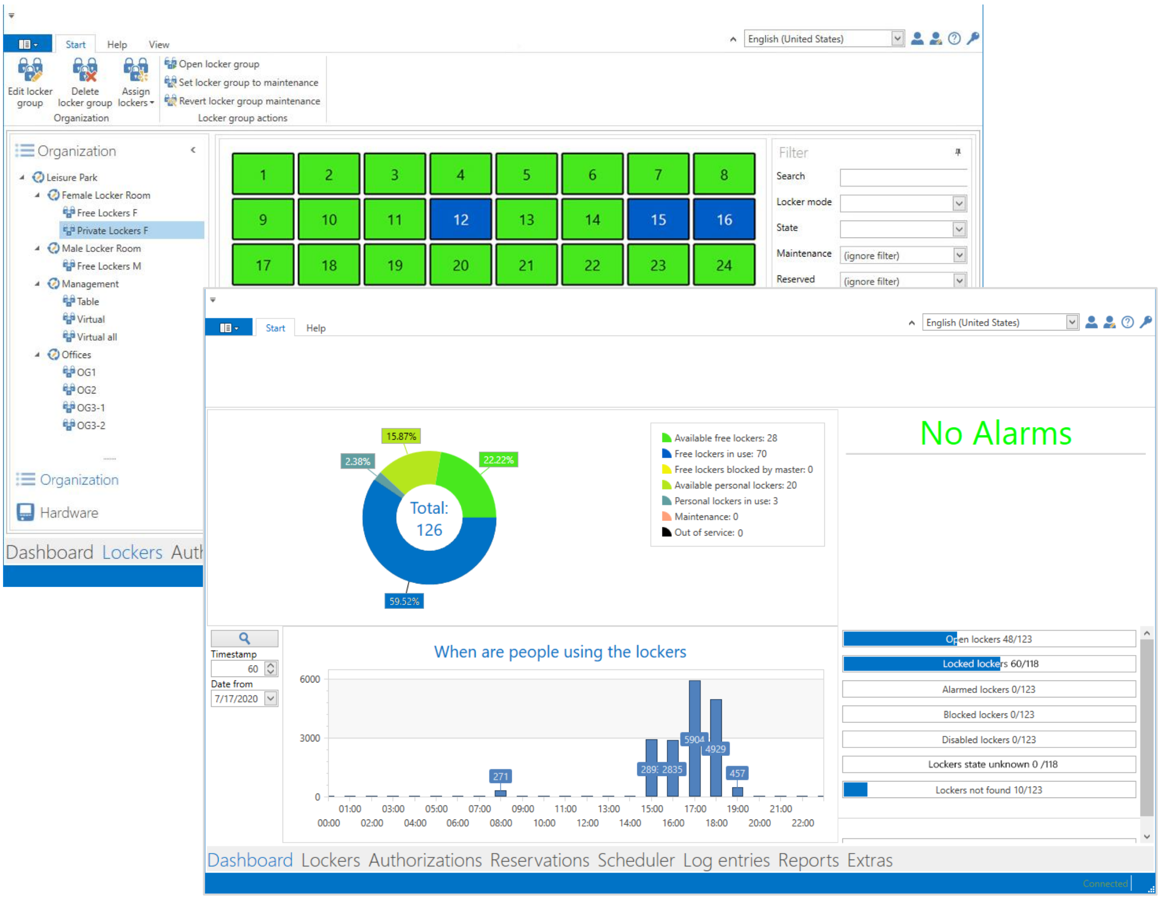
Relaxx 2020

Configuration Software for GANTNER Electronic Locking Systems



Operating Instructions
Document Version 5.2.0
Software Version 5.2.0

Liability

Any claims against the manufacturer based on the hardware or software products described in this manual shall depend exclusively on the conditions of the guarantee. Any further-reaching claims are excluded, and in particular the manufacturer accepts no liability for the completeness or accuracy of the contents of this manual. The right is reserved to make alterations, and alterations may be made at any time without prior notice being given.

Trademarks

Attention is drawn at this point to markings and registered trademarks used in this manual. All product and company names, which are mentioned in this manual, are only used for identification and explanation purposes. Some of these names may be trademarks or registered trademarks of the corresponding company.

Contact

The contact information for questions regarding Relaxx or for general enquiries is listed below:

Contact address of manufacturer

GANTNER Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria
www.gantner.com/locations

⚠ General Warning and Safety Instructions

Dear Customer,

We congratulate you on selecting a product (appliance or software) from GANTNER Electronic GmbH. Our aim is to ensure our product operates with safety and to your complete satisfaction. To achieve this aim, please take this opportunity to familiarize yourself with the following guidelines:

1. The installation, commissioning, operation, and maintenance of the product must be carried out in accordance with the technical conditions of operation as described in the corresponding product documentation.

2. Before installing, commissioning, operating, or maintaining the product, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.

3. If there are some points which are not entirely clear, please do not take a chance. All queries can be clarified by your GANTNER representative or by ringing the GANTNER support hotline.

4. Where not otherwise specifically documented, the appropriate installation, commissioning, operation and maintenance of the product is the customer’s responsibility.

5. Directly on receipt of the goods, inspect both the packaging and the product itself for any signs of damage. Also check that the delivery is complete and includes all accessories, documentation, auxiliary devices, etc.

6. If the packaging or product has been damaged in transport, or should you suspect that it may have a fault, the product must not be put into service. Contact your GANTNER representative who will resolve the problem as quickly as possible.

7. The installation, commissioning, and servicing of our products must be performed by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association (e.g., ÖVE [Austrian], VDE [Germany]).

8. Where not otherwise stated, installation and maintenance work on our products must be carried out when disconnected from the power supply. This applies in particular to appliances that are normally supplied by low-voltage current.

9. It is prohibited to alter the products or remove protective shields and covers.

10. Do not attempt to repair a product after a defect, failure, or damage is detected. In addition, do not put the product back into operation. In such cases, it is essential to contact your GANTNER representative or the GANTNER support hotline.

11. GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.

12. Although care is taken, and we are continuously aiming for improvement, we cannot completely exclude the possibility of errors appearing in our documentation. GANTNER Electronic GmbH therefore accepts no responsibility for the completeness or the accuracy of this manual. The right is reserved to make alterations at any time without prior notice.

13. Should you discover any fault with the product or in its accompanying documentation, or you have any suggestions for improvement, you may confidently inform your GANTNER representative or GANTNER Electronic GmbH directly.

14. We especially look forward to hearing from you if you just want to tell us that everything is functioning perfectly.

We wish you a successful experience with our product and look forward to welcoming you again as a customer soon.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 About this Manual

This manual describes the operation of Relaxx, i.e., how a GANTNER electronic locker system is installed and configured and how to operate Relaxx for daily work, e.g., how to monitor the lockers, perform reservations, grant authorizations, and establish schedules.

For instructions on installing and updating Relaxx, please also read the Relaxx Installation Manual and perform the described tasks.

Chapter "2 GENERAL SETTINGS" describes the general settings in Relaxx, valid throughout the software. This includes, e.g., the settings for communication, database, and alarm notifications, and also the general system-wide hardware settings. These settings usually only have to be defined once after installing Relaxx but can also be adjusted later if required.

In chapter "3 OPERATION”, the structure and operation of the Relaxx user interface is explained. It also explains the basic steps for defining a locker system. By following these steps, your locker system should be set-up quickly and be ready for operation with Relaxx.

Chapter "4. AUTHORIZATION MANAGEMENT" describes how to define users in Relaxx and how to configure authorizations for them. The administration of rolls, which organizes the authorizations of users into groups, and the data of the predefined users in Relaxx are also covered in this chapter.

Chapter "5. LICENSE MANAGEMENT" includes information regarding the licensing and activation of Relaxx. Normally, this information is needed only once directly after installing Relaxx.

1.2 Formatting

Important, function-critical information is displayed in this manual using the following formatting (with sample text). These instructions must be read and followed.

NOTE! This signal word is used to indicate important information, relating to the current topic, which must be read and followed in order to complete a task.

Important, but not safety-critical, information and helpful tips are formatted as follows (with sample text).

ℹ *The text next to this symbol contains interesting information relating to the current topic. The information will help you better understand the description in this section or provide interesting tips for using the software.*

Action steps, to be performed by the reader, and the results of these actions are formatted as follows.

► This symbol represents an action or instruction that you must follow.

o This symbol represents the result after executing the previous action.

1.3 General Information

Relaxx provides a platform to configure, control and monitor the electronic locker locks as well as the access and information terminals from GANTNER Electronic GmbH. Relaxx operates on computers that use a Microsoft Windows® operating system (refer to the Relaxx Installation Manual).

Relaxx consists of a Windows® service that operates in the background to handle communication with the locker, and a user interface that is used to configure and control the locker system and online devices and to display the locker states.

The Relaxx WEB User Interface is a component of Relaxx that provides a visualization of the locker system including basic control options via a web browser (desktop or mobile). A detailed description of this component is available in a separate manual.

The license module and the user administration enable the installation of several clients on different computers, which can jointly use the Relaxx installation. On the one hand, it is possible to work with a single Relaxx client, installed on the same PC as the Relaxx service, on the other hand several clients can be used, which may be installed on other computers in the network. These clients can also login to the same Relaxx system and database with their own username and passwords.

The electronic locker locks from GANTNER are used for the locking and unlocking of lockers, safe deposit boxes, etc., in facilities such as fitness clubs, spas, and public baths. The following GANTNER devices can be used with Relaxx.

Locker locks:

- GAT Lock 5020 (B, F, and ISO) (only in conjunction with GAT NET.Controller M 7000, see "System requirements" in the Relaxx Installation Manual)
- GAT SMART.Lock 7001
- GAT NET.Lock 7000
- GAT NET.Lock 7020

Controllers:

- GAT Lock.Controller 5010 X (B, F, and ISO) (only in conjunction with GAT NET.Controller M 7000, see "System Requirements" in the Relaxx Installation Manual)
- GAT SMART.Controller S 7000
- GAT SMART.Controller S 7020
- GAT NET.Controller S 7000, GAT NET.Controller M 7000
- GAT NET.Controller S 7020, GAT NET.Controller M 7020
- GC7.2000 M, GC7.2000 M lite, GC7.3000 with the G7 Main Controller App (see chapter “1.4 Terminology”)

Online devices:

- GAT Access 6xxx (B, F and ISO)
- GAT Info 6xxx (B, F and ISO)
- GAT SMART.LockAxx 6350 (B, F, and ISO)
- GT7 devices (with "Info" app for information display, with "Access" app for access control, with "Central Locker" app for SMART.Lock system)

1.4 Terminology

The following terms are frequently used in the manual:

Authorization list
The authorization list includes data carriers, for which validities can be defined specifically for certain times or certain lockers/locker groups. The authorization list can be enabled or deactivated. If it is enabled, data carriers can be authorized either only for certain times or for certain locker groups.
In the authorization list, the personal lockers are also assigned to the respective data carriers.

Controller
Control units for the electronic locks. A distinction is made between the main controllers and sub controllers. The electronic locks are connected to the sub controllers. There is a sub controller for every type of lock. The sub controllers are controlled by a main controller or by a GAT SMART.Lock Axx 6350 or GT7 Central Locker terminal in the case of the GAT SMART.Lock 7001.
The main controllers are available in different versions. In this manual, the term "NET.Controller Main" is used for the GAT NET.Controller M 7000 and 7020 and the term "G7 Main" is used for the GC7.2000 and 3000 controllers.

Data carrier
An ID credential that is available in various forms, e.g., card, wristband, or key tag. The data carriers are used to identify the users of a facility at the GANTNER devices. The identification occurs via radio frequency (RFID).

Reservation
Reservations can be used to reserve data carriers for specific locks. During the reservation times, the reserved lockers can only be used with the associated data carriers.

Lock / locker lock
These terms are used in the manual to describe a GANTNER electronic locker lock that is used to lock lockers. There are various types of locks:

- GAT NET.Lock 70x0: Denotes a GAT NET.Lock 7000 or 7020. Connected to a GAT NET.Controller S 7000 or 7020. The identification occurs via RFID data carriers directly at the GAT NET.Lock 70x0 (or at the locker door).
- GAT SMART.Lock 7001: Connected to a GAT SMART.Controller S 7000 or 7020. The identification of users takes place at a central terminal (e.g., GAT SMART.Lock Axx 6350 or GT7 Central Locker) rather than directly at the locker door.
- GAT Lock 5020: Previous version of the GAT NET.Lock 70x0. This lock is connected to a GAT Lock Controller 5010 with identification occurring directly at the GAT Lock 5020 (or at the locker door).

Locker mode

The electronic locks in the lockers can be operated in various modes:

- Free locker: A locker in free locker mode can be locked and unlocked by any data carrier, under the following conditions: The data carrier has not already locked more than the set maximum number of lockers, the data carrier is valid in the facility (valid FID or site key) and, when the authorization list is enabled, the data carrier has a valid authorization according to the authorization settings for the desired unoccupied free locker.
- Personal locker: A locker in personal locker mode can only be locked and unlocked by a data carrier assigned to it in the authorization list. It is also possible to assign several data carriers to one personal locker (e.g., family lockers).
- Reservable locker: A reservable locker can only be locked and unlocked by a data carrier assigned to it in the reservation, and only as long as the reservation period is active. Once the reservation period has expired, the locker is automatically set to maintenance mode and deactivated until maintenance mode is disabled again.
- Dynamic locker: A locker in dynamic locker mode is a combination between a free locker and a personal locker. When the locker has no authorization assigned to it, it acts as a free locker and can be locked by any valid data carrier. When the locker is locked by a data carrier, this data carrier is automatically added to the authorization list of Relaxx and the dynamic locker is assigned to this data carrier. The locker then acts as a personal locker. An example of usage for this locker mode is a group of lockers that are used for service stuff (e.g. towels). Only users belonging to a certain group can use these lockers, but they can freely choose between one of the lockers. The lockers can be dynamically assigned.

An overview of the locker modes including how they are configured and used in Relaxx is available in section "3.4.1. Overview of Authorization Settings and Locker Modes" and the following pages.

Maintenance mode

A locker can be set to maintenance mode either manually or automatically (after a reservation has expired). In this state, the lock is out of operation (LED flashes red/green) and cannot be used with a regular user data carrier. This function is intended for maintenance work, e.g., cleaning of the locker after the reservation has expired. The maintenance state of the locker can be disabled using the maintenance data carrier or via Relaxx, thereby allowing the locker to be used normally again.

NOTE! Please note that maintenance mode as described here is only applicable for GAT NET.Lock 70x0 locker locks. Maintenance mode is only recommended for the GAT NET.Lock 70x0 due to the following restrictions that apply for the previous generation GAT Lock 5020 locks:

- The LED of the GAT Lock 5020 does not indicate when maintenance mode is operating.
- When a user locks a locker with their data carrier and the GAT Lock 5020 then switches into maintenance mode, the user can still open the locker using their data carrier again.

2 GENERAL SETTINGS

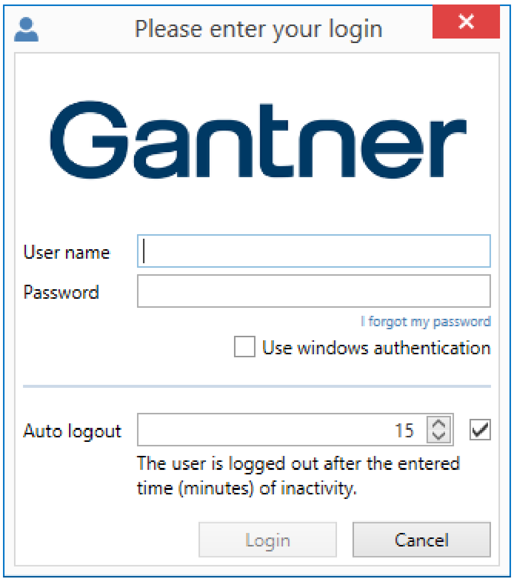
All the basic functions that affect the general operation of Relaxx can be set in the general settings. In most installations, these settings need only be configured once after installing Relaxx, however, they can be accessed and subsequently changed at any time.

2.1 Login

After starting Relaxx and connecting successfully to the Relaxx service and database, the login screen appears. To begin working with Relaxx, it is necessary to log in with a Relaxx username and password or using Active Directory (Windows user).

Relaxx provides a user management system that is used to create new users and manage existing users and their operational settings. Different features and functions in Relaxx can be authorized for individual users to allow access. The default users that are supplied with Relaxx are described in section “4.3.2. Default ”.

NOTE! If the "Active Directory" function is enabled (see “4.3 User Management”), users can also log in using their Windows Active Directory user names and passwords.



Please enter your login

User name

Password

I forgot my password

□ Use windows authentication

Auto logout 15 ☑

The user is logged out after the entered time (minutes) of inactivity.

Figure 2.1 *- Relaxx login window*

- ► Enter your username in the "Username" field.
- ► Enter your password in the "Password" field.

  NOTE! The input is case sensitive; ensure to enter your login details correctly.
- ► If you want to log in with your Windows user account via Active Directory in the future, select the "Use Windows authentication" field. In this case, you will be automatically logged in each time you start Relaxx, provided that the current Windows user account with which you are logged in to Windows is entered in the Active Directory. The connection to the Active Directory must be configured correctly in the user administration, see "4.3.1 Active Directory".

NOTE! To deactivate this function, log out of GAT Relaxx (symbol at the top right). The login screen is displayed again. Deactivate the field "Use Windows authentication" and then log in with a Relaxx username and password.

- When the “Auto logout” option is selected, the current user is automatically logged out of Relaxx after a definable period of inactivity. The logout period is defined in minutes in the input field.

  NOTE! The automatic logout function provides security against the unauthorized use of Relaxx at workstations where the user has forgotten to log out.
- Click on “Login”.
  - You are now logged in to Relaxx and the main window of Relaxx is displayed.

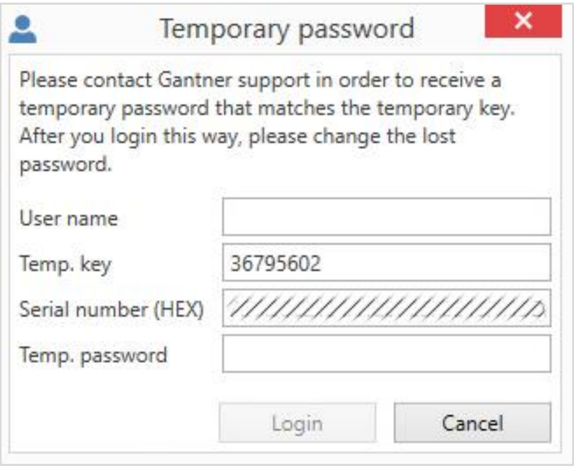
NOTE! Relaxx is delivered with predefined default users and passwords (see section “4.3.2. Default ”). To maintain security, change the default user passwords to secure passwords after the initial login.

2.1.1 Password Recovery

If you forget your password, GANTNER support can issue a temporary password that you can use to log in to Relaxx in order to change your password.

The option for the password recovery must be activated in the program settings of Relaxx (see "2.2.1. General"). Otherwise, the option for password recovery is not shown on the login screen.

- While the login window of Relaxx is open, click on "I forgot my password".
  - The "Temporary password" window is displayed.



Temporary password

Please contact Gantner support in order to receive a temporary password that matches the temporary key. After you login this way, please change the lost password.

User name

Temp. key: 36795602

Serial number (HEX)

Temp. password

Figure 2.2 *- Temporary password*

- Enter your username in the "Username" field. Note that this input is case sensitive.
- Inform GANTNER support of your username and the values in the "Temp. key" and "Serial number" fields.
  - You are sent a temporary password.

NOTE! Do not close the temporary password window before you enter the temporary password. The temporary password is verified using the "Temp. key" and this value is regenerated each time the window is opened.

- ► Enter the temporary password and click "Login".
  - ○ You are now logged in to Relaxx.
- ► Change the temporary password in the user management system to a new and secure password.

2.2 Software Settings

The software settings are organized into different pages.

- ► Start Relaxx and log in using your username and password.
- ► To access the software settings, click on the ▤▾ icon.
  - ○ All the setting categories available for Relaxx are displayed.

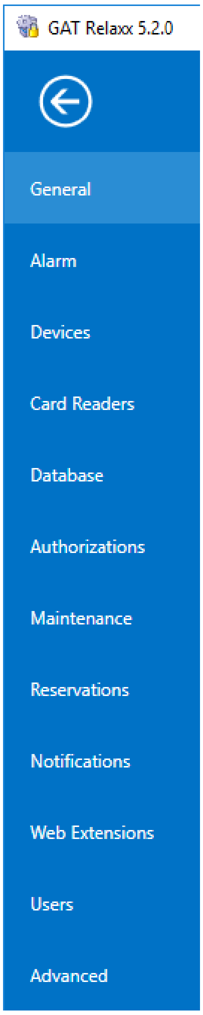


Figure 2.3 *- Software settings*

The different setting categories are described in the following pages.

NOTE! If modifications are made on a settings page, they must be saved using the “Save” button. Settings pages with modified but not yet saved settings are shown in red.

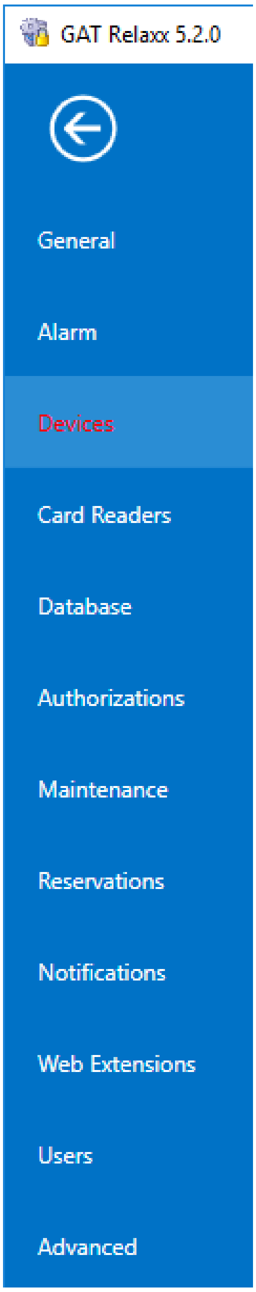
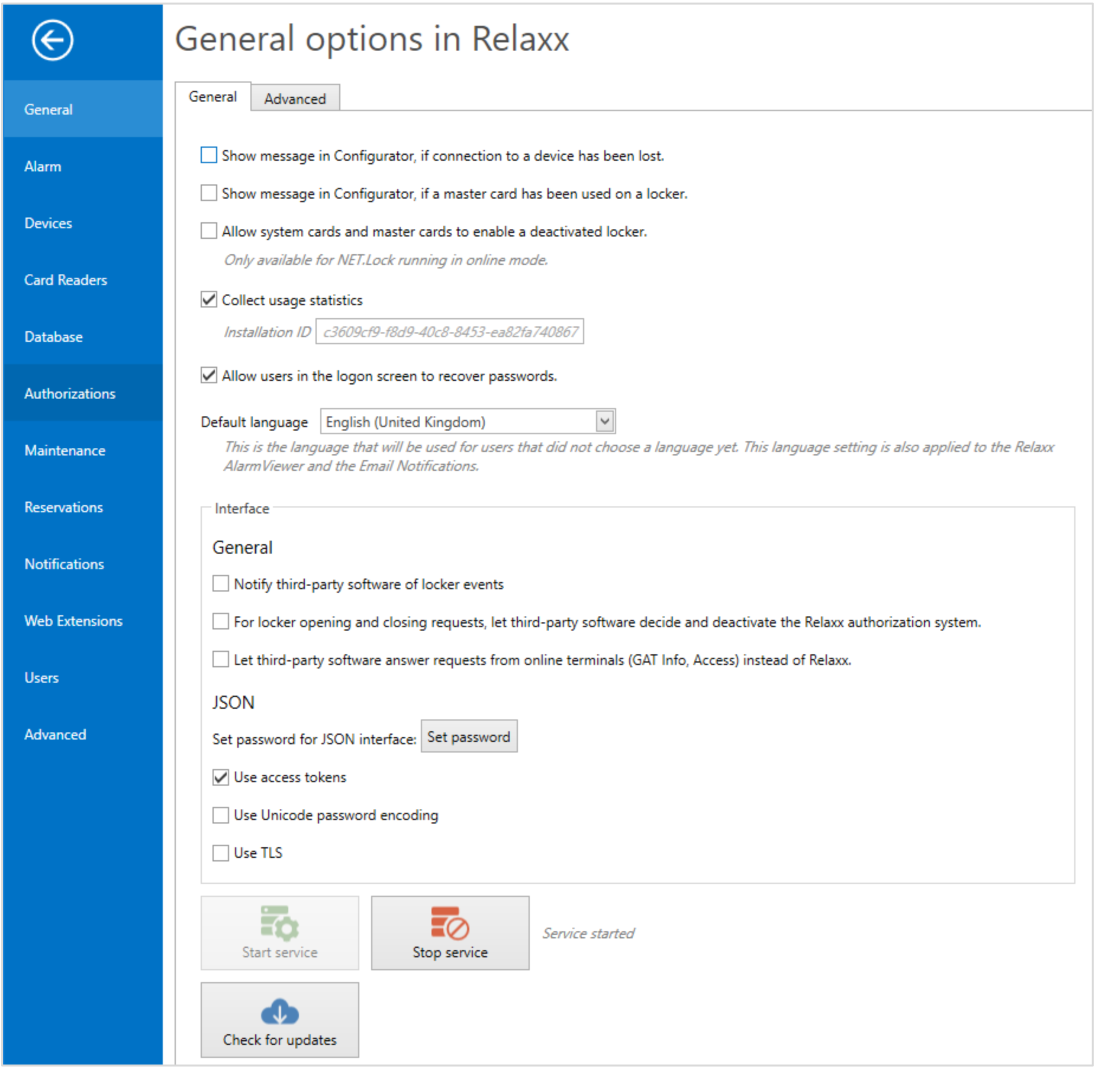


__Figure 2.4__ - Settings pages with unsaved modifications

2.2.1 General



General options in Relaxx

□ Show message in Configurator, if connection to a device has been lost.

□ Show message in Configurator, if a master card has been used on a locker.

□ Allow system cards and master cards to enable a deactivated locker.
Only available for NET.Lock running in online mode.

☑ Collect usage statistics
Installation ID c3609cf9-f8d9-40c8-8453-ea82fa740867

☑ Allow users in the logon screen to recover passwords.

Default language: English (United Kingdom)
This is the language that will be used for users that did not choose a language yet. This language setting is also applied to the Relaxx AlarmViewer and the Email Notifications.

Interface

General

□ Notify third-party software of locker events

□ For locker opening and closing requests, let third-party software decide and deactivate the Relaxx authorization system.

□ Let third-party software answer requests from online terminals (GAT Info, Access) instead of Relaxx.

JSON

Set password for JSON interface:

☑ Use access tokens

□ Use Unicode password encoding

□ Use TLS

Service started

Figure 2.5 *- General settings*

This window contains the functions and settings that apply to Relaxx in general. The window contains two tabs. The most important settings are located on the first "General" tab, and include the following:

- Show message in Configurator, if connection to a device has been lost:

  When this option is enabled, Relaxx displays an error message when a controller is deactivated in the system.

- Show message in Configurator, if a master card has been used on a locker:

  When this option is enabled, Relaxx displays a corresponding message when a locker is opened using a master card.

- Allow system cards and master cards to enable a deactivated locker:

  When this option is enabled, a deactivated locker can be enabled using a system or master card directly at the locker.
  NOTE! Only in online mode and only for GAT NET.Lock systems.

- Collect usage statistics: When this option is enabled, Relaxx usage data, e.g., functions used or error information, is sent to GANTNER for analysis. This information helps us to improve our software and GANTNER ensures that your privacy is protected. See the Relaxx Privacy Policy for more information.
- Allow users in the logon screen to recover passwords:
  When this option is enabled, a link is shown on the log-in screen that allows a user to recover his password in case he lost it. If this option is not marked, this recovery link is not shown.
- Default language: This option sets the default language that will be used in Relaxx for users that have not chosen a language yet. This setting also defines the country-specific settings, e.g., the displayed date format. The language selected here is also used for the Relaxx Alarm Viewer and the date/time format for email notifications.
- Interface: The behavior of the JSON interface (if used) can be defined in this area. These settings must be adjusted to the prevailing system requirements. If the JSON interface is not used, these settings are not considered.

  General

  - Notify third-party software of locker events: Enable this option to send the locker events, i.e., event data from the locker system, to third-party software via the interface.
  - For locker opening and closing requests, let third-party software decide and deactivate the Relaxx authorization system: Enable this option to send locker requests (open/close) to third-party applications.
  - Let third-party software answer requests from online terminals (GAT Info, Access) instead of Relaxx: Enable this option to forward request data from GAT Access/Info online devices to third-party applications. Note that the configuration settings of the device must be set correctly to allow the functionality. See the manual of the respective online device for further information.

  JSON

  - Set password for JSON interface: Click on this button to set the password of the JSON interface.

    NOTE! For security reasons, it is highly recommended to change the default password to a strong password if using the JSON interface. If you forget the interface password, a new password must be set. A blank password cannot be set.
  - To set the security for the JSON interface, there are several options for grading the security:

    a) With/without TLS encryption:

    Select the option "Use TLS" to enable TLS encryption for the communication.

    b) Authentication via JWT (JSON Web Token) or with username/password:

    Select the option "Use access tokens" to enable authentication via JWT.

    c) Use Unicode password encoding:

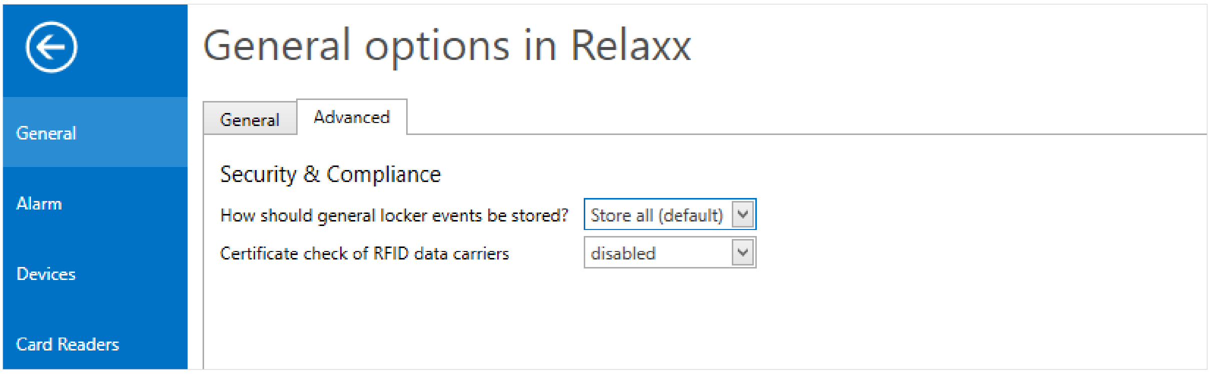
    Select the option "Use Unicode password encoding" to encode the communication password in Unicode. Otherwise, ASCII is used.

    Note: In order to achieve the same behavior as with Relaxx version <5, the 3 parameters must all be deactivated.

- Start / Stop service: These icons are used to start and stop the Relaxx service. The service must be running for Relaxx to communicate with the locker locking system.
- Check for updates: Via this icon, Relaxx contacts the GANTNER server via Internet and checks whether an update is available for the current Relaxx installation. If an update is available, it can be ordered from GANTNER support.

  NOTE! If several Relaxx clients are installed on different PCs, an update must be made for the server, as well as for all clients.

On the "Advanced" tab, you can select how the locker events should be stored.



General options in Relaxx

Security & Compliance

How should general locker events be stored? Store all (default)

Certificate check of RFID data carriers disabled

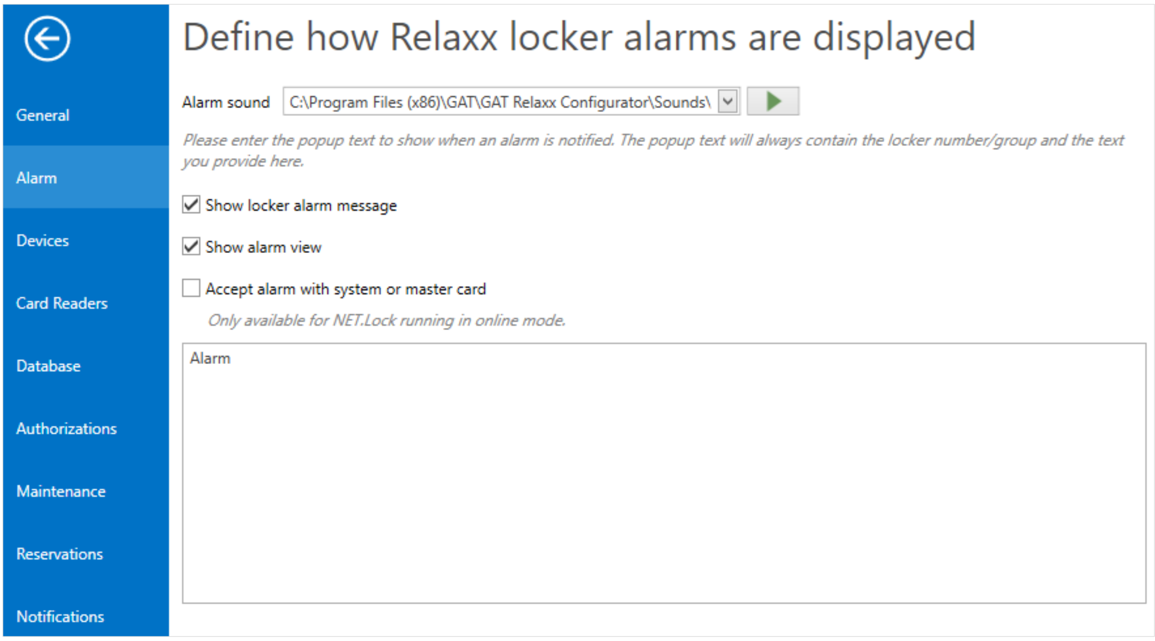
***Figure 2.6** - General settings - Advanced*

- Security & Compliance: With these settings, company or operator requirements and GDPR requirements with regard to the privacy of persons can be taken into account by regulating which events in Relaxx shall be logged in the log file (to show this report, see "3.7. Log Entries").
  - Store all (default): With this setting, all actions at the lockers as well as system messages are written to a log file.
  - Do not store events: Uncritical and successful operations, such as successfully opening or locking a locker, are not saved. These are the log entries with the category "Operational" and the severity "Informational" (you can find these settings in the log entry view, see "3.7. Log Entries").
- Certificate check of RFID data carriers:

  This option allows you to enable and disable the certificate checking of data carriers in the facility. If it is disabled, all valid data carriers can be used in the system. If the check is enabled, only data carriers from GANTNER Electronic can be used. This option is only available when the "Force Certificate Check" option is not set or inactive in the Relaxx license.

Please note that with the "Do not store events" setting, the following scenarios cannot be covered, i.e., when such a scenario occurs, it is not possible to prove the opposite:
- A user forgets to lock their locker.
- One or more items are stolen from an unlocked locker.
- The user claims that they have locked the locker.

2.2.2 Alarm



Define how Relaxx locker alarms are displayed

Alarm sound C:\Program Files (x86)\GAT\GAT Relaxx Configurator\Sounds\

Please enter the popup text to show when an alarm is notified. The popup text will always contain the locker number/group and the text you provide here.

☑ Show locker alarm message

☑ Show alarm view

□ Accept alarm with system or master card

Only available for NET.Lock running in online mode.

Alarm

Figure 2.7 *- Alarm settings*

- Alarm sound: Various alarm sounds can be selected from the dropdown menu. Click on the “Play” symbol in order to listen to the tunes for testing.

  If the Relaxx AlarmViewer is used (see "3.10.3. Relaxx AlarmViewer") and this is installed on a computer without Relaxx Client, the desired alarm signal must be selected separately with the Relaxx AlarmViewer.

- Show locker alarm message:

  If this option is checked, alarms generated at lockers (e.g., break-in) are indicated in Relaxx by individual, red fields at the border of the screen.

  NOTE! The locker alarm message disappears automatically after a few seconds.

- Show alarm view: If this option is checked, a pop-up window will be opened in the event of an alarm, displaying information regarding the alarm.

- Accept alarm with system or master card:

  If this option is checked, an alarm generated at a locker can be acknowledged at the locker using a master card. Please note, that this is not possible for systems with a GAT Lock Controller 5010 in offline mode.

- Text field for alarm message:

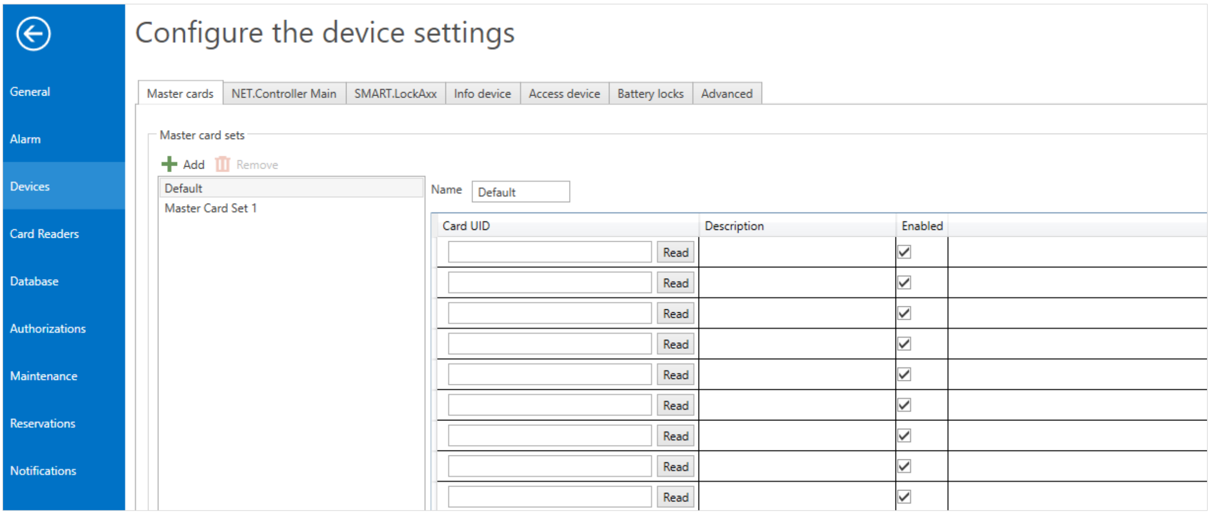
  Text can be entered here that will be displayed in a pop-up window when an alarm is activated. In addition to the text, the locker number and the locker group are also displayed in the pop-up window.

2.2.3 Devices

The default device settings for the different devices that can be controlled by Relaxx each have their own settings tab. These settings are valid globally for Relaxx, which means that, e.g., the time settings configured for "NET.Controller Main" apply to all GAT NET.Controllers in the system. The following devices can be configured here:

- GAT NET.Controller M 7000: Main controller for the GAT NET.Lock 7000 system (and GAT Lock 5020 locks).
- GAT SMART.LockAxx 6350: Central terminal for the GAT SMART.Lock 7000 system.
- GAT Info 6xxx: Information terminal for displaying user information like e.g. the used locker number.
- GAT Access 6xxx: Access control terminal for authorization checks and entry control into certain areas.
- Battery locks: Battery-powered locker locks that can communicate wirelessly with Relaxx.

