proceed as follows:

- Click on "Locks" in the main menu.
- Click on "New". The "Edit lock" configuration window opens.
- You can now create a virtual lock. Enter at least the name for the virtual lock and add further information if necessary. Permissions can be assigned to the virtual lock in the "Permissions" tab.

- Click on "Save" to confirm the entries and create the virtual lock.
- The virtual lock appears in the lock list with a blue star in front of the name.
- You can now also assign authorizations for the virtual lock in the matrix.
- You can create any number of virtual locks in the same way.

In order to transfer the virtual lock profiles to real locks, the real locks must be connected to controllers that have already been programmed and a network connection must be available between the locks and the LMS. Then do the following:

- Open the app LEHMANN Data Transfer app on your smartphone.
- Click on "Data transfer" in the main menu.
  ATTENTION: The virtual locks are not displayed as programming requirements under "Data transfer".
- Place the smartphone on the USB desktop reader and wait until the green tick appears and the data transfer is completed. The data from the virtual locks is transferred to the app LEHMANN Data Transfer.
- Go to the first lock for which you have created a virtual lock profile. Hold the smartphone in front of the lock.
- An input field appears in which you can enter the name of lock. Below you find a list with the names of the virtual locks that were created in the LMS.
- Select the appropriate name.
- Then hold the smartphone in front of the lock again. The selected name including the lock profile is transferred to the lock. The lock reports back to the LMS via the network. The lock replaces the preconfigured virtual lock.
- The virtual lock profiles are now assigned to the real locks and all settings are adopted accordingly. The locks no longer appear with a blue star in front of the name.
- Click on "Controller" in the main menu.
- Here you find the new locks under the respective controller, which are marked with a blue dot.
- If you do not want to make any more changes to the lock configurations, mark the locks, click on "Edit" and then on "Save".
- The locks are now ready to use and visible in the matrix.

4 CHAPTER 4: General system and user settings

4.1 LMS users

4.1.1 Hierarchy levels for users of the LEHMANN Management Software

There is a distinction between the following authorization levels in the LMS software:

Admin:

- Change settings in the LMS software
- Activation of activity logging at RFID systems
- Display of lock activities
- Add, edit and delete projects
- Add, edit and delete LMS users
- Add and manage licence keys
- Add, edit and delete transponders
- Add, edit and delte RFID systems
- Authorization management in matrix

Manager (for single projects):

- Add, edit and delete transponders
- Add, edit and delete RFID systems
- Authorization management in matrix
- Limited settings in the LMS software

Editor (for single projects):

- Authorization management in matrix

Viewer (for single projects):

- Looking into the software is possible. There are no further permissions within the software.

4.1.2 Add new LMS users

Note: Only LMS users with admin rights are able to see an overview of all LMS users. To create new users, a sufficient number of licences must be activated (see 4.3).

- Click on “LMS users” in the main menu.
- Click on ”New“.
- Assign a name and the password for the new LMS user.
- Repeat the password.
- Click the button ”+“.
- Select the project in the drop-down list, for which the new LMS user should be authorized.

- Select the authorization level in the drop-down list for the new LMS user in this project.
- Click on “Save”.
- Click on “Save” in the remaining popup window.

4.1.3 Edit permissions for LMS users

- Click on “LMS users” in the main menu.
- Select the LMS user in the overview, for which authorization changes should be made and click on “Edit”.
- Make the changes (e.g. username, password) directly in the window “Edit LMS user”.
- If the permission hierarchy is to be changed for the LMS user, select the project and click on the button  .
- Change the permission hierarchy in the drop-down list and click on “Save”.
- Click on “Save” in the window “Edit User”.

4.1.4 Delete permissions for LMS users

- Click on “LMS users” in the main menu.
- Select the LMS user in the overview, for which authorization changes should be made and click on “Edit”.
- Select the project for which the authorization should be deleted and click on the button  .
- Confirm that you want to delete the authorization.
- The original authorization is no longer displayed in the window “Edit user”.
- Click on “Save”.

4.1.5 Change password for LMS users

- Click on “LMS users“ in the main menu.
- Click on ”Change password“.
- Enter the current password.
- Enter a new password.
- Repeat the new password.
- Click on ”Save“.

4.2 Projects and Project settings (only with admin permissions)

Several projects can be managed in the LMS software. A project corresponds to a matrix with the RFID systems, transponders and authorisations. Depending on the storage space on the transponders, transponders can be used in up to 5 projects. Different LMS users with different authorizations can be assigned to projects. A change between the projects is possible with the appropriate authorizations.

IMPORTANT: A RFID system can only be used in one project.

4.2.1 Add a project

- Click on “Project” in the main menu.
- Click on ”New“.
- You have the option of adjusting the deletion intervals for the project (see 4.2.2).
- Enter a name for the new project and click “Save”.

4.2.2 Delete intervals

The LMS software stores certain data about the RFID systems and the transponders. This also applies to deleted RFID systems and transponders. This information is stored in the transponder archive or lock archive. You can find the archives by clicking on "Transponders" or “Locks” in the main menu. Click on “Transponder archive” or “Lock archive” in the upper right corner.