Settings for the Master Cards



Default
Master Card Set 1

Name: Default

Card UID	Description	Enabled
Read		☑
Read		☑
Read		☑
Read		☑
Read		☑
Read		☑
Read		☑
Read		☑
Read		☑

***Figure 2.8** – Settings for the master cards*

NOTE! Master Cards.

- As master cards can open all lockers that have been assigned to the master card set, it is paramount to keep these cards in a safe place where they are protected against unauthorized use.
- A master card must only be used as a master card. It cannot be entered into the authorization list and used at the same time, e.g., as a system or maintenance data carrier.

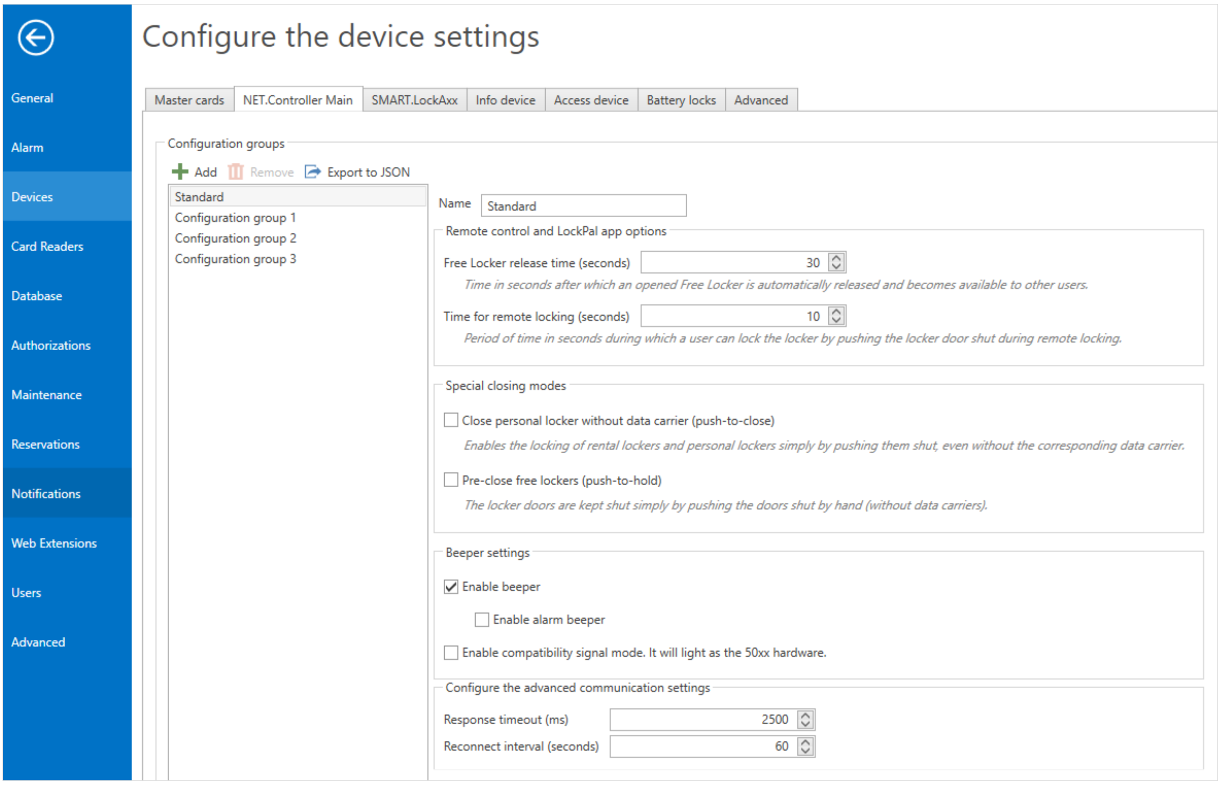
The settings for the master cards used in the system are defined here. Each main controller is assigned a set of max.10 master cards in the hardware settings (see "3.2.3 Modifying the Device Settings -> a) GAT NET.Controller Main"). By default, each newly created main controller is assigned the "default" set. For larger systems, several master card sets can also be defined and assigned to the corresponding controllers.

► Enter the master card number directly into the field or read the number by placing the master card onto a connected card reader and clicking on the “Read” button.

► To delete a master card, empty the input field.

► You can temporarily disable the master card by deselecting the “Enabled” option.

Device settings for the Main Controller GAT NET.Controller M 70x0



Configure the device settings

Configuration groups

- Standard
- Configuration group 1
- Configuration group 2
- Configuration group 3

Name: Standard

Remote control and LockPal app options

Free Locker release time (seconds): 30

Time in seconds after which an opened Free Locker is automatically released and becomes available to other users.

Time for remote locking (seconds): 10

Period of time in seconds during which a user can lock the locker by pushing the locker door shut during remote locking.

Special closing modes

□ Close personal locker without data carrier (push-to-close)

Enables the locking of rental lockers and personal lockers simply by pushing them shut, even without the corresponding data carrier.

□ Pre-close free lockers (push-to-hold)

The locker doors are kept shut simply by pushing the doors shut by hand (without data carriers).

Beeper settings

☑ Enable beeper

□ Enable alarm beeper

□ Enable compatibility signal mode. It will light as the 50xx hardware.

Configure the advanced communication settings

Response timeout (ms): 2500

Reconnect interval (seconds): 60

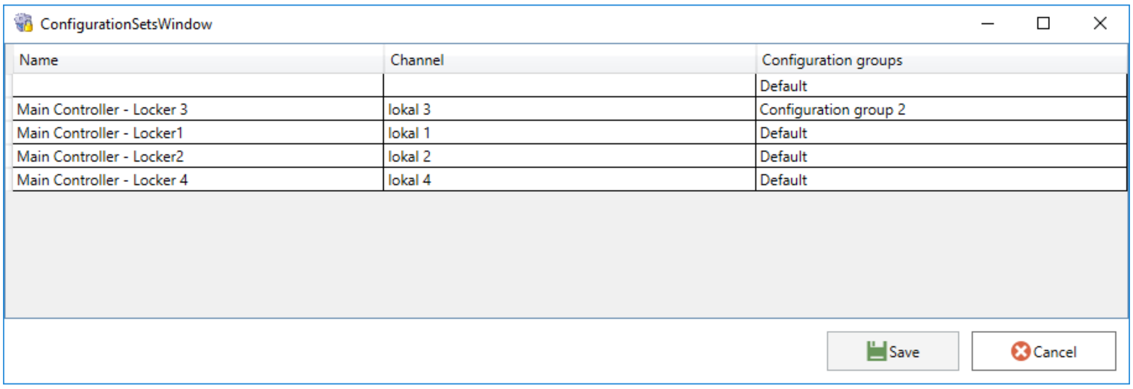
***Figure 2.9** – Device settings for the NET.Controller Main*

General settings for all GAT NET.Controller M 70x0 in the system are defined here. To the left under “Configuration groups” entries (configuration groups) can be created that summarize a specific combination of configuration settings. The configuration settings can then be assigned to the controllers in the system (see "3.2.3 Modifying the Device Settings"). The “Standard" configuration group is predefined.

► To change the name of the configuration group, enter the desired name into the “Name” field.

► To add another configuration group, click on “+ Add”, and define a name for the group.

  - A window opens with a list of all active controllers.



Name	Channel	Configuration groups
		Default
Main Controller - Locker 3	lokal 3	Configuration group 2
Main Controller - Locker1	lokal 1	Default
Main Controller - Locker2	lokal 2	Default
Main Controller - Locker 4	lokal 4	Default

***Figure 2.10** – Selecting a controller*

► Select the controller with the configuration that is to be used as the basis for the configuration group.

► Confirm with "Save". The settings are shown to the right:

- Remote control and LockPal app options:
  - Free Lock release time (seconds): Time in seconds after which an opened free locker is released thereby making it available to other users.
  - Time for remote locking (seconds): If a locker is locked via remote control (e.g., LockPal App), the user must push the locker door shut within the time specified here in order to lock it.
- Special closing modes: Special locker closing modes are configured here.
  - Close personal locker without data carrier (push-to-close): This function allows the locking of personal lockers simply by pushing them shut, even without the corresponding data carrier. In order to enable this function, the controller must be restarted.
  - Pre-close free lockers (push-to-hold): If this function is enabled, the locker door is kept shut by the GAT NET.Lock 70x0 simply by pushing the door shut by hand (without data carrier).

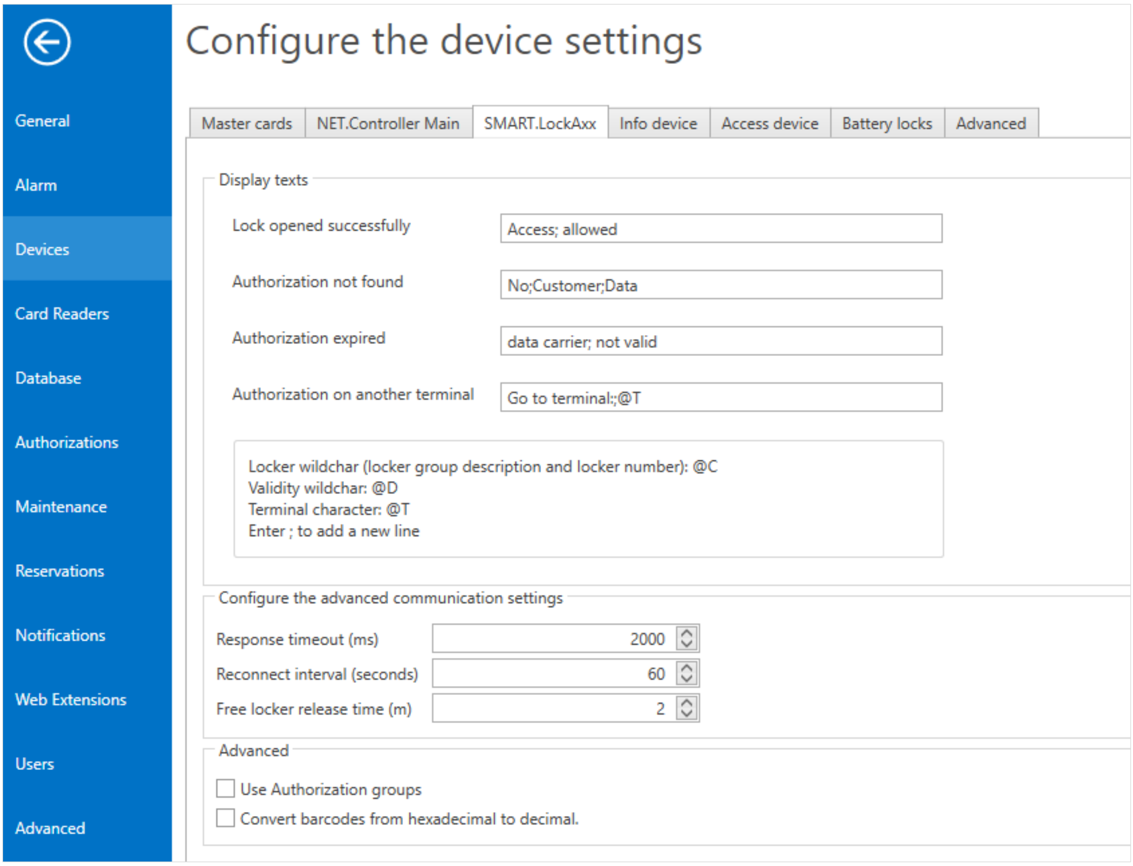
    NOTE! With this function, the locker door is kept shut but is not locked (the status LED is green). The user still must lock the locker using a data carrier.
- Beeper settings: Three options for setting the beeper behavior of the GAT NET.Controller and GAT NET.Lock are mentioned below.
  - Enable beeper: If this option is checked, certain states, e.g. the locking of a lock are indicated by a corresponding acoustic signal on the GAT NET.Lock 70x0. If this option is not checked, no acoustic signal resounds on any device of the GAT NET.Lock system.
  - Enable alarm beeper: If this functionality is enabled, acoustic signals are generated at the locker lock in the case of an alarm (e.g. illegal break-in).
  - Enable compatibility signal mode: With this option, the same LED light signals are generated as with the older GAT Lock 50xx.
- Configure the advanced communication settings:

  The timing of the controllers is set here.
  - Response timeout: This time defines how long Relaxx will wait for a response from a controller after sending a command or data to a controller.
  - Reconnect interval: This time (in seconds) defines the interval when Relaxx will attempt to establish a new connection to a controller if the connection has been interrupted. A value of "0" means that reconnection will not be attempted.
- Advanced configuration: This button opens a new window where all the configuration settings of a controller are displayed. A detailed description of these settings can be found in the controller manual.

  NOTE: The configuration group "Standard" or "Default", which is pre-installed after the Relaxx installation, does not contain any advanced configuration settings. All advanced settings for a controller in this group are set individually in the hardware view. For controllers in another group, most of the advanced settings are applied via the parameters configured in the "Advanced settings" of the group. Only the controller-specific parameters (IP address, NETBios name, etc.) are defined individually for each controller in the hardware view. Accordingly, the parameters can only be read or changed.

- ► After defining the controller settings, click on “Save” at the bottom of the window.
- ► To delete a configuration group, select the group in the list and click on “Delete”.
  - ○ The configuration group is deleted provided it is no longer in use, i.e., no controllers are assigned to it.
- ► The “Export to JSON” button allows you to export the group’s controller settings to a JSON file.

Device settings for the GAT SMART.LockAxx 6350



Configure the device settings

Display texts

Lock opened successfully: Access; allowed

Authorization not found: No;Customer;Data

Authorization expired: data carrier; not valid

Authorization on another terminal: Go to terminal:;@T

Locker wildchar (locker group description and locker number): @C
Validity wildchar: @D
Terminal character: @T
Enter ; to add a new line

Configure the advanced communication settings

Response timeout (ms): 2000

Reconnect interval (seconds): 60

Free locker release time (m): 2

Advanced

□ Use Authorization groups

□ Convert barcodes from hexadecimal to decimal.

Figure 2.11 *- Device settings for GAT SMART.LockAxx 6350*

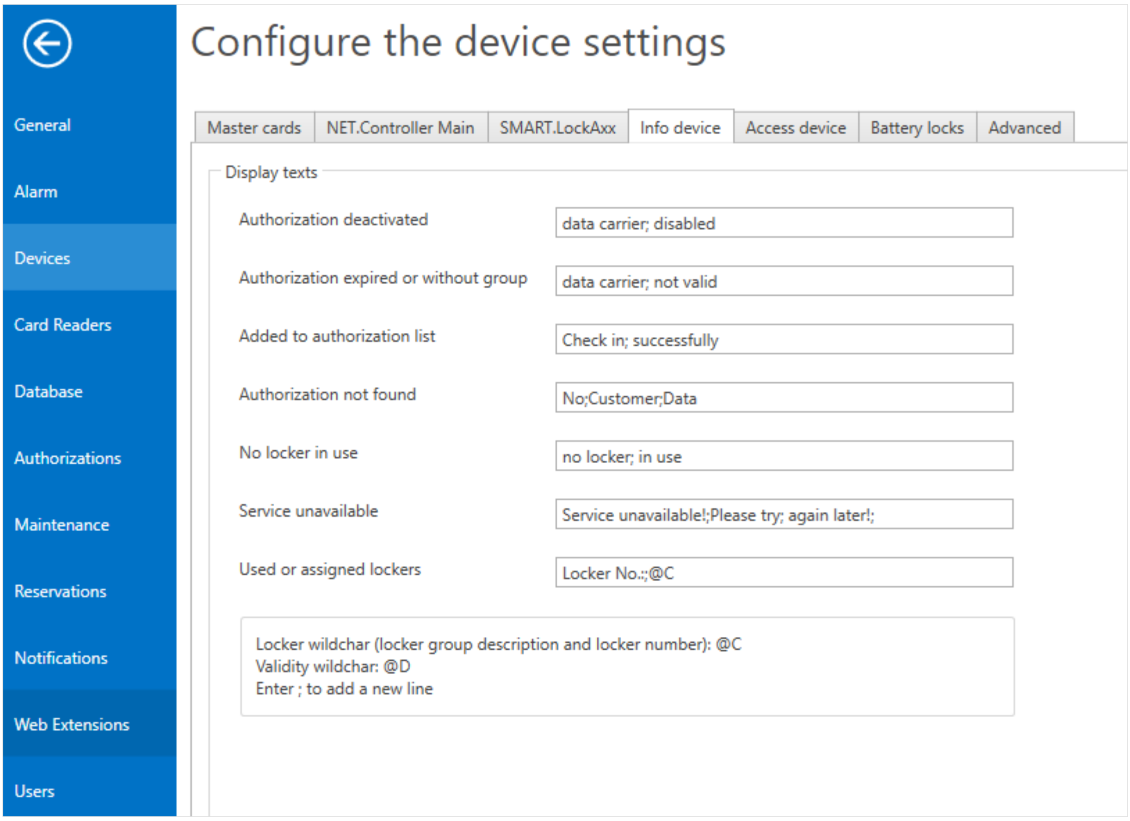
With this tab, the general settings for the GAT SMART.Lock 7001 system can be performed.

- Display texts: Here you can enter standard values for the display texts that are shown on the display of the GAT SMART.LockAxx 6350 devices. A description of the possible wildcards can be seen below the input fields. With the ";" sign you can start a new line on the display. For each GAT SMART.LockAxx 6350 device in the system you can set individual texts (in the device setting, see "3.2.3. Modifying the Device Settings") or use the standard texts that are entered here.
- Communication settings: The time behavior of the GAT SMART.Controller and the GAT SMART.LockAxx 6350 is set here.

- Response timeout: This time defines how long Relaxx will wait for a response from a controller after sending a command or data to a controller.
- Reconnect interval: This time (in seconds) defines the interval when Relaxx will attempt to establish a new connection to a controller if the connection has been interrupted. A value of "0" means that reconnection will not be attempted.
- Free locker release time: If a locker with a GAT SMART.Lock 7001 lock is opened via a GAT SMART.LockAxx 6350 terminal, the same locker can be used again (locked) with the same data carrier within the time set here.

- Advanced:
  - The field "Use authorization groups" is intended for future applications. This option should always be disabled.
  - If the "Convert barcodes from hexadecimal to decimal" option is activated, the GAT SMART.LockAxx 6350 automatically converts the read barcodes from hexadecimal to decimal format.

Device Settings for the Info Devices



Configure the device settings

Display texts

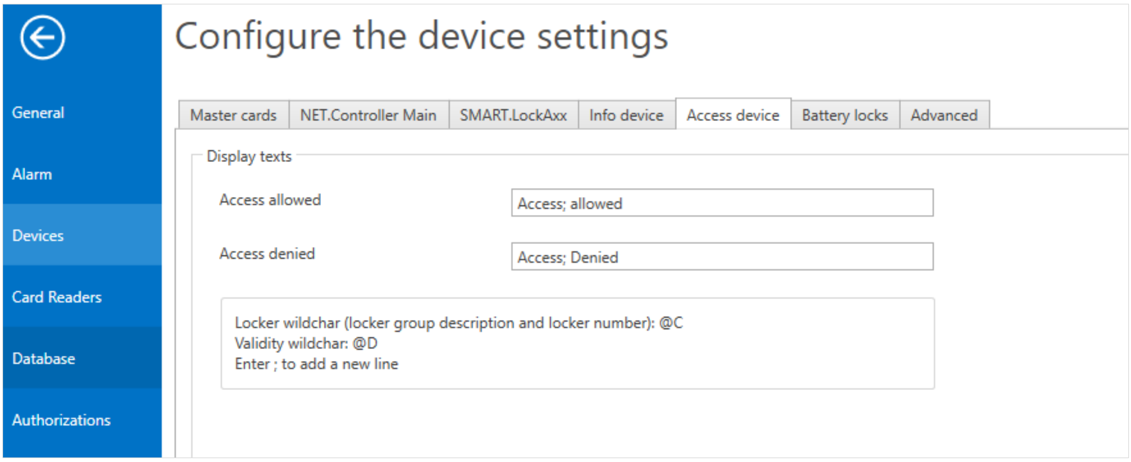
Authorization deactivated	data carrier; disabled
Authorization expired or without group	data carrier; not valid
Added to authorization list	Check in; successfully
Authorization not found	No;Customer;Data
No locker in use	no locker; in use
Service unavailable	Service unavailable!;Please try; again later!;
Used or assigned lockers	Locker No.:;@C

Locker wildchar (locker group description and locker number): @C
Validity wildchar: @D
Enter ; to add a new line

Figure 2.12 *- Device settings for Info devices*

Here you can enter standard values for the display texts that are shown on the display of the Info devices. A description of the possible wildcards can be seen below the input fields. With the ";" sign you can start a new line on the display. For each Info device in the system you can set individual texts (in the device setting, see "3.2.3. Modifying the Device Settings") or use the standard texts that are entered here.

Device Settings for the Access Devices



Configure the device settings

Display texts

Access allowed: Access; allowed

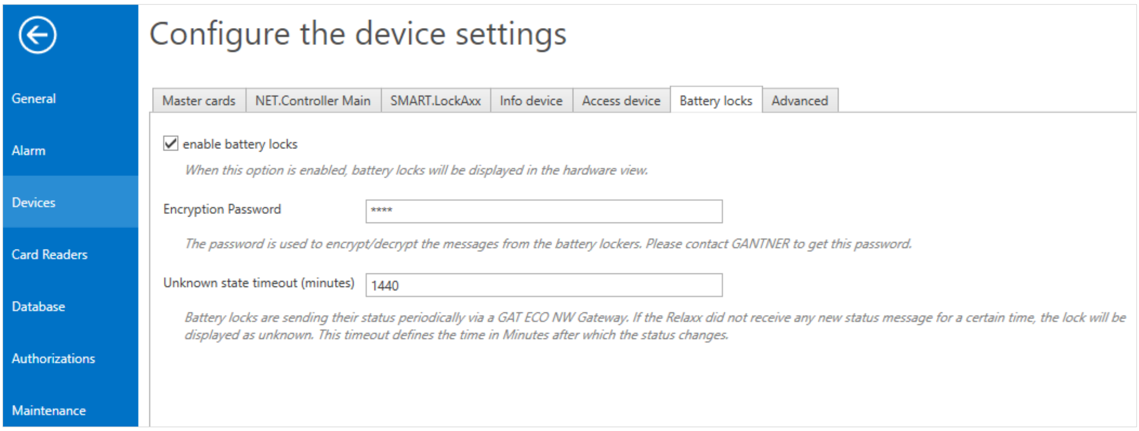
Access denied: Access; Denied

Locker wildchar (locker group description and locker number): @C
Validity wildchar: @D
Enter ; to add a new line

Figure 2.13 - *Device settings for Access devices*

Here you can enter standard values for the display texts that are shown on the display of the Access devices. A description of the possible wildcards can be seen below the input fields. With the ";" sign you can start a new line on the display. For each Access device in the system, you can set individual texts (see "3.2.3. Modifying the Device Settings") or use the standard texts that are entered here.

Device Settings for Battery Locks



Configure the device settings

☑ enable battery locks

When this option is enabled, battery locks will be displayed in the hardware view.

Encryption Password: ****

The password is used to encrypt/decrypt the messages from the battery lockers. Please contact GANTNER to get this password.

Unknown state timeout (minutes): 1440

Battery locks are sending their status periodically via a GAT ECO NW Gateway. If the Relaxx did not receive any new status message for a certain time, the lock will be displayed as unknown. This timeout defines the time in Minutes after which the status changes.

Figure 2.14 - *Hardware settings for battery locks*

Battery locks are GANTNER battery-powered locker locks, e.g., GAT ECO.Lock 7xxx, which can communicate with Relaxx wirelessly via a suitable receiver (e.g., Minew) over the Rest API. The rest of the API must be installed using the Relaxx installation package (see the Relaxx Installation Manual). In Relaxx, the current status of these locks is displayed in the hardware and organization views (see “3.2.3 Modifying the Device Settings” and “3.2.6. Setting up the Organization System”).

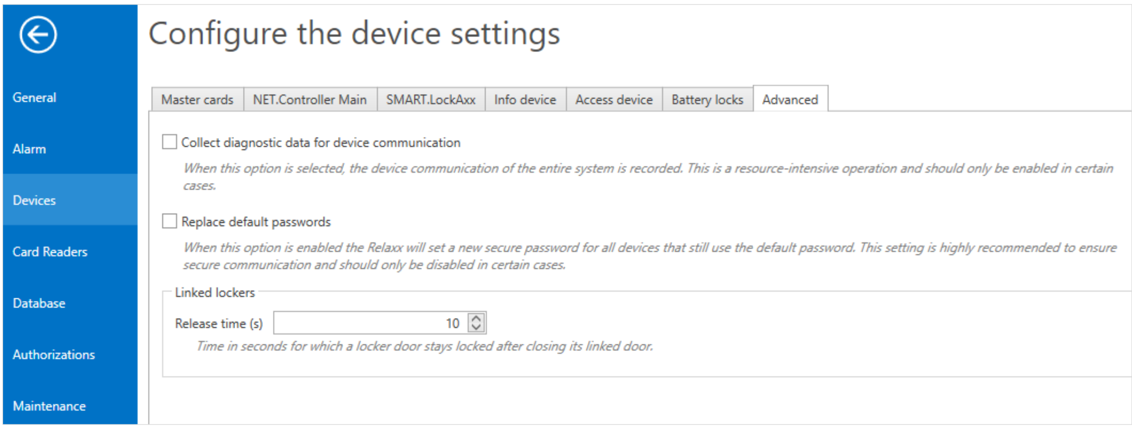
► To be able to use battery locks, select the "enable battery locks" option.

   ○ In the hardware view, an entry called "Battery locks" is added to the devices list to the left where you can define the locks (see “3.2.3 Modifying the Device Settings”).

The following settings are available here.

- Encryption Password: The password for communication with the battery locks. Contact GANTNER or your sales partner if you do not know the password.
- Unknown state timeout: This value (in minutes) determines how long Relaxx will wait for a status update from a battery lock. If there is no signal from the lock within this time, the status of the lock is set to "unknown".

Advanced device settings



Configure the device settings

□ Collect diagnostic data for device communication

When this option is selected, the device communication of the entire system is recorded. This is a resource-intensive operation and should only be enabled in certain cases.

□ Replace default passwords

When this option is enabled the Relaxx will set a new secure password for all devices that still use the default password. This setting is highly recommended to ensure secure communication and should only be disabled in certain cases.

Linked lockers

Release time (s) 10

Time in seconds for which a locker door stays locked after closing its linked door.

***Figure 2.15** - Advanced device settings*

Here, the advanced settings applicable for all devices are available.

Collect diagnostic data for device communication:
The setting for the communications monitoring applies irrespective of the type of device. If you select the option "Collect diagnostic data for device communication" the entire communication of Relaxx will be recorded.

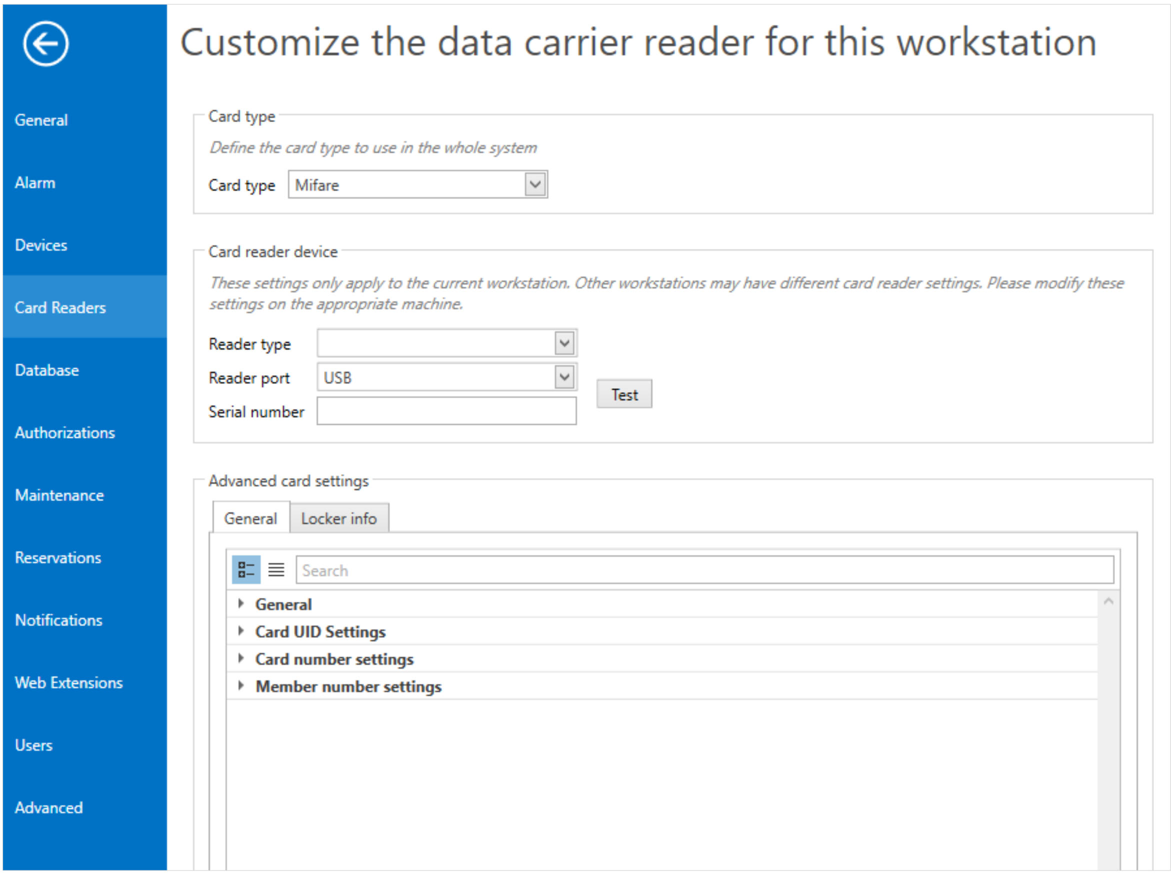
NOTE! This function should only be used for troubleshooting in the event of an error, as it slows the system down.

Replace default passwords: When this setting is enabled, Relaxx will set a new secure password for all devices that still use the default password. When a device still uses the default password, a warning symbol next to the "Change password" button in the hardware view and a warning text "Insecure password" are shown.

NOTE! This setting is highly recommended to ensure secure communication and should only be disabled in certain cases.

Linked lockers: Time in seconds for which a locker door stays locked after closing the door of the locker linked to it. If the locker is locked with a data carrier within this time, the linked lockers remain locked. If no identification takes place within this time, the lockers are available again. Lockers are linked to each other via the “Linked lockers” function on the “Extras” page (see “3.9.4 Linked Lockers” for more information).

2.2.4 Card Readers



Customize the data carrier reader for this workstation

Card type

Define the card type to use in the whole system

Card type: Mifare

Card reader device

These settings only apply to the current workstation. Other workstations may have different card reader settings. Please modify these settings on the appropriate machine.

Reader type:

Reader port: USB

Serial number:

Advanced card settings

- General
- Card UID Settings
- Card number settings
- Member number settings

Figure 2.16 *- Card reader settings*

The settings for the RFID data carriers and the connected read/write station ("GAT Writer") are entered in this window. A read/write station is not a requirement to work with Relaxx, but greatly simplifies the process of adding data carriers to the system. The following settings are available.

- Card type: Select the type of data carrier technology used in the system (MIFARE, LEGIC, ISO 15693).
- Card reader device: Select here the type of read/write station. GANTNER offers different types of read/write stations for different RFID systems (MIFARE, LEGIC, ISO 15693).
  - Reader port: Select the interface where the read/write station is connected (USB or serial COM interface).
  - Serial number: If more than one read / write station is used on the same PC, enter the serial number of the read / write station that will be used with Relaxx.

  NOTE! To confirm that the read / write station is communicating with Relaxx, place a data carrier onto the station then click “Test”. The data carrier data should be displayed to the right.

- Advanced card settings (General):
  - Site key: The company identification number is entered here. This number is unique for each locker system and must match the site keys or FIDs of the data carriers used.
  - Sub site number: A sub site number enables the partition of a large site into sub sites. Leave this field empty if no sub site numbers are used.

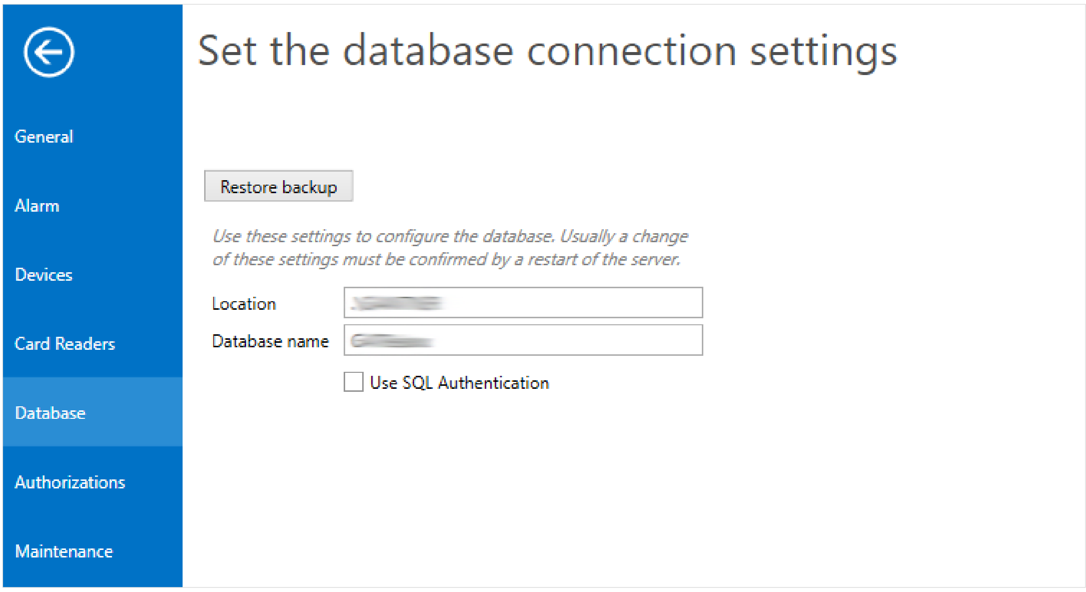
The remaining settings in the “General” tab are used to define the structure of the data carriers and whether a data carrier number and a member number should be used. The settings available vary depending on the type of RFID technology selected in the “Card type” field. As these settings must be defined individually for each system, please contact GANTNER or your local GANTNER representative for further information regarding configuration.

- Advanced card settings (Locker info):

  In the locker info tab, you can define the positions of the two locker segments on the data carriers. Define the segments by clicking on the “Add” button or remove segments via the “Delete” button. The following positions are used by default:
  - MIFARE: locker 1 = 4, locker 2 = 5
  - ISO: locker 1 = 19, locker 2 = 23
  - LEGIC: locker 1 = 1, locker 2 = 2

  You can see the locker positions on data carriers using the "Write data carrier" function in the authorization section (see "3.4.7. Read/Write Data Carriers").

2.2.5 Database



Set the database connection settings

Restore backup

Use these settings to configure the database. Usually a change of these settings must be confirmed by a restart of the server.

Location [redacted]

Database name [redacted]

☐ Use SQL Authentication

Figure 2.17 *- Database settings*

On this setting page, the settings of the connection to the Relaxx database are defined. It is also possible to restore a previous database backup.

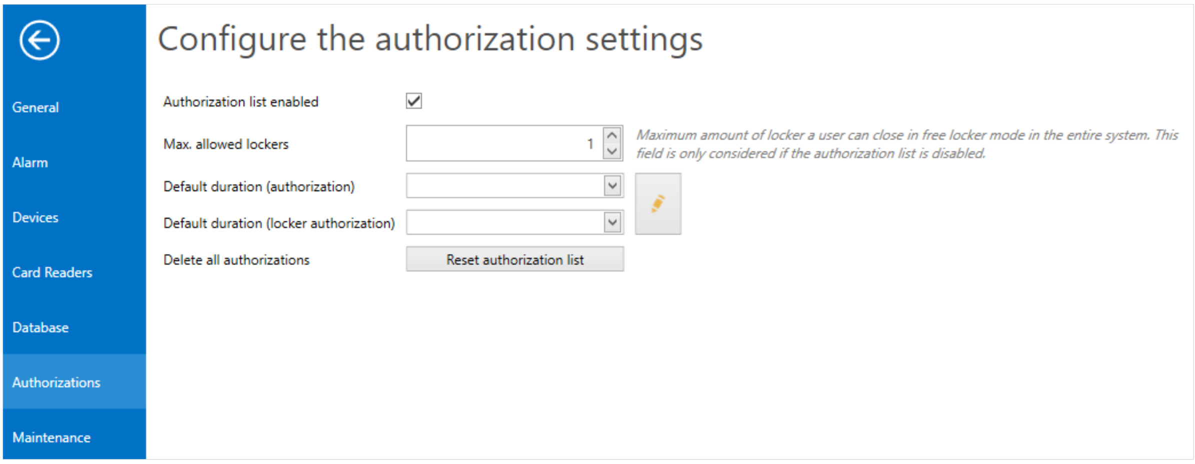
- Restore backup: By clicking on this button, a backup of the Relaxx database is restored.

  NOTE! Please note that all data and settings in Relaxx will be overwritten.

  A description of how to make a backup of the database is found in the description of the scheduler functionality under "3.6.2. Actions for the Scheduler".
- Entry fields for database connection:

  With the fields "Location", "Database name" and "Use SQL authentication", the settings of the connection to the Relaxx database are defined. Normally, this is necessary only once after the installation of Relaxx (refer to the Relaxx Installation Manual).

2.2.6 Authorizations



Configure the authorization settings

Authorization list enabled ☑

Max. allowed lockers 1

Maximum amount of locker a user can close in free locker mode in the entire system. This field is only considered if the authorization list is disabled.

Default duration (authorization)

Default duration (locker authorization)

Delete all authorizations [Reset authorization list]

Figure 2.18 *– Authorization settings*

The settings displayed here affect the authorization list of Relaxx. This list is used in online systems to specify which data carriers are authorized for use with lockers operating in free locker mode. When the authorization list is enabled, only the data carriers assigned to the list can use the lockers defined in the list.

The following authorization list settings are available.

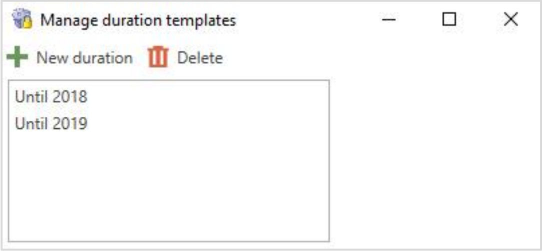
- Authorization list enabled: Select this option box to activate/deactivate the authorization list. It is also possible to activate/deactivate the authorization list via the "Authorization list enabled" option box in the "Authorization" window. For more information about the authorization list, see "3.4. Administration of Visitors / Data Carriers (Authorization List)").
- Max. allowed lockers: This field is only considered if the authorization list is disabled and determines the maximum number of lockers, operating in free locker mode, which can be used by a data carrier. The maximum number of lockers value can also be defined in the settings of the locker groups. The lower of the two values determines the applicable maximum value.
  Example: Value in the "General software settings" = 5, value for the locker group = 3 -> applicable value = 3.
  Example: Value in the "General software settings" = 3, value for the locker group = 5 -> applicable value = 3.
- Default duration (authorization):
  Select a default duration from the drop-down menu. This setting is used as the default expiry date/time for all newly-created free locker authorizations (refer to “3.4.5 Assigning Data Carriers to Authorization Groups). See the following information for instructions on defining a default duration.
- Default duration (locker authorization):
  Select a default duration from the drop-down menu. This duration will be used as the default expiry date/time for all newly-created personal locker authorizations (refer to “3.4.6 Assigning Personal Lockers”). See the following information for instructions on defining a default duration.

- Delete all authorizations: Press the “Reset authorization list” button to delete all authorizations currently stored in Relaxx. This function can be used when you need to clear the entire authorization list when testing, e.g., file importation or JSON commands.

In order to use the default duration settings, first define a duration via the pen icon.

► Click on the pen icon.

  ○ The “Manage duration templates” window opens.

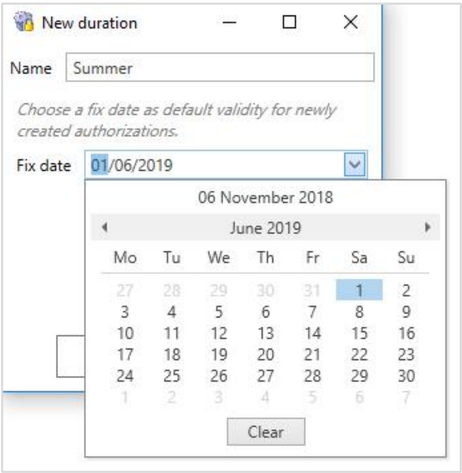


Until 2018
Until 2019

***Figure 2.19** – “Manage duration templates” window*

► Click on “New duration” then select a type of duration from the drop-down menu:

- Fix date: Select this option to define a fixed date that will be used as the default validity for newly created authorizations.



Name: Summer

Choose a fix date as default validity for newly created authorizations.

Fix date: 01/06/2019

06 November 2018

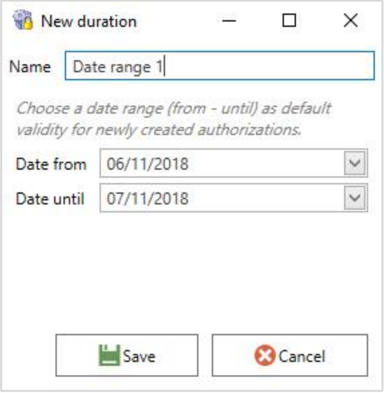
June 2019

Mo	Tu	We	Th	Fr	Sa	Su
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

***Figure 2.20** – “Fix date” duration definition*

► Enter a name for the duration and select the desired fixed date from the drop-down menu. Click on “Save” to finalize the duration.

- Date range: Select this option to define a date range (from – to) that will be used as the default validity for newly-created authorizations.



Name: Date range 1

Choose a date range (from - until) as default validity for newly created authorizations.

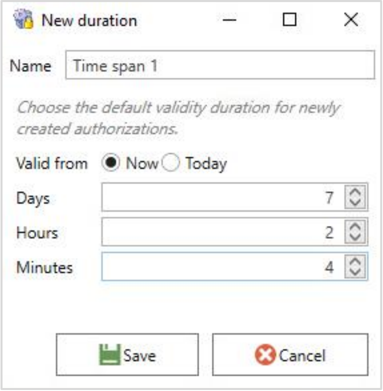
Date from: 06/11/2018

Date until: 07/11/2018

***Figure 2.21** – "Date range" duration definition*

► Enter a name for the duration and select the desired date range from the drop-down menus. Click on "Save" to finalize the duration.

- Time span: Select this option to define a time span to use as the default validity for newly created authorizations.



Name: Time span 1

Choose the default validity duration for newly created authorizations.

Valid from ● Now ○ Today

Days: 7

Hours: 2

Minutes: 4

***Figure 2.22** – "Time span" duration definition*

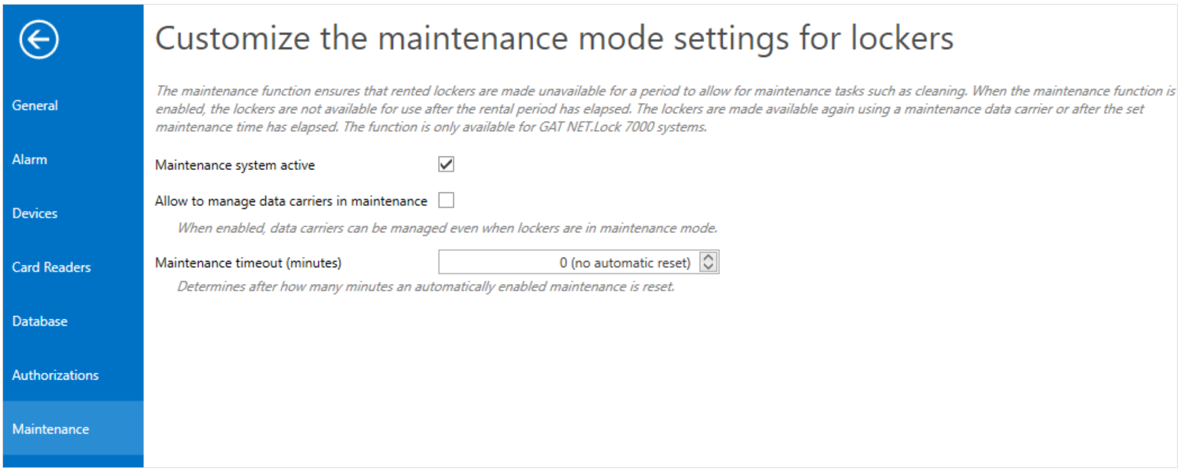
► Enter a name for the duration and select the desired start and the number of days, hours and minutes for the time span.

► Click on "Save" to finalize the settings.

   - All defined durations are listed in the "Duration Definition View" window and are available for selection in the default duration menus.

► Click on a duration in the "Duration Definition View" window to view, edit, or delete the settings.

2.2.7 Maintenance



Customize the maintenance mode settings for lockers

The maintenance function ensures that rented lockers are made unavailable for a period to allow for maintenance tasks such as cleaning. When the maintenance function is enabled, the lockers are not available for use after the rental period has elapsed. The lockers are made available again using a maintenance data carrier or after the set maintenance time has elapsed. The function is only available for GAT NET.Lock 7000 systems.

Maintenance system active ☑

Allow to manage data carriers in maintenance □

When enabled, data carriers can be managed even when lockers are in maintenance mode.

Maintenance timeout (minutes) 0 (no automatic reset)

Determines after how many minutes an automatically enabled maintenance is reset.

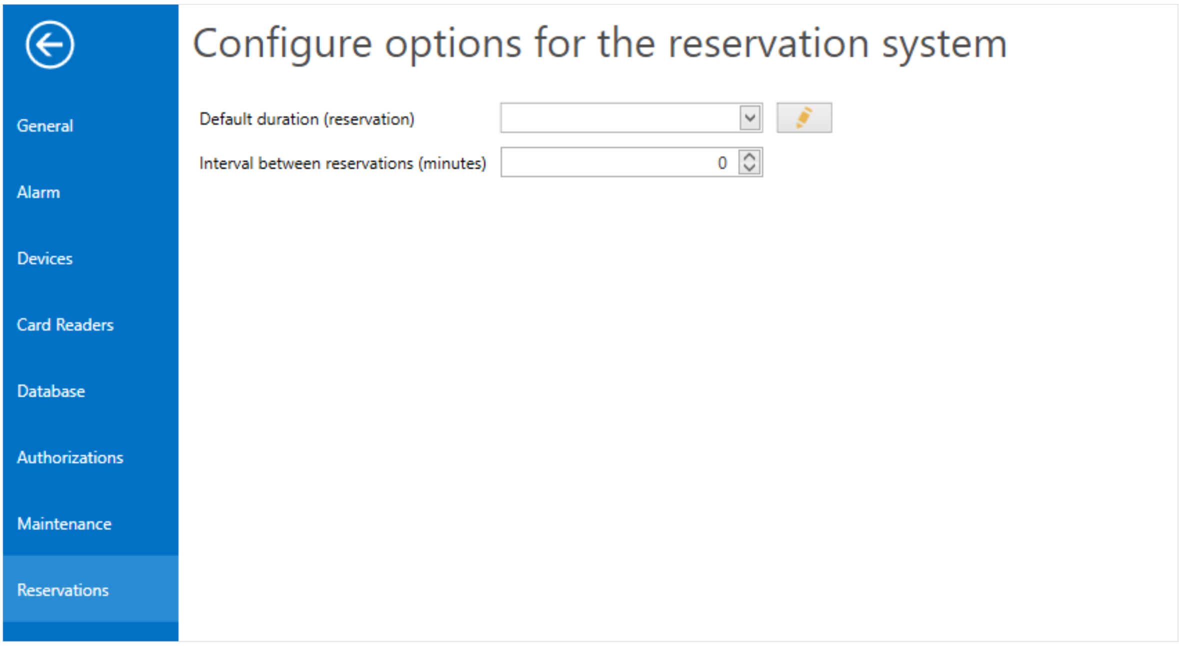
***Figure 2.23** - Maintenance settings*

On this setting page, the maintenance function can be enabled, and the function settings can be configured. The maintenance function ensures that rented lockers are made unavailable for a period to allow maintenance tasks such as cleaning to be completed. When the maintenance function is enabled, the lockers are not available for use after the rental period has elapsed. The lockers are made available again using a maintenance data carrier or after the set maintenance time has elapsed.

- Maintenance system active: This option activates the maintenance system.
- Allow to manage data carriers in maintenance: If this option is checked, data carriers can be loaded even while the maintenance function is active.
- Maintenance timeout: Determines after how many minutes an automatically enabled maintenance is reset. If the entered value is "0", the maintenance state is not disabled automatically, but has to be reset manually.

NOTE! The maintenance function is only available for GAT NET.Lock 70x0 systems.

2.2.8 Reservations



Configure options for the reservation system

Default duration (reservation)

Interval between reservations (minutes) 0

Figure 2.24 *- Reservations settings*

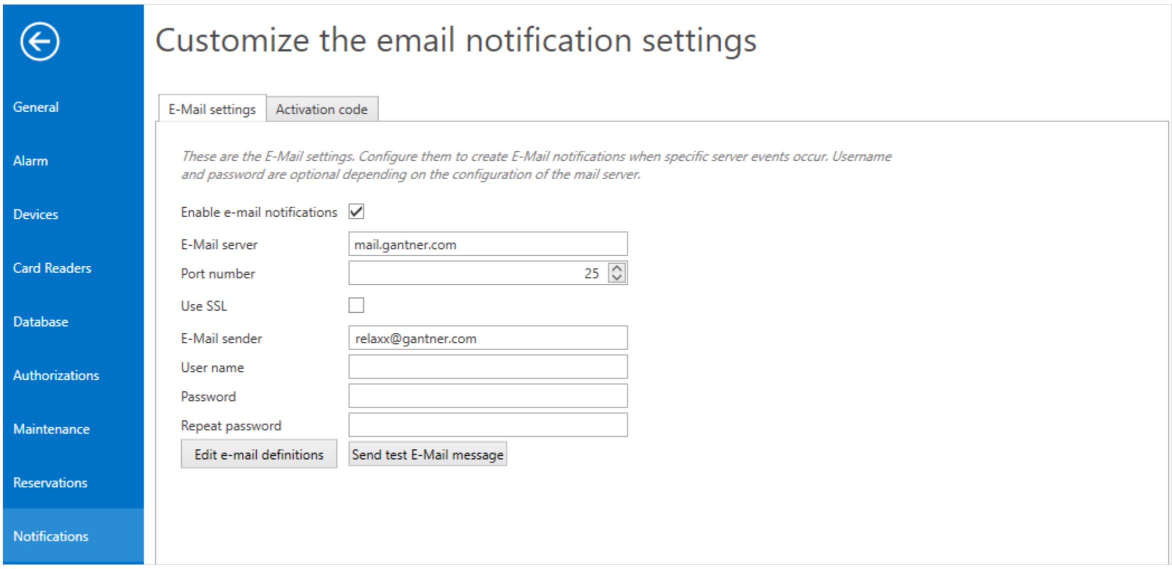
The reservations settings that can be defined here refer to the reservation functionality in Relaxx (see "3.5 Locker Reservations"). The following settings are possible:

- Default duration (reservation):

  Select a default duration from the drop-down menu. This setting is used as the default duration time for all newly-created reservations (refer to "3.5 Locker Reservations"). You can add a new standard duration in the list or change an existing one. This is done in the same way as described in section "2.2.6. Authorizations". Both settings pages use the same list.
- Interval between reservations:

  The value entered here (in minutes) defines the time interval that must pass between the lapsing of the reservation of a locker until the next reservation can be made for this locker.
  NOTE! This setting must match the maintenance settings (refer to "2.2.7 Maintenance").

2.2.9 Notifications



Customize the email notification settings

These are the E-Mail settings. Configure them to create E-Mail notifications when specific server events occur. Username and password are optional depending on the configuration of the mail server.

Enable e-mail notifications ☑
E-Mail server: mail.gantner.com
Port number: 25
Use SSL ☐
E-Mail sender: relaxx@gantner.com
User name
Password
Repeat password

Figure 2.25 *– Notification settings*

Email Settings

On this settings page, the settings regarding email notifications are defined (optional).

- Enable e-mail notifications: Select this option to enable/disable the email notification function.
- E-mail server: Enter the address of your email server in this field.
- Port number: Enter the port number of the email server (standard without SSL = 25, standard with SSL = 465).
- Use SSL: Select this option to use SSL (encryption) for sending emails.

  NOTE! Only "explicit SSL" is supported, where the encrypted connection is requested via STARTTLS.
- E-mail sender: Enter the email address of the sender here. The default address is "relaxx@gantner.com".
- Username / Password: Enter the username and password (if required by the email server) used to log in to the email server.
- Repeat password: Enter the password again to ensure it is correct.

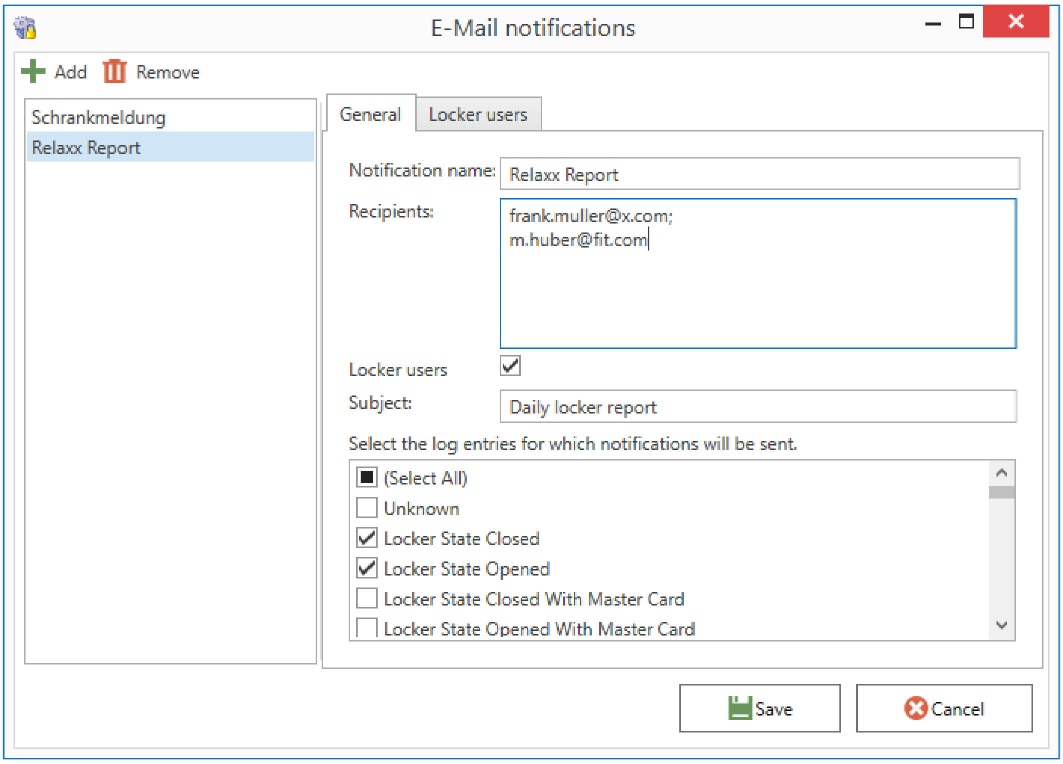
► To confirm that the email settings are correct and that a notification will be sent, click on the “Send test E-Mail message” button and enter a recipient, e.g., your email address.

  - The entered recipient should receive the test email after approximately 1 minute. If the notification is not received, reconfirm that the email settings are correct or contact your network administrator.

NOTE! The email settings defined here operate in combination with the settings defined in the “Scheduler” view. To define when email notifications are sent, you must configure a scheduler definition for exporting data. Refer to “Export data” in “3.6 Scheduler” from more information.

► Click on the “Edit e-mail definitions” button to define specific notification data. Here you can define the type of events, for which a notification email will be sent.

  ○ The following window opens:



Notification name: Relaxx Report

Recipients: frank.muller@x.com;
m.huber@fit.com

Locker users ☑

Subject: Daily locker report

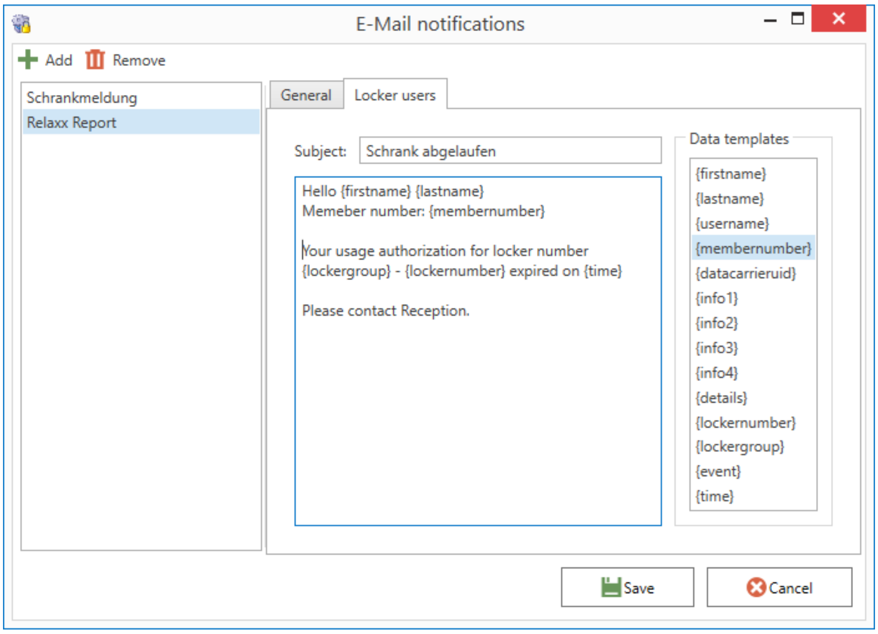
Select the log entries for which notifications will be sent.

■ (Select All)
□ Unknown
☑ Locker State Closed
☑ Locker State Opened
□ Locker State Closed With Master Card
□ Locker State Opened With Master Card

***Figure 2.26** - Email notifications window*

In this window, you can define specific data regarding the notification being sent. You can create notification templates by clicking on the “+ Add” button and defining the following information.

- Notification name: Define a name for the notification, which will be used to identify the notification in the list in the left column.
- Recipients: Enter the email address(es) of those who are to receive the notification. Multiple addresses must be separated by a semicolon (;).
- Locker users: When this option is enabled, an email is sent out to all locker users. The content of the email can be generated automatically for each locker user using placeholders.



Subject: Schrank abgelaufen

Hello {firstname} {lastname}
Memeber number: {membernumber}

Your usage authorization for locker number {lockergroup} - {lockernumber} expired on {time}

Please contact Reception.

{firstname}
{lastname}
{username}
{membernumber}
{datacarrieruid}
{info1}
{info2}
{info3}
{info4}
{details}
{lockernumber}
{lockergroup}
{event}
{time}

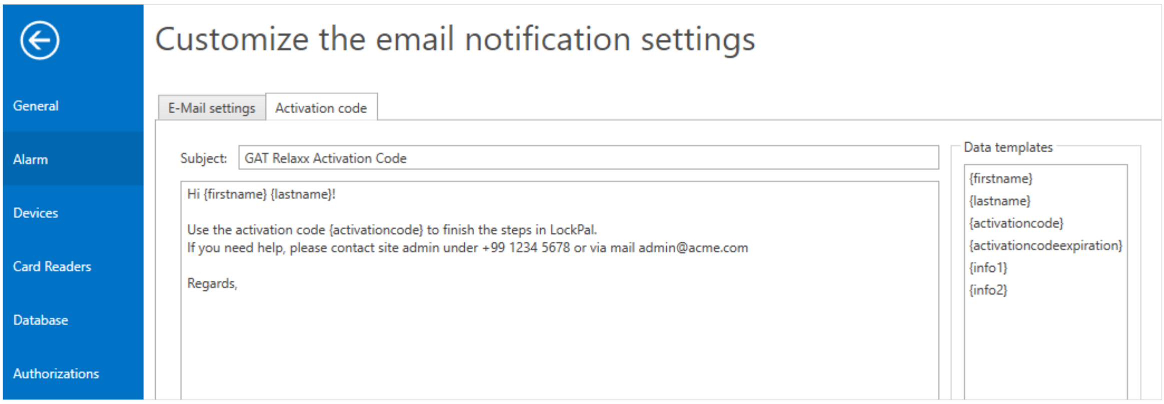
Figure 2.27 *- Email content for the locker users*

Enter the email subject and content into the two text boxes. The placeholders that are replaced with the current data when the email is sent can be selected from the "Data templates" list on the right.

- Subject: Enter a short text here that will be used in the email subject line.
- Log entry selection: Define the events (log entries), for which a notification will be sent. You can select individual log entries or mark “Select all” to include all data types. When a selected event occurs, the recipient(s) will receive an email with information about the event (event type, date and time, channel and controller, used data carrier, etc.).

Activation code for LockPal:

On the "Activation code" tab, you can define an email with subject that will be sent to users of the LockPal App so that the user can register via Relaxx using this app. With the LockPal App, lockers can be remotely controlled from a mobile device via the network. For more information on LockPal, see section “3.11 Remote-Controlled Locker Operation via Mobile Device (REST API)”.



Customize the email notification settings

Subject: GAT Relaxx Activation Code

Hi {firstname} {lastname}!

Use the activation code {activationcode} to finish the steps in LockPal.
If you need help, please contact site admin under +99 1234 5678 or via mail admin@acme.com

Regards,

{firstname}
{lastname}
{activationcode}
{activationcodeexpiration}
{info1}
{info2}

Figure 2.28 *- Email with activation code for LockPal*

You can define the email as follows:

- ► In the "Subject" field, enter the text for the subject of the email.
- ► Define the content of the email in the field below.
- ► In the email text, you can use the placeholders from the list on the right for variable information. Each placeholder is replaced by the relevant information when the email is sent.

- {firstname}:	First name of the person
- {lastname}:	Last name of the person
- {activationcode}:	Here the activation code for LockPal as generated by Relaxx is inserted. With this code, the app linked to the respective user in Relaxx can be activated.
- {info 1}, {info 2}:	Freely definable information fields. These originate from the Relaxx authorizations.

- ► After changes are made to the email, the "Save" button appears below. Click on it to save the changes.

2.2.10 Web Extensions

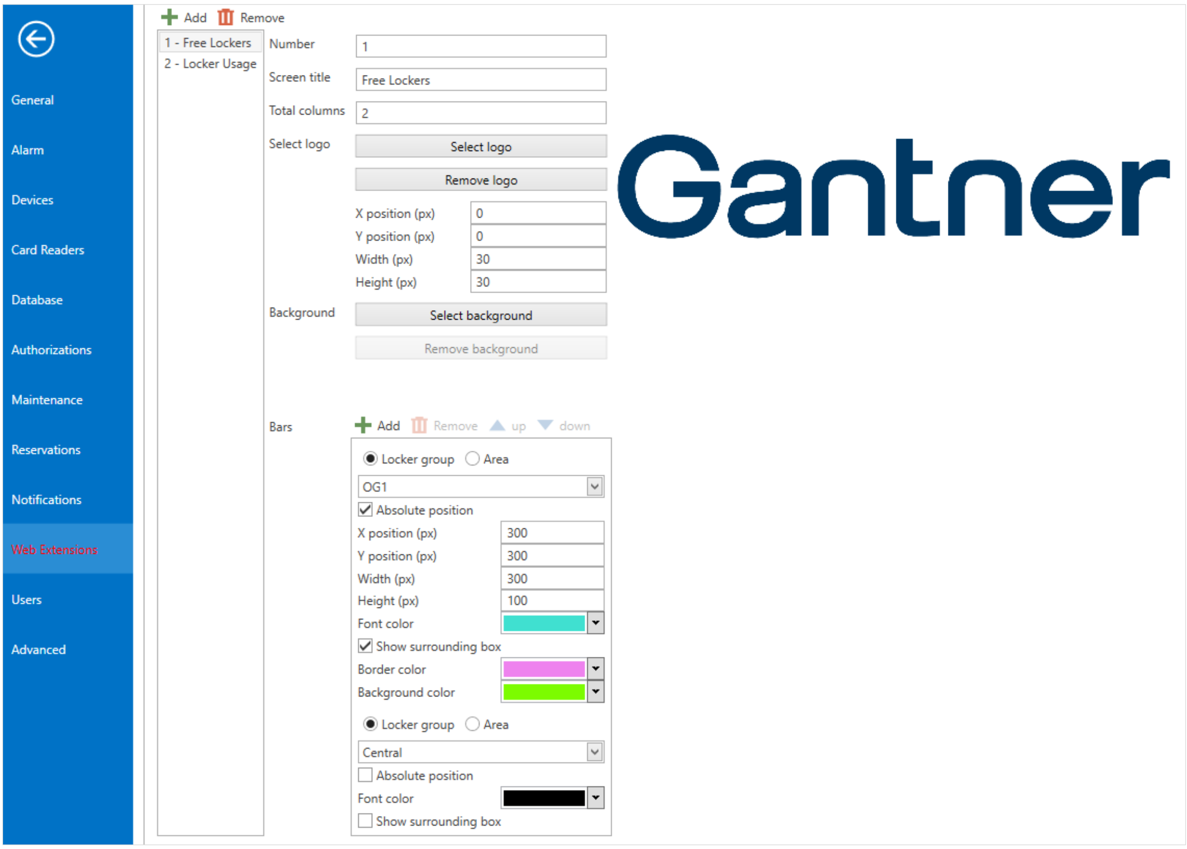
On this page you can configure the web extension settings for locker usage (“Relaxx WEB Locker Usage Screen”) and information display (“Relaxx WEB Locker InfoScreen”). These modules are extensions for the "Relaxx WEB User Interface" application and are only available in the Enterprise License of Relaxx. After acquiring the license, you are able to use the extension in the Relaxx WEB User Interface to display system information (depending on the type of extension) via a web browser.

The Relaxx WEB User Interface is a component of Relaxx that displays status information about the locker system, locker layout, or activated alarms via a standard web browser.

A detailed description of the Relaxx WEB User Interface and web extensions is available in a separate manual.

The settings for the web extensions are divided into two separate tabs.

Locker Usage (Relaxx WEB Locker Usage Screen)



1 - Free Lockers
2 - Locker Usage

Number	1
Screen title	Free Lockers
Total columns	2
X position (px)	0
Y position (px)	0
Width (px)	30
Height (px)	30

Bars

● Locker group ○ Area

OG1

☑ Absolute position

X position (px)	300
Y position (px)	300
Width (px)	300
Height (px)	100
Font color	🟦

☑ Show surrounding box

Border color	🟪
Background color	🟩

● Locker group ○ Area

Central

□ Absolute position

Font color ⬛

□ Show surrounding box

Figure 2.29 *– Settings for the “Locker Usage” extension*

Different “screens” can be defined for the "Locker Usage" extension, which are added to the list on the left. When a screen is selected, its settings are displayed on the right. In this way, screens with different layouts and information content can be configured that can later be used according to the requirements for the information display.

► Select "Add" to add a new screen.

  ○ A new entry is added to the list and the corresponding setting fields are displayed on the right.

► Configure the screen settings. The following settings are available:

- Number: Each screen is assigned a unique number that is used for identification and display in a web browser.
- Screen title: Text used for the screen title in the list.
- Total columns: Number of columns for the progress display. It is recommended not to set this value higher than "4".
- Select / Remove logo: Here you can select (or remove) a logo bitmap graphic (.jpg, .jpeg, .png, .bmp) that is displayed in the upper corner of the info screen. Ensure that the graphic is saved in RGB format.

  You can determine the position of the logo in the "X/Y Position" fields. The values indicate the distance from the upper-left corner of the browser window in which the screen is displayed. The information can be given in pixels or as a percentage of the browser window size:

  - Absolute position:
    Pure numerical values are interpreted as pixels. X Position = 0 and Y Position = 0 is the top-left corner of the browser window.
  - Relative values:
    For numbers with percent signs, the positions are calculated as a percentage of the size of the browser window. Example: X position = 50% means that the top-left edge of the logo is placed horizontally in the center of the browser window.

  With the "Width/Height" fields, you can define the size of the logo. The information can be defined in pixels as a percentage of the browser window size and automatically:

  - Absolute values:
    Pure numerical values are interpreted as pixels. Example: Width = 200, Height = 100 means that the logo is always displayed with a width of 200 pixels and a height of 100 pixels, regardless of the size of the browser window.
  - Relative values:
    For numbers with percent signs, the size is calculated as a percentage of the size of the browser window. Example: Width = 20%, Height = 100 means that the height of the logo is always 100 pixels and the width is 20% of the size of the browser window. The percentage is useful in combination with the automatic value.
    - Automatic:
    If you enter "auto" for the width or height of the logo, the relevant value is determined automatically. Example: Width = auto, Height = 10% means that the logo is displayed with 10% of the height of the browser window. The width is determined automatically, so that the logo is always displayed in the correct aspect ratio.

- Select / Remove background: Here you can select (or remove) a bitmap graphic (.jpg, .jpeg, .png, .bmp) that is inserted as a background image for the info screen. When a graphic is not selected, light gray is used for the background color. **Important:** The graphic must be saved in RGB format, must be smaller than 1 MB, and the file name must not contain any spaces.

- Bars: Assign the lockers to be displayed in the locker usage graphic here. Click on the "Add" button to insert the locker groups and/or locker areas that contain the lockers to be displayed.

  If the "Absolute position" field is marked, you can enter the position and size of the locker occupancy bar in pixels (see description under "Logo"). You can also set the font color and, if desired, insert a frame around the bar.

► Click on “Save” to finalize any changes made to the settings.

Example display:

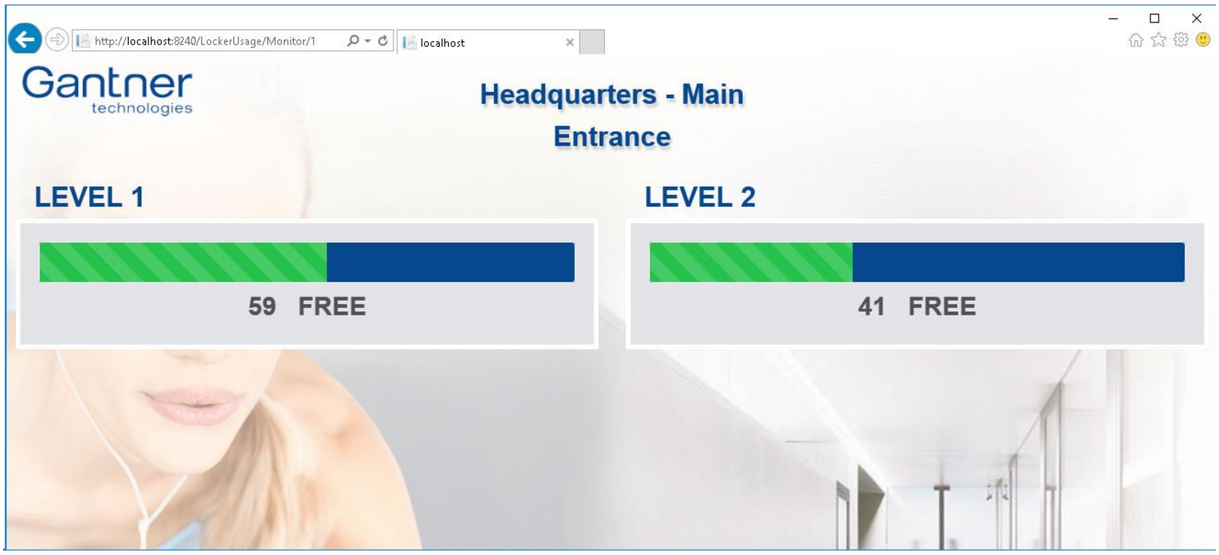
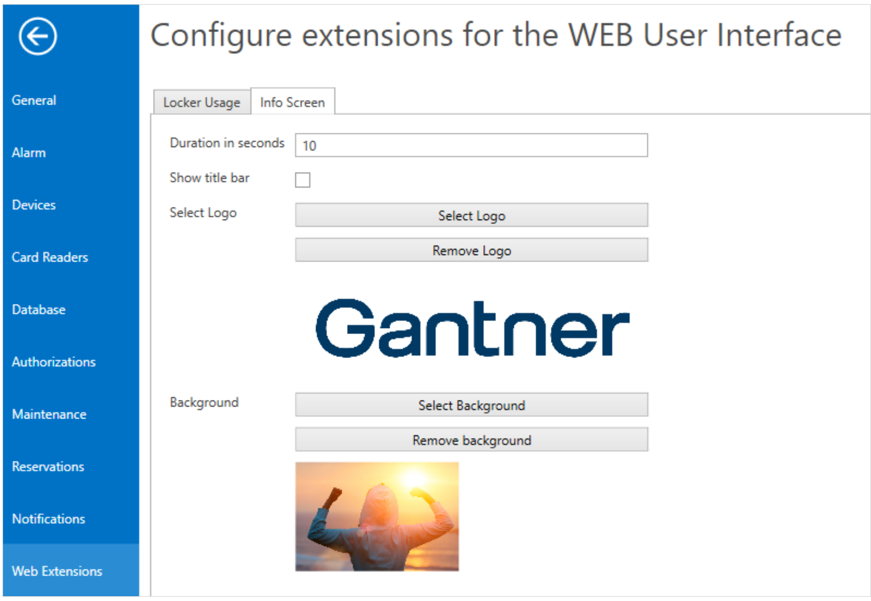

http://localhost:8240/LockerUsage/Monitor/1
localhost
Gantner technologies
Headquarters - Main Entrance
LEVEL 1
59 FREE
LEVEL 2
41 FREE

Figure 2.30 *– Example information screen for the "Locker Usage" extension*

Info Screen (Relaxx WEB Locker Info Screen)



Configure extensions for the WEB User Interface

Duration in seconds: 10

Show title bar: □

Select Logo

Background

Figure 2.31 *– Settings for the “Info Screen” extension*

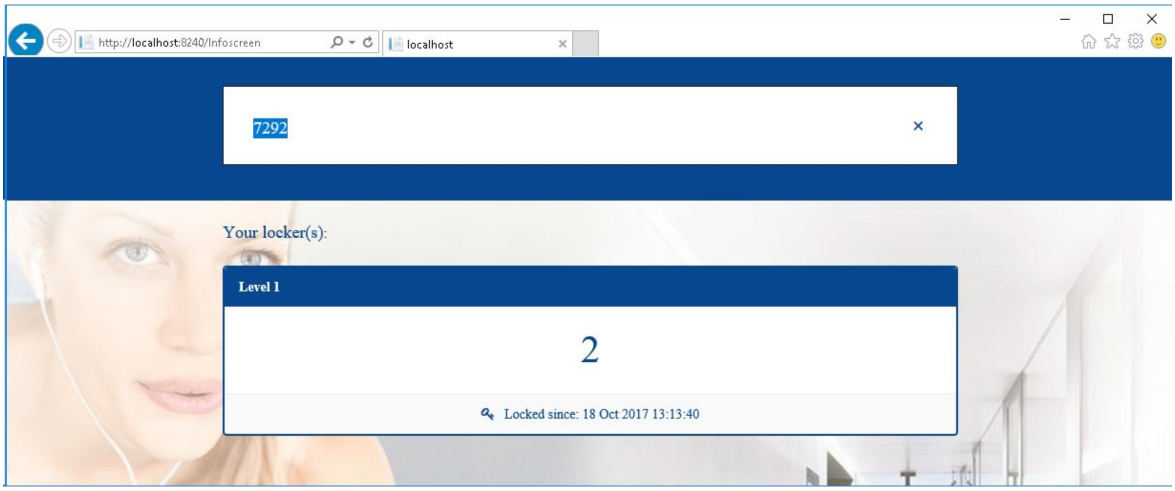
Here you can configure the settings for the "Info Screen" extension. This extension allows locker usage information to be displayed in a web browser for users after their data carrier is read by a connected reader (see Figure 2.32).

The following settings are available:

- Duration in seconds: Define the display time of the info screen in seconds. The default screen is displayed after the set time has elapsed.
- Show title bar: Here you can select whether to display (marked field) or not display (unmarked field) the title bar.
- Select / remove logo: Here you can select (or remove) a logo bitmap graphic (.jpg, .jpeg, .png, .bmp) that is displayed in the upper corner of the info screen.

Select / remove background: Here you can select (or remove) a bitmap graphic (.jpg, .jpeg, .png, .bmp) that is inserted as a background image for the info screen. When a graphic is not selected, light gray is used for the background color.

► Click on “Save” to finalize any changes made to the settings.



7292

Your locker(s):

Level 1

2

Locked since: 18 Oct 2017 13:13:40

__Figure 2.32__ – Example information display for the "Info Screen" extension

2.2.11 Users

On this page, the settings regarding the users of Relaxx are available for configuration. Refer to section “4.3 User Management” for more information.

2.2.12 Advanced

Here you will find additional settings for Relaxx, divided into the following 3 tabs:

- Reports: Select logos for reports.
- Colors: Choose colors for the display of the locker states.
- Communication: Advanced settings for Relaxx communication.

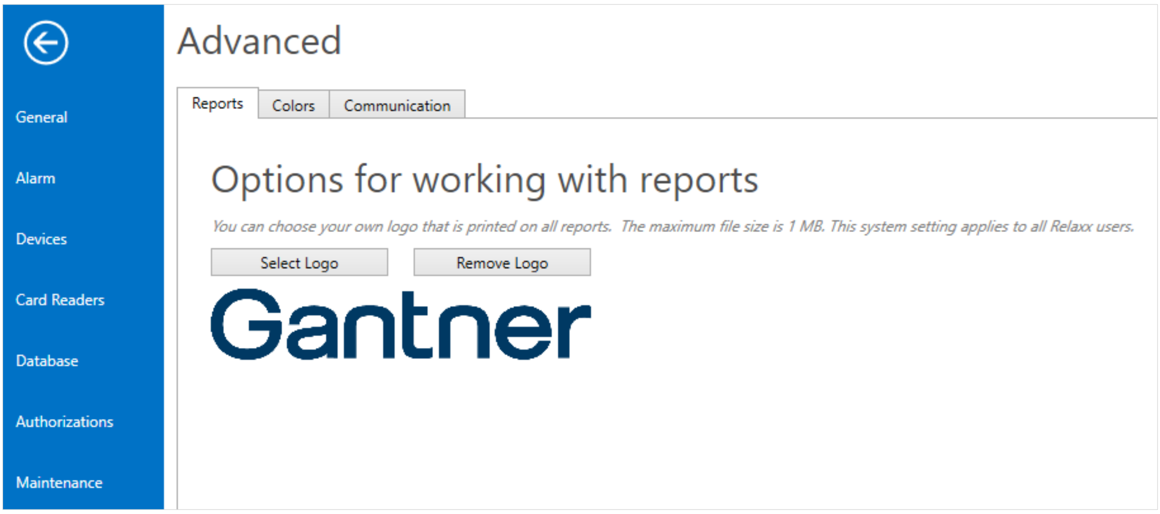
Reports

On this setting page, a logo, such as the logo of the facility where Relaxx is operating, can be selected that will be inserted at the top of the reports. Refer to section “3.8 Reports” for more information regarding the report functionality.