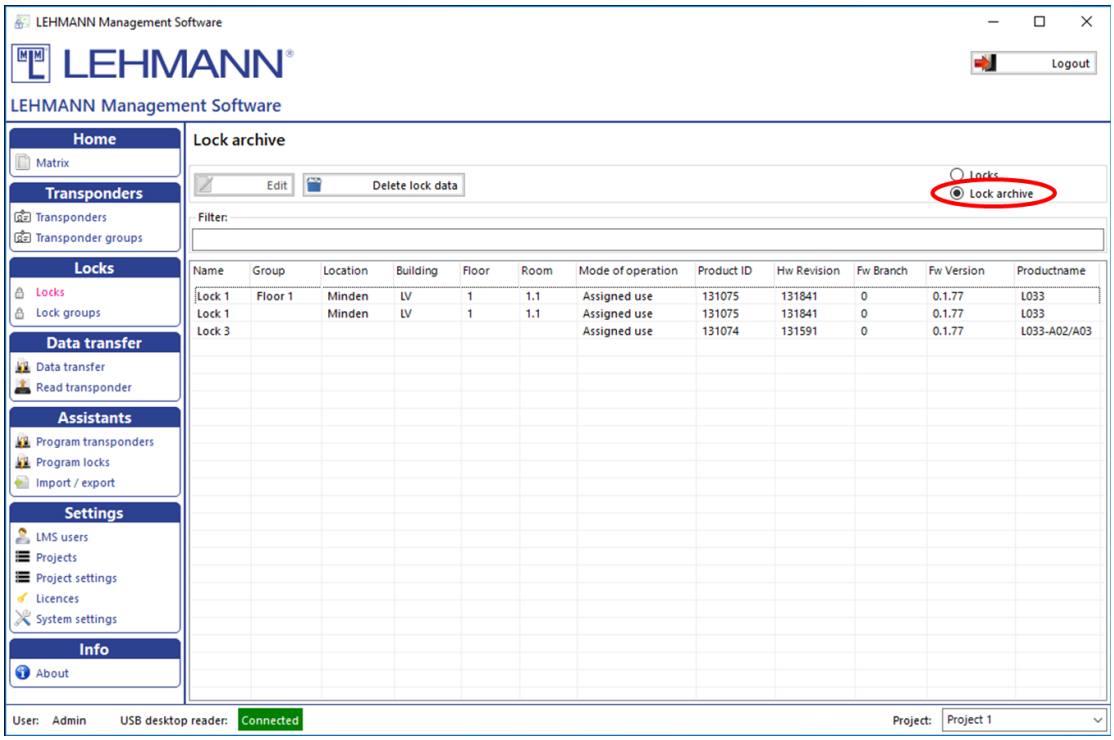


Figure: Lock archive

By default, the delete interval is set to 14 days. After 14 days, all data in the lock archive and transponder archive are deleted except the UID.

To change the deletion interval of project archiving, proceed as follows:

- Click on “Project settings” in the main menu.
- Select the project for which the deletion interval is to be set.
- Click on “Edit”.
- Select the tab “Delete intervals”.
- Change the value after “Delete project archiving after X days”.
- Click on ”Save“.

Furthermore, the operations at the RFID systems can be logged in the LMS software. This function is always deactivated (see 2.9.2 (offline) and 3.9.2(online)). After activating this feature, the data is stored for 14 days in the software.

To change the deletion interval of the log files, proceed as follows:

- Click on “Project settings“ in the main menu.
- Select the project for which the deletion interval is to be set.
- Click on “Edit”.
- Select the tab “Delete intervals”.
- Change the value after “Delete lock operations after X days”.
- Click on ”Save“.

4.2.3 Transponder types

The transponder types used in a project must be registered in the LMS software. This already takes place during the set-up of the project, but can also be entered manually at a later point of time.

Register transponder types manually (only with admin permissions):

- Click on “Project settings“ in the main menu.
- Click on the tab “Transponder types“.
- Click on ”New“.
- Place the transponder on the USB desktop reader and click on “Detect transponder type”.
- The field “Transponder type” is filled automatically.
- Click on “Save”.

If you use existing transponders from third party providers, which are secured with a master password, then you must enter this master password in the transponder type so that the transponders can be used with the LMS software. In this case, you will get the master password from the provider of your transponders (for example from the manufacturer / operator of your access control system).

4.2.4 Switching between projects

In order to switch quickly between projects, select the project in the drop-down list called “Project” in the lower right corner. Prerequisite for switching projects are the corresponding authorizations for the required project (see 2.10).

4.2.5 Change project name

- Click on “Projects” in the main menu.
- Select the project and click on “Edit”.
- Change the name of the project and click on “Save”.

4.2.6 Delete projects

Projects can only be deleted if transponders and locks have been removed beforehand.

- Click on “Projects” in the main menu.
- Select the project that should be deleted and click on “Delete”.
- Confirm that the project should be deleted.

4.3 Licence keys

Licence keys for certain software modules are managed in the main menu under “Licences”. A licence extension is necessary, e.g. for additional LMS users. For the verification of the licence key an internet connection is necessary.

- Click on “Licences” in the main menu.
- Click on “New”.
- Place the card with the licence key on the USB desktop reader and click on “Read card with licence key”. Alternatively, you can enter the license key on the keyboard.
- Click on “Save”.

4.4 System settings

Click on “System settings” in the main menu to change one of the following settings. Please note that for some settings admin rights are required:

4.4.1 Change language

- Click on the tab “Language” and select your preferred language.
- Click on “Save”.

4.4.2 Proxy settings

If you run LMS in a corporate network that uses a proxy, you must specify the proxy so that the LMS software can connect to the Internet. The licence key for the software LMS cannot be verified without a valid internet connection.

Attention: Incorrect settings can mean that it is no longer possible to log on to the LMS. Settings should be made when installing the LMS. Changes to the proxy settings should only be made if there are changes to the network structure and by an experienced system administrator.

4.4.3 User Interface / Manage backup alerts

In the tab "User Interface" under the “System settings” in the main menu, you can deactivate and reactivate the warning about outdated backup copies.

Attention: A loss of the LMS database means that the locks contained in the database are no longer accessible and therefore no configuration or authorization changes can be made. The locks become unusable! It is therefore strongly recommended to create a current backup and to keep it safe at the latest after programming new locks. It is therefore also recommended to leave the Back-up warning activated.

4.5 Import & Export (backup)

Attention:
Deleting the LMS database will result in an unusable RFID reader unless the RFID system is reset to factory defaults before the database is deleted. Regular backups are strongly recommended. The software shows you a warning every two weeks if no backup copy has been made after configuration or authorization changes. This warning also appears each time the software is restarted if a backup copy has not been made after creating a new lock. This function can be deactivated in the warning window. To reactivate the warning see point 4.4.3.

You can import or export data as well as the entire database.

- Click on “Import / export” in the main menu.
- The software will guide you through the next steps.

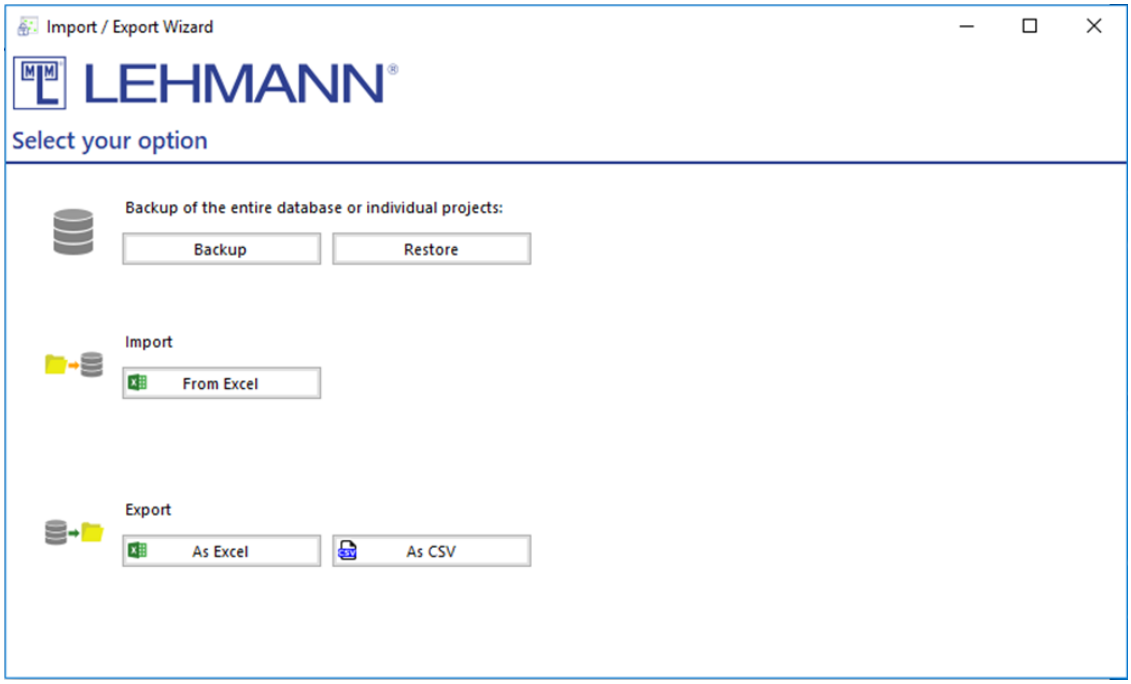


Figure: Import / export

4.5.1 Backup of the entire database or of individual projects

Here you can create or restore a complete backup of the entire database or individual projects.
To create a backup of a database or individual projects, proceed as follows:

- Click on “Import / export” in the main menu.
- Click on “Backup”.
- Select the projects for which you want to create a backup. To save the entire database, select all projects.
- Select an export path where to save the backup file. Click on “Select file”. Enter a file name for the backup file and click “Save”.
- If required, enter a password to protect the backup file.
- Click on “Export“.

To restore a database or individual projects, proceed as follows:

- Click on “Import / export” in the main menu.
- Click on “Restore”.
- To select the file that should be imported, click “Select File”.
- If the backup file is protected with a password, enter the password.
- Select one or more projects to be imported and click on “Import”.

ATTENTION: If more LMS users have been created in the imported project than you have activated in your current LMS software, an error message appears. Permissions for the LMS users on the imported project may need to be reassigned (see 4.1 and 4.3).

4.5.2 Import (from Excel)

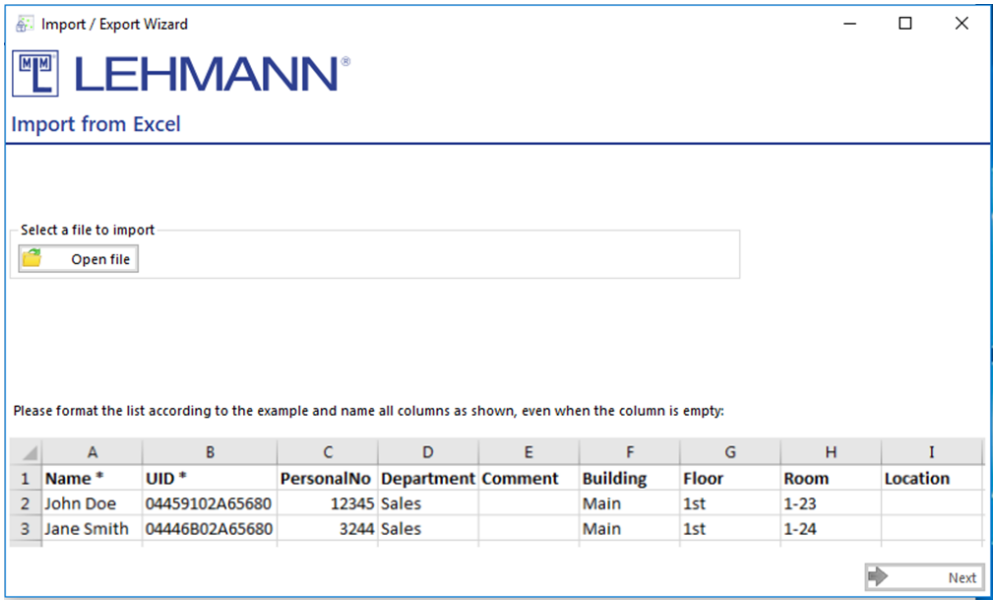
Here you can import data from Excel, e.g. for adding new transponders. This is not possible for restoring back-up files. Click “Yes” if you have a list with UIDs from existing transponders that should be used in LMS. In this case, the transponders do not have to be placed on the USB desktop reader when the transponder is added to LMS. Only for later usage, the transponder must be placed once on a USB desktop reader to write the necessary LMS application data on the transponder.

If no UIDs of transponders are contained in the Excel file, click on “No”. In this case, you must place the transponders individually on the USB desktop reader when they are added to LMS. You need a corresponding number of compatible transponders.

Import a list **with UIDs** of transponders to be useed:

- Click on “Import / export” in the main menu.
- Click on “From Excel”.
- Click on “Yes“ and then on “Import“.
- Click on “Open file“ to select an Excel file.

ATTENTION: The column headings in the list to be imported must all be the same as in the following figure:



	A	B	C	D	E	F	G	H	I
1	Name *	UID *	PersonalNo	Department	Comment	Building	Floor	Room	Location
2	John Doe	04459102A65680	12345	Sales		Main	1st	1-23	
3	Jane Smith	04446B02A65680	3244	Sales		Main	1st	1-24	

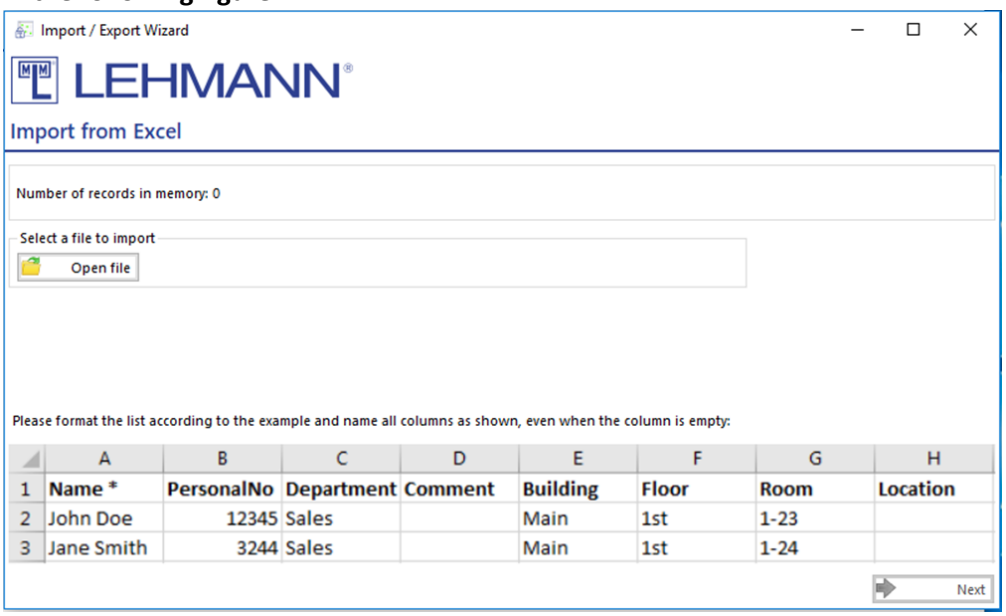
Figure: Required column headers when importing a list with UID

- The compatible data is automatically imported into the project.
- You will find all imported data in the matrix or in the main menu under “Transponders“. Before the transponders can be used, they must be placed once on the USB desktop reader in order to save LMS application data on the transponder.