The logo should be in a resolution suitable for use in the reports. Logos are scaled down to suit. To select a logo:

► Click on "Select Logo".
  - The “Explorer” window opens

► Locate the logo file in the local directory then click on “Open”.
  - The logo file is inserted onto the report settings page.



Advanced

Options for working with reports

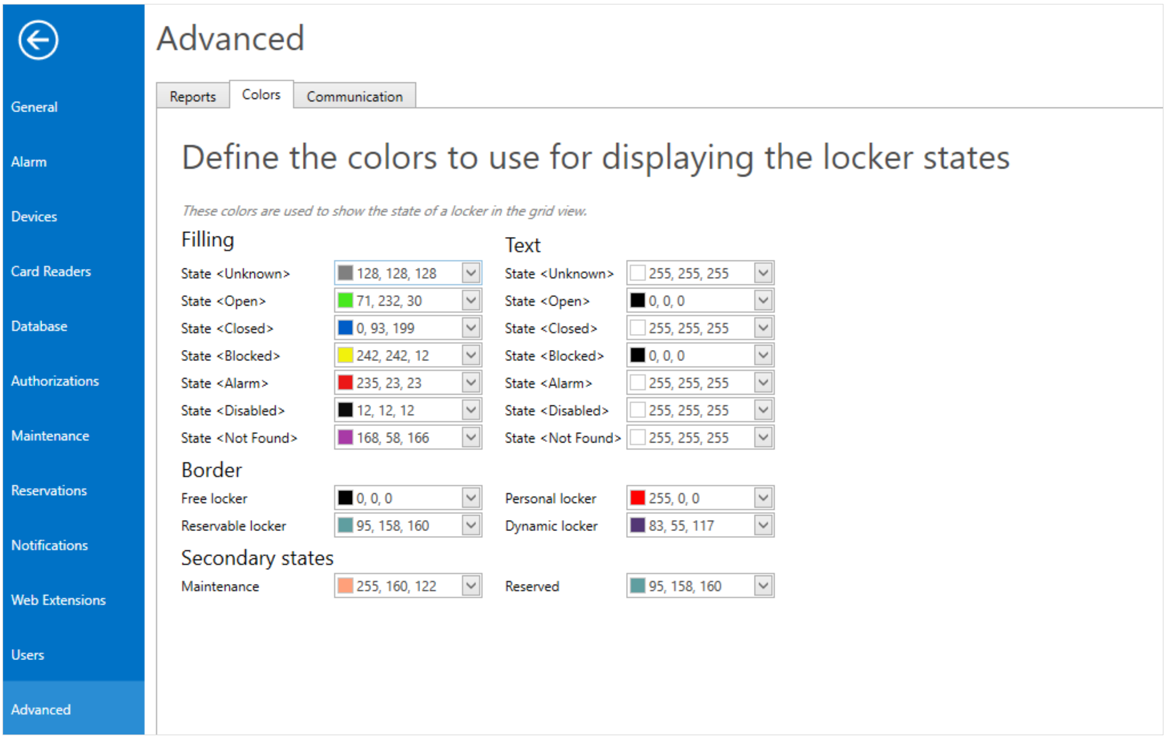
You can choose your own logo that is printed on all reports. The maximum file size is 1 MB. This system setting applies to all Relaxx users.

***Figure 2.33** – Settings for the “Reports” function*

► Click on “Remove Logo” or “Cancel” if you do not want to keep the logo or click on “Save” to confirm the setting.
  - The logo is in included at the top of certain Relaxx reports.

► Click on “Delete logo” to delete an inserted logo.
  - The logo is no longer added to the reports.

Colors



Advanced

Define the colors to use for displaying the locker states

These colors are used to show the state of a locker in the grid view.

Filling		Text	
State <Unknown>	128, 128, 128	State <Unknown>	255, 255, 255
State <Open>	71, 232, 30	State <Open>	0, 0, 0
State <Closed>	0, 93, 199	State <Closed>	255, 255, 255
State <Blocked>	242, 242, 12	State <Blocked>	0, 0, 0
State <Alarm>	235, 23, 23	State <Alarm>	255, 255, 255
State <Disabled>	12, 12, 12	State <Disabled>	255, 255, 255
State <Not Found>	168, 58, 166	State <Not Found>	255, 255, 255

Border

Free locker	0, 0, 0	Personal locker	255, 0, 0
Reservable locker	95, 158, 160	Dynamic locker	83, 55, 117

Secondary states

Maintenance	255, 160, 122	Reserved	95, 158, 160

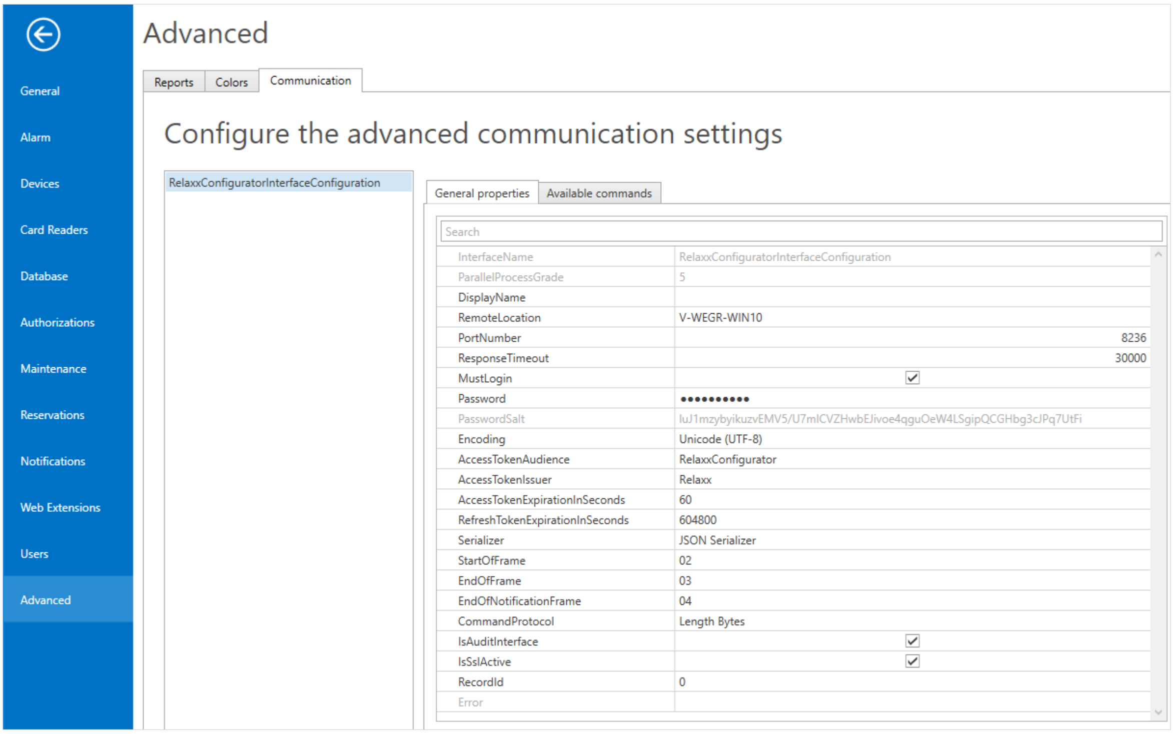
***Figure 2.34** – Color settings for the locker states*

On this page, the color settings used to represent the different locker states are defined. Refer to section “3.3.7 Color Legend” for more information.

If desired, the default colors can be individually changed in the following manner.

- ► In the "Filling" area, the background color of the described state field can be determined.
- ► In the "Border" area, the colors of the lines used to indicate a free locker, a rental locker and a reservable locker are defined.
- ► In the "Text" area, the color of the text in the state fields is determined.
- ► In the "Secondary states" area, the colors of the marking fields used for displaying the maintenance and reserved state in the locker fields of the overview are determined.
- ► Save any changes made to the settings by clicking the "Save" icon.

Communication



Advanced

Configure the advanced communication settings

RelaxxConfiguratorInterfaceConfiguration

InterfaceName	RelaxxConfiguratorInterfaceConfiguration
ParallelProcessGrade	5
DisplayName	
RemoteLocation	V-WEGR-WIN10
PortNumber	8236
ResponseTimeout	30000
MustLogin	☑
Password	●●●●●●●●●●
PasswordSalt	luJ1mzybyikuzvEMV5/U7mICVZHwbEJivoe4qguOeW4LSgipQCGHbg3cJPq7UtFi
Encoding	Unicode (UTF-8)
AccessTokenAudience	RelaxxConfigurator
AccessTokenIssuer	Relaxx
AccessTokenExpirationInSeconds	60
RefreshTokenExpirationInSeconds	604800
Serializer	JSON Serializer
StartOfFrame	02
EndOfFrame	03
EndOfNotificationFrame	04
CommandProtocol	Length Bytes
IsAuditInterface	☑
IsSslActive	☑
RecordId	0
Error	

Figure 2.35 *- Communication settings – General properties*

The communication settings define the parameters used by Relaxx for the communication with the locker locking system and the GANTNER devices.

► Select the entry "RelaxxConfiguratorInterfaceConfiguration" in the left column.

  ○ The possible communication settings are displayed on the right.

► Set the corresponding values and option fields in the tab "General properties". For a default installation, keep the default settings. Important settings are:

- RemoteLocation: The IP address or network name of the PC/server, on which the Relaxx service runs. In the event of a local installation, enter "localhost" here.
- PortNumber: The port number for the connection with the Relaxx service (default = 8236). This number must not be blocked by a firewall or similar.
- ResponseTimeout: Maximum time (in milliseconds) for waiting for an answer from the service before an error message is generated.
- MustLogin: Defines whether a login is required for the connection between a client and the service. Keep these default settings and the following password, otherwise it may happen that Relaxx no longer can connect to the service.

Only the fields written in black can be changed. Fields written in light gray cannot be changed.

► In the "Available commands" tab, the commands that Relaxx should process can be checked. The default setting is that all commands are checked.

3 OPERATION

After starting Relaxx the user must log in with their username and password. There are default users with assigned passwords and roles integrated into Relaxx (refer to "4.3.1. Default Users"). The role assigned to the user defines which functions are available to them in Relaxx. This chapter describes the operation for the SYSTEM user, who is able to access all software functions.

The operation of Relaxx can be roughly divided into the following tasks. Instructions are provided for these tasks in the following chapters.

- 3.2 - Configuring Devices and Systems (communications channels, controllers, locks, etc.).
- 3.3 - Operating / Monitoring the Locker System and GANTNER Devices (daily operation)
- 3.4 - Administration of Visitors / Data Carriers (Authorization List)
- 3.5 - Locker Reservations
- 3.6 - Scheduler
- 3.7 - Log Entries
- 3.8 - Reports

After installing Relaxx and configuring the software settings (refer to the previous chapter), the devices and the system must be configured. Please read chapter "3.2. Configuring Devices and Systems" first in order to configure your system accordingly. Any further configuration required for Relaxx depends on the desired functionality of the system, e.g., establishing an authorization list. Refer to the chapters listed above for further instructions.

The "Dashboard" is available to monitor the locker system during operation (see "3.3.1 Dashboard") and is displayed after starting and logging in to Relaxx. Clearly displayed on this page are the current occupancy and time usage statistics of the lockers.

3.1 Software Window Elements

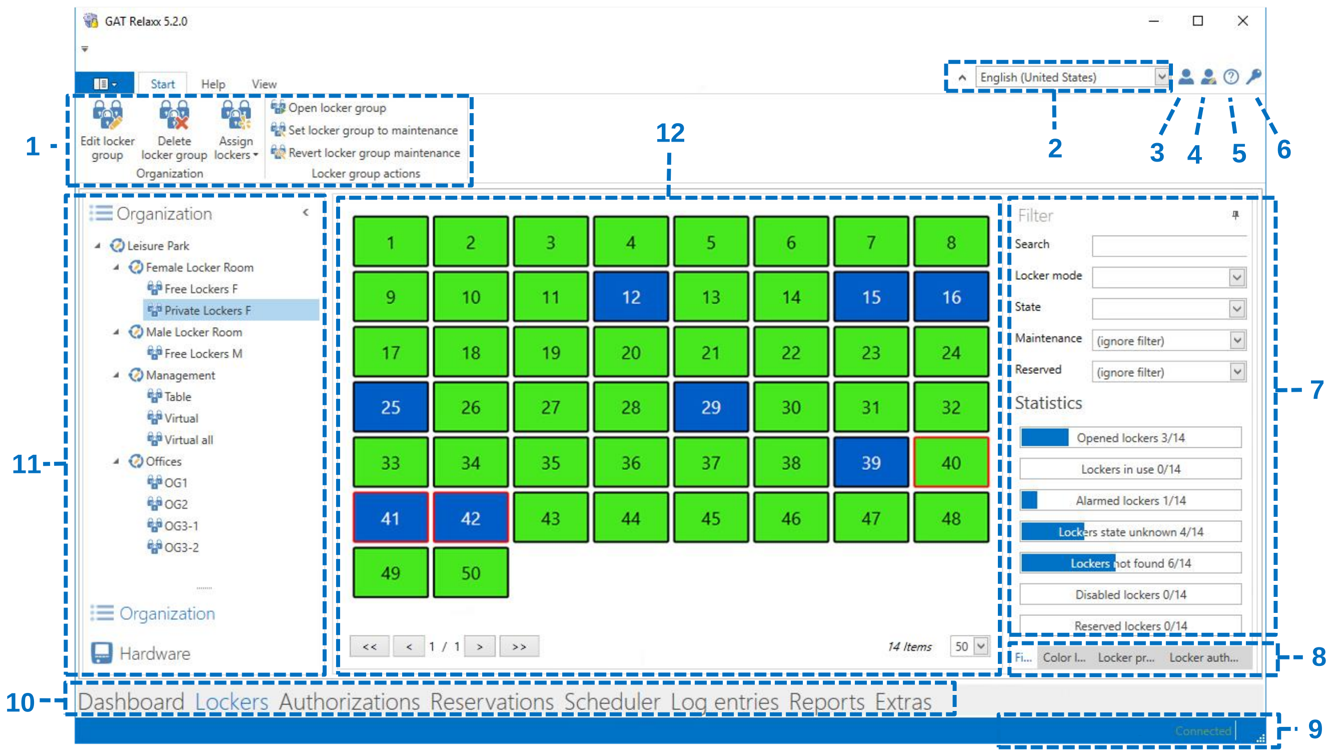


Figure 3.1 – Key elements of the Relaxx software window - Lockers

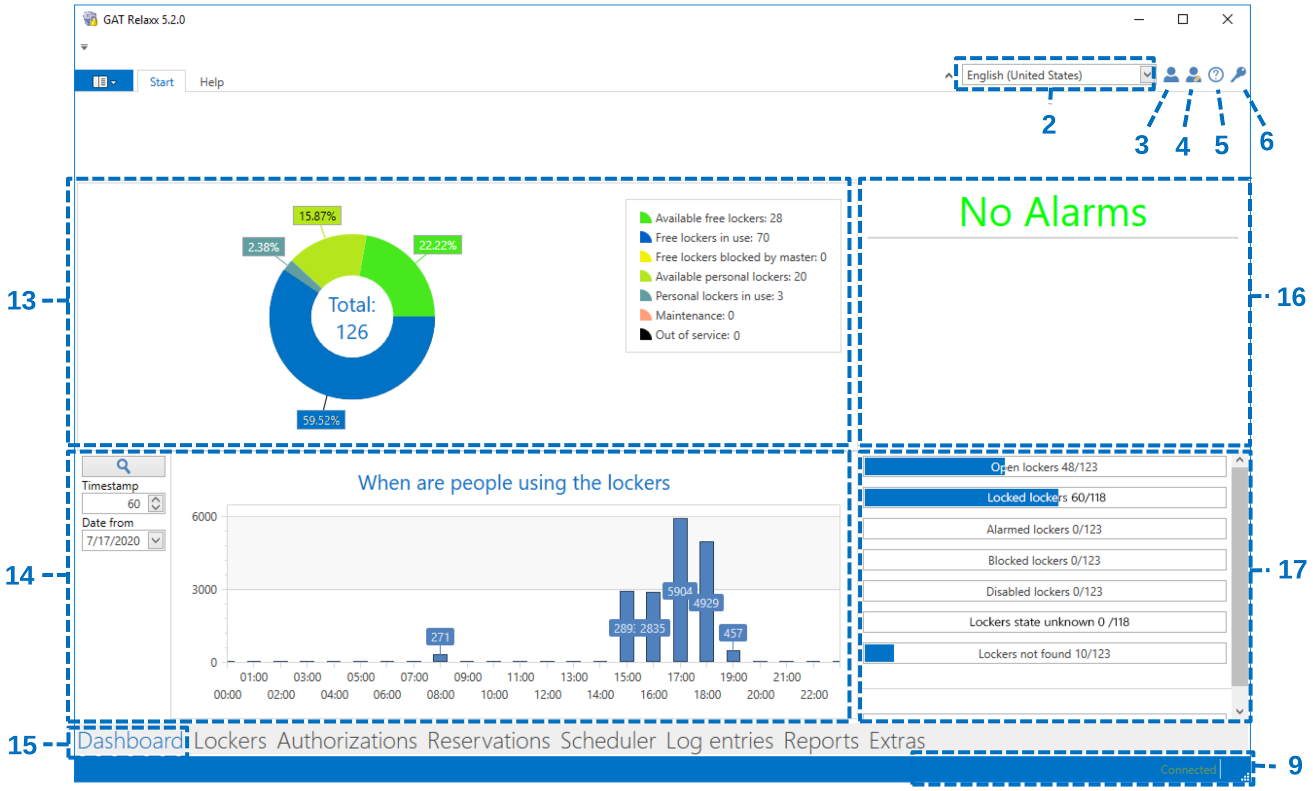


Figure 3.2 - Key elements of the Relaxx software window - Dashboard

1 Function bar: This area shows all the functions that are available for the currently selected view (see 10).

2 Language selection: Click on the drop-down menu to change the language of the Relaxx user interface. Restarting Relaxx is not necessary.

3 Logout user: Click on this icon to log out of Relaxx.

4 Change password: Click on this icon to change your password.

5 About Relaxx: Click on this icon to view detailed information about the current version of Relaxx.

6 Licensing: Click on this icon to view software licensing information and to add new license codes (e.g. for expansion modules). You can also activate the base license of Relaxx with this icon.

7 Locker information area: Information, statistics, and other tools for the locker selected in the overview (12) are available in this area.

8 Locker information tabs: Four tabs are provided here for selecting the type of information displayed in the locker information area (7).

9 Status bar: The status bar indicates whether the Relaxx service is running and whether the connection is ok.

10 Views: Depending on the required task, the different views of Relaxx are available for selection here.

11 Organization / Hardware system overview: This area is where the two main components of the locker system are displayed. Select between Organization and Hardware at the bottom of the area to display the system structure.

<u>Organization</u>:

Here all lockers in the system are logically organized into areas and groups of lockers (e.g., male changing room, female changing room, etc.). Clicking on an area or locker group displays the corresponding lockers and their respective states in the locker overview (12).

The way lockers are organized in this area represents a logical assignment and does not represent the physical connection of lockers to controllers.

<u>Hardware:</u>

The communication channels and their assigned controllers, Access devices, and Info devices are listed here. Information and configuration options are displayed for each device after selection in the list. The following colored icons indicate the status of each device:

🟩 = Device is in operation

🟨 = Connection to device lost (trying to reconnect)

🟥 = Connection to device stopped (not trying to reconnect)

🟨 = Device initializing, or bookings being read

⬜ = Device disabled

❓ = Device status unknown

⚠ = Device cannot be started (too few or missing licenses)

12 Locker overview / Device information: Depending on the system selected in the organization / hardware system overview (11), different information is displayed here.
<u>Locker overview</u>:
When an area or a locker group is selected, the lockers assigned to the selected area or group are displayed together with the current locker states.
<u>Device information</u>:
When a hardware device (controller, Access device, Info device, etc.) is selected, this area displays the configuration settings of the device.

13 Live locker use: The quantity of lockers for each locker state (occupied and unoccupied free lockers and personal lockers, etc.). The display consists of a pie graph that clearly shows the numerical relationships. The graph is updated automatically. The color coding of the various locker states is described in the legend.

14 Locker usage in time: The bars show how many lockers were used and at what times. The time scale can be set using the fields on the left.

15 Dashboard view: Clicking this link opens the dashboard view.

16 Alarm display: Display of the currently reported alarms, e.g., locker opening, in the system.

17 Live locker status: Here you see an overview of all current locker status. The bar graphs are updated continuously.

3.2 Configuring Devices and Systems

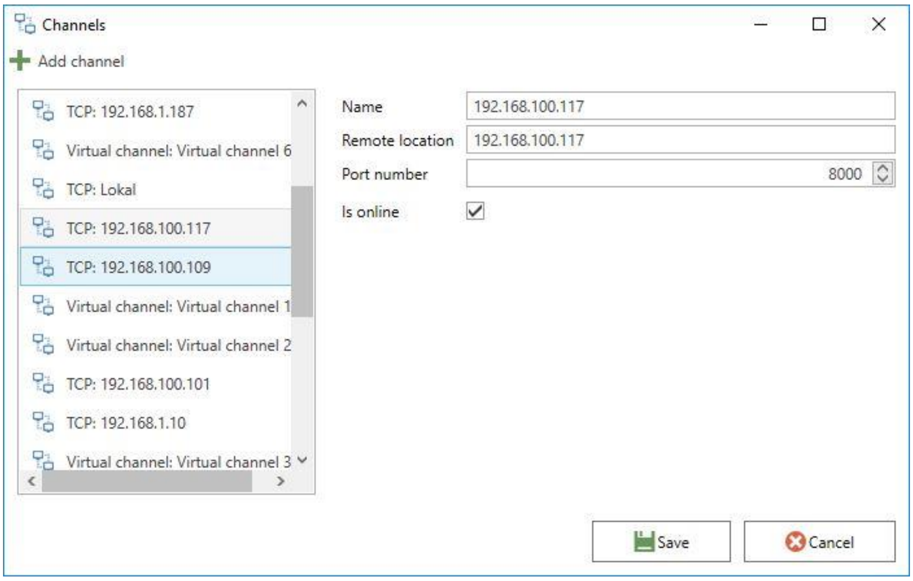
After installing Relaxx, complete the following steps to configure the locker system.

3.2.1 Communication Channels

The devices within the system can communicate with the server or Relaxx via different methods, which is why Relaxx defines communication channels with set properties for each connection type. Every device added to the Relaxx system must therefore be assigned to the correct communication channel.

The communication channels can be edited while adding the devices to Relaxx (refer to "3.2.2 Setting up the Hardware System") or on the respective configuration pages of the devices in the hardware list (refer to "3.2.3 Modifying the Device Settings").

► Click on "Configure channels" while adding a device or on the device configuration page.
 o The "Channels" window opens.



Channels

Add channel

- TCP: 192.168.1.187
- Virtual channel: Virtual channel 6
- TCP: Lokal
- TCP: 192.168.100.117
- TCP: 192.168.100.109
- Virtual channel: Virtual channel 1
- Virtual channel: Virtual channel 2
- TCP: 192.168.100.101
- TCP: 192.168.1.10
- Virtual channel: Virtual channel 3

Name: 192.168.100.117
Remote location: 192.168.100.117
Port number: 8000
Is online: ☑

***Figure 3.3** – Define channels*

► Select a channel from the displayed list in order to display and edit the channel settings.

► To create a new channel, click on "Add channel" and select a channel type from the menu.

► Enter a suitable name for the new channel together with the other channel data. Depending on the channel type, different data is required.
- TCP/IP: IP address in the IPv4 format and port number (default = 8000).
- Serial: Serial PC interface (COM Port) and baud rate.
- Virtual channel: Only the name is required. Used for virtual test lockers.

► Select the "Is online" option to operate the locker system in online mode.

► Close the window via the "X" icon in the upper-right corner.

Starting and stopping communication channels

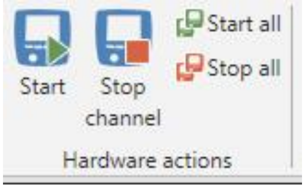


Figure 3.4 *– Hardware actions*

The "Start" and "Stop channel" buttons in the "Hardware actions" area allow you to start and stop the communication channels selected in the hardware list. The "Start all" and “Stop all” buttons start or stop all communication channels simultaneously.

When a channel is stopped, Relaxx does not communicate with the connected devices and the devices operate in offline or emergency mode during this time. Depending on their configuration, the devices perform an autonomous authorization check until the channel is started again.

3.2.2 Setting up the Hardware System

The hardware system is defined by adding communication channels, controllers, and locks in the hardware view of Relaxx. If GANTNER Info or Access devices are also used in the system, they are configured in the same way. Once devices are added to the hardware system, they can be easily located via the “Filter” field at the top of the list, a feature that is especially useful in larger systems where many devices are in operation. Enter an identifier such as the device name to filter the hardware list and display only devices that match the search criteria.

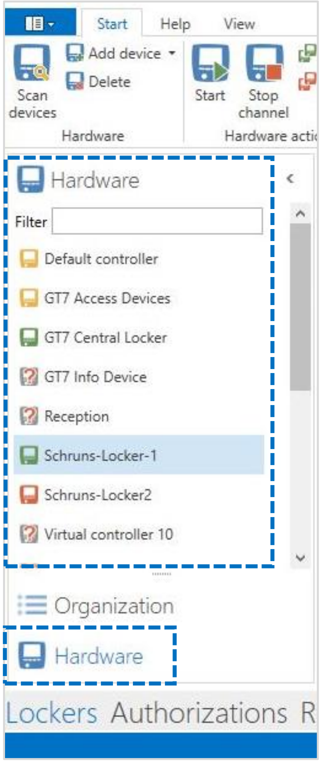


Figure 3.5 *- Relaxx hardware configuration*

There are two ways to add a new device:

a) Adding it manually by selecting the type of device

b) Scanning the local network for existing devices

a) Manually adding a new device

► Change to the "Lockers" view and select “Hardware”.

► Click on “Add device”.

- A selection list with the following devices opens.

- NET.Controller Main: GAT NET.Controller M 7000 or GAT NET.Controller M 7020 controller that is used for the GAT NET.Lock 7000 or GAT NET.Lock 7020 locker locks.

  Note: The GAT SMART.Controller S 7000 together with the GAT SMART.Lock 7001 locker locks can also be used with a GAT NET.Controller M 70x0. In this case, also select "NET.Controller Main".
- G7 Main: A GC7.2000 M, GC7.2000 M lite, or GC7.3000 controller with G7 Main Controller App, which is used for the GAT NET.Lock 7000 or GAT NET.Lock 7020 locker locks.

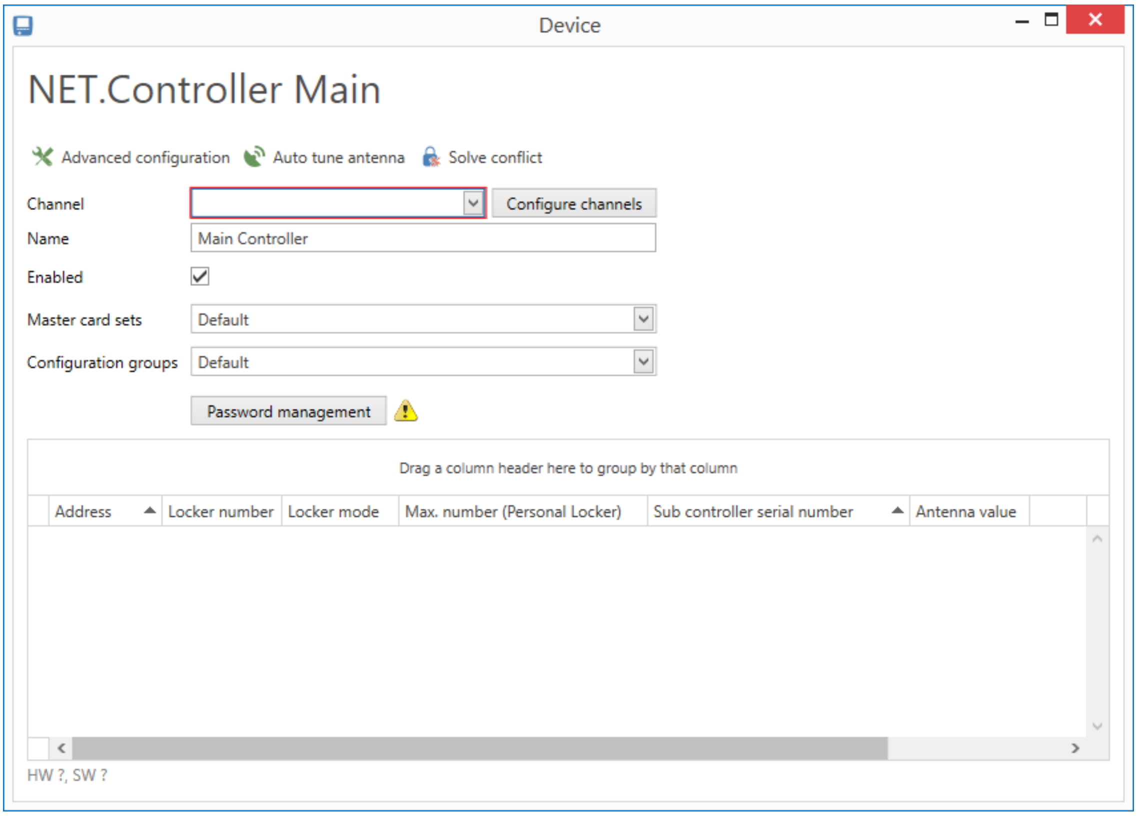
  Note: The GAT SMART.Controller S 7020 can also be used with a G7 Main Controller for the GAT SMART.Lock 7001 locks. In this case, "G7 Main" can also be selected.
- GT7 Central Locker: For the central control of GAT SMART.Lock 7001 or GAT NET.Lock 70x0 locker locks.
- GT7 Info: A GT7 terminal of the latest generation, used as an information terminal.
- GT7 Access: A GT7 terminal of the latest generation, used as an access control terminal.
- Info 6000 Series: A GAT 6000 Series information terminal.
- Access 6000 Series: A GAT 6000 Series access control terminal.
- SMART.LockAxx: Central terminal for the GAT SMART.Lock 7001 locker locks.
- Virtual device: A device with no actual connection to the PC or Relaxx (e.g., for test purposes).

► Select the device to be added.

- A “Device” window opens where the device settings can be configured. The settings available in the window depend on the type of device selected (see relevant description on following pages).

NET.Controller Main (GAT NET.Lock 70x0 System or GAT SMART.Lock 7001 + GAT NET.Controller M 70x0)

This option adds a “NET.Controller Main” communication channel to which either one or more GAT NET.Controller S (for GAT NET.Lock 70x0 locker locks) and/or GAT SMART.Controller S 7020 (for GAT SMART.Lock 7001) can be connected.



NET.Controller Main

Channel	
Name	Main Controller
Enabled	☑
Master card sets	Default
Configuration groups	Default

Address	Locker number	Locker mode	Max. number (Personal Locker)	Sub controller serial number	Antenna value

HW ?, SW ?

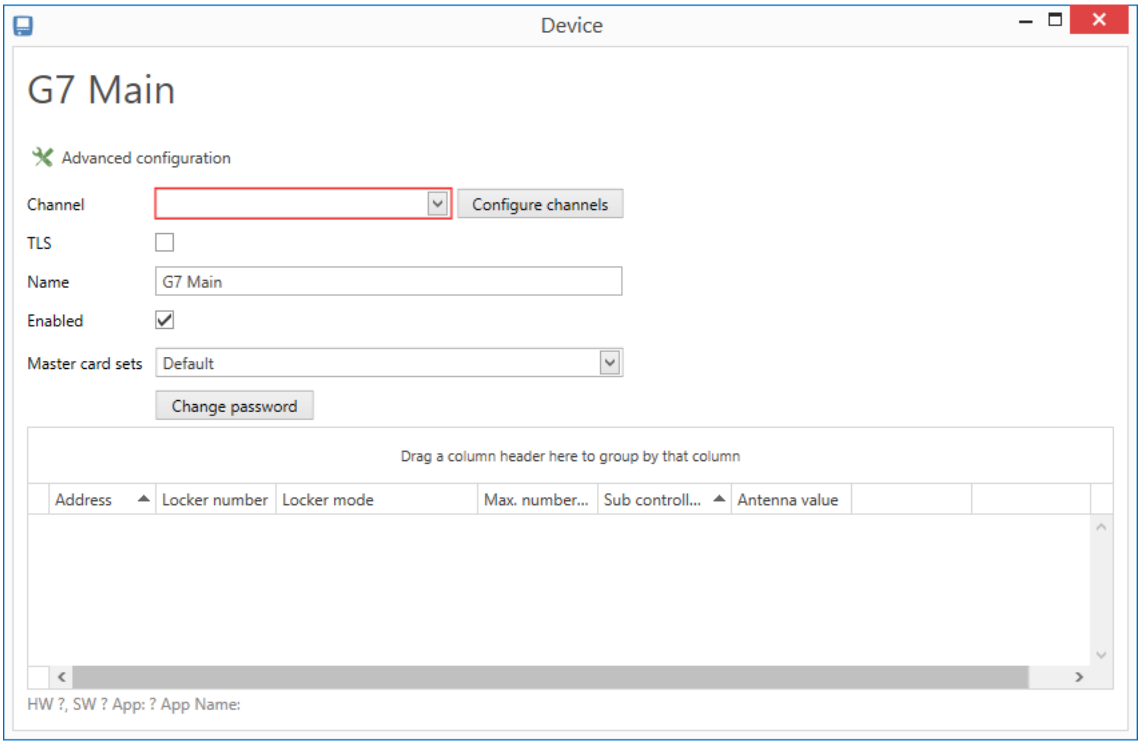
__Figure 3.6__ – Adding a NET.Controller Main channel

- ► Select the communication channel to which the GAT NET.Controller M 70x0 is connected. Either add an available channel from the selection list or define a new channel with the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".
  NOTE! For the GAT NET.Controller M 70x0, a TCP/IP channel only can be used.
- ► Enter a name for the controller or channel. The controller will be displayed with this name in the hardware list.
- ► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- ► Click on “Save“. The new controller or channel is inserted into the hardware list.
  - o The new channel is inserted into the hardware list.

NOTE! In addition to the exclusive use of the GAT Lock Controller 5010 or the GAT NET.Controller 70x0 in a system, it is also possible to use a GAT NET.Controller M 70x0 main controller together with a GAT Lock Controller 5010 as sub controller. In this case, select "NET.Controller Main" as the controller type.

G7 Main (GC7.2000 M and GC7.2000 M lite)

This option adds a “G7 Main” channel to which either one or more GAT NET.Controller S (for the GAT NET.Lock 70x0 locker locks) or GAT SMART.Controller S 7020 (for the GAT SMART.Lock 7001) can be connected.



Device

G7 Main

Advanced configuration

Channel: [ ] Configure channels

TLS: □

Name: G7 Main

Enabled: ☑

Master card sets: Default

Change password

Drag a column header here to group by that column

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value

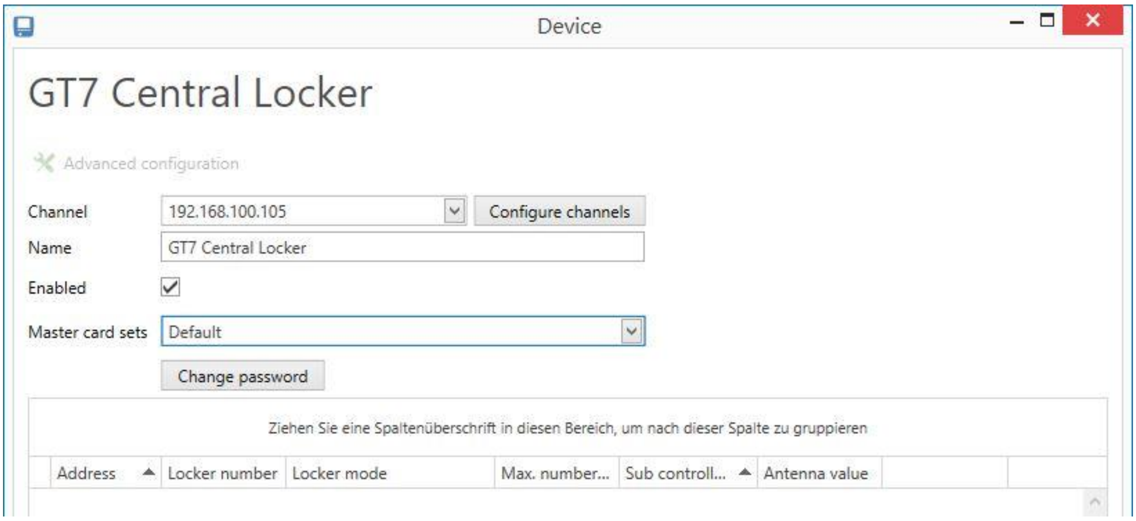
HW ?, SW ? App: ? App Name:

***Figure 3.7** – Adding a GC7.2000 M (lite) Controller channel*

- ► Select the communication channel to which the G7 main controller is connected. Either add an available channel from the selection list or define a new channel with the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".
  NOTE! For the G7 main controller, a TCP/IP channel only can be used.
- ► Enter a name for the controller or channel. The controller will be displayed with this name in the hardware list.
- ► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- ► Click on “Save“. The new controller or channel is inserted into the hardware list.
  - o The new channel is inserted into the hardware list.

GT7 Central Locker (Central terminal for the GAT SMART.Lock 7000 System)

This option adds a GT7 Central Locker communication channel to which a GT7 Central Locker terminal (for the GAT SMART.Lock 7001 locks) can be assigned.



Device

GT7 Central Locker

Channel: 192.168.100.105

Name: GT7 Central Locker

Enabled: ☑

Master card sets: Default

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value

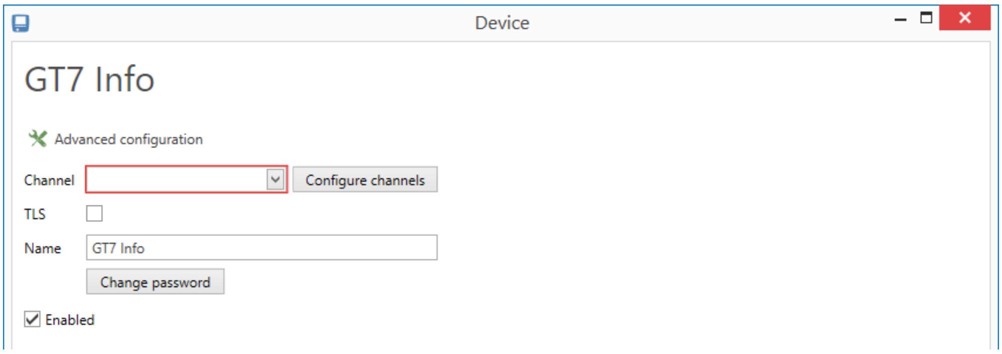
Figure 3.8 – *Adding a GT7 Central Locker channel*

- ► Select the communication channel to which the device is connected. Either add an available channel from the selection list or define a new channel via the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".