Import a list **without UIDs** from transponders:

- Click on “Import / export” in the main menu.
- Click on “From Excel”.
- Click on “No”, then click on “Import”.
- Click on “Open file” to select an Excel file.

ATTENTION: The column headings in the list to be imported must all be the same as in the following figure:



	A	B	C	D	E	F	G	H
1	Name *	PersonalNo	Department	Comment	Building	Floor	Room	Location
2	John Doe	12345	Sales		Main	1st	1-23	
3	Jane Smith	3244	Sales		Main	1st	1-24	

Figure: Required column headers when importing a list without UID

- The number of found records is displayed. Click on “Continue”. If you still have data in the memory, you can also click on “Next” without reading in a file.
- You will see the available names from the Excel list.
- Place a transponder on the USB desktop reader and select a name by double-clicking it from the list. The programming process of the transponder starts automatically.
- Repeat this process until you have programmed all transponders and the list is empty.

4.5.3 Export

For data export, the formats Excel and CSV are available. A data export does not replace a backup and is not intended to create a backup. During an export process, you can export LMS users, transponders and locks of the current project.

- Click on “Import / export” in the main menu.
- Click on “As Excel” or “As CSV”.
- First select the data to be exported.
- Click on “Select File” to set the export path and select a file name. Click on “Save”.
- Click on “Export”.

ATTENTION: Deleting the LMS database will result in an unusable RFID reader unless the lock is reset to factory settings before the database is deleted. For this reason, backup copies are strongly recommended.

4.6 LEGIC specific functions and information in LMS

When using LEHMANN LEGIC RFID systems in LMS, there are special configuration steps as well as functions and information available. This mainly involves additional steps in the process of creating a new project, configuring the USB desktop reader for the first time and programming the RFID systems. The basic processes in the authorization management, in the configuration during operation, and all other processes (e.g. replacement of lost transponders) remain unchanged and can be found in the individual sections of this manual.

4.6.1 Select LEGIC as the RFID technology in the project

If you are using LEHMANN LEGIC RFID systems in the LMS project, you must first make a change in the project settings regarding the supported RFID technology. To do this, proceed as follows:

- Click on "Project Settings" in the main menu.
- Activate the "LEGIC advant" type in the "General Settings" tab.
- Click on "Save".

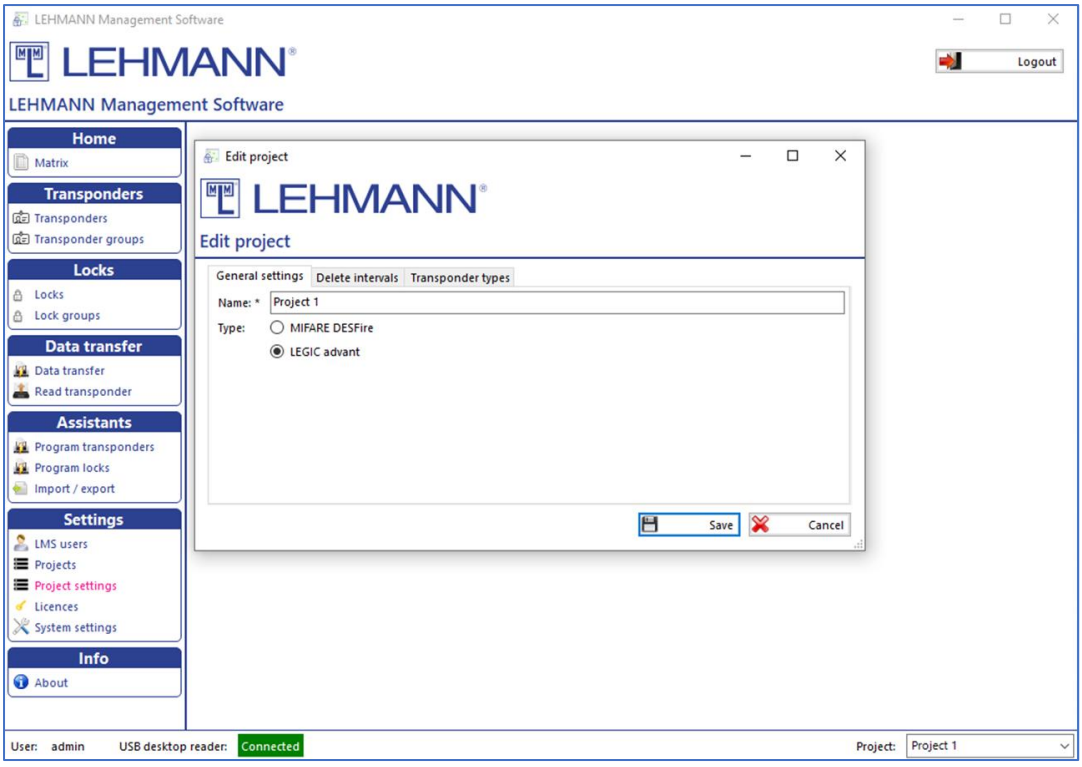


Figure: Selection of RFID technology per project

Only one RFID technology is supported within a project. Please note the supported transponder types (see point 1.2.2). It is possible to use LEHMANN MIFARE® RFID systems in the first project and LEHMANN LEGIC RFID systems in other projects.

4.6.2 Launch USB desktop reader with LEGIC SAM

After activating LEGIC advant under the project settings, the additional item "LEGIC" appears in the main menu. Before LEHMANN LEGIC RFID systems or the corresponding transponders can be programmed, the USB desktop reader must first be launched with a LEGIC SAM. To do this, proceed as follows:

- Click on "Launch data wizard" in the main menu under “LEGIC”.
- Place your LEGIC SAM transponder on the USB desktop reader and leave it there until the data has been transferred.

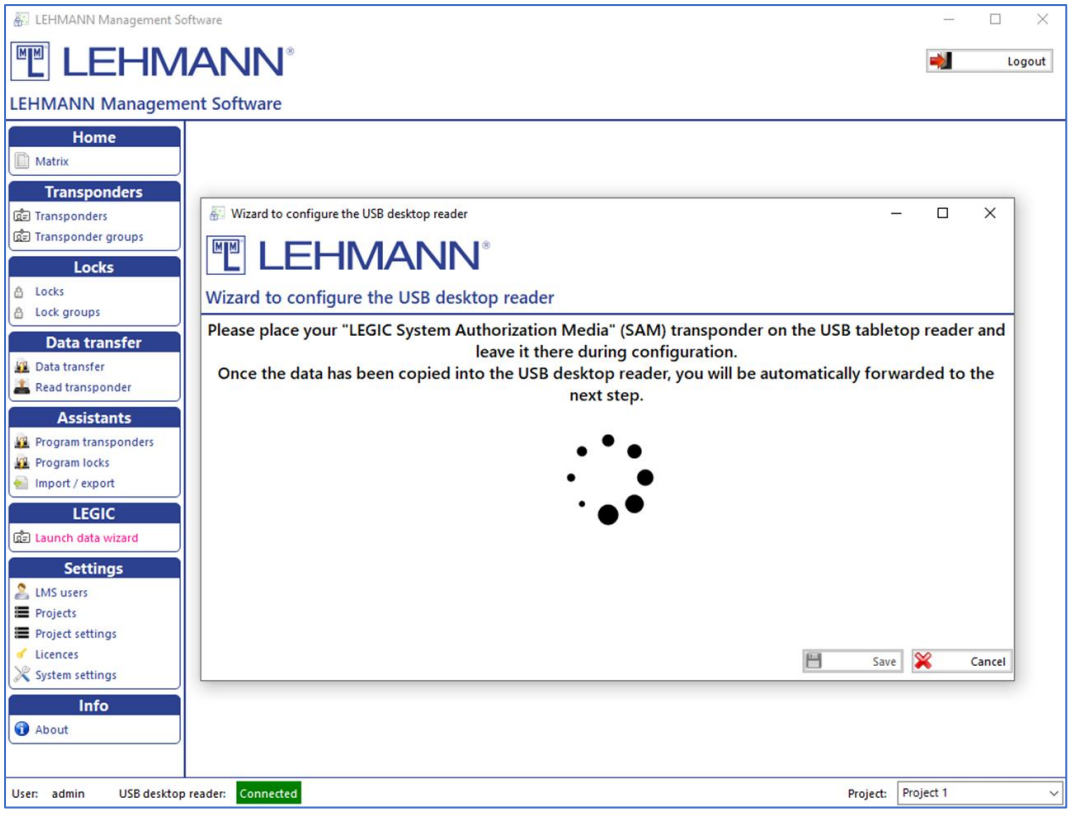


Figure: Configuration of the USB desktop reader with LEGIC SAM (1)

- Optionally, you can give the LEGIC SAM Stamp a name (e.g. location of the locks or project name). This name is displayed under "Project Settings" in the "Transponder Types" tab and in the main menu under "Transponder" in the respective transponder settings.

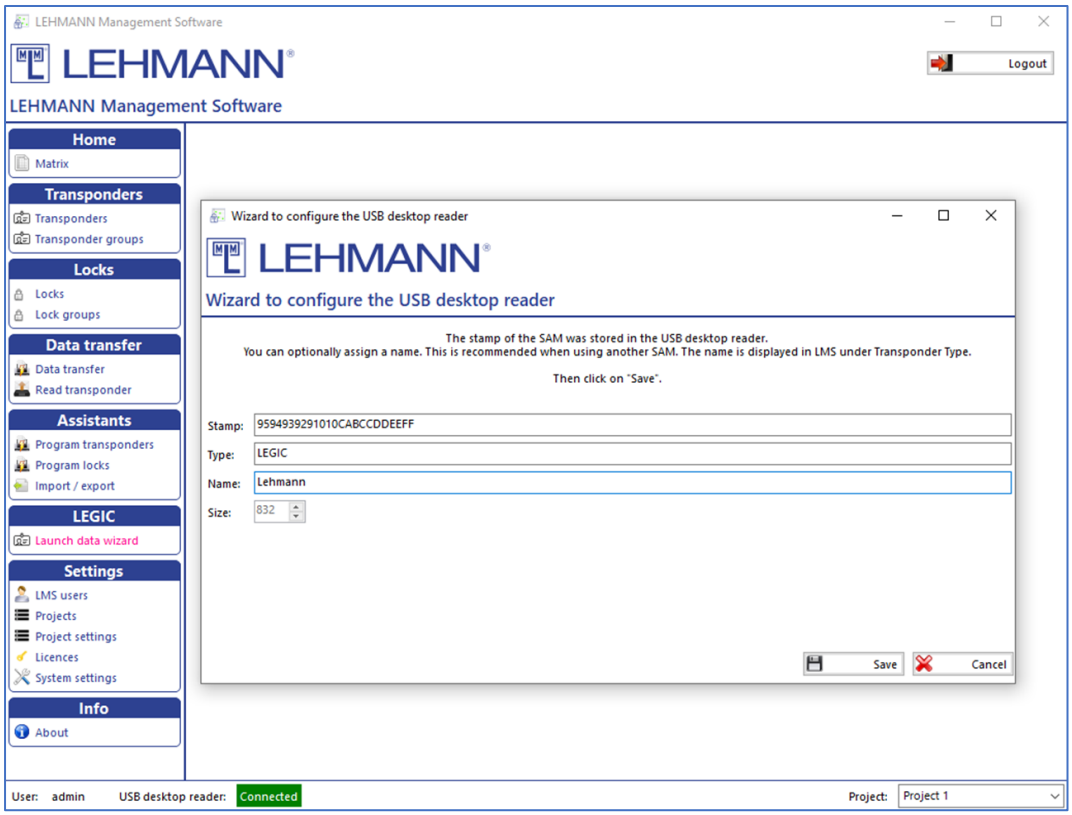


Figure: Configuration of the USB desktop reader with LEGIC SAM (2)

- Click on "Save".
- Several LEGIC SAMs can also be transferred to a USB desktop reader. To do this, repeat the process.
- You can now program LEGIC transponders and assign authorisations. To do this, follow the instructions in points 2.3.2 and 2.8.

In the event that a LEGIC SAM is to be deleted from the USB desktop reader, proceed as follows:

- Click on „Launch data wizard” in the main menu.
- Place the appropriate LEGIC SAM64 transponder on the USB desktop reader and leave it there until the data in the USB desktop reader has been deleted.

In order to check whether the USB desktop reader has been configured with a LEGIC SAM, proceed as follows:

- Click on “System settings“ in the main menu.
- Click on the tab „USB desktop reader” in the window “Edit settings”.
- In the table "Activated LEGIC SAMs on the USB desktop reader" you can see with which SAM the USB desktop reader was configured.