  NOTE! Only a TCP/IP channel can be used for this device.
- ► Enter a name for the device or channel. The device is displayed with this name in the hardware list.
- ► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- ► Click on “Save“.
  - o The new channel is inserted into the hardware list.

GT7 Access / GT7 Info

This option adds a channel to which a GT7 device with Access App ("GT7 Access") or a GT7 device with Info App ("GT7 Info") can be added. The settings are identical for both device types. The following figure shows the window for a GT7 with Info App as an example.



Device

GT7 Info

Channel:

TLS: □

Name: GT7 Info

☑ Enabled

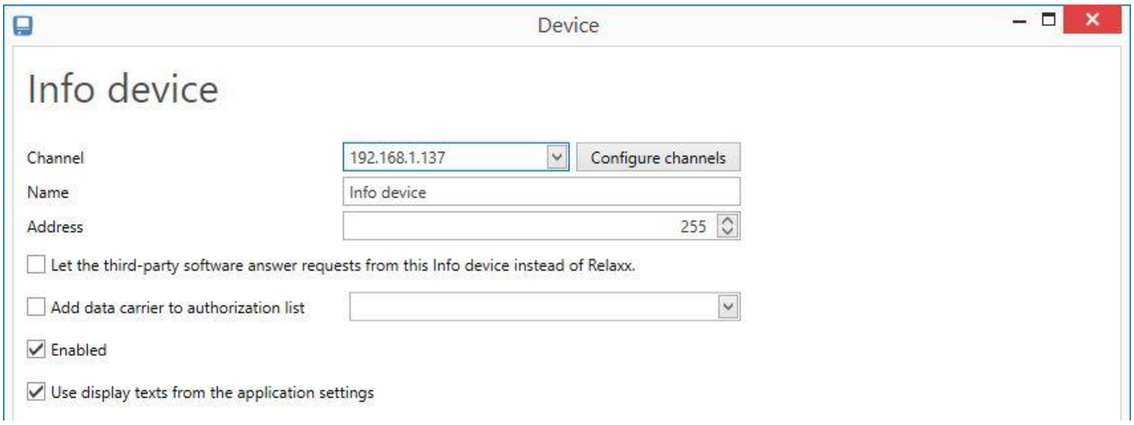
Figure 3.9 – *Adding a GT7 Info channel*

- Select the communication channel to which the device is connected.

  NOTE! Only a TCP/IP channel can be used for this device.
- Either add an available channel from the selection list or define a new channel via the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".
- Enter a name for the device or channel. The device is displayed with this name in the hardware list.
- For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- Click on “Save”.
  - The new channel is inserted into the hardware list.

Info 6000 Series

This option adds a communication channel for a GAT 6000 Series Info device, which displays relevant information to visitors within a facility.



Device

Info device

Channel: 192.168.1.137

Name: Info device
Address: 255

□ Let the third-party software answer requests from this Info device instead of Relaxx.

□ Add data carrier to authorization list

☑ Enabled

☑ Use display texts from the application settings

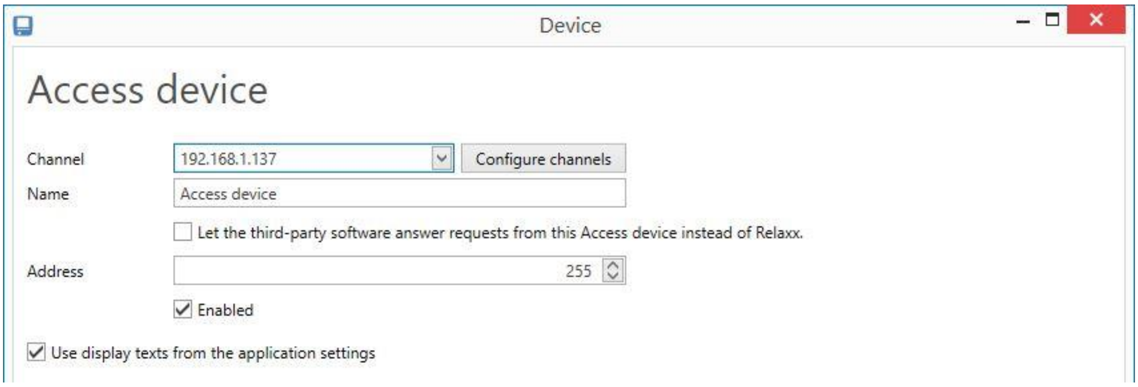
***Figure 3.10** – Adding an Info device*

- Select the communication channel to which the device is connected. Either add an available channel from the selection list or define a new channel via the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".

  NOTE! Only a TCP/IP channel can be used for this device.
- Enter a name for the device or channel. The device is displayed with this name in the hardware list.
- Leave the default “Address” setting at 255.
- For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- Click on “Save”.
  - The new channel is inserted into the hardware list.

Access 6000 Series

This option adds a communication channel for a GAT 6000 Series Access device, which provides access control for visitors at entry/exit points such as turnstiles and doors.



Device

Access device

Channel: 192.168.1.137

Name: Access device

□ Let the third-party software answer requests from this Access device instead of Relaxx.

Address: 255

☑ Enabled

☑ Use display texts from the application settings

***Figure 3.11** – Adding an Access device*

- ► Select the communication channel to which the device is connected. Either add an available channel from the selection list or define a new channel via the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".

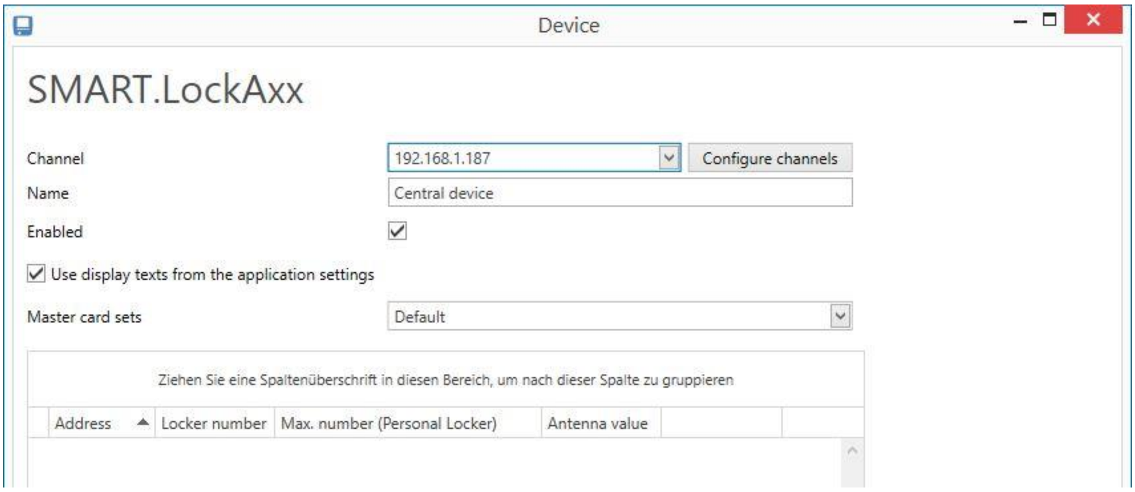
  NOTE! Only a TCP/IP channel can be used for this device.
- ► Enter a name for the device or channel. The device is displayed with this name in the hardware list.
- ► Leave the default “Address” setting at 255.
- ► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- ► Click on “Save”.
  - o The new channel is inserted into the hardware list.

SMART.LockAxx (Central Terminal for the GAT SMART.Lock 7000 System)

This option adds a GAT SMART.LockAxx 6350 communication channel, to which further GAT SMART.Controller S 7000 (for the GAT SMART.Lock 7001 locks) can be connected later.

First, a query box opens asking whether the GAT SMART.Lock 7001 system should operate in personal locker mode. The operating mode must be defined when adding a GAT SMART.Lock 7001 system as this setting cannot be changed at a later stage and does not refer to an individual lock but is set at the controller level.

► Select "Yes" if the GAT SMART.Lock 7001 is to operate in personal locker mode, otherwise select "No".
  - The following window opens.



Device

SMART.LockAxx

Channel: 192.168.1.187

Name: Central device

Enabled: ☑

☑ Use display texts from the application settings

Master card sets: Default

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Address	Locker number	Max. number (Personal Locker)	Antenna value

Figure 3.12 – Adding a GAT SMART.LockAxx 6350

► Select the communication channel, to which the GAT SMART.LockAxx 6350 is connected. Either add an available channel from the selection list or define a new channel with the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".
NOTE! Only a TCP/IP channel can be used for the GAT SMART.LockAxx 6350.

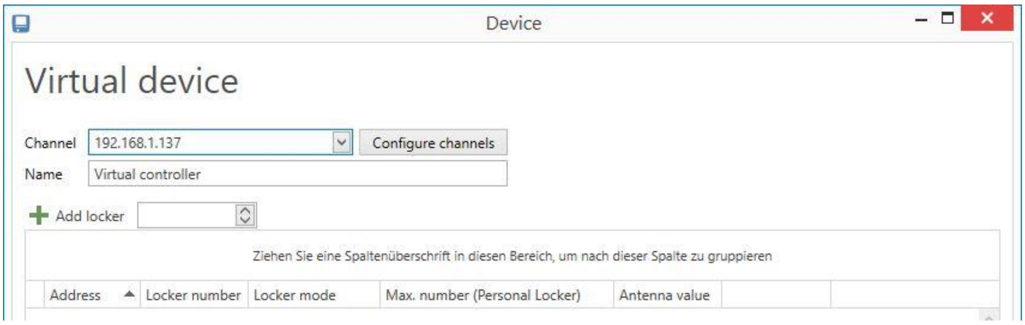
► Enter a name for the GAT SMART.LockAxx 6350 or channel. The GAT SMART.LockAxx 6350 will be displayed with this name in the hardware list.

► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".

► Click on “Save”.
  - The GAT SMART.LockAxx 6350 or channel is inserted into the hardware list.

Virtual device

This option adds a virtual, non-existent controller with locks (e.g., for test purposes).



Device

Virtual device

Channel: 192.168.1.137

Name: Virtual controller

Configure channels
Add locker
Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren
Address
Locker number
Locker mode
Max. number (Personal Locker)
Antenna value

***Figure 3.13** – Adding a virtual device*

- ► Select the communication channel, to which the virtual device is connected. Either add an available channel from the selection list or define a new channel with the "Configure channels" button. For further information regarding the communication channels, refer to "3.2.1 Communication Channels".

  NOTE! Please note that a virtual device requires a virtual channel.
- ► Enter a name for the virtual controller or channel. The controller will be displayed with this name in the hardware list.
- ► For further information regarding the configuration, refer to "3.2.3 Modifying the Device Settings".
- ► Click on “Save”.
  - o The virtual controller or channel is inserted into the hardware list.

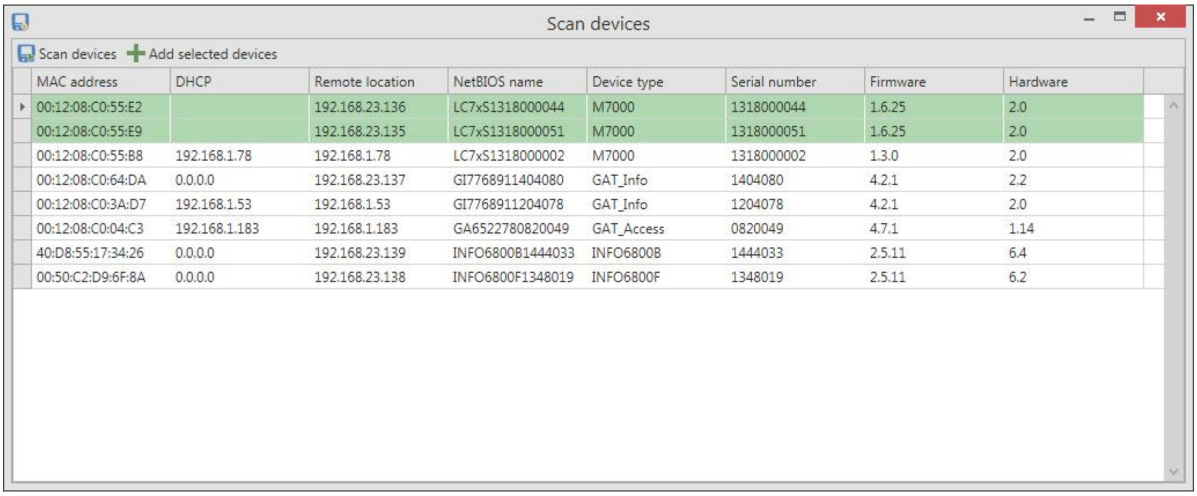
b) Scanning the local network for existing devices

Relaxx offers the functionality of scanning the local network for controllers, GAT SMART.LockAxx, Info or Access devices and adding existing devices directly to the hardware list.

► Switch to the "Lockers" view.

► Click on the "Scan devices" symbol.

 ○ The "Scan devices" window is displayed.



MAC address	DHCP	Remote location	NetBIOS name	Device type	Serial number	Firmware	Hardware
00:12:08:C0:55:E2		192.168.23.136	LC7xS1318000044	M7000	1318000044	1.6.25	2.0
00:12:08:C0:55:E9		192.168.23.135	LC7xS1318000051	M7000	1318000051	1.6.25	2.0
00:12:08:C0:55:B8	192.168.1.78	192.168.1.78	LC7xS1318000002	M7000	1318000002	1.3.0	2.0
00:12:08:C0:64:DA	0.0.0.0	192.168.23.137	GI7768911404080	GAT_Info	1404080	4.2.1	2.2
00:12:08:C0:3A:D7	192.168.1.53	192.168.1.53	GI7768911204078	GAT_Info	1204078	4.2.1	2.0
00:12:08:C0:04:C3	192.168.1.183	192.168.1.183	GA6522780820049	GAT_Access	0820049	4.7.1	1.14
40:D8:55:17:34:26	0.0.0.0	192.168.23.139	INFO6800B1444033	INFO6800B	1444033	2.5.11	6.4
00:50:C2:D9:6F:8A	0.0.0.0	192.168.23.138	INFO6800F1348019	INFO6800F	1348019	2.5.11	6.2

Figure 3.14 *- Scan devices*

► Find the desired device in the list, e.g., via its serial number and type, and mark the device by clicking on the row. Select additional devices by clicking on the row while pressing “CTRL”.

► Select "Add selected devices".

 ○ Relaxx adds the device(s) to the hardware list, where the network name and IP address of each device are displayed.

► Click on an added device in the hardware list in order to view and configure its settings, which are displayed to the right (refer also to "3.2.3 Modifying the Device Settings").

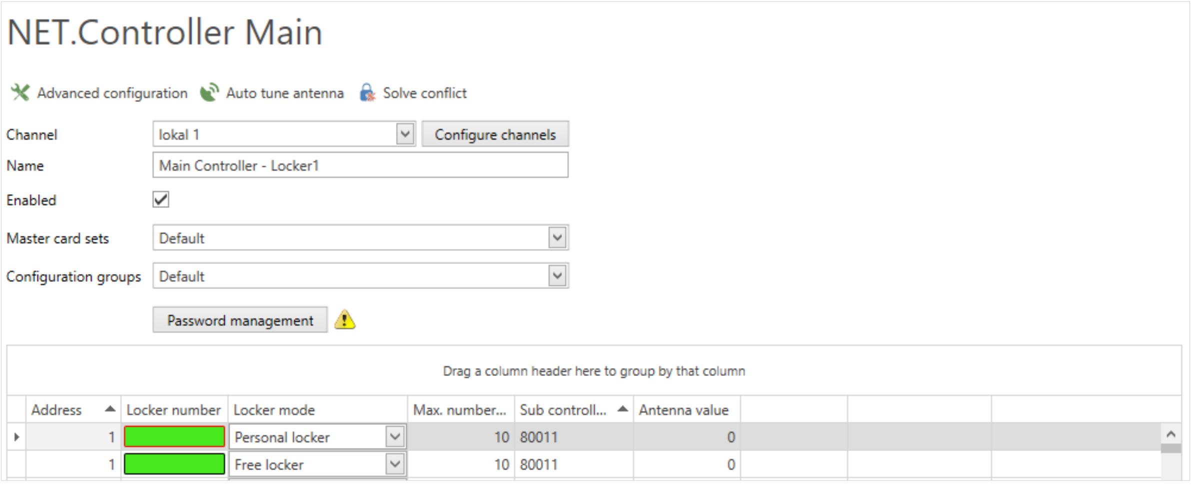
3.2.3 Modifying the Device Settings

The device settings can be configured directly after adding a device to Relaxx. To view or configure the settings of a device at any time, select the device (or the corresponding communication channel) in the Relaxx hardware list. The settings of the selected device/channel are then displayed to the right of the hardware list.

NOTE! Click on the "Save" button at the bottom right to confirm any changes made to the device settings or click on "Cancel" to leave the settings unchanged. These buttons only appear once a change has been made.

The following settings are available for the various devices.

a) NET.Controller Main



NET.Controller Main

Channel: lokal 1

Name: Main Controller - Locker1

Enabled: ☑

Master card sets: Default

Configuration groups: Default

Drag a column header here to group by that column

	Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value
▸	1	🟩	Personal locker	10	80011	0
	1	🟩	Free locker	10	80011	0

Figure 3.15 *- GAT NET.Controller M 70x0 configuration settings*

- Advanced configuration: Establishes a connection to the GAT NET.Controller M 70x0 and loads the configuration data stored in the controller. The data can be edited in the displayed window. Further information regarding this data is available in the GAT NET.Lock 70x0 manual.
- Auto tune antenna: Click on this button to automatically calibrate and optimize the antenna reading range on all GAT NET.Lock 70x0 locks connected to the controller.
  NOTE! The calibration is only performed if the lockers are closed.
- Solve conflict: After changing hardware at a channel, e.g., after exchanging a controller or disconnecting/connecting locks, conflicts can arise as the GAT NET.Controller M 70x0 configuration no longer corresponds to the actual hardware setup. These conflicts are displayed in the locker list at the bottom of the window and are solved either directly in the locker list or via the “Solve conflict" button. For more information on solving conflicts, see section "3.2.4 Solving Configuration Conflicts after Changing Hardware Components.”
- Channel: Selection of the communication channel to which the GAT NET.Controller 70x0 is connected. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- Name: Name of the controller as displayed in the hardware list.
- Enabled: If this box is checked, Relaxx communicates with the controller and continually displays the current locker states. If the box is not checked, there is no communication with the controller and the connected locks are not functional. This can be helpful, e.g., when installing a system or during servicing, to prevent Relaxx from continuously attempting to establish a connection.

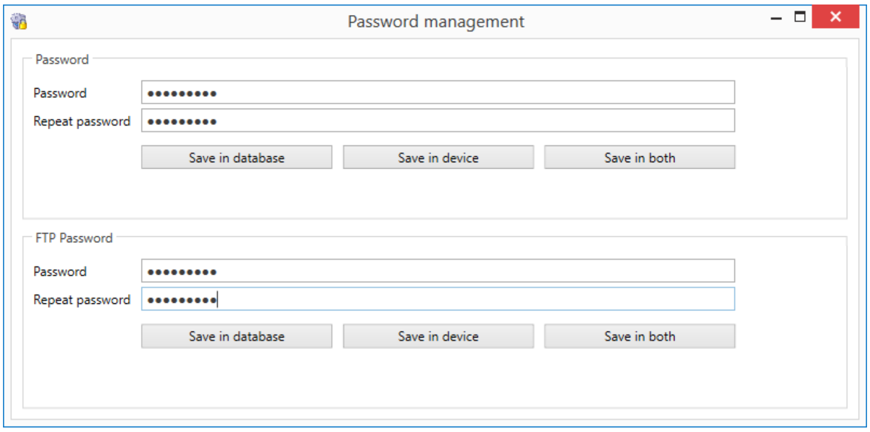
- Master card sets: In this field, assign a master card set to use with the controller. The "Default" set is always assigned by default. Master card sets are defined in the “Device” settings section (see “2.2.3 Devices”).

- Configuration groups: All settings for a GAT NET.Controller M 70x0 are summarized and preconfigured in a configuration group. By selecting a configuration group, these settings are applied to the controller in one step. For controllers with the standard configuration group, all parameters contained therein can be individually adjusted using the "Advanced configuration" button (see above). For controllers with other configuration groups, only the controller-specific parameters such as IP address or NETBios name can be adjusted. Configuration groups are set in the program settings (see “Device settings for the Main Controller GAT NET.Controller M 70x0” in chapter "2.2.3 Devices").

- Password management: This opens the “Password management” window, which effects the communication between Relaxx and the controller. A password can be set to access the controller and another password for the FTP communication, which is used to download log files and for firmware updates. You can select to save the password in the database only, in the device only, or in both.

  If an exclamation mark is displayed next to this button, the default password is still being used. See also the information on the "Advanced" tab in section "2.2.3 Devices".

  NOTE! The passwords are intended for service purposes. Change the default passwords to secure passwords and keep them in a secure place. Without the passwords, communication with the controller is not possible and there is also no possibility for password recovery.



Password management

Password

Password ●●●●●●●●●

Repeat password ●●●●●●●●●

FTP Password

Password ●●●●●●●●●

Repeat password ●●●●●●●●●

***Figure 3.16** – “Password management” window*

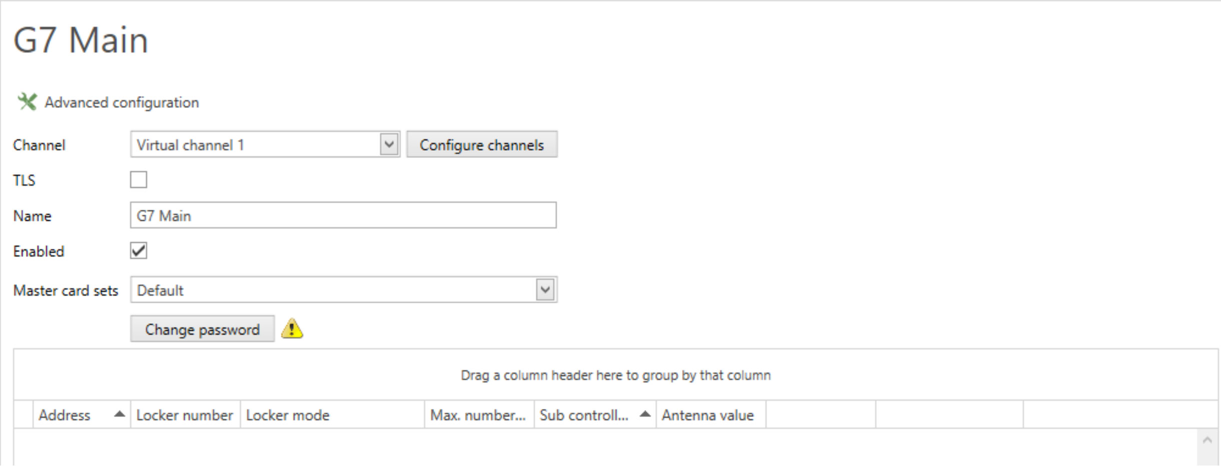
- Locker list: This list includes all the locks connected to the GAT NET.Controller M 70x0. Note that several sub controllers (GAT NET.Controller S 70x0 or GAT SMART.Controller S 7000) can connect to a main controller. The list shows all locks connected to all sub controllers in one continuous list. The locks can be configured directly in the list. The columns in the list are defined as follows:

  - Address: Controller port where the lock is physically connected.

  - Locker number: The number assigned in Relaxx to the respective locker. The lockers are displayed with these numbers in the organization view. The locker numbers can be freely assigned but should match the locker number printed on the locker. Locker numbers are assigned when the lockers are being added to the locker groups in the organization view (refer to "3.2.6. Setting up the Organization System").

- Locker mode: The operating mode of the locker. Refer to "1.4 Terminology" for definitions of the various locker modes. To set all lockers to the same mode, right-click on a locker already set to the desired mode then select “Use this mode for all lockers”.
- Max. number (Personal Locker): The maximum number of data carriers that can be authorized for use with the respective locker while it is operating in personal locker mode.
- Sub Controller serial number: Serial number of the sub controller to which the respective locker is connected.
- Antenna value: Only required for installation and service purposes.

b) G7 Main Controller


G7 Main

Advanced configuration

Channel: Virtual channel 1 | Configure channels

TLS: □

Name: G7 Main

Enabled: ☑

Master card sets: Default

Change password ⚠

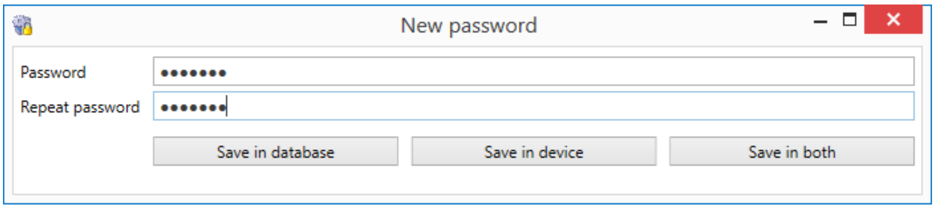
Drag a column header here to group by that column

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value

***Figure 3.17** - GC7.2000 M (lite) Controller configuration settings*

- Advanced configuration: Establishes a connection to the G7 device and loads the configuration data stored in the controller. The data can be edited in the displayed window. Further information regarding this data is available in the GC7 manual.
- Channel: Selection of the communication channel to which the G7 main controller is connected. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- TLS: If this option is enabled, the communication to the G7 main controller is encrypted with TLS. To do this, the TLS encryption must be set up and enabled correctly in the configuration of the G7 main controller (see manual for the G7 main controller).
- Name: Name of the controller as displayed in the hardware list.
- Enabled: When this option is enabled, Relaxx communicates with the controller and continually displays the current locker states. When not enabled, there is no communication with the controller and the connected locks are not functional. This can be helpful, e.g., when installing a system or during servicing to prevent Relaxx from continuously attempting to establish a connection.
- Master card sets: In this field, assign a master card set to use with the controller. The "Default" set is always assigned by default. Master card sets are defined in the “Device” settings section (see “2.2.3 Devices”).
- Password management: This function is optional and opens the "New password" window. A password for communication between the G7 main controller and Relaxx can be defined here. This is independent of the password used to log in to the web interface. You can select to save the password in the database only, in the device only, or in both.
  If an exclamation mark is displayed next to this button, the default password is still being used. See also the information on the "Advanced" tab in section "2.2.3 Devices".

NOTE! The passwords are intended for service purposes. Change the default passwords to secure passwords and keep them in a secure place. Without the passwords, communication with the controller is not possible and there is also no possibility for password recovery. Resetting the communication password is only possible via the web interface of the G7 main controller with separate access.

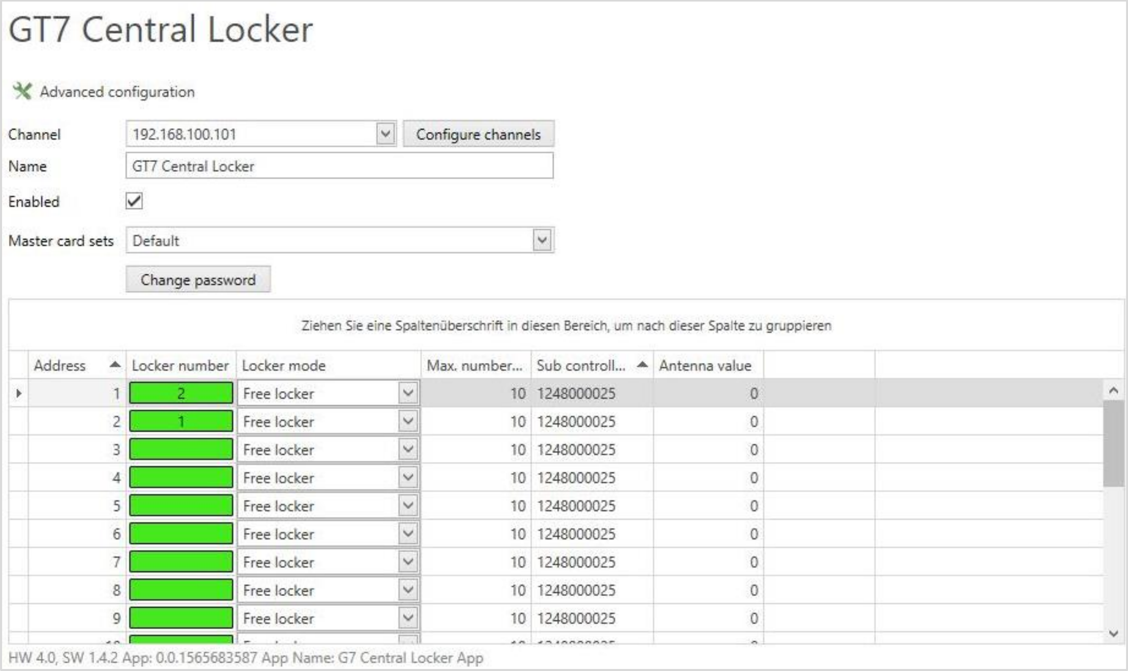


Password: •••••••
Repeat password: •••••••

Figure 3.18 *- Password setting for communication*

- Locker list: This list includes all the locks connected to the G7 main controller. Be aware that several sub controllers (GAT NET.Controller S 70x0 und/or GAT SMART.Controller S 70x0) can be connected to a G7 main controller. The list shows all locks connected to all sub controllers in one continuous list. The locks can be configured directly in the list. The columns in the list are defined as follows:
  - Address: Controller port where the lock is physically connected.
  - Locker number: The number assigned in Relaxx to the respective locker. The lockers are displayed with these numbers in the organization view. The locker numbers can be freely assigned but should match the locker number printed on the locker. Locker numbers are assigned when the lockers are being added to the locker groups in the organization view (refer to "3.2.6. Setting up the Organization System").
  - Locker mode: The operating mode of the locker. Refer to "1.4 Terminology" for definitions of the various locker modes. To set all lockers to the same mode, right-click on a locker already set to the desired mode then select “Use this mode for all lockers”.
  - Max. number (Personal Locker): The maximum number of data carriers that can be authorized for use with the respective locker while it is operating in personal locker mode.
  - Sub Controller serial number: Serial number of the sub controller to which the respective locker is connected.
  - Antenna value: Only required for installation and service purposes.

c) GT7 Central Locker



GT7 Central Locker

Channel: 192.168.100.101

Name: GT7 Central Locker

Enabled: ☑

Master card sets: Default

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value
1	🟩 2	Free locker	10	1248000025	0
2	🟩 1	Free locker	10	1248000025	0
3	🟩	Free locker	10	1248000025	0
4	🟩	Free locker	10	1248000025	0
5	🟩	Free locker	10	1248000025	0
6	🟩	Free locker	10	1248000025	0
7	🟩	Free locker	10	1248000025	0
8	🟩	Free locker	10	1248000025	0
9	🟩	Free locker	10	1248000025	0

HW 4.0, SW 1.4.2 App: 0.0.1565683587 App Name: G7 Central Locker App

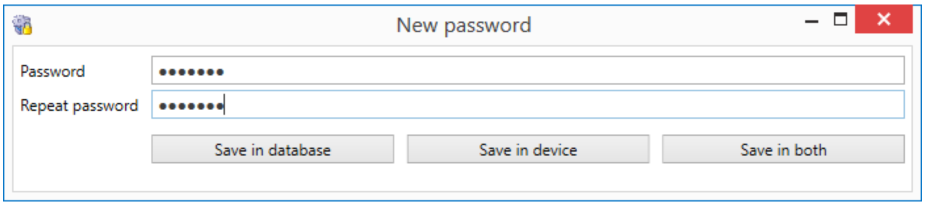
***Figure 3.19** – GT7 Central Locker configuration settings*

- Advanced configuration: Establishes a connection to the device and loads the GT7 web interface. The device settings can be viewed and edited in the displayed window after logging in. Further information regarding this data is available in the GT7 Central Locker manual.
- Channel: Selection of the communication channel to which the device is connected. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- Name: Name of the device as displayed in the hardware list.
- Enabled: If this box is checked, Relaxx communicates with the device and continually displays the current locker states. If the box is not checked, there is no communication and the connected locks are not functional. This function can assist, e.g., when installing a system or during servicing, to prevent Relaxx from continuously attempting to establish a connection.
- Master card sets: In this field, assign a master card set to use with the device. The "Default" set is always assigned by default. Master card sets are defined in the “Device” settings section (see “2.2.3 Devices”).
- Change password: This function is optional and opens the “New password” window in which a password can be defined for communication between the device and Relaxx. This password is not the password required to log into the web interface of the device. You can select to save the password in the database only, in the device only, or in both.

  If an exclamation mark is displayed next to this button, the default password is still being used. See also the information on the "Advanced" tab in section "2.2.3 Devices".

  NOTE! The passwords are intended for service purposes. Change the default passwords to secure passwords and keep them in a secure place. Without the passwords, communication with the controller is not possible and there is also no possibility for password recovery.

Resetting the communication password is only possible via the web interface of the G7 main controller with separate access.



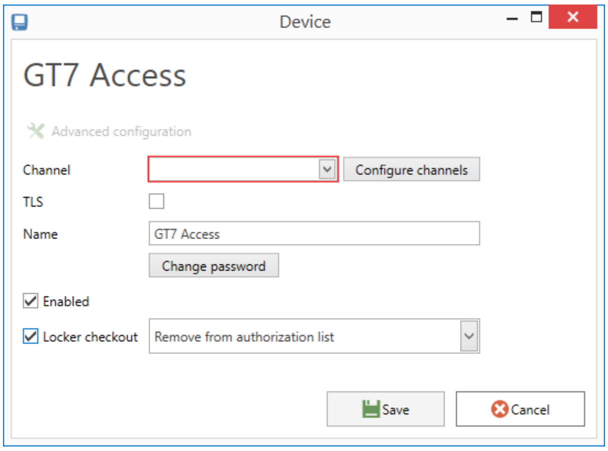
Password: •••••••

Repeat password: •••••••

***Figure 3.20** – Password setting for communication*

- Locker list: This list includes all locks connected to all sub controllers in one continuous list. The locks can be configured directly in the list with the settings defined as follows:
  - Address: Controller port where the lock is physically connected.
  - Locker number: The number assigned in Relaxx to the respective locker. The lockers are displayed with these numbers in the organization view. The locker numbers can be freely assigned but should match the locker number printed on the locker. Locker numbers are assigned when the lockers are being added to the locker groups in the organization view (refer to "3.2.6. Setting up the Organization System").
  - Locker mode: The operating mode of the locker. Refer to "3.4.1. Overview of Authorization Settings and Locker Modes" for definitions of the various locker modes. To set all lockers to the same mode, right-click on a locker already set to the desired mode then select “Use this mode for all lockers”.
  - Max. number (Personal Locker): The maximum number of data carriers that can be authorized for use with the respective locker while it is operating in personal locker mode.
  - Sub controller serial number: Serial number of the sub controller to which the respective locker is connected. The serial numbers of the sub controllers can be found on their type labels.
  - Antenna value: Only required for installation and service purposes.

d) GT7 Access and GT7 Info Devices



Device

GT7 Access

Channel

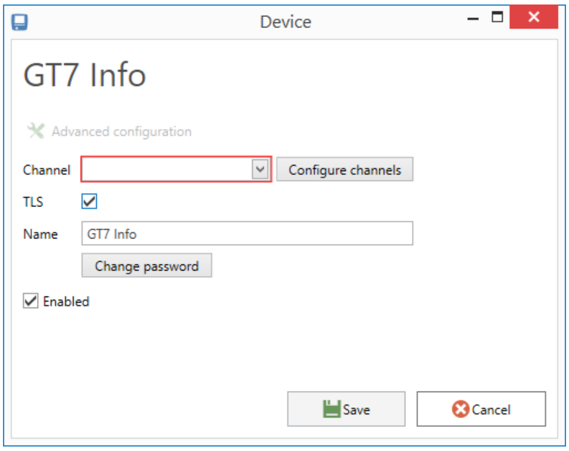
TLS □

Name: GT7 Access

☑ Enabled

☑ Locker checkout: Remove from authorization list

***Figure 3.21** – Configuration settings for GT7 Access*



Device

GT7 Info

Channel

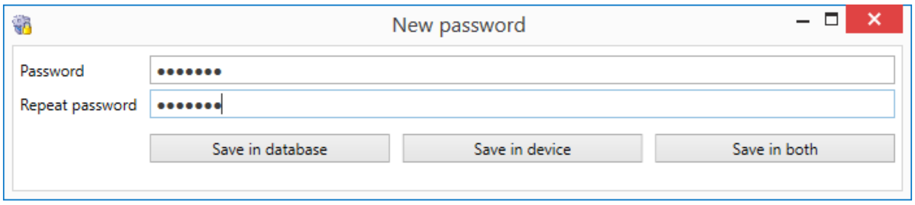
TLS ☑

Name: GT7 Info

☑ Enabled

Configuration settings for GT7 Info

- Advanced configuration: Establishes a connection to the device and loads the GT7 web interface. The device settings can be viewed and edited in the displayed window after logging in. Further information regarding this data is available in the manual of the corresponding device or application.
- Channel: Selection of the communication channel to which the device is connected. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- TLS: If this option is activated, the communication to the GT7 device is encrypted with TLS. To do this, the TLS encryption must be configured and enabled correctly in the configuration of the GT7 device (see manual for GT7 Access or GT7 Info).
- Name: Name of the device as displayed in the hardware list.
- Change password: This function is optional and opens the "New password" window. A password for communication between the GT7 device and Relaxx can be defined here. This is independent of the password used to log in to the web interface. You can choose whether the password should be saved in the Relaxx database, in the device, or in both.
  If an exclamation mark is displayed next to this button, the default password is still being used. See also the information on the "Advanced" tab in section "2.2.3 Devices".
  NOTE! The passwords are intended for service purposes. Change the default passwords to secure passwords and keep them in a secure place. Without the passwords, communication with the controller is not possible and there is also no possibility for password recovery. Resetting the communication password is only possible via the web interface of the G7 main controller with separate access.



New password

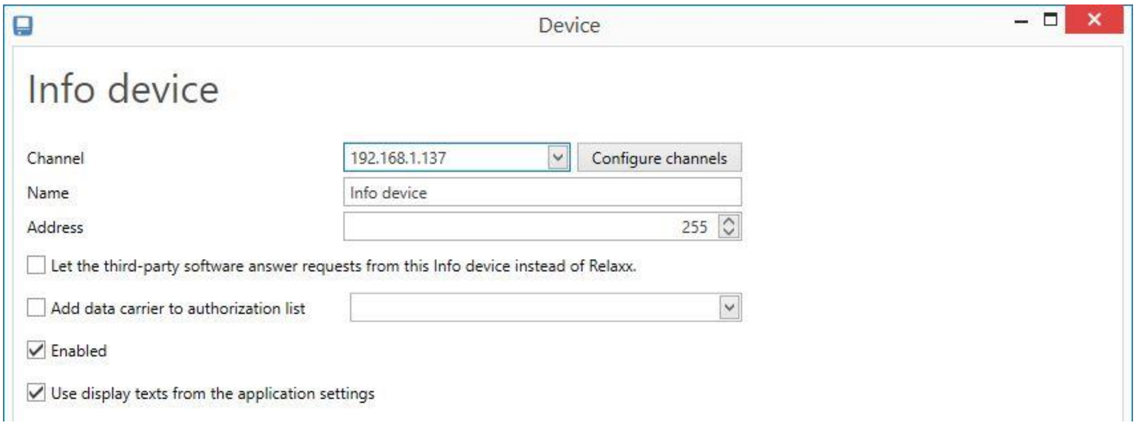
Password: •••••••

Repeat password: •••••••

***Figure 3.22** - Password setting for communication*

- Enabled: If this box is checked, Relaxx communicates with the device. If the box is not checked, there is no communication with the device. This function can assist, e.g., when installing a system or during servicing to prevent Relaxx from continuously attempting to establish a connection.
- Locker checkout: When the "Locker checkout" option is enabled, users can perform a locker checkout of their lockers (of type dynamic, personal, or reservable lockers). Locker checkout automatically removes all user authorizations of these locker types in the configured locker groups from the GT7 Access device. The locker group assignments are defined in the access authorization definition, see "3.4.9. Access Authorizations". Via this checkout, the lockers are directly available again for other users. The exact behavior can be controlled by selecting one of the following options:
  - Remove from authorization list: When performing a checkout, the data carrier is removed from the authorization list.
  - Release lockers: Only deletes the locker authorizations from the data carrier but will keep the data carrier UID in the authorization list.

e) Info Device 6000 Series



Channel: 192.168.1.137 — Configure channels

Name: Info device

Address: 255

□ Let the third-party software answer requests from this Info device instead of Relaxx.