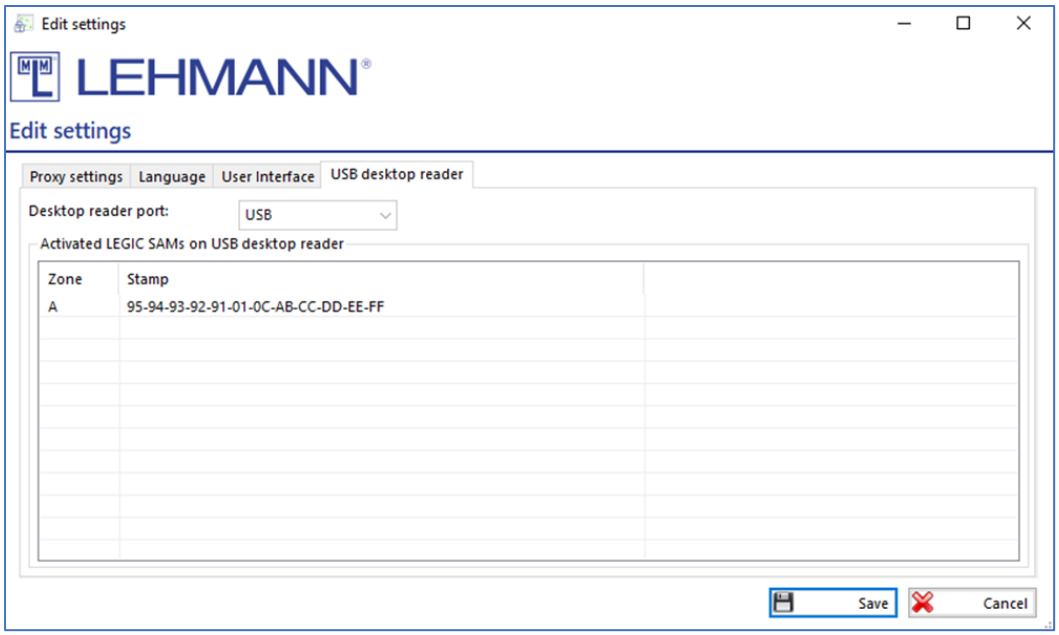


Figure: Configured LEGIC SAMs on the USB desktop reader

4.6.3 Program LEGIC RFID systems (transfer of LEGIC SAM63)

If LEGIC RFID systems should be used in LMS, the RFID systems must be configured with your LEGIC SAM63 before the locks can be programmed in LMS.

Launch of RFID systems with LEGIC SAM before programming them in LMS:

- The RFID systems must be in factory delivery mode.
- Hold the LEGIC SAM63 in front of the RFID reader for approx. 2 seconds until you hear an acoustic signal and a green flash on the LED of the RFID reader. If the RFID reader has already been launched with a SAM, the LED flashes twice red and twice green with simultaneous acoustic signals.
- The RFID system can now be programmed into the LMS software. To do this, follow the instructions in points 2.3.1 or 2.9.1.

Launch of RFID systems with LEGIC SAM after programming them in LMS (e.g. if the LEGIC stamp should be changed):

- Follow the instructions in points 2.3.1 or 2.9.1 to program the RFID systems.
- After programming the RFID systems, the LEGIC SAM63 must be transferred to the RFID systems. As long as this has not taken place, all transponders are rejected by the RFID systems. The missing SAM transmission is shown with a warning symbol in the matrix and in the lock settings. Furthermore, in the overview of all locks (click on "Locks" in the main menu), a "0" is shown in the "Stamps" column because no SAM has been transferred yet.

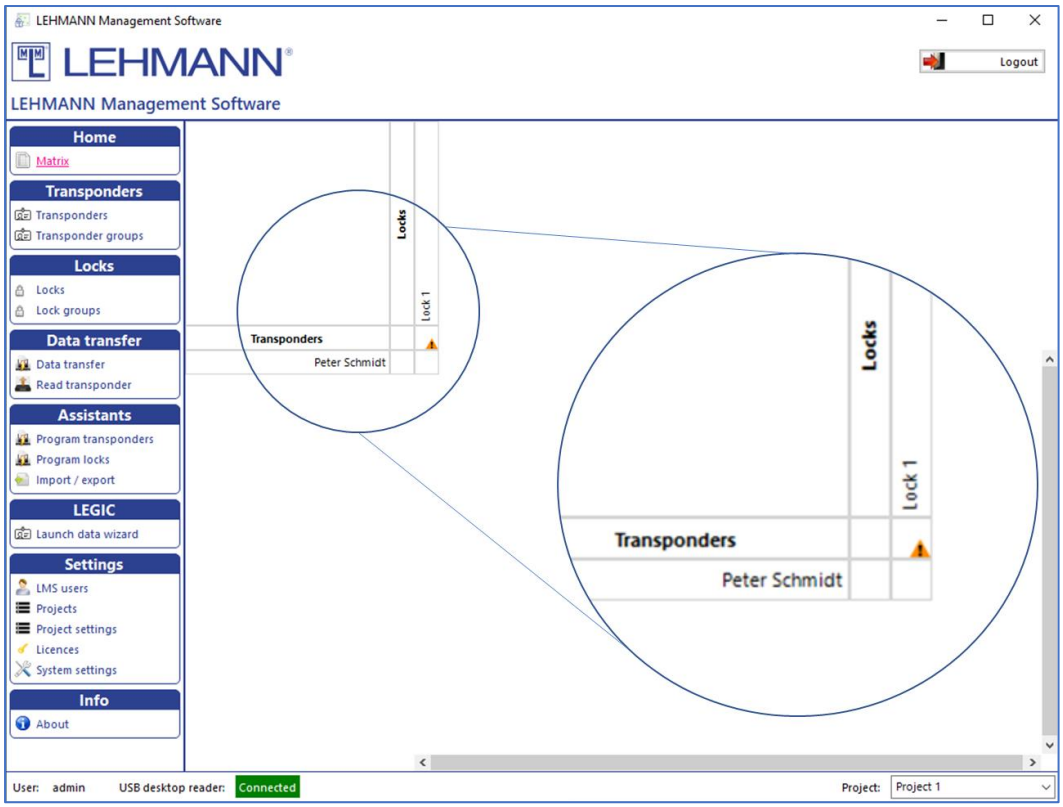


Figure: Warning symbol if LEGIC SAM is not transmitted to the RFID system

- Click on “Locks“ in the main menu.
- Select the required locks in the overview of all locks click on "Edit".
- Click on the button „LEGIC launch” in the tab “More options” and then on “OK”.
- Click on "Data transfer“ in the main menu.
- Place the smartphone with the opened app LEHMANN Data Transfer on the USB desktop reader.
- Hold the smartphone with the opened app LEHMANN Data Transfer in front of the RFID reader of the corresponding lock. The lock is placed in a mode for 5 minutes in which the LEGIC SAM63 can be transferred.
- Hold the LEGIC SAM63 in front of the RFID reader for approx. 2 seconds until you hear an acoustic signal and a green flash.
- **Hold the smartphone with the opened app LEHMANN Data Transfer in front of the RFID reader of the corresponding lock** (contrary to the instructions on the display).
- Place the smartphone with the opened app LEHMANN Data Transfer on the USB desktop reader and transfer the data to the LMS software. To do this, you must be in the menu item "Data transfer".
- The RFID system now accepts authorized transponders.
- The warning symbol in the matrix has disappeared and in the overview of all locks (click on "Locks" in the main menu) there is now a "1" instead of "0" in the "Stamps" column.
- If the warning symbol and the "0" are still displayed in the overview, hold the smartphone with the opened app LEHMANN Data Transfer in front of the lock's RFID reader again. Then place the smartphone with the opened app on the USB desktop reader and transfer the data to the LMS software. To do this, you must be in the menu item "Data transfer". The warning symbol should have disappeared after the

data transfer. Otherwise, please repeat the entire process again and make sure that the data transfer of the LEGIC SAM63 to the RFID reader is confirmed correctly.