□ Add data carrier to authorization list

☑ Enabled

☑ Use display texts from the application settings

Figure 3.23 *- Configuration settings for an Info device*

- Channel: Selection of the communication channel for the Info device selected in the hardware list. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- Name: Name of the Info device, as displayed in the hardware list.
- Address: Keep the default setting 255 as Info device address.
- Let the third-party software answer requests from this Info device instead of Relaxx:

  Select this option to allow third-party software to display additional user information on the device when a data carrier is read. The information to be displayed is sent from third-party software via the JSON interface.
- Add data carrier to authorization list:

  Select this option and select an authorization group from the list in order to automatically add data carriers, which are not yet saved in the locker system, to the authorization list of Relaxx. The selected authorization group is automatically assigned to these data carriers. The validity dates for the data carriers are automatically set to the preset values in the authorization settings of Relaxx (see "2.2.6 Authorizations").
- Enabled: Select this option to activate the Info device for use in Relaxx. When this option is not selected, the Info device is not deleted in Relaxx, but it does not have any function. This is useful for service tasks.

  If you want to use the device, this option must be selected.
- Use display texts from the application settings:

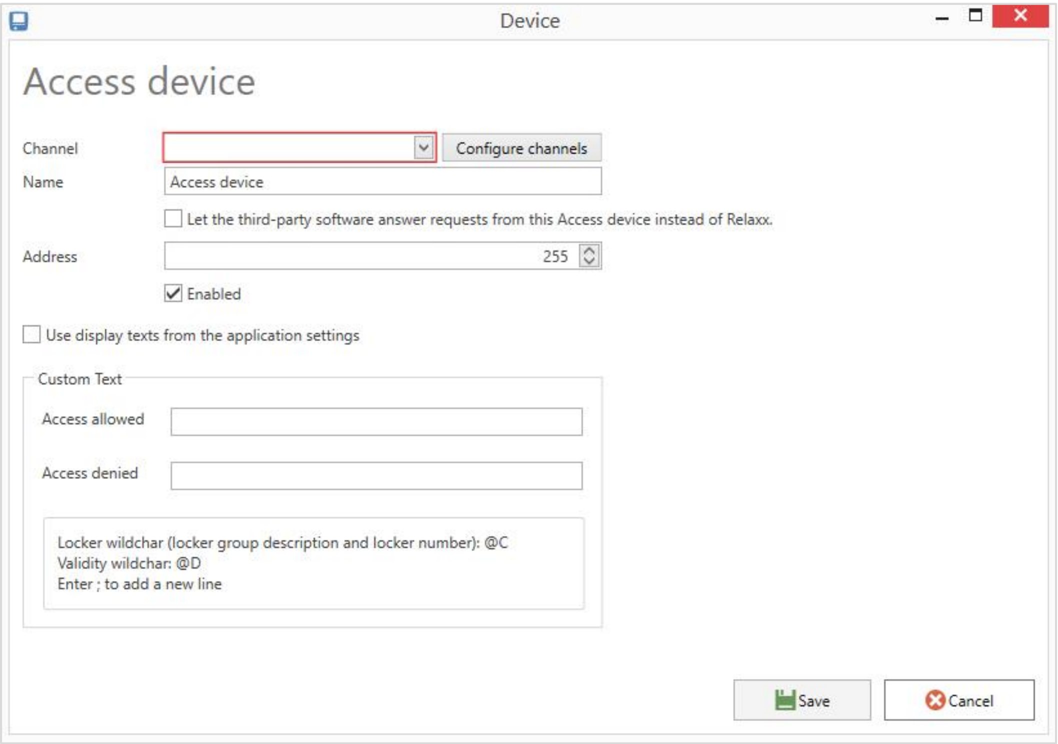
  Select this option if you want to use the default display texts for the Info device, which are pre-defined in the program settings (see "2.2.3. Devices").

  Deselect this option if you want to use custom texts for the currently opened Info device. After deselection, the text fields are displayed below the option as shown in Figure 3.23. Define the texts that will be displayed on the Info device.

Placeholders can be used in the text, e.g., for the current date or time. The use of these placeholders is explained during the text entry.

NOTE! The GAT Info 6100 screen can display a maximum of 4 lines of text with 20 characters per line. If the text length exceeds these values, an "Out of range!" error message is shown on the display. This is especially important when using place holders which can show information of variable length.
Recommendation for showing the locker number in the field "UsedOrAssigned":
`Locker No.:;@C` (the ";" character starts a new line).

f) Access Device 6000 Series



Device
Access device
Channel
Configure channels
Name
Access device
□ Let the third-party software answer requests from this Access device instead of Relaxx.
Address
255
☑ Enabled
□ Use display texts from the application settings
Custom Text
Access allowed
Access denied
Save
Cancel

Locker wildchar (locker group description and locker number): @C
Validity wildchar: @D
Enter ; to add a new line

***Figure 3.24** - Configuration settings for an Access device*

- Channel: Selection of the communication channel for the Access device selected in the hardware list. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels").
- Name: Name of the Access device, as displayed in the hardware list.
- Let the third-party software answer requests from this Access device instead of Relaxx:

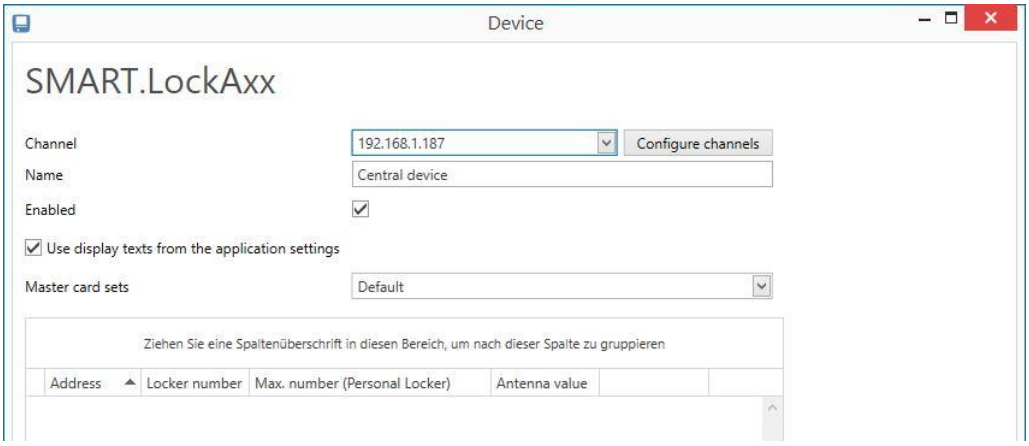
  Select this option to allow third-party software to grant/deny access via the JSON interface when a data carrier is read at the Access device.
- Address: Keep the default setting of 255 for the Access device address.
- Enabled: Select this option to activate the Access device for use in Relaxx. When this option is not selected, the Access device is not deleted in Relaxx, but it does not have any function. This is useful for service tasks.

  If you want to use the device, this option must be selected.
- Use display texts from the application settings:

  Select this option if you want to use the default display texts for the Access device, which are pre-defined in the program settings (see "2.2.3. Devices").
  Deselect this option if you want to use custom texts for the currently opened Access device. After deselection, the text fields are displayed below the option as shown in Figure 3.24. Define the texts that will be displayed on the Access device.

Placeholders can be used in the text, e.g., for the current date or time. The use of these placeholders is explained during the text entry.

g) GAT SMART.LockAxx 6350



Channel: 192.168.1.187

Name: Central device
Enabled: ☑
☑ Use display texts from the application settings
Master card sets: Default

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Address	Locker number	Max. number (Personal Locker)	Antenna value

Figure 3.25 *- GAT SMART.LockAxx 6350 with GAT SMART.Controller S 7000 configuration settings*

- Channel: The communication channel via which the GAT SMART.LockAxx 6350 is connected. With the "Configure channels" button, the channel settings can be edited and new channels defined (refer also to "3.2.1 Communication Channels")
- Name: Name of the GAT SMART.LockAxx 6350, as displayed in the hardware list.
- Enabled: If this box is checked, Relaxx communicates with the GAT SMART.LockAxx 6350 and continually displays the current locker states. If the box is not checked, there is no communication with the controller and the connected locks are not functional. This can be helpful, e.g., when installing a system or during servicing, to prevent Relaxx from continuously attempting to establish a connection.
- Use display texts from the application settings:

  If you want to use the standard display texts, which are already pre-defined in the program settings (see "2.2.3. Devices"), for the GAT SMART.LockAxx 6350 than mark this option.

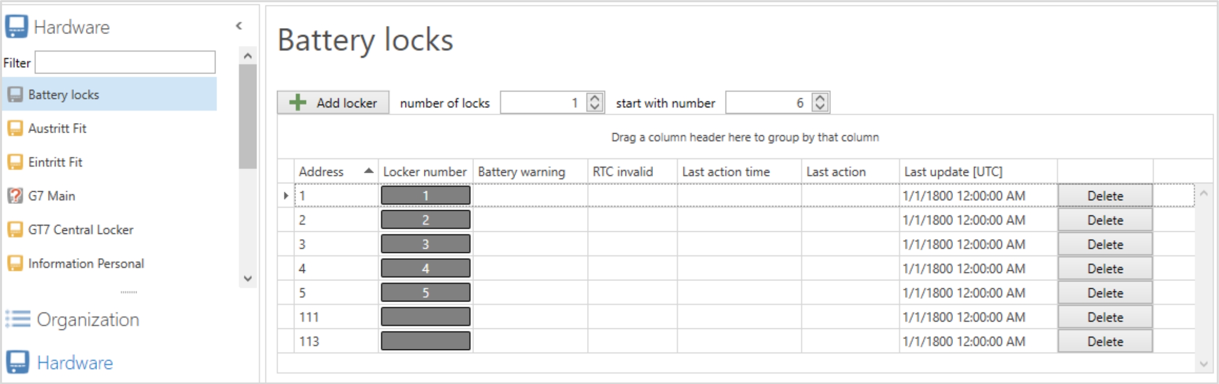
  If you want to use individual texts for the currently opened GAT SMART.LockAxx 6350 then please unmark this option. In this case the text fields are shown below the option field (see example pictures). Define the texts that will be displayed on the GAT SMART.LockAxx 6350.

  Placeholders can be used in the text, e.g., for the current date or time. The use of these placeholders is explained during the text entry.

- Locker list: This list displays all locks connected to the GAT SMART.LockAxx 6350 and the connected sub controllers. The lockers can be configured directly in the list. The columns of the list have the following meanings:

- Address: Controller port where the lock is physically connected.
- Locker number: The logic locker number assigned in Relaxx to the respective locker. In the organization view, the lockers are displayed with these numbers. The locker numbers can be freely assigned but should match the locker number printed on the respective locker. The assigning occurs at the moment of adding the lockers to the locker groups in the organization view (refer to "3.2.6. Setting up the Organization System").
- Max. number (Personal Locker): The maximum number of data carriers that can be authorized for use with the respective locker while it is operating in personal locker mode.
- State: Current state of the locker. The display includes a corresponding message text. In addition, the locker state is also indicated by a color in the column "Locker number". For information regarding the various colors, refer to the legend in section “3.3.7 Color Legend".
- Antenna value: Needed only for installation and service purposes.

h) Battery Locks



Battery locks

number of locks 1 start with number 6

Drag a column header here to group by that column

Address	Locker number	Battery warning	RTC invalid	Last action time	Last action	Last update [UTC]	
1	1					1/1/1800 12:00:00 AM	Delete
2	2					1/1/1800 12:00:00 AM	Delete
3	3					1/1/1800 12:00:00 AM	Delete
4	4					1/1/1800 12:00:00 AM	Delete
5	5					1/1/1800 12:00:00 AM	Delete
111						1/1/1800 12:00:00 AM	Delete
113						1/1/1800 12:00:00 AM	Delete

***Figure 3.26** – Configuration settings for battery locks*

Battery locks are battery-powered locker locks without a permanent wired connection to Relaxx. Communication takes place wirelessly via radio frequency. To add and configure battery locks, the use of battery locks must be first activated in the program settings (see "2.2.3 Devices”). An entry "Battery locks" is then displayed in the hardware list. Click on this entry to display the list of battery locks.

► The "Add locker" button inserts a certain number of locks in the list starting with a selectable address. Set the following information before inserting:

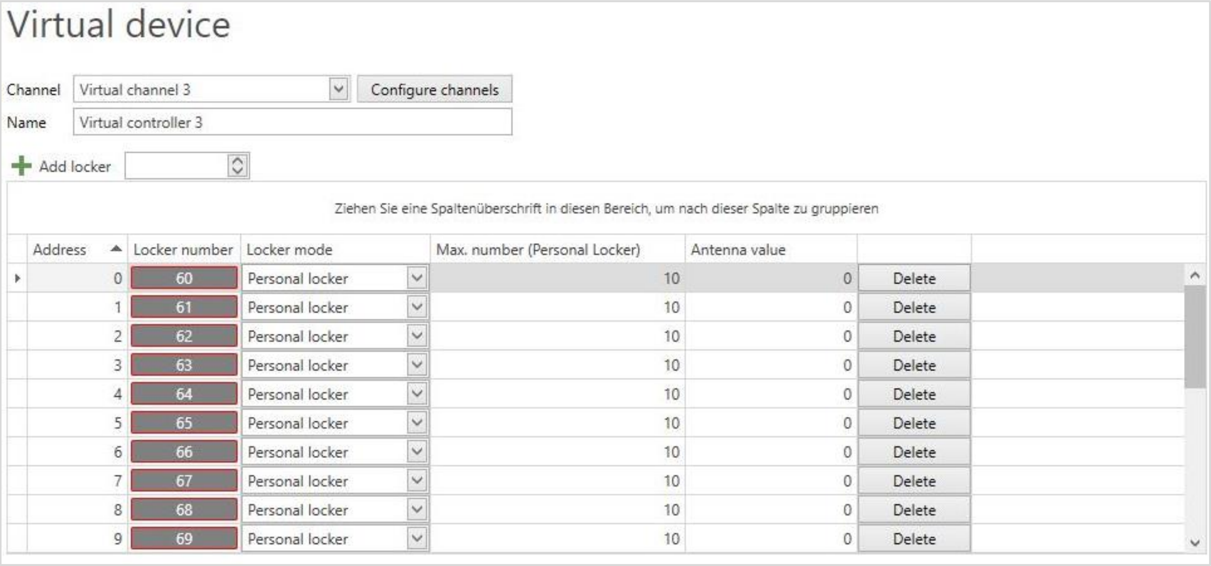
- Number of locks: Enter the number of locks that you want to add in one step.
- Start with number: Enter the first address of the locks to be added here.

All battery locks are displayed in the locker list. The table columns have the following meaning:

- Address: The locker number that is configured in the battery lock.
- Locker number: The logical locker numbers that are assigned to the respective battery locks in Relaxx. In the organization view, the lockers are shown with these numbers. The locker numbers can be freely assigned but should match the locker numbers printed on the respective locker. The assignment is made when adding the lockers to the locker groups in the organization view (see "3.2.6 Setting up the Organization System").
- Battery warning: Information is displayed here if the battery lock signals a battery warning when the battery charge is too low.
- RTC invalid: Warning if the time in the lock has not been set.
- Last action time: Time in the lock when the last action was logged.
- Last action: Last action that occurred at the lock.
- Last update [UTC]: Time stamp of Relaxx when the last message was received (in coordinated UTC time).

► To delete battery locks, select one or more locks in the list and click on the corresponding "Delete" button.

i) Virtual device



Virtual device

Channel: Virtual channel 3 [Configure channels]

Name: Virtual controller 3

+ Add locker

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Address	Locker number	Locker mode	Max. number (Personal Locker)	Antenna value	
0	60	Personal locker	10	0	Delete
1	61	Personal locker	10	0	Delete
2	62	Personal locker	10	0	Delete
3	63	Personal locker	10	0	Delete
4	64	Personal locker	10	0	Delete
5	65	Personal locker	10	0	Delete
6	66	Personal locker	10	0	Delete
7	67	Personal locker	10	0	Delete
8	68	Personal locker	10	0	Delete
9	69	Personal locker	10	0	Delete

Figure 3.27 - Configuration settings for a virtual controller

- Channel: Selection of the virtual communication channel for the controller selected in the hardware list. With the "Configure channels" button, the channel settings can be edited and new channels can be defined (refer also to "3.2.1 Communication Channels").
- Name: Name of the communication channel or virtual controller, as displayed in the hardware list.

- Add locker: With this icon button, the number of lockers entered into the adjoining field will be added to the locker list of the controller.
- Locker list: This list shows all locks or lockers connected to the selected virtual controller, in one continuous list. The lockers can be configured directly in the list. The columns of the list have the following meanings:
- Address: Controller port where the lock is connected (virtual connection).
    - Locker number: The logical locker number assigned to the respective locker in Relaxx. In the organization view, the lockers are displayed with these numbers. The locker numbers can be freely assigned. The assigning occurs at the moment of adding the lockers to the locker groups in the organization view (refer to "3.2.6. Setting up the Organization System").
    - Locker mode: Selection of the mode that defines how the locker is operated. For the functionalities of the various locker modes, refer to "1.4 Terminology". To set all lockers to the same mode, right-click on a locker already set to the desired mode and select “Use this mode for all lockers”.
    - Max. number (Personal Locker): The maximum number of data carriers that can be authorized for use with the respective locker while it is operating in personal locker mode.
    - State: Current state of the locker. The display includes a corresponding message text. In addition, the locker state is also indicated by a color in the column “Locker number “. For information regarding the various colors, refer to the legend in section “3.3.7 Color Legend".
    - Antenna value: Needed only for installation and service purposes.
    - Delete: With this button, individual lockers can be removed from the virtual controller.

3.2.4 Solving Configuration Conflicts after Changing Hardware Components

After a hardware component is changed, e.g., after exchanging a controller or the lock cabling, conflicts can arise between the Relaxx configuration and the actual hardware setup. Different situations are possible here and Relaxx provides functions for automatic conflict resolution. Generally, there are two situations to distinguish between.

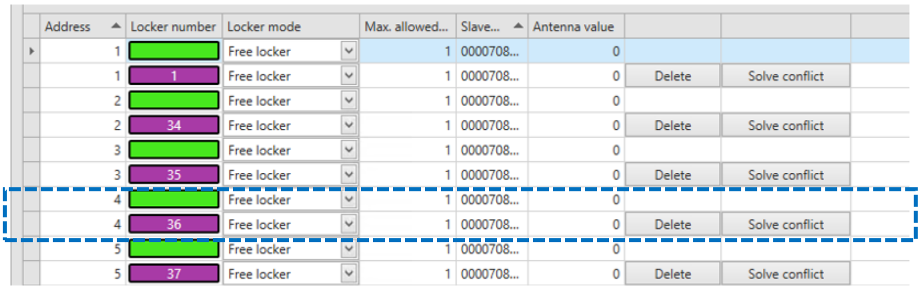
a) Channel with only GAT NET.Lock 7000 components

Replacement of a GAT NET.Controller M 7000 Main Controller
The system will automatically find the new main controller when the channel is restarted. You may have to adjust the controller configuration (site key, RFID settings, etc.)

Replacement of a GAT NET.Controller S 7000 sub controller
The system will automatically find the new sub controller (after approx. 1 minute) when the channel is restarted. For locked lockers, the information from the data carrier used last is lost, which means that lockers can no longer be unlocked using the data carrier with which they were last locked.

Transfer of a GAT NET.Lock 7000 to a different port on the sub controller
The lock will be automatically re-identified after a few seconds.

Replacement of a GAT NET.Lock 7000
This creates a conflict that must be resolved manually. It may take up to 1 minute for Relaxx to identify the new lock. The conflict is displayed in the locker list when configuring the GAT NET.Controller M 7000 and can be resolved using the "Delete" or "Solve conflict" button.



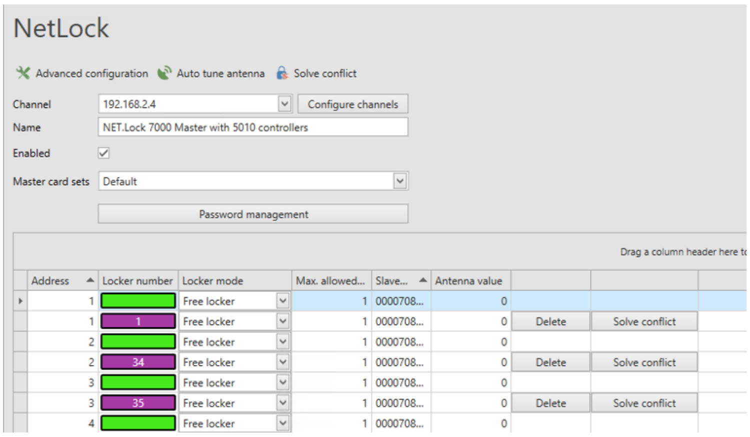
	Address	Locker number	Locker mode	Max. allowed...	Slave...	Antenna value		
▸	1	🟩	Free locker	1	0000708...	0		
	1	1	Free locker	1	0000708...	0	Delete	Solve conflict
	2	🟩	Free locker	1	0000708...	0		
	2	34	Free locker	1	0000708...	0	Delete	Solve conflict
	3	🟩	Free locker	1	0000708...	0		
	3	35	Free locker	1	0000708...	0	Delete	Solve conflict
	4	🟩	Free locker	1	0000708...	0		
	4	36	Free locker	1	0000708...	0	Delete	Solve conflict
	5	🟩	Free locker	1	0000708...	0		
	5	37	Free locker	1	0000708...	0	Delete	Solve conflict

***Figure 3.28** – Display of a conflict for a lock*

- ► With "Solve conflict", the predefined solution is used.
- ► Click on "Delete" to delete the lock. Be aware that the recorded lock history is also deleted.

b) Channel with GAT NET.Controller M 7000 and GAT Lock Controller 5010

<u>Replacing a GAT NET.Lock M 7000 Main Controller with connected GAT Lock Controller 5010</u>
The previously configured locks of the exchanged controller are displayed in purple with their assigned locker number. As the new controller does not know this configuration yet, the existing locks connected to the new controller are identified as "new" and displayed in the current status without locker numbers. Relaxx automatically assigns the existing configuration to the locks. You can check and confirm these entries ("Solve conflict") or delete the existing lock configuration (via "Delete"). However, for delete, the existing lock history is also deleted, and you have to re-assign the locker numbers.



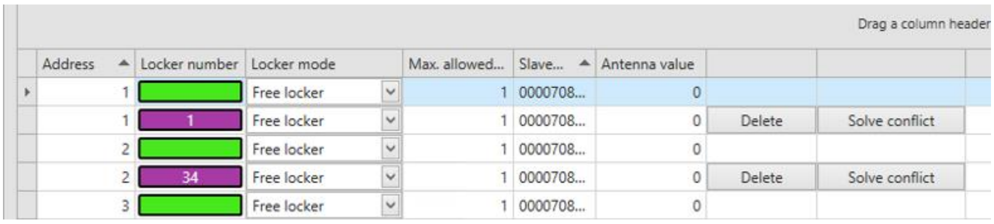
Channel: 192.168.2.4
Name: NET.Lock 7000 Master with 5010 controllers
Enabled: ☑
Master card sets: Default

Address	Locker number	Locker mode	Max. allowed...	Slave...	Antenna value		
1	🟩	Free locker	1	0000708...	0		
1	🟪 1	Free locker	1	0000708...	0	Delete	Solve conflict
2	🟩	Free locker	1	0000708...	0		
2	🟪 34	Free locker	1	0000708...	0	Delete	Solve conflict
3	🟩	Free locker	1	0000708...	0		
3	🟪 35	Free locker	1	0000708...	0	Delete	Solve conflict
4	🟩	Free locker	1	0000708...	0		

Figure 3.29 *– Solving conflicts*

The recommended procedure for exchanging a GAT NET.Controller M 7000 to retain the configuration of the locks is as follows:

- ▶ Remove the faulty main controller.
- ▶ Connect the Ethernet network cable and power supply to the new main controller (but do not connect the sub controllers yet).
- ▶ Reset the new controller to the default settings (see the GAT NET.Lock 70x0 manual).
- ▶ Ensure that the new controller has the same or a newer firmware version as the old controller.
- ▶ Set the IP address of the controller or existing channel.
  NOTE! If you create a new controller in Relaxx, you will lose the existing locker configuration.
- ▶ Connect the sub controllers to the main controller.
- ▶ Start the channel of the new main controller.
- ▶ In the device settings of the new main controller, open the “Advanced configuration” (the controller and channel must be connected and started).
  - o The configuration of the controller is loaded and displayed.
- ▶ Go to "Communication -> Sub Interface -> Protocol" and set this value to "FUNLINE_F / ISO" or "FUNLINE_LEGIC", depending on the type of controller connected.
- ▶ Optional: configure the remaining settings according to the requirements.
- ▶ Save the configuration.
- ▶ Wait (up to 1 minute) until Relaxx displays the locks with the new main controller and their current status.
  - o If the lock arrangement has not changed, you should see two entries for each lock channel; the old configuration highlighted in purple with locker number and “Not found” status, and also the newly found lock connected to the new controller.



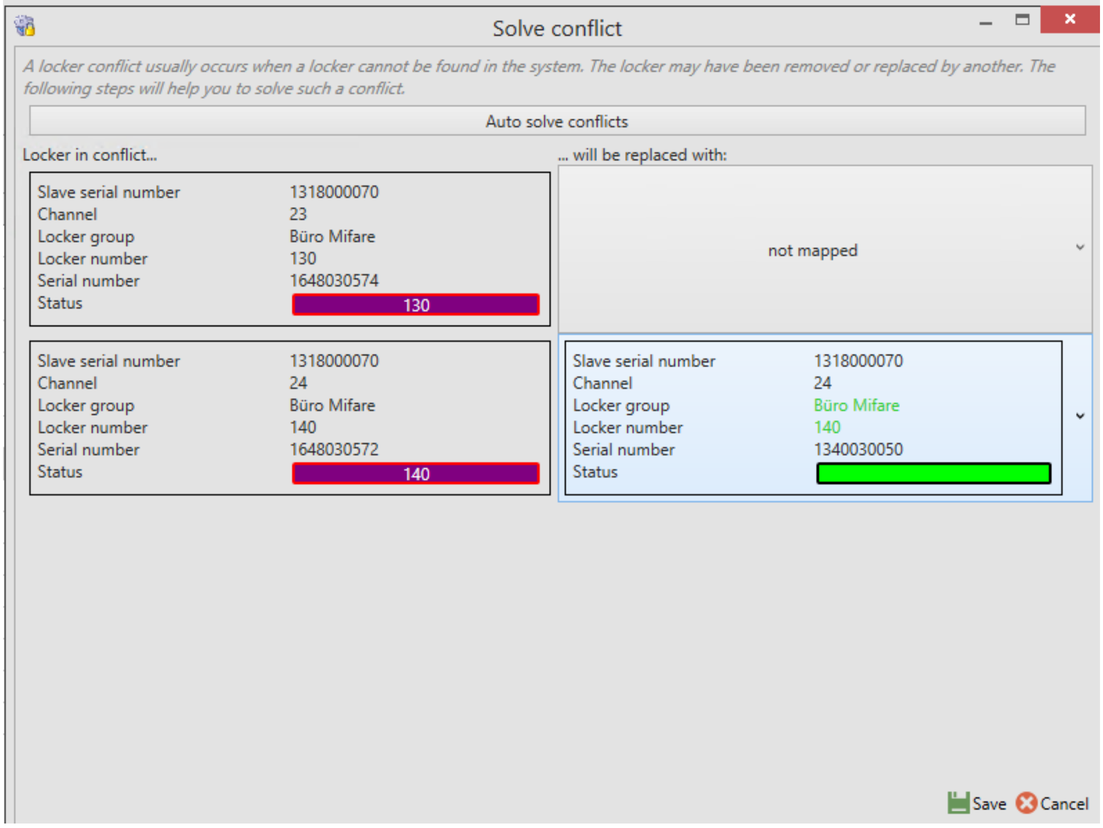
Drag a column header

	Address	Locker number	Locker mode	Max. allowed...	Slave...	Antenna value		
▸	1	🟩	Free locker	1	0000708...	0		
	1	1	Free locker	1	0000708...	0	Delete	Solve conflict
	2	🟩	Free locker	1	0000708...	0		
	2	34	Free locker	1	0000708...	0	Delete	Solve conflict
	3	🟩	Free locker	1	0000708...	0		

***Figure 3.30** – Solving conflicts manually*

- ▶ To resolve this conflict, click on the "Solve conflict" button next to a lock or at the top of the controller configuration.
  - ○ The "Solve conflict" window opens, in which all current conflicts and their suggested solutions are displayed.

The following figure shows an example where Relaxx can automatically solve the conflict at lock channel 24, but not at channel 23 as this lock is connected to channel 22. In this case, you must resolve the conflict manually by selecting the correct lock.



Solve conflict

A locker conflict usually occurs when a locker cannot be found in the system. The locker may have been removed or replaced by another. The following steps will help you to solve such a conflict.

Auto solve conflicts

Locker in conflict...

... will be replaced with:

Locker in conflict...		... will be replaced with:	
Slave serial number	1318000070	not mapped	
Channel	23		
Locker group	Büro Mifare		
Locker number	130		
Serial number	1648030574		
Status	130		
Slave serial number	1318000070	Slave serial number	1318000070
Channel	24	Channel	24
Locker group	Büro Mifare	Locker group	Büro Mifare
Locker number	140	Locker number	140
Serial number	1648030572	Serial number	1340030050
Status	140	Status	🟩

Save Cancel

***Figure 3.31** – Solving conflicts automatically*

- ▶ The settings list on the far right allows you to make changes to the automatic assignments.
- ▶ Click on the "Auto solve conflicts" button to resolve the conflicts as indicated by Relaxx.
- ▶ Save the changes by clicking on "Save".

Limitation:

- When a locker has been previously locked, the information on the data carrier last used to lock the locker is lost after the controller exchange. Although this has no effect on locker usage and all authorized data carriers can use the locker, it may affect the reports or filter results in Relaxx.

Automatic conflict resolution for lockers is only possible when the following conditions are met:

- The locker number was previously assigned to the locker in Relaxx and this number currently has a "Not found" status.
- An unassigned locker is identified by the controller.
- Both previous points refer to the same sub controller and the same lock interface on the controller.

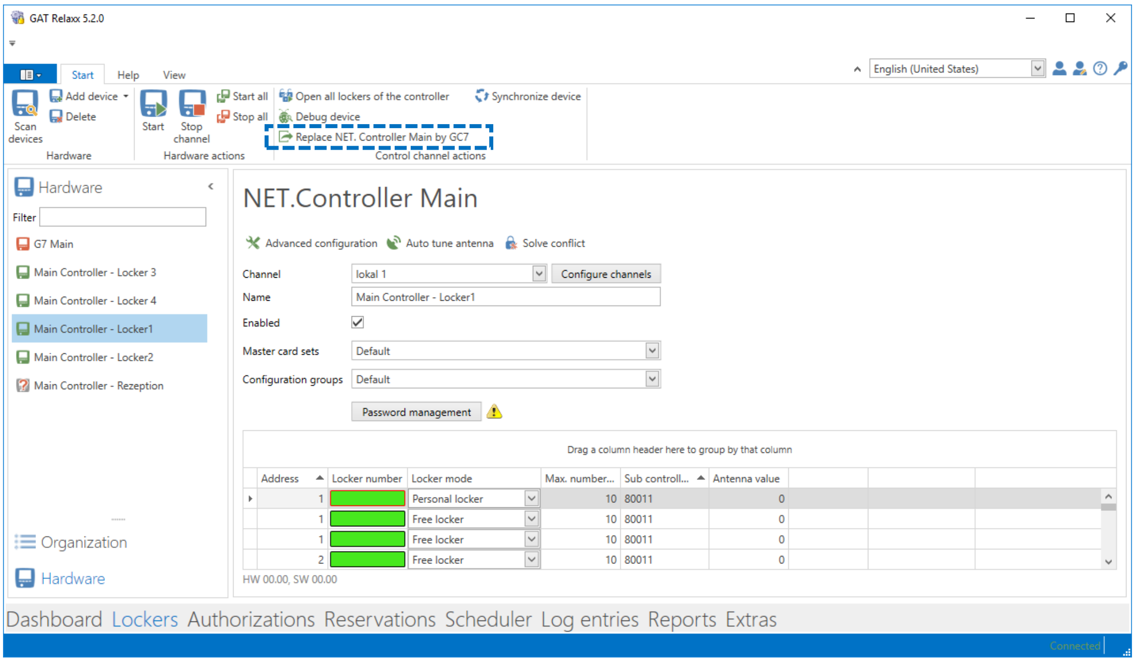
Replacing a GAT Lock Controller 5010 that is attached to a GAT NET.Lock M 7000 main controller
In this case, you must resolve the conflicts manually by setting the correct configuration for the new GAT Lock Controller 5010.

3.2.5 Replacing a GAT NET.Controller M 70x0 with a G7 Main Controller

To replace an existing GAT NET.Controller M 7000 or 7020 with a new G7 main controller, an assistant is integrated in Relaxx that guides you through the exchange process step by step. The locker assignments, both to the locker groups and to the authorizations, and the used free lockers are retained.

► Go to the "Lockers" view and open the "Hardware" page.

► Open the wizard by clicking on the "Replace NET.Controller Main by GC7" option.



NET.Controller Main

Channel: lokal 1
Name: Main Controller - Locker1
Enabled: ☑
Master card sets: Default
Configuration groups: Default

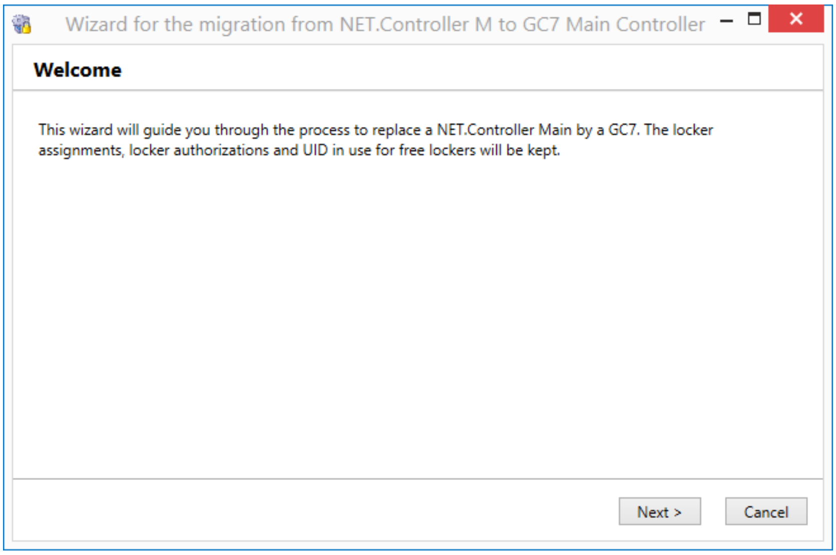
Drag a column header here to group by that column

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value
1	🟩	Personal locker	10	80011	0
1	🟩	Free locker	10	80011	0
1	🟩	Free locker	10	80011	0
2	🟩	Free locker	10	80011	0

HW 00.00, SW 00.00

***Figure 3.32** – Opening the wizard*

- The wizard window opens.



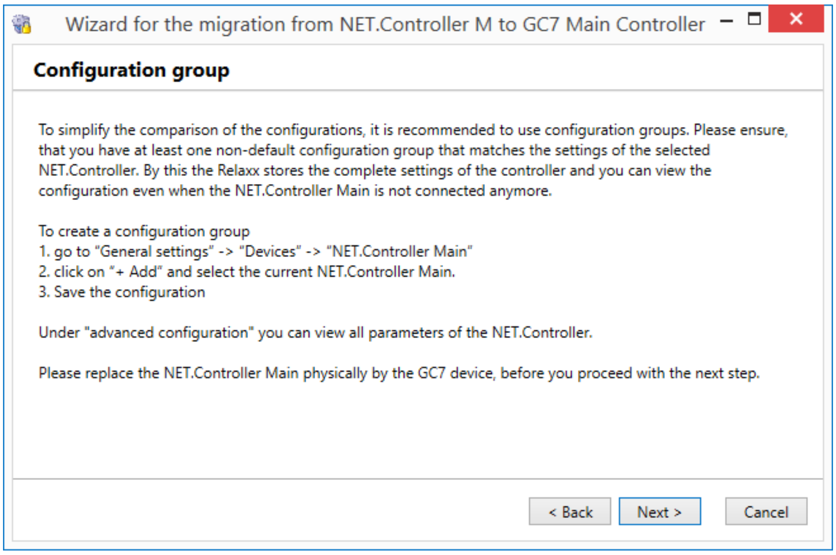
Wizard for the migration from NET.Controller M to GC7 Main Controller

Welcome

This wizard will guide you through the process to replace a NET.Controller Main by a GC7. The locker assignments, locker authorizations and UID in use for free lockers will be kept.

Figure 3.33 *– Wizard to replace a GAT NET.Controller M 70x0 with a G7 main controller - Step 1*

► Click on "Next" in the wizard window.



Wizard for the migration from NET.Controller M to GC7 Main Controller

Configuration group

To simplify the comparison of the configurations, it is recommended to use configuration groups. Please ensure, that you have at least one non-default configuration group that matches the settings of the selected NET.Controller. By this the Relaxx stores the complete settings of the controller and you can view the configuration even when the NET.Controller Main is not connected anymore.

To create a configuration group
1. go to "General settings" -> "Devices" -> "NET.Controller Main"
2. click on "+ Add" and select the current NET.Controller Main.
3. Save the configuration

Under "advanced configuration" you can view all parameters of the NET.Controller.

Please replace the NET.Controller Main physically by the GC7 device, before you proceed with the next step.

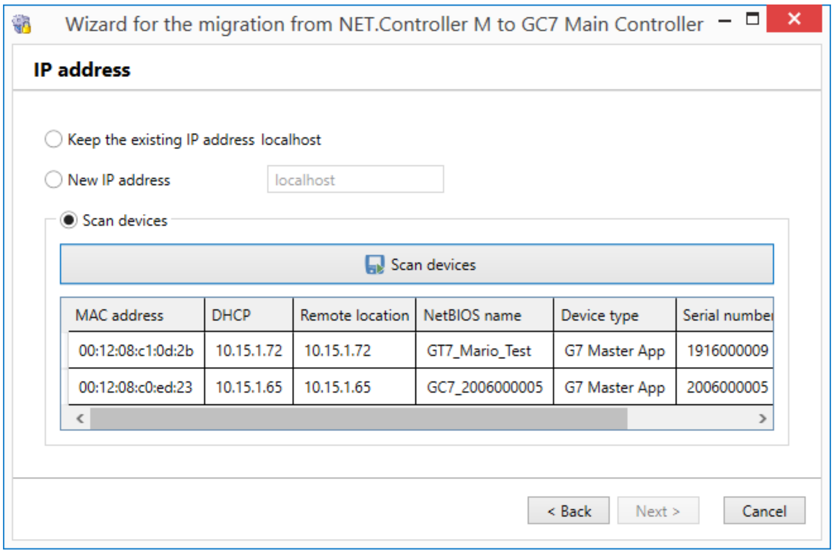
Figure 3.34 *– Wizard to replace a GAT NET.Controller M 70x0 with a G7 main controller - Step 2*

► Create a configuration group with the GAT NET.Controller M 70x0. To do this, open the "Devices" settings page in the program settings and go to the “NET.Controller Main” tab. Select the controller to be replaced and click on “+ Add”.
Note: When creating the configuration group, the configuration settings of the selected controller are saved in the configuration group. This will help later to set the same configuration for the new G7 main controller.

► Stop the channel of the GAT NET.Controller M 70x0.

► Now replace the GAT NET.Controller M 70x0. Disconnect the power supply and network cable and connect the new G7 main controller to the network and power supply.

► Click on “Next”.



Wizard for the migration from NET.Controller M to GC7 Main Controller

IP address

○ Keep the existing IP address localhost

○ New IP address localhost

● Scan devices

Scan devices

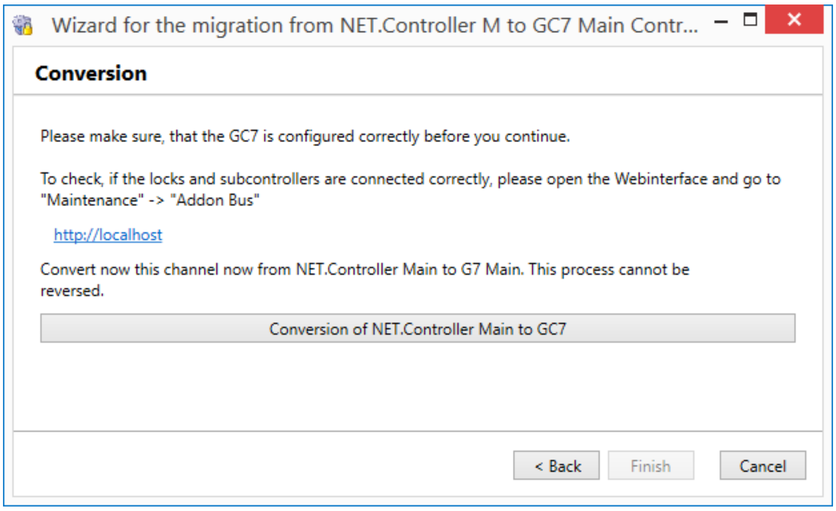
MAC address	DHCP	Remote location	NetBIOS name	Device type	Serial numbe
00:12:08:c1:0d:2b	10.15.1.72	10.15.1.72	GT7_Mario_Test	G7 Master App	1916000009
00:12:08:c0:ed:23	10.15.1.65	10.15.1.65	GC7_2006000005	G7 Master App	2006000005

Figure 3.35 – *Wizard to replace a GAT NET.Controller M 70x0 with a G7 main controller - Step 3*

► Select the new G7 main controller to be added here. You have the following options:

- Keep the existing IP address:	The new G7 main controller is configured so that it uses the same IP address as the GAT NET.Controller being replaced.
- New IP address:	If the G7 main controller is using a different IP address to that of the GAT NET.Controller being replaced, enter it here.
- Search devices:	If you do not know the IP address, click on "Scan devices" and select the G7 main controller that will replace the GAT NET.Controller M 70x0 from the list of found controllers.

► Click on “Next”.



Wizard for the migration from NET.Controller M to GC7 Main Contr...

Conversion

Please make sure, that the GC7 is configured correctly before you continue.

To check, if the locks and subcontrollers are connected correctly, please open the Webinterface and go to "Maintenance" -> "Addon Bus"

http://localhost

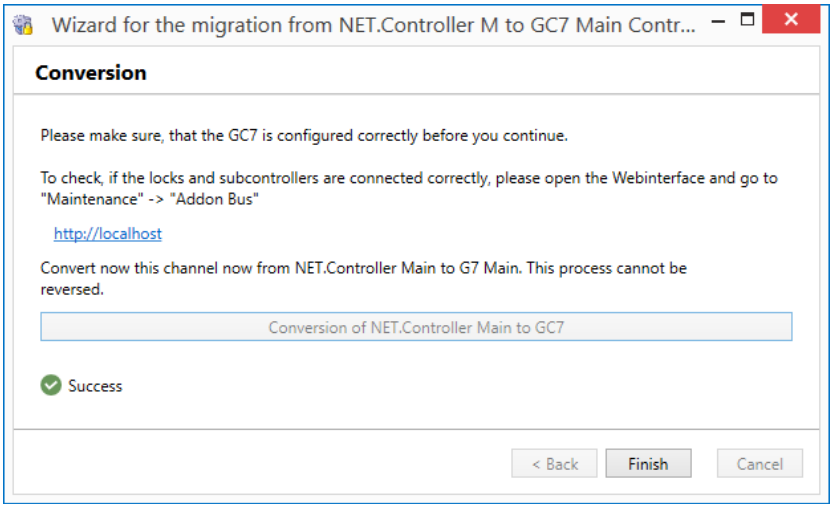
Convert now this channel now from NET.Controller Main to G7 Main. This process cannot be reversed.

Figure 3.36 – *Wizard to replace a GAT NET.Controller M 70x0 with a G7 main controller - Step 4*

- ► Now configure the new G7 main controller with the same settings as the GAT NET.Controller M 70x0 being replaced.

The controller can be configured using a web browser either directly in the web interface of the G7 controller or via G7 Connect (if available). You will need the username and password for the G7 controller web interface or G7 Connect access. Also see the information in the conversion wizard.

- ► If the configuration has been carried out correctly, click on "Conversion of NET.Controller Main to GC7".
  - ○ The replacement is carried out in Relaxx. This step cannot be undone.
  - ○ You will receive a corresponding message to notify of the successful replacement.



Wizard for the migration from NET.Controller M to GC7 Main Contr...

Conversion

Please make sure, that the GC7 is configured correctly before you continue.

To check, if the locks and subcontrollers are connected correctly, please open the Webinterface and go to "Maintenance" -> "Addon Bus"

http://localhost

Convert now this channel now from NET.Controller Main to G7 Main. This process cannot be reversed.

Conversion of NET.Controller Main to GC7

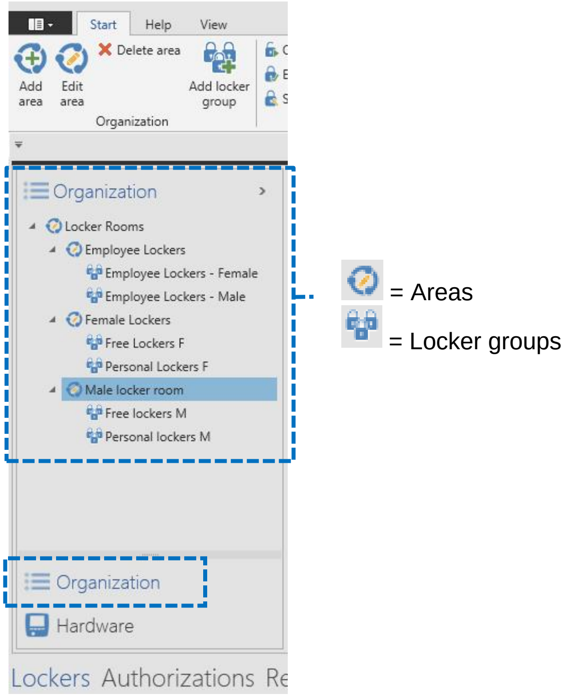
✓ Success

***Figure 3.37** – Wizard to replace a GAT NET.Controller M 70x0 with a G7 main controller - Step 5*

- ► Click on "Finish".
  - ○ The new G7 main controller is added to Relaxx and, if configured correctly, operates with the connected sub controllers and locks in the same way as the replaced GAT NET.Controller M 70x0.
  - ○ The replaced GAT NET.Controller M 70x0 is deleted from Relaxx.

3.2.6 Setting up the Organization System

In the organization view, an overview of the locker system can be configured by creating different areas to which locker groups are assigned. For example, one area can be created as the male locker room and another area as the female locker room, and in each of those two areas one locker group called “Free Lockers” and another locker group called “Personal lockers” can be assigned as shown in the following figure.



= Areas

= Locker groups

Figure 3.38 *- Relaxx organization view*

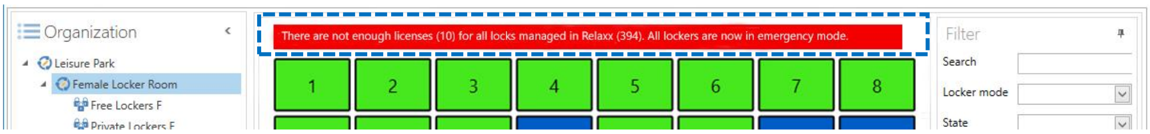
It is recommended to structure the organization system based on the physical arrangement of areas and locker groups so that they match the actual floor plan and locker groupings of the system. This logical arrangement simplifies daily operational tasks such as monitoring the lockers and assigning lockers to users.

The procedure for configuring the organization view is as follows:

Step 1 - Create an "area" in the organization view
Step 2 - Assign one or more locker groups to the area
Step 3 - Assign lockers to the locker groups

Repeat this process as often as required until the entire system is defined. The steps are explained in greater detail in the following sections.

The Relaxx license defines how many locks can be used. If you add more than the maximum number of licensed locks, a warning is displayed in the locker overview and <u>all</u> lockers are set to emergency mode, i.e., they continue to function autonomously according to their configuration. Additional restrictions apply in this instance; see the license definition in "5. LICENSE MANAGEMENT" for more information.



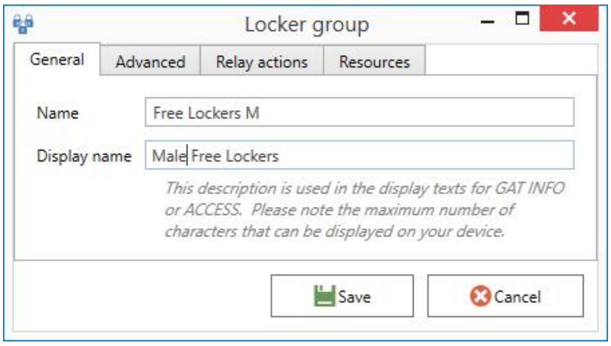
There are not enough licenses (10) for all locks managed in Relaxx (394). All lockers are now in emergency mode.

Step 1 - Creating an "area"

- ► In the organization list, click on an existing area. By default, one empty area is preset that can be configured or deleted.
- ► Click on the "Add area" button.
  - o The "Area" window opens.
- ► Enter a name for the area and confirm by clicking on "Save".
  - o The new area is added below the previously selected area.
- ► To change the name of an area, select the area then click on the "Edit area" button.
- ► To delete an area, select the area then click on the "Delete area" button.
  - o All locker groups assigned to the area are automatically deleted.

Step 2 - Adding a "locker group" to an area

- ► In the organization list, click on an existing area.
- ► Click on the "Add locker group" button.
  - o The "locker group" window opens.



Name: Free Lockers M

Display name: Male Free Lockers

This description is used in the display texts for GAT INFO or ACCESS. Please note the maximum number of characters that can be displayed on your device.

***Figure 3.39** – Locker group window*

In the “General” tab:

- ► Enter a name for the locker group in the "Name" field. The locker group will be displayed with this name in the organization list.
- ► Enter a descriptive text of the locker group in the "Description" field.

In the “Advanced” tab:

- ► Define the following settings (if applicable):

- Free lockers amount: This value determines the maximum number of free lockers in the group that can be locked by a data carrier when the authorization list is disabled.

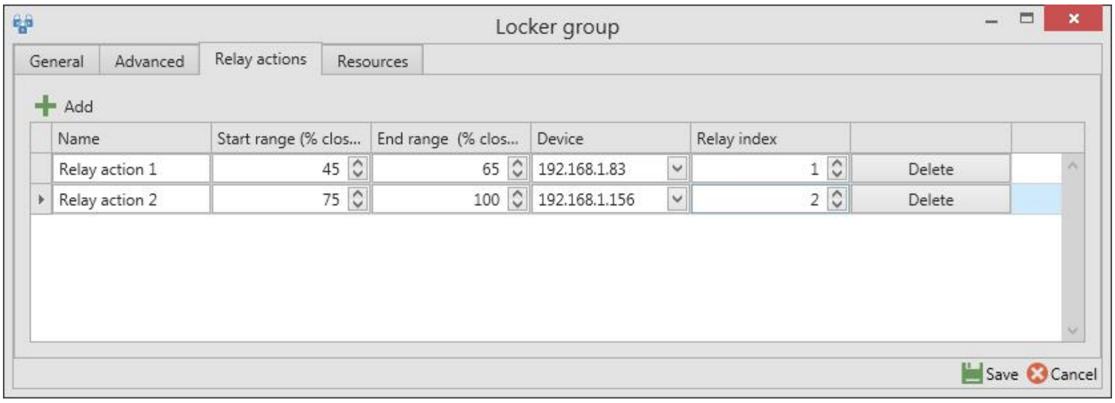
- Custom locker sector (battery lockers):

Define a custom segment for battery lockers used for writing locker authorizations to the data carriers. If you want to use the card settings, leave the field blank. Custom segments are only supported with ISO 15693 and MIFARE data carriers.

- External Id: Here, a unique number for each locker group can be entered that external applications can use to identify the locker group. If this function is not used, the field can be left blank.

In the “Relay actions” tab:

- ► This step is optional. Configure the relays of the controller assigned to the locker group. The relays can be configured to activate once a certain occupancy rate is reached, e.g., 50% of lockers occupied. This feature is useful, e.g., for signaling the occupancy rate via a connected device in order to help manage the locker system.
  - ○ For new locker groups, this window is empty. The following figure is an example with two defined relay actions.



Locker group

Name	Start range (% clos...	End range (% clos...	Device	Relay index	
Relay action 1	45	65	192.168.1.83	1	Delete
Relay action 2	75	100	192.168.1.156	2	Delete

***Figure 3.40** – Defined relay actions (example)*

- ► Click on "+ Add" to define a new relay (max. 4).
  - ○ A new line is added to the list of relay actions.
- ► Enter a "Name" for the relay action (optional).
- ► Enter a start range and an end range in %. If the percentage of locked lockers, i.e., the ratio of locked lockers compared to the total number of lockers in the locker group, is within the range entered here, the relay action is activated.
- ► In the "Device" field, select the main controller (via its IP address) where the action will be implemented.
- ► In the "Relay index" field, enter the number of the relay to be activated.

In the “Resources” tab:

- ► Define the following setting (if applicable):

- Planned usage time: Define a maximum usage time for all lockers in the group. The default value of “00:00:00” means that no maximum usage time is set for the lockers.

- ► Confirm the locker group settings by clicking on "Save".
  - ○ The new locker group is added to the selected area.
- ► To edit the locker group settings, select the locker group then click on the "Edit locker group" button.
- ► To move a locker group to another area, drag and drop the locker group from the current area to the new area.
  - ○ All lockers assigned to the locker group are automatically moved to the new area.
- ► To delete a locker group, select the locker group then click on the "Delete locker group" button.
  - ○ All lockers assigned to the locker group are automatically deleted.

Step 3 - Assigning lockers to a locker group

Lockers can be assigned to the locker groups manually or automatically. Complete the following steps.

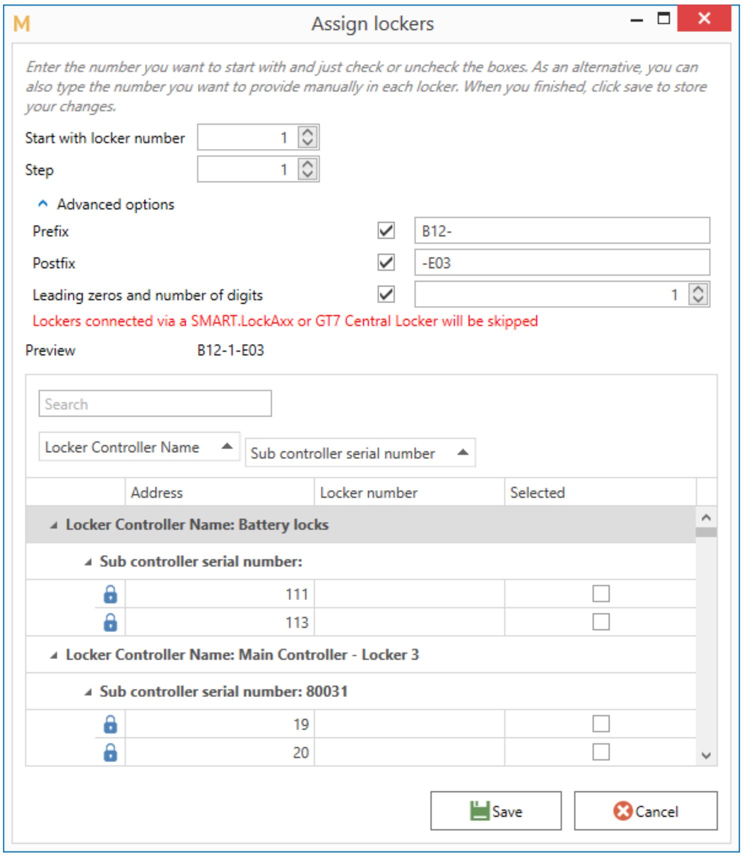
NOTE! In offline mode, it is important that every locker within the system uses a unique locker number. This is particularly important if the system includes both wired locks (e.g., GAT NET.Lock 7000) and battery-powered locks (e.g., GAT ECO.Side Lock 7000).

► In the organization list, click on an existing locker group.

► Click on the "Assign lockers" button then select either manual or automatic locker assignment from the menu:

a) Manual locker assignment

Manual locker assignment allows you to manually assign individual lockers to the locker group from all the available lockers connected to any controller. The following window is displayed after selecting this option:



Assign lockers

Enter the number you want to start with and just check or uncheck the boxes. As an alternative, you can also type the number you want to provide manually in each locker. When you finished, click save to store your changes.

Start with locker number: 1

Step: 1

Advanced options

Prefix	☑	B12-
Postfix	☑	-E03
Leading zeros and number of digits	☑	1

Lockers connected via a SMART.LockAxx or GT7 Central Locker will be skipped

Preview: B12-1-E03

	Address	Locker number	Selected
Locker Controller Name: Battery locks			
Sub controller serial number:			
🔒	111		□
🔒	113		□
Locker Controller Name: Main Controller - Locker 3			
Sub controller serial number: 80031			
🔒	19		□
🔒	20		□

Figure 3.41 – Manual locker assignment

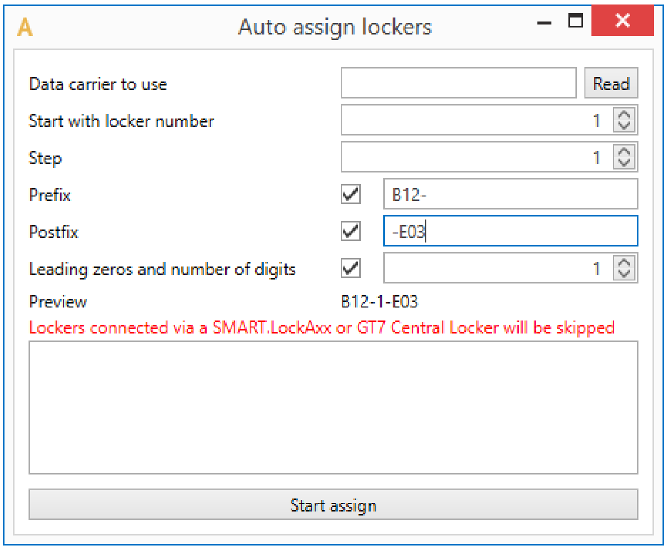
► In the "Start with locker number" field, enter the number to assign to the first selected locker.

► In the "Step" field, you can enter a step size for numbering the cabinets. Example: With "2" you can assign all even or odd numbers depending on the start value.

- ► Click on "Advanced Settings" to open further options:
  - In the "Prefix" and "Postfix" fields, you can enter alphanumeric values that are inserted before or after the locker numbers.
  - If you select the "Leading zeros and number of digits" option, you can enter a number that determines the length of the displayed locker number. Missing places are filled with leading zeros. Example: "4" -> 0001, 0002, 0012, 0123, 1234.
  - The text in the "Preview" field is a continuously updated display of how the number will be displayed with the settings.
- ► In the “Selected” column of the displayed list, mark all lockers to be assigned to the locker group.
  - o The locker numbers are assigned automatically, beginning with the entered start number, and increasing by the entered increment.
- ► It is also possible to change individual locker numbers manually.
- ► After assigning all lockers, click on "Save".

b) With data carrier locker assignment

With this method, the lockers are locked on-site using a data carrier or simply by pressing the locker door shut, which automatically assigns the locker to the selected locker group with a number. The following window is displayed:



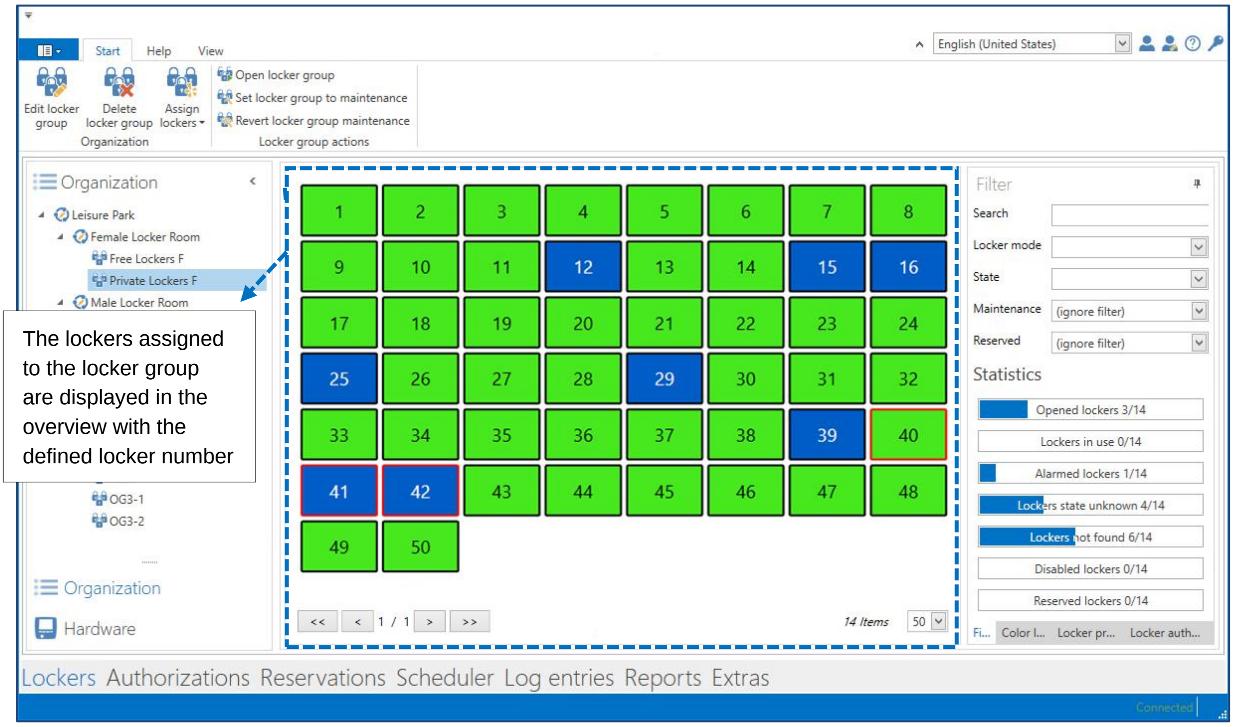
Data carrier to use		
Start with locker number		1
Step		1
Prefix	☑	B12-
Postfix	☑	-E03
Leading zeros and number of digits	☑	1
Preview	B12-1-E03	

Lockers connected via a SMART.LockAxx or GT7 Central Locker will be skipped

Figure 3.42 *- Automatic locker assignment*

- ► If you want to use a data carrier for the automatic locker assignment, enter the UID number of the data carrier into the “Data carrier to use” field. Via the "Read" button, the UID number can be entered automatically by placing the data carrier onto a connected read / write station (GAT Writer).

  NOTE! It is possible to assign the lockers without using a data carrier simply by pressing the locker doors shut in succession. However, this method is more error-prone, and it is recommended to assign the lockers using a data carrier.
- ► In the "Start with locker number" field, enter the number to assign to the first selected locker.
- ► In the "Step" field, you can enter a step size for numbering the cabinets. Example: With "2" you can assign all even or odd numbers depending on the start value.
- ► In the "Prefix" and "Postfix" fields, you can enter alphanumeric values that are inserted before or after the locker numbers.
- ► If you select the "Leading zeros and number of digits" option, you can enter a number that determines the length of the displayed locker number. Missing places are filled with leading zeros. Example: "4" -> 0001, 0002, 0012, 0123, 1234.
- ► The text in the "Preview" field is a continuously updated display of how the number will be displayed with the settings.
- ► Click on "Start assign".
- ► Lock all lockers in the order that they should be assigned to the selected locker group.
  - ○ The lockers are assigned numbers in increasing order, beginning with the entered start number, and assigned to the locker group.
- ► Once all lockers are assigned, close the window via the red "X" icon.
- ► The lockers locked during the assignment process can all be opened again via the “Open locker group” button (refer to "3.3.4 Locker Actions").
  - ○ The assigned lockers are displayed in the locker overview when the locker group is selected.



The lockers assigned to the locker group are displayed in the overview with the defined locker number

***Figure 3.43** – Display of the assigned lockers of a locker group*

NOTE! When an area is selected, the lockers included in all the locker groups assigned to the area are displayed. Information about a selected locker is displayed in "Locker properties" to the right of the locker overview.

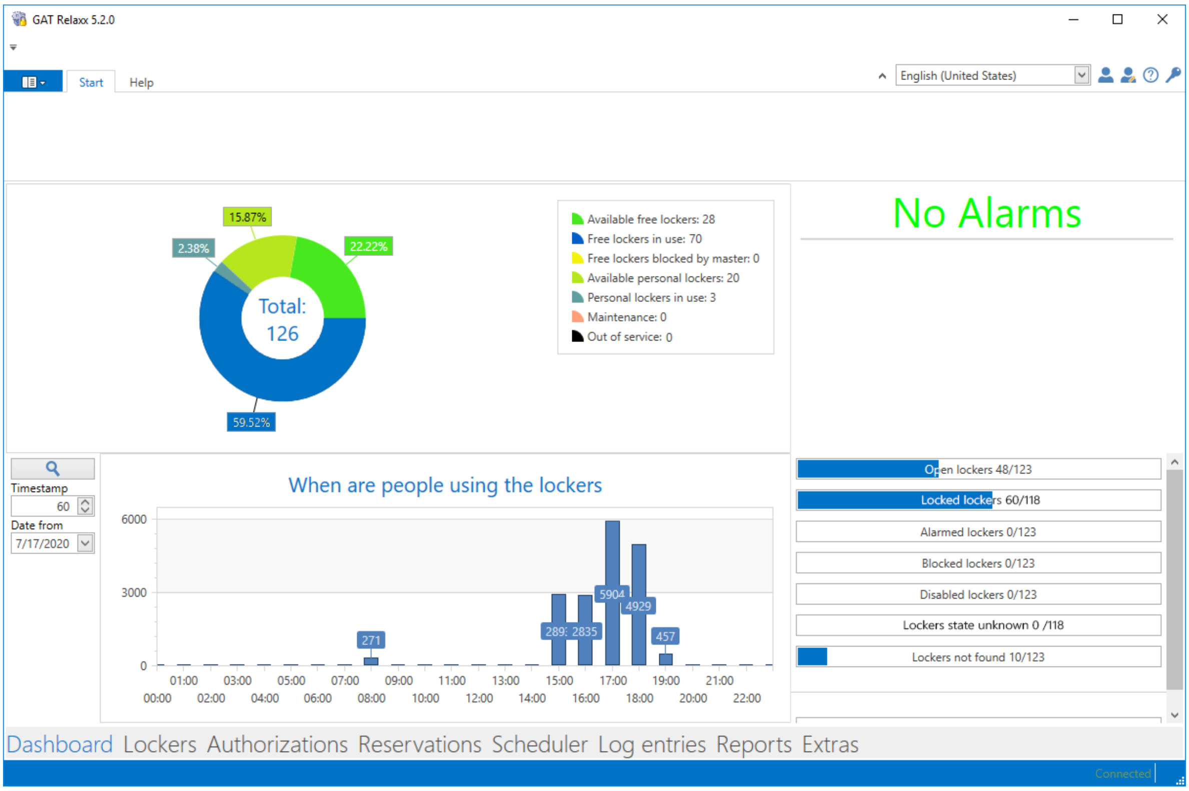
3.3 Operating / Monitoring the Locker System and GANTNER Devices

The organization view or the dashboard page can be used to monitor the lockers within a system. When an area or a locker group is selected in the organization list, the assigned lockers are displayed in the overview. Above the overview, actions are available to complete different tasks. These actions change depending on whether an area, sub area, or a locker group is selected in the organization list.

The locker information area to the right of the overview provides information and statistics on individual lockers. The area is divided into four sections – filter, color legend, locker properties, and locker authorizations – with each section accessible by clicking on the tabs at the bottom of the area.

3.3.1 Dashboard

After starting and logging in to Relaxx, the dashboard is displayed. Clearly displayed in this window are the current occupancy and time usage statistics of the lockers. The dashboard can also be opened at any time by clicking on the "Dashboard" work area.



Available free lockers: 28
Free lockers in use: 70
Free lockers blocked by master: 0
Available personal lockers: 20
Personal lockers in use: 3
Maintenance: 0
Out of service: 0

Open lockers 48/123
Locked lockers 60/118
Alarmed lockers 0/123
Blocked lockers 0/123
Disabled lockers 0/123
Lockers state unknown 0 /118
Lockers not found 10/123

Bild 3.44 *- Dashboard*

The dashboard is helpful for a statistical overview of all lockers in the system. An exact status display of each individual locker and operation of the lockers is not possible here (see the following points). For information on the display elements, see "3.1 Software Window Elements".

3.3.2 Organization Actions

The organization actions displayed in the first section of the function bar are used to set up the organization view. This process is explained in section “3.2.6 Setting up the Organization System”.

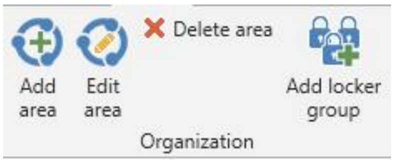


Figure 3.45 *- Organization actions*

3.3.3 Locker Group Actions

When a locker group is selected in the organization overview, various actions can be conducted on all lockers within that group. The following actions are available in the function bar:

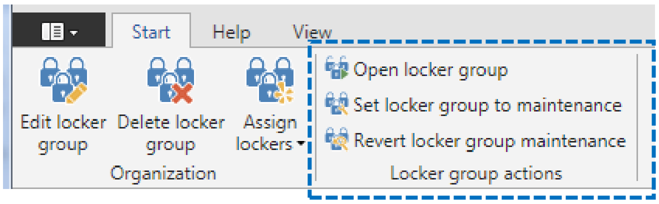
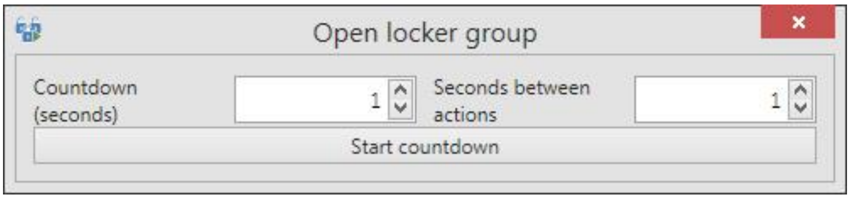


Figure 3.46 *- Locker group actions*

For security reasons, the user must enter their username and password in order to execute a locker group action. This option can be configured for individual users via the authorization settings (see "Login for locker commands" in "4.3.2. Default ").

All locker group actions performed by the user are recorded by Relaxx in the log system (refer to “3.7 Log Entries), thereby allowing executed actions to be reviewed at a later date.

- Open locker group: Opens all lockers in the locker group, irrespective of the locker mode or reservation state. After selecting the action and entering the user information, the following window is displayed.



Countdown (seconds) 1
Seconds between actions 1

Figure 3.47 *– Open locker group*

The value in the "Countdown" field determines how many seconds after clicking on the "Start countdown" button the first locker will be opened. All subsequent lockers will be opened consecutively at intervals defined in the "Seconds between actions" field.

- Set locker group to maintenance:
  This action sets all lockers in the locker group to maintenance mode (the status LED flashes red/green). The lockers are not available for use while maintenance mode is enabled. This action does not change the current locker state (locked or unlocked). Lockers in maintenance mode are identified with an orange marking (refer to "3.3.7 Color Legend").
- Revert locker group maintenance:
  This action returns all lockers in the locker group that are operating in maintenance mode to their normal operating mode.

3.3.4 Locker Actions

When a locker is selected in the locker overview, various actions can be conducted on that locker. The following actions are available in the function bar or via a pop-up menu after right-clicking on the locker in the overview.

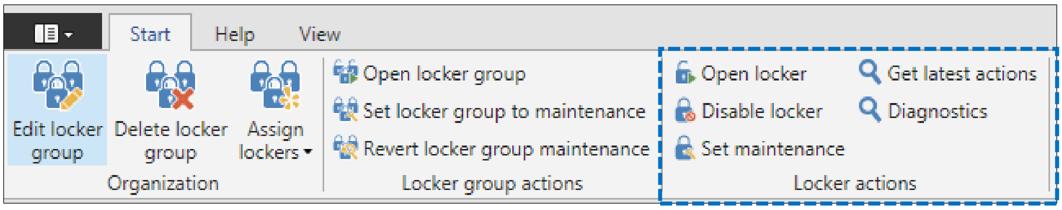


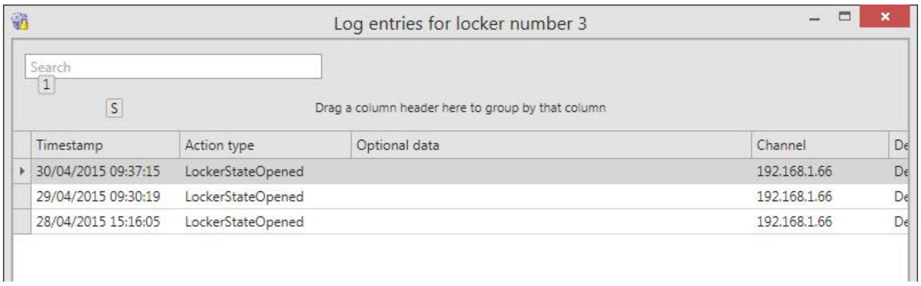
Figure 3.48 *- Locker actions*

For security reasons, the user must enter their username and password in order to execute certain locker actions. This option can be configured for individual users via their authorization settings (see "Login for locker commands" in "4.3.2. Default ").

NOTE! All locker actions executed by the user are recorded by Relaxx in the log system (refer to “3.7 Log Entries), thereby allowing executed actions to be reviewed at a later point in time.

- Open locker: Opens the selected locker, irrespective of the locker mode or reservation state.
- Enable / disable locker: If a locker is disabled, it is out of service and cannot be used any more, until it is enabled again.
- Set/Revert maintenance mode:
  When a locker is put into maintenance mode, it is out of service and cannot be used any more. Maintenance mode is also enabled automatically after a reservation has expired to allow for cleaning before being used again.

- Get latest actions: The following “Log entries” window opens after clicking on this button.



Log entries for locker number 3

Search

1

S

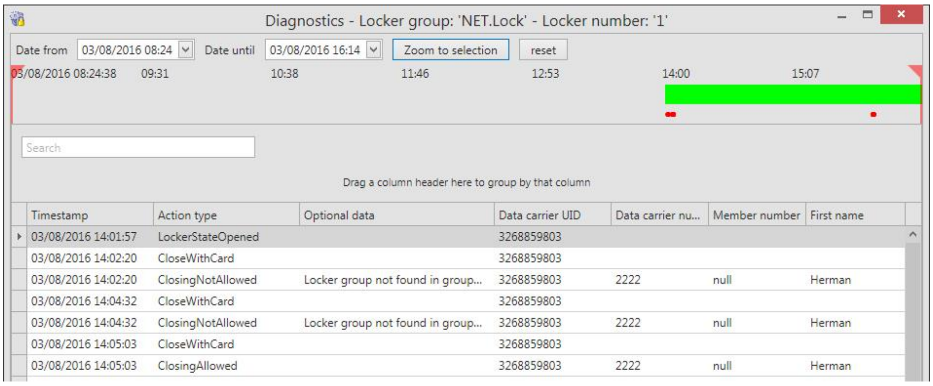
Drag a column header here to group by that column

Timestamp	Action type	Optional data	Channel	De
30/04/2015 09:37:15	LockerStateOpened		192.168.1.66	De
29/04/2015 09:30:19	LockerStateOpened		192.168.1.66	De
28/04/2015 15:16:05	LockerStateOpened		192.168.1.66	De

***Figure 3.49** – Log of the latest locker actions*

This window lists all actions executed on this locker, including all actions implemented by users in Relaxx, e.g., opening all lockers (action type = "UserActionRequested").

- Diagnostics: The following “Diagnostics” window opens after clicking on this button. In this window you can see all actions that were recorded at the selected locker.



Diagnostics - Locker group: 'NET.Lock' - Locker number: '1'

Date from 03/08/2016 08:24 Date until 03/08/2016 16:14

Search

Drag a column header here to group by that column

Timestamp	Action type	Optional data	Data carrier UID	Data carrier nu...	Member number	First name
03/08/2016 14:01:57	LockerStateOpened		3268859803			
03/08/2016 14:02:20	CloseWithCard		3268859803			
03/08/2016 14:02:20	ClosingNotAllowed	Locker group not found in group...	3268859803	2222	null	Herman
03/08/2016 14:04:32	CloseWithCard		3268859803			
03/08/2016 14:04:32	ClosingNotAllowed	Locker group not found in group...	3268859803	2222	null	Herman
03/08/2016 14:05:03	CloseWithCard		3268859803			
03/08/2016 14:05:03	ClosingAllowed		3268859803	2222	null	Herman

***Figure 3.50** - Diagnostics window for locker groups*

The default date range for displayed actions is one week, which can be adjusted via the “Date from / Date until” fields or by sliding the red flags and clicking on “Zoom to selection”. The red dots in the date range indicate when an action was recorded at the locker with specific information about each action displayed below. The list only shows the actions within the selected timespan.

3.3.5 Channel Actions

When a channel is selected in the hardware list, the following actions become available in the menu bar that can be applied to all lockers assigned to the channel.