4.6.4 LEGIC RFID-Systeme zurücksetzen / LEGIC SAM löschen

If the RFID system is completely reset to the factory settings (see point 2.9.4), the information that was previously transferred by using the LEGIC SAM63 is also deleted. The RFID system is again in the factory settings mode.

It is possible to delete the previously transferred information from the LEGIC SAM transponder in the RFID system (reasons: e.g. wrong LEGIC SAM transmitted; locks should receive a new LEGIC-SAM). The LEGIC SAM64 is required for this.

The RFID system has not yet been programmed. The LEGIC SAM63 was transferred to the RFID reader in the factory settings mode:

- Hold the LEGIC SAM64 in front of the RFID reader for approx. 2 seconds until you hear three acoustic signals and you see three red flashes in the LED. If no LEGIC SAM63 has been transferred beforehand, the LED flashes twice red and twice green with simultaneous acoustic signals.
- A LEGIC SAM63 can now be transferred to the RFID reader. To do this, follow the instructions in point 4.6.3.

The RFID system is already programmed in the LMS software:

- Click on “Locks” in the main menu.
- Select one or more locks in the overview of all locks and click on "Edit".
- Click on the tab “More options“ and then on „LEGIC launch“ followed by “OK”.
- Click on “Data transfer“ in the main menu.
- Place the smartphone with the opened app LEHMANN Data Transfer on the USB desktop reader.
- Hold the smartphone with the opened app LEHMANN Data Transfer in front of the RFID reader of the corresponding lock. The lock is set for 5 minutes in a mode in which the relevant data on the RFID reader can be removed by using LEGIC SAM64.
- Hold the LEGIC SAM64 in front of the RFID reader at the lock for approx. 2 seconds until three acoustic signals and three red flashes are emitted.
- **Hold the smartphone with the opened app LEHMANN Data Transfer again in front of the RFID reader of the lock** (contrary to the instructions on the display).
- Place the smartphone with the opened app LEHMANN Data Transfer on the USB desktop reader and transfer the data to the LMS software. To do this, you must be in the menu item "Data transfer".
- The RFID system does not accept any transponder any longer.
- A warning symbol is displayed next to the lock name in the matrix. In the overview of all locks (click on "Locks" in the main menu) there is now a "0" instead of "1" in the "Stamps" column. If this is not the case, hold the smartphone with the opened app LEHMANN Data Transfer in front of the RFID reader of the lock. Then place the smartphone with the opened app on the USB desktop reader and transfer the data to the LMS software. To do this, you must be in the menu item "Data transfer".

- A LEGIC SAM63 can now be transferred to the RFID reader. To do this, follow the instructions in point 4.6.3.

4.7 Updating the LEHMANN Management Software

If the PC or laptop on which the LMS software is installed is connected to the Internet, you will automatically receive notification of updates. If you wish, you can check for updates manually:

- Click on “About” in the main menu.
- Click on “Search for updates”.

4.8 Time settings in the RFID systems

When the RFID systems are initialised by using the smartphone and the app LEHMANN Data Transfer, the time is transferred to the RFID systems. A correct time setting is necessary for time-depending functions, as opening and closing is otherwise not possible. Pay attention to the correct time zone in the settings of the RFID systems (see 2.9.2). The time is transmitted directly from the server for locks in online mode.

Attention when changing the batteries: Hold the smartphone with the open App LEHMANN Data Transfer in front of the RFID reader of the lock, where a battery change has been carried out in order to update the time. For RFID systems with time-dependent functions, a correct operation is otherwise not possible.

4.9 Data protection

The software is not operated on behalf of a customer by LEHMANN. Furthermore, LEHMANN does not manage or store any user data as part of the LMS software or the app. The customer is responsible for the usage and operation of the software. It is expressly mentioned that the buyer respective the user of the software is responsible for the legally compliant usage of the software and must comply with the country-specific laws. This applies in particular to the data protection requirements and participation rights of the users of the LMS software or the users of the RFID systems. Of course, in addition to the corresponding deletion functions of personal data, the software also offers further technical and organizational measures to enable the requirements of the General Data Protection Regulation (DSGVO) to be implemented. The software is installed by the customer within the customer’s IT infrastructure, which means that all data remains in the responsibility of the customer.

4.10 App LEHMANN Data Transfer

For Android and NFC-enabled smartphones, the LEHMANN Data Transfer app is available on Google PlayStore. With the app you can exchange data between the LEHMANN Management Software LMS and the LEHMANN RFID Systems. Note that the NFC functionality must be enabled and the LEHMANN Data Transfer app must be open.

Information about the operation of the app LEHMANN Data Transfer can be found in the menu of the app under the item “Help”.

A yellow arrow (left arrow direction) in the app means that a data transfer with the LEHMANN Management Software is necessary (see 2.5).

A green arrow (right arrow direction) in the app means that a data transfer at the RFID lock is necessary (see 2.5).
When transferring data to the RFID reader, hold the smartphone with the opened app in front of the RFID reader of the lock. Hold the smartphone in such a way that the NFC antenna of your smartphone is centered in front of the RFID reader. If necessary, check the operating instructions of your smartphone where the NFC antenna is located. The data exchange is indicated on the display by a symbol. Keep the smartphone in front of the RFID reader of the lock during the entire data transfer until you see a green check mark.

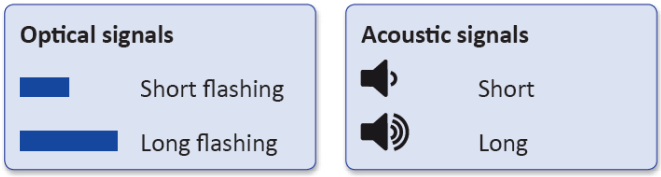
For the data transfer at the USB desktop reader, first click on “Data transfer” in the LEHMANN Management Software. Place the smartphone with the opened app on the USB desktop reader. Make sure that the NFC antenna of the smartphone is centered on the USB desktop reader. Leave the smartphone on the USB desktop reader during the entire data transfer. The data exchange is displayed on your smartphone as well as in the LEHMANN Management Software. If necessary, check the operating instructions of your smartphone where the NFC antenna is located.

If data is displayed in the app that cannot be processed, this data can be deleted in the app in the menu item “Delete all data”.

5 Chapter 5: Operations of the RFID systems

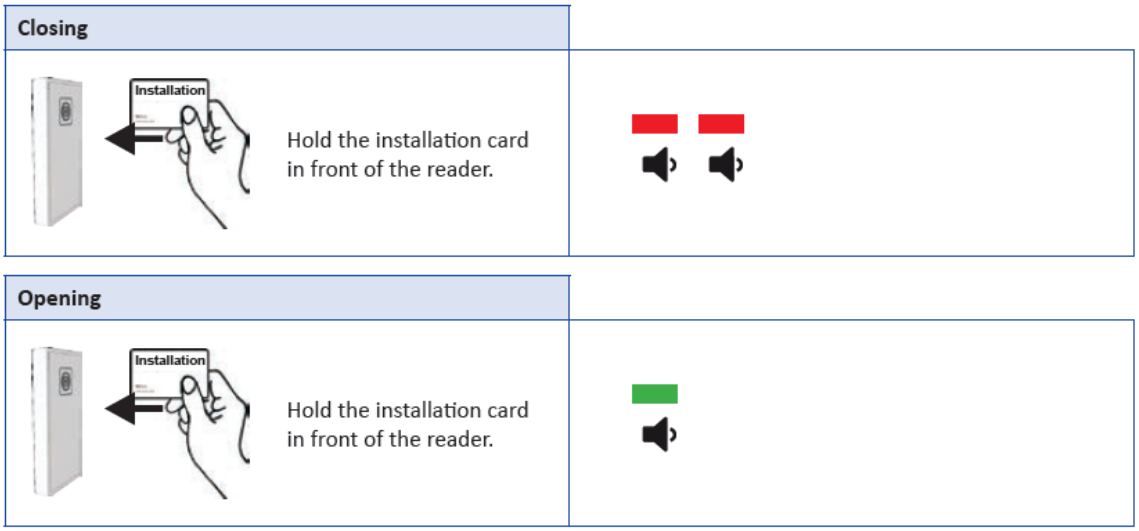
5.1 Acoustic and optical signals of the RFID systems

The RFID systems have acoustic and optical signals, which are differentiated as follows:



5.2 Use of Installation card

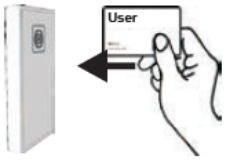
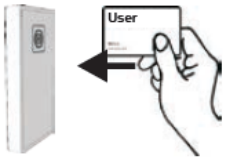
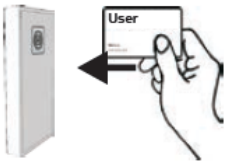
During installation, one or more installation cards can be used. The installation cards are ready for immediate use and do not have to be programmed. With the installation cards, the basic functions (opening and closing) can be carried out on the lock. The installation card cannot be used any longer on a lock once the RFID system has been initialized in the LMS software. After the lock has been reset to the factory settings, the installation card is valid again.



5.3 Programming transponders (user cards)

Information about adding transponders can be found in 2.3.2, 3.3.2, 2.8.1 and 3.8.1. Information about permissions can be found in 2.3, 2.6, 2.7, 2.9, 3.3, 3.6, 3.7 and 3.9.

5.4 Closing and opening

Closing	
 Hold the user card in front of the reader.	
Opening	
 Hold the user card in front of the reader.	
Rejection of an unauthorised user card	
 Unauthorised user card is held in front of the reader. The card is rejected.	

5.5 Emergency opening

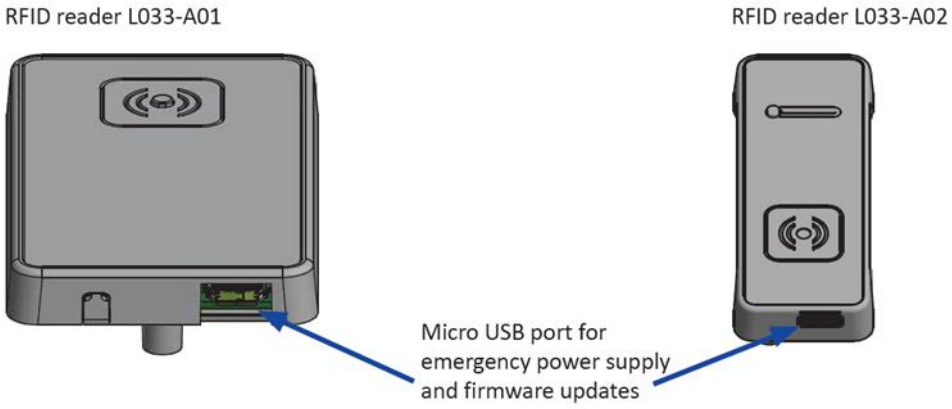
In order to carry out an emergency opening, assign the authorisation for the lock to be opened to a transponder that is already available in the project. Information about permissions can be found in 2.3, 2.6, 2.7, 2,9, 3.3, 3.6, 3.7 and 3.9.

5.6 Emergency power supply (only for battery operated locks)

If the batteries are completely discharged and you cannot reach the battery compartment inside the furniture, you still have the option of obtaining an emergency power supply if you have an external RFID reader. To do this, you can use a standard power bank (additional rechargeable battery) with a USB port complying with the USB 2.0 standard. A micro USB Type B connector is required for the emergency power supply of the RFID reader. Use the emergency power supply only for a short period of time for the one-off opening of a lock. Before use, it is essential that you should read the operating instructions of the power bank. Please proceed as follows:

- First remove the protective rubber cap on the micro USB port on the underside of the RFID reader.
- Connect the charged power bank to the RFID reader using the micro USB port.
- Please take account of the operating instructions of the power bank, e.g. for starting and ending the charging process.
- Please do not perform any further actions until the RFID reader gives an acoustic and a visual signal (see acoustic and visual signals when inserting the batteries).

- Then open the lock with an authorized transponder card.
- Then carefully disconnect the power bank from the RFID reader.
- Replace the protective rubber cap on the micro-USB port of the RFID reader.
- Replace the batteries in the lock (see operating instructions of the RFID system).
- Perform a function test (opening and closing) while the furniture is open.



Online locks are connected with a controller and get power supply via the controller. However, if this energy supply fails, for example due to a power failure or due to a defective power supply unit etc., then the locks can no longer be operated. This should be taken into account and, if necessary, an emergency power supply system can significantly increase reliability. The components used, such as power supplies and controllers, should be placed in such a way that they can be quickly replaced in the event of a defect.