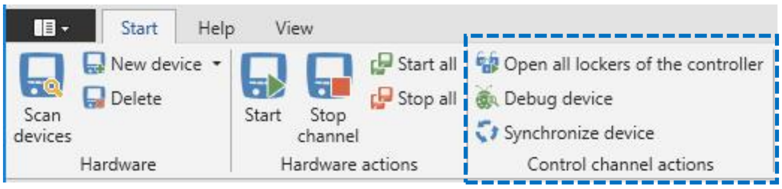


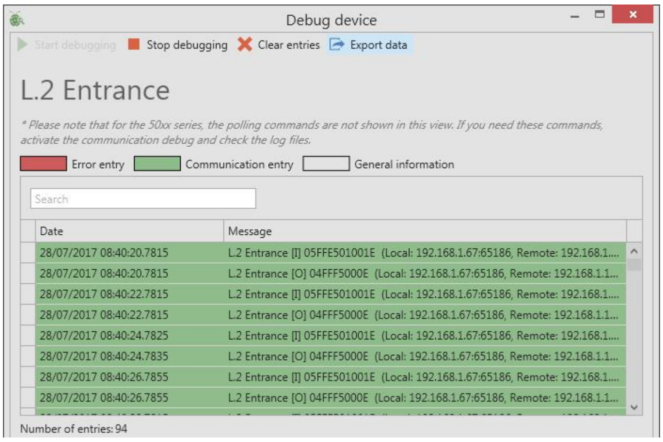
***Figure 3.51** – Channel actions*

NOTE! All channel actions and the user who executed the action are recorded by Relaxx (refer to “3.7 Log Entries), thereby allowing executed actions to be reviewed at a later point in time.

- Open all lockers of the controller:

  Opens all lockers connected to the controllers of that channel, irrespective of the locker mode or reservation state. The user must enter their username and password in order to execute this action.

- Debug device: This action opens the "Debug device" window.



L.2 Entrance

** Please note that for the 50xx series, the polling commands are not shown in this view. If you need these commands, activate the communication debug and check the log files.*

🟥 Error entry 🟩 Communication entry □ General information

Search

Date	Message
28/07/2017 08:40:20.7815	L2 Entrance [I] 05FFE501001E (Local: 192.168.1.67:65186, Remote: 192.168.1....
28/07/2017 08:40:20.7815	L2 Entrance [O] 04FFF5000E (Local: 192.168.1.67:65186, Remote: 192.168.1.1...
28/07/2017 08:40:22.7815	L2 Entrance [I] 05FFE501001E (Local: 192.168.1.67:65186, Remote: 192.168.1....
28/07/2017 08:40:22.7815	L2 Entrance [O] 04FFF5000E (Local: 192.168.1.67:65186, Remote: 192.168.1.1...
28/07/2017 08:40:24.7825	L2 Entrance [I] 05FFE501001E (Local: 192.168.1.67:65186, Remote: 192.168.1....
28/07/2017 08:40:24.7835	L2 Entrance [O] 04FFF5000E (Local: 192.168.1.67:65186, Remote: 192.168.1.1...
28/07/2017 08:40:26.7855	L2 Entrance [I] 05FFE501001E (Local: 192.168.1.67:65186, Remote: 192.168.1....
28/07/2017 08:40:26.7855	L2 Entrance [O] 04FFF5000E (Local: 192.168.1.67:65186, Remote: 192.168.1.1...

Number of entries: 94

***Figure 3.52** – Debug device window*

The commands forwarded by this channel are displayed directly in the window, which is helpful for troubleshooting. One command at a time is displayed. To display the next command, click on "Stop debugging" once then "Start debugging" again. To export the debug device information to a CSV file, click on “Export data”.

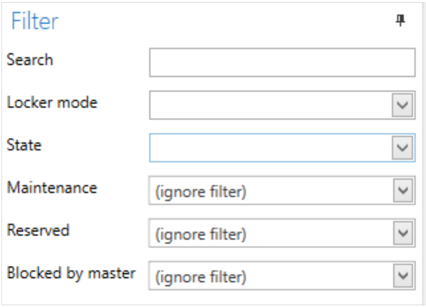
NOTE! This function should only be used for troubleshooting in the event of an error as it can slow the system down.

- Synchronize device: With this button the device at the selected channel is synchronized. In this process the following steps are performed:

  1. Load locker configuration of all lockers into the device:
     - Locker number, locker group, mode
     - Assigned personal locker authorizations
     - Set/reset "Reserved" state
     - Read locker state
  2. Stop device
  3. Start device

3.3.6 Filter and Locker Statistics

The “Filter and Statistics” tab in the locker information area allows you to search for an individual locker or locker type. For example, you can quickly find all unoccupied free lockers in a specific area or filter the entire locker system for any lockers that have had an alarm activated. Four filter parameters are provided in this area to refine the search. After entering the parameter(s), all lockers that match the filter criteria are automatically displayed in the overview.



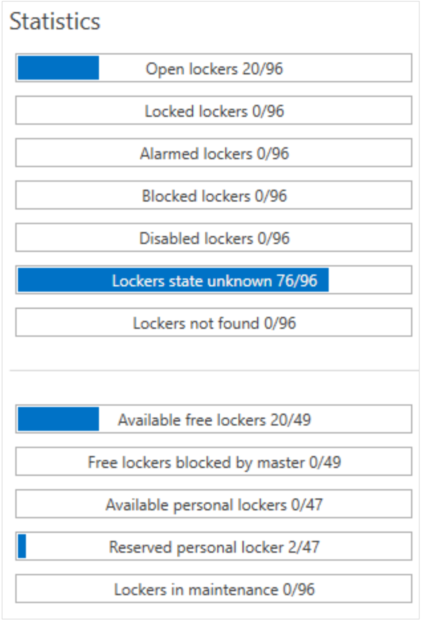
Filter

Search	
Locker mode	
State	
Maintenance	(ignore filter)
Reserved	(ignore filter)
Blocked by master	(ignore filter)

Figure 3.53 – *Filter for search terms*

- Search: You can enter a search term here and then press "Enter". All locker numbers, locker groups, and data carriers that are in use (free and personal lockers) are searched and all found elements that contain the search term are displayed.
- Locker mode / State: Select one or more locker modes or states. All lockers with these modes or states are displayed. If nothing is selected, all lockers are displayed.
- Maintenance, Reserved, Blocked by master: Select whether lockers in maintenance mode, reserved lockers and/or lockers that are blocked with a MASTER data carrier should be displayed or not. With "(ignore filter)", all relevant lockers are displayed.

Beneath the filter in the statistics area, different status data relating to the entered parameters are displayed in bar graph format. If no parameters are entered into the filter, the statistics shown represent the entire selected locker group or area.



Statistics

Open lockers 20/96
Locked lockers 0/96
Alarmed lockers 0/96
Blocked lockers 0/96
Disabled lockers 0/96
Lockers state unknown 76/96
Lockers not found 0/96

Available free lockers 20/49
Free lockers blocked by master 0/49
Available personal lockers 0/47
Reserved personal locker 2/47
Lockers in maintenance 0/96

- Open lockers: Number of unlocked lockers.
- Locked lockers: Number of locked lockers.
- Alarmed lockers: Number of lockers with an activated alarm.
- Blocked lockers: Number of lockers that have a mechanically blocked door.
- Disabled lockers: Number of deactivated lockers that are not available for use (no function).
- Locker state unknown: Number of lockers where the operating state is unknown, i.e., communication with the locker cannot be established.
- Lockers not found: Number of lockers where communication with the locker has been broken.
- Available free lockers: Number of free lockers available for use.
- Free lockers blocked by master: Free lockers that are currently not usable (locked/blocked with a MASTER data carrier).
- Available personal lockers: Number of personal lockers available for use.
- Reserved lockers: Number of reserved lockers with a currently active reservation time.
- Lockers in maintenance: Number of lockers currently in maintenance mode (e.g., after a reservation has expired).

Figure 3.54 - *Locker statistics*

3.3.7 Color Legend

Every locker in the locker overview is represented with a background color indicating the current state of the locker. The different locker states are represented by the following default colors, which can be changed via the color settings (refer to “2.2.12. Advanced”).

Open	Locker available (not locked). Locker LED flashes green.
Closed	Locker closed (locked). Locker LED flashes red.
Alarm	An alarm has been triggered for the locker. Locker LED flashes 3 x red.
Blocked	Locker locked and blocked (only for the GAT Lock 5020 system).
Disabled	Locker out of operation (not useable).
Not found	Communication to the locker interrupted.
Unknown	Status unknown (e.g., no communication with the locker / controller).

Furthermore, the mode of a locker is represented by a colored frame. Refer to "1.4 Terminology" for an explanation of the various locker modes.

□ : Free locker	□ : Dynamic locker
□ : Personal locker	□ : Reservable locker

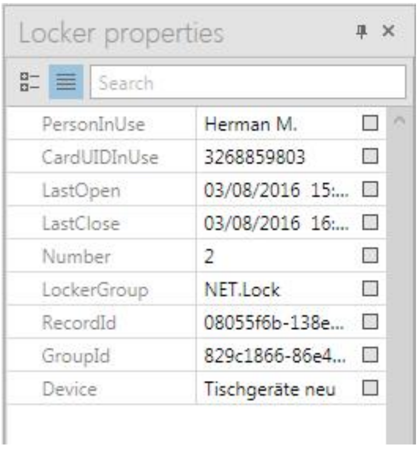
Secondary locker states are displayed as follows:

Reserved	Locker is reserved and the reservation period is currently active. If the locker is locked during this period, the LED on the locker is red with a short green flash every 2 seconds.
Maintenance	Locker is in maintenance mode (not usable). LED on the locker is disabled.

If desired, the default colors can be individually changed in the system settings (refer to "2.2.12. Advanced”).

3.3.8 Locker Properties

The locker properties section provides detailed information about individual lockers. To view the information, simply click on a locker in the overview.



Locker properties

Search

PersonInUse	Herman M.	□
CardUIDInUse	3268859803	□
LastOpen	03/08/2016 15:...	□
LastClose	03/08/2016 16:...	□
Number	2	□
LockerGroup	NET.Lock	□
RecordId	08055f6b-138e...	□
GroupId	829c1866-86e4...	□
Device	Tischgeräte neu	□

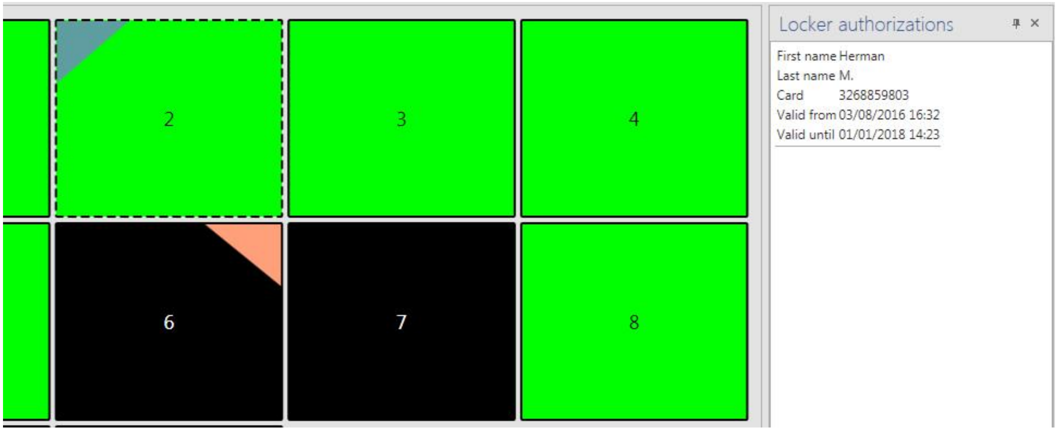
Figure 3.55 *- Locker properties*

The fields are defined as follows:

- PersonInUse: If a locker is locked, the name of the person currently using the locker is displayed here. The name is determined via the UID number of the data carrier used and the authorization list of Relaxx. If the data carrier is not assigned to the authorization list, e.g., because the authorization list is not enabled, this field remains empty and only the UID number of the data carrier is displayed.
- CardUIDInUse: If a locker is currently locked, the UID number of the data carrier used to lock the locker is displayed here.
- LastOpen: Shows the date and time when the locker was last unlocked.
- LastClose: Shows the date and time when the locker was last locked.
- Number: The locker number assigned to the locker. Also displayed in the locker overview.
- LockerGroup: Name of the locker group to which the locker is assigned.
- RecordId: ID number of the locker (assigned by Relaxx).
- GroupId: ID number of the locker group (assigned by Relaxx).
- Device: The name of the main controller via which the lock is communicating with Relaxx.

3.3.9 Locker Authorizations

The locker authorization section provides information about the authorizations that are assigned to the currently selected locker. Authorizations can be assigned to rental lockers, which are indicated by a blue triangle in the top-left corner. To view the information, click on a locker in the overview then click on the locker authorizations tab.



First name Herman
Last name M.
Card 3268859803
Valid from 03/08/2016 16:32
Valid until 01/01/2018 14:23

Figure 3.56 *- Locker authorizations assigned to a selected locker*

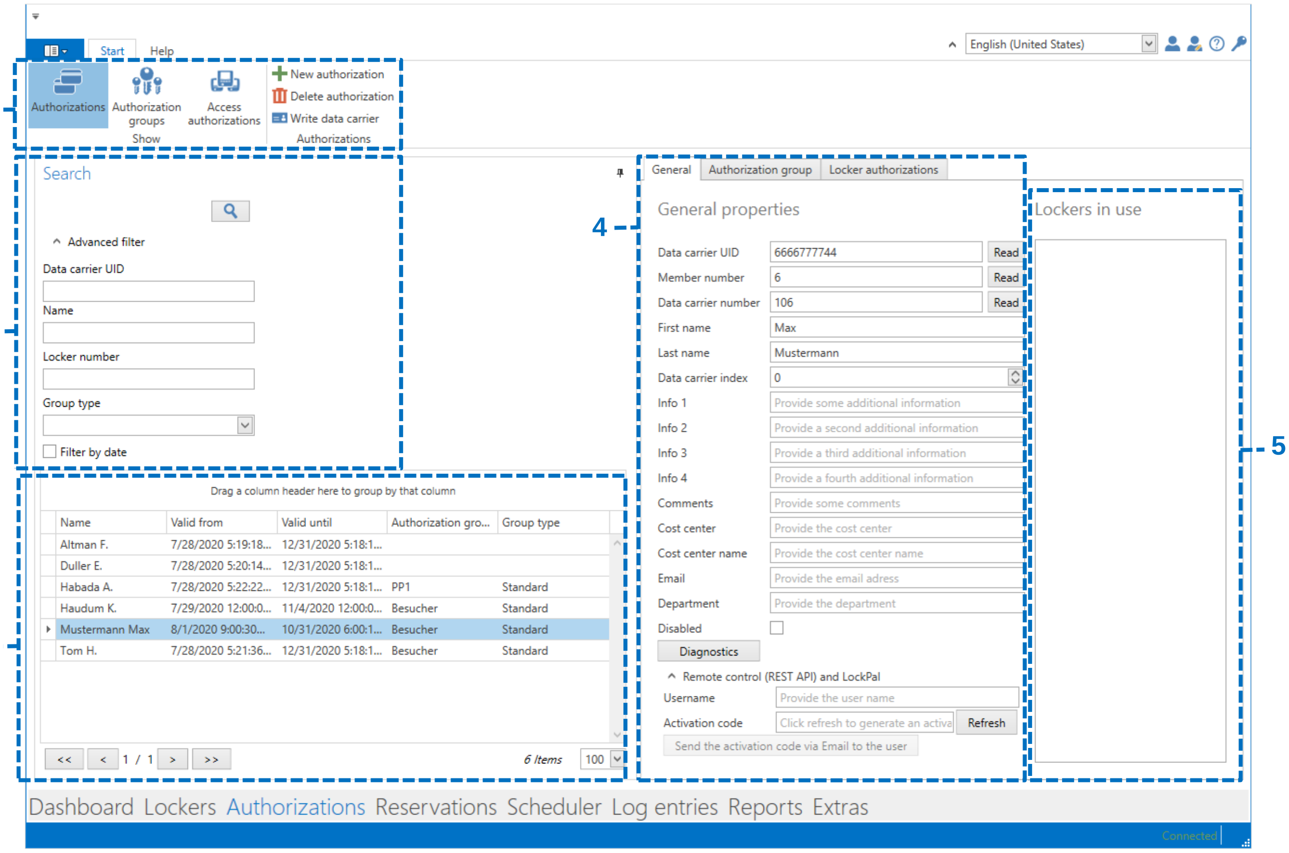
Refer to section “3.4 Administration of Visitors / Data Carriers (Authorization List)” for more information regarding authorizations.

3.4 Administration of Visitors / Data Carriers (Authorization List)

The purpose of the authorization list is to authorize data carriers, and the people assigned to them, for use in the locker system. The following actions are possible:

- Create and assign data carriers to system users.
- Authorize or deauthorize data carriers for lockers operating in free locker mode.
- Assign data carriers to personal lockers.

Switch to the "Authorizations" view to view and configure the authorization list. The authorizations view is empty after opening, even when data carriers and authorizations have been previously defined. It is necessary to click on the “Search” icon to display all previously defined data carriers.



Name	Valid from	Valid until	Authorization gro...	Group type
Altman F.	7/28/2020 5:19:18...	12/31/2020 5:18:1...		
Duller E.	7/28/2020 5:20:14...	12/31/2020 5:18:1...		
Habada A.	7/28/2020 5:22:22...	12/31/2020 5:18:1...	PP1	Standard
Haudum K.	7/29/2020 12:00:0...	11/4/2020 12:00:0...	Besucher	Standard
Mustermann Max	8/1/2020 9:00:30...	10/31/2020 6:00:1...	Besucher	Standard
Tom H.	7/28/2020 5:21:36...	12/31/2020 5:18:1...	Besucher	Standard

Data carrier UID: 6666777744
Member number: 6
Data carrier number: 106
First name: Max
Last name: Mustermann
Data carrier index: 0

__Figure 3.57__ - Authorizations list

The authorizations view is divided into several areas:

1 Multifunction bar: All functions that are available for the currently selected view are displayed here. Via the first 3 symbols you can switch to the respective view for editing the data carrier authorizations, the authorization groups, and the access authorizations.

2 Search area: The authorization list can be searched here. To do this, enter the information you are looking for (e.g., a name or a data carrier number). Only partial information can be entered. More search options are available by clicking on "Advanced filter".

3	Data carrier list:	All data carriers in the authorization list that match the search criteria are displayed here.
4	Data carrier settings:	The settings of the data carrier selected in the list can be viewed and edited here. Click on "∨ Advanced" to display more settings. Three sections are available for selection: - "General" -> General data for data carriers and persons. - "Authorization group" -> Settings for free lockers. - "Locker authorizations" -> For assigning personal lockers.
5	Lockers in use:	Any lockers that are currently in use (locked) by the selected data carrier are displayed here.

3.4.1 Overview of Authorization Settings and Locker Modes

The "Authorizations" view provides access to various authorization settings that affect how data carriers interact with lockers operating in free locker and personal locker mode. These settings operate in combination to determine which lockers can be used by which data carrier.
The "Reservations" view provides access to the reservable lockers and is used to create reservations for customers (i.e. data carriers) in the system.

Free Locker Mode:
The "Authorization list enabled" option in the general settings of Relaxx (see "2.2.6 Authorizations") determines how data carriers are handled with lockers operating in free locker mode. There are two possibilities:

a) Disabled authorization list:
Every valid data carrier in the system, i.e., with a valid site key and correct RFID standard, is authorized to use any available free locker in the system. Locker groups are not checked, and data carriers do not have to be added to the authorization list.

b) Enabled authorization list:
Several settings determine whether a data carrier can use lockers operating in free locker mode and which lockers the data carrier can use:

- The data carrier must be added to the authorization list.
- The data carrier must be assigned to an authorization group via the "Authorization group" tab. The assigned authorization group determines which group of free lockers the data carrier can use.
- Authorization groups are defined via the "Authorization groups" icon in the multifunction bar (1). There are different possibilities for controlling the authorizations of an authorization group, e.g., type of authorization group, assigned locker groups and/or locker areas, time intervals, number of simultaneously usable lockers.
- The "Max. allowed lockers" setting determines how many lockers can be simultaneously locked by a data carrier. This setting is configured collectively for the authorization group and individually for each data carrier. The lower of these two values determines the actual max. number.

Personal Locker Mode:
Lockers operating in personal locker mode can only be used by data carriers that are specifically assigned to the personal locker. The process for authorizing data carriers for personal lockers is:

- Add the data carrier to the authorization list via the "New authorization" button on the "Authorizations" tab.

- Assign the selected data carrier to one or more personal lockers via the "Locker authorizations" tab.
- Define a validity period for the data carrier (optional).
- Set the max. allowed number of data carriers for each personal locker via the "Hardware" section of the "Lockers" view.
- The "Authorization list enabled" setting in the multifunction bar (1) is only valid for free locker mode and does not affect personal locker mode.

Reservable Locker Mode:
Lockers operating in reservable locker mode can only be used by data carriers that are specifically assigned to the reservable locker. The process for authorizing data carriers for reservable lockers is:

- Add a new reservation via the "Reservations" view and define a validity period for the reservation.
- Assign a reservable locker to the reservation.
- Assign a data carrier to the reservable locker in the reservation.
- It is possible to assign several reservable lockers and data carriers to one reservation.
- Following configuration, the data carrier(s) can use the reservable locker within the set validity period.

Dynamic Locker Mode:
Lockers operating in dynamic locker mode function the same way as a free locker (see above) as long as no authorization is assigned. The same data carrier processes are performed (check whether the authorization list is enabled, check for locker groups, etc.). When a valid data carrier locks an available dynamic locker, the data carrier is automatically assigned to the locker and an authorization for the data carrier is added to the authorization list. From then on, the locker operates as a personal locker. Note the following limitations:

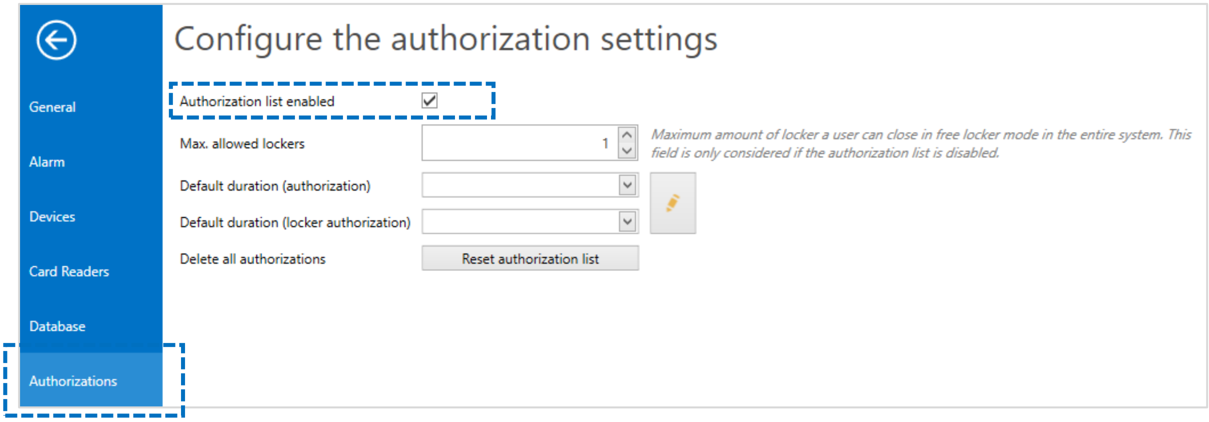
- Dynamic mode is only possible in online systems.
- Only one locker authorization is automatically assigned. However, it is possible to add additional locker authorizations manually in Relaxx.
- If a data carrier already has an authorization for a dynamic locker, it cannot be automatically added to another dynamic locker.
- Incompatible with the GAT SMART.LockAxx 6350 and GAT Lock 50xx systems. Partial compatibility with emergency mode (no locker authorizations can be added in emergency mode).
- Special LED status signals are only supported by the GAT NET.Lock 7000.

3.4.2 Enable or Disable the Authorization List

The authorization list can be enabled or disabled and is only applicable for lockers in free locker mode. When the authorization list is enabled, the authorizations defined in the authorization list apply. Data carriers not included in the authorization list, or with an expired authorization period, cannot use (lock/unlock) lockers operating in free locker mode. When the authorization list is disabled, all data carriers (provided they have a valid FID) can lock and unlock lockers that are operating in free locker mode.

NOTE! Personal lockers and reserved lockers are not affected by whether the authorization list is enabled or disabled.

- ► Open the software settings (icon) and click on the "Authorizations" settings.
- ► Click on the "Authorization list enabled" setting to enable (option selected) or disable (option not selected) the authorization list.



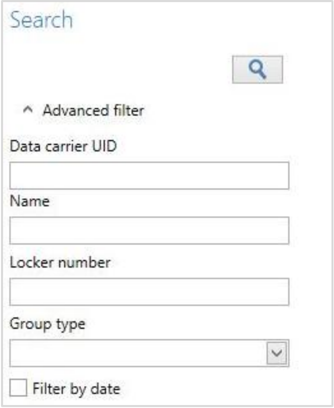
Configure the authorization settings

Authorization list enabled	☑	
Max. allowed lockers	1	Maximum amount of locker a user can close in free locker mode in the entire system. This field is only considered if the authorization list is disabled.
Default duration (authorization)		
Default duration (locker authorization)		
Delete all authorizations	Reset authorization list	

Figure 3.58 – *Enable/disable the authorization list*

3.4.3 Searching the Authorization List

You can search for a specific data carrier in the authorization list by entering an identifier, e.g., the data carrier UID, into the search fields that are displayed after clicking on the “Advanced filter” button.



Search

Data carrier UID

Name

Locker number

Group type

□ Filter by date

Figure 3.59 – *Search the authorization list*

- ► Enter the details of a data carrier into the fields then click on the “Search” icon .
  - o All data carriers that match the search criteria are displayed.

If the cursor is within the "Data carrier UID" field, the data carrier UID is automatically read and displayed when a data carrier is placed on a connected RFID reader.

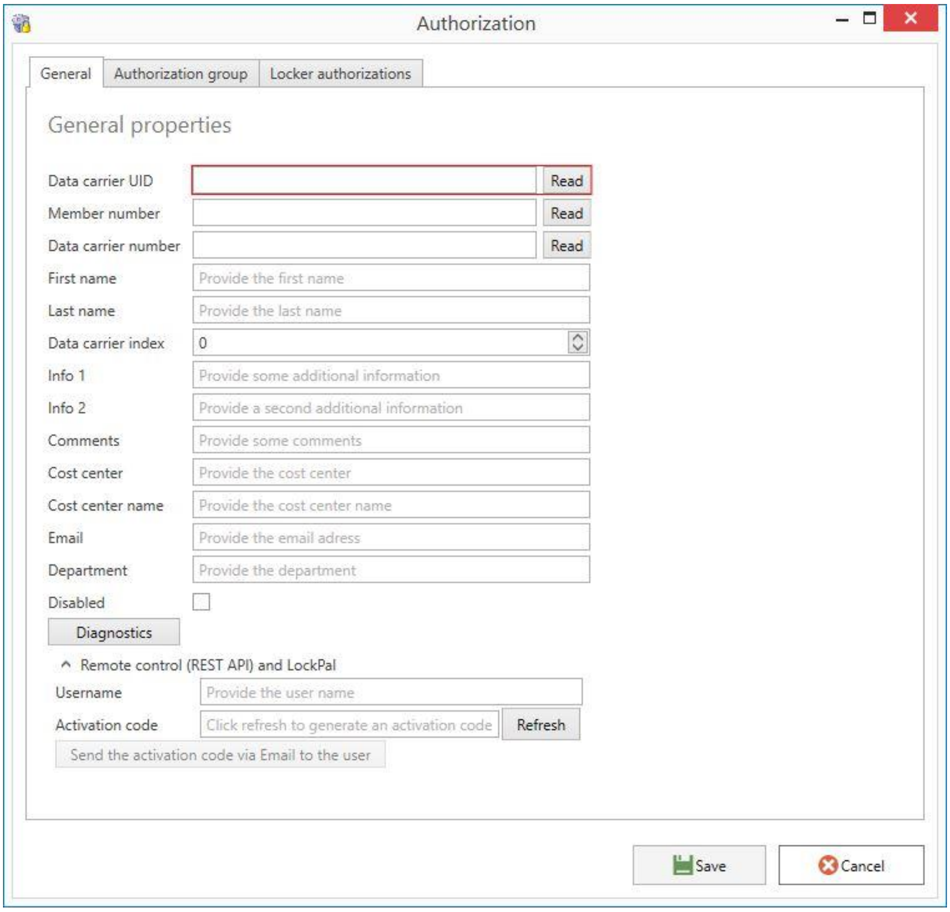
Note regarding the search:
A complete UID number must be entered into the “Data carrier UID” field as partially entered numbers do not return a result. However, you can enter partial information for the "Name" and "Locker number" fields. Please note that, depending on the system configuration, two different lockers may exist with the same locker number.

3.4.4 Adding Data Carriers to the Authorization List

The first task when configuring the authorization list is to add data carriers to the system, which are then listed in the “Search” area after pressing the search icon.

► Click on the "New authorization” button in the "Authorizations" area of the multifunction bar.

○ The "Authorization" window is displayed.



Authorization

General properties

Data carrier UID		Read
Member number		Read
Data carrier number		Read
First name	Provide the first name	
Last name	Provide the last name	
Data carrier index	0	
Info 1	Provide some additional information	
Info 2	Provide a second additional information	
Comments	Provide some comments	
Cost center	Provide the cost center	
Cost center name	Provide the cost center name	
Email	Provide the email adress	
Department	Provide the department	
Disabled	□	

^ Remote control (REST API) and LockPal

Username	Provide the user name	
Activation code	Click refresh to generate an activation code	Refresh

***Figure 3.60** - Authorization window for a new data carrier*

► Enter information for the new data carrier. The following settings are available:

- Data carrier UID: Unique number of the data carrier (written in decimal numbers). Click on "Read" to read the unique number of a data carrier using a connected GAT Writer device.
- Member number: The number of the member assigned to the data carrier. Only enter this number if your system uses member numbers. Click on "Read" to read the member number of a data carrier using a connected GAT Writer device.
- Data carrier number: An additional data carrier number used for the internal organization of the data carriers. Only enter this number if your system uses data carrier numbers. Click on "Read" to read the number of a data carrier using a connected GAT Writer device.

- First name/Last name: Name of the person to whom the data carrier is being assigned. These fields are optional.
- Data carrier index: This field is optional. The index is used in the event that a data carrier is lost and needs to be reissued. The higher index number ensures that only the recently issued data carrier is valid.
- Info 1 / Info 2: Additional data carrier information that is displayed in the log files. These fields are optional.
- Comments: A comment regarding the data carrier can be added in this field.
- Cost center / Cost center name:

  The use of authorizations in companies may require that a data carrier can provide additional information such as cost center, cost center name, email address, and department.
- Email: Email address of the employee. Used for email communication with the employee, e.g., notification if the locker is occupied and not released over a defined period.
- Department: Department to which the employee is assigned.
- Disabled: Select this option to temporarily disable a data carrier from being used. The data carrier settings remain saved and the data carrier can be enabled again by deselecting this option.
- Diagnostics: After clicking on this button, the “Diagnostics Card UID” window opens.
- Remote control (REST API) and LockPal:

  These details allow the assigned user of the data carrier to control their locker remotely via the LockPal app. Following activation, the user’s smartphone functions as a data carrier to lock and unlock their locker. To generate an activation code, click on “Refresh”. To complete the activation, the user must install the LockPal app on their smartphone and enter the activation code shown here.

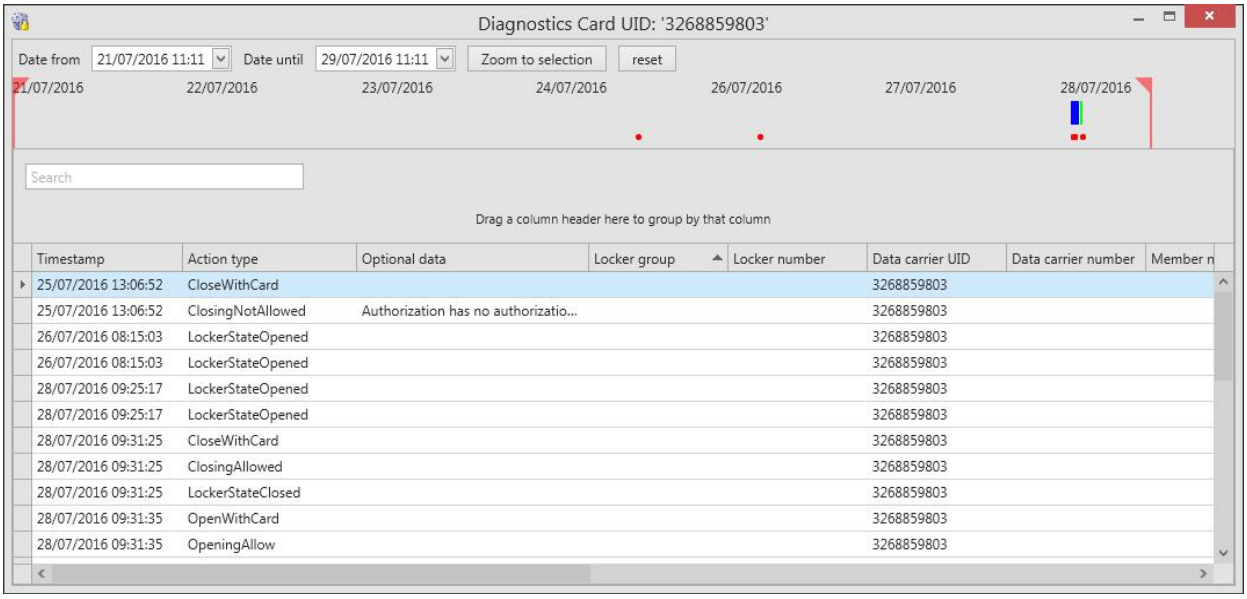
► Confirm the settings by clicking on "Save".

  ○ The new data carrier is added to the authorization list.

► To delete a data carrier from the authorization list, select the data carrier then click on the "Delete authorization" icon.

  ○ If the authorization list is active, the deleted data carrier no longer has authorization in the system.

Beneath the data carrier properties, the “Diagnostics” button opens a window where you can view all actions performed by the data carrier.



Date from 21/07/2016 11:11 Date until 29/07/2016 11:11

Timestamp	Action type	Optional data	Locker group	Locker number	Data carrier UID	Data carrier number	Member n
25/07/2016 13:06:52	CloseWithCard				3268859803		
25/07/2016 13:06:52	ClosingNotAllowed	Authorization has no authorizatio...			3268859803		
26/07/2016 08:15:03	LockerStateOpened				3268859803		
26/07/2016 08:15:03	LockerStateOpened				3268859803		
28/07/2016 09:25:17	LockerStateOpened				3268859803		
28/07/2016 09:25:17	LockerStateOpened				3268859803		
28/07/2016 09:31:25	CloseWithCard				3268859803		
28/07/2016 09:31:25	ClosingAllowed				3268859803		
28/07/2016 09:31:25	LockerStateClosed				3268859803		
28/07/2016 09:31:35	OpenWithCard				3268859803		
28/07/2016 09:31:35	OpeningAllow				3268859803		

Figure 3.61 *- Diagnostics window*

The default date range for displayed actions is one week, which can be adjusted via the “Date from / Date until” fields or by sliding the red flags and clicking on “Zoom to selection”. The red dots in the date range indicate when an action was recorded by the data carrier with specific information about each action displayed below. The list only shows the actions within the selected timespan.

3.4.5 Assigning Data Carriers to Authorization Groups

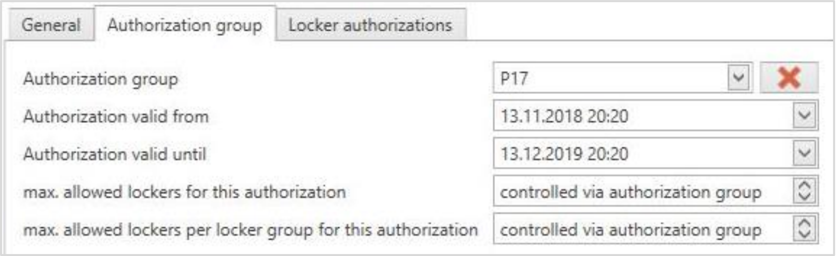
Authorization groups are templates that include different parameters such as time plans and locker groups. Once the authorization groups are defined, data carriers in the authorization list can be assigned to the authorization groups. Refer to "3.4.8 Authorization Groups" for information on defining authorization groups.

An authorization group must only be assigned if the data carrier is to be used with lockers operating in free locker mode and the authorization list is enabled. If the data carrier is to be used only with personal lockers, an authorization group is not necessary as these settings are not considered for personal lockers.

► To assign a data carrier to an authorization group, first select the data carrier from the authorization list.

► Click on the "Authorization group" tab in the data carrier settings area.

► Select an authorization group, e.g., "System", from the drop-down menu.



Authorization group	P17
Authorization valid from	13.11.2018 20:20
Authorization valid until	13.12.2019 20:20
max. allowed lockers for this authorization	controlled via authorization group
max. allowed lockers per locker group for this authorization	controlled via authorization group

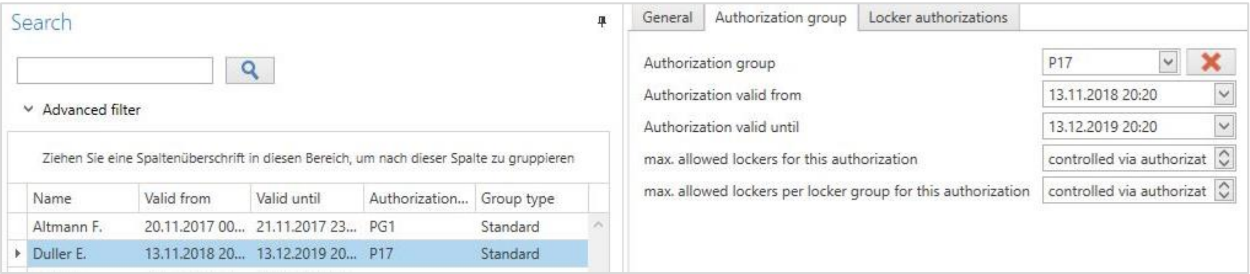
***Figure 3.62** – Authorization group tab*

The following settings are available:

- Authorization group: Assign the data carrier to an authorization group (see "3.4.8 Authorization Groups").
- Valid from / Valid until: Define a validity period for the data carrier. The default values (as used here) can be changed. You can also predefine the used standard values in the general authorization settings of Relaxx (see "2.2.6.Authorizations").
  NOTE! The authorization group settings also affect a data carrier's validity. The data carrier can only be used when it is authorized according to both the authorization group settings and the entered validity period.
- Max. allowed lockers for this authorization: Define the maximum number of free lockers that the data carrier is authorized to use.
- Max. allowed lockers per locker group for this authorization: Define the maximum number of free lockers that the data carrier is authorized to use within one locker group.

► Confirm the settings by clicking on "Save".

- ○ The assigned authorization group is shown in the authorization list (3) in the column "Authorization group".



Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Name	Valid from	Valid until	Authorization...	Group type
Altmann F.	20.11.2017 00...	21.11.2017 23...	PG1	Standard
Duller E.	13.11.2018 20...	13.12.2019 20...	P17	Standard

Authorization group	P17
Authorization valid from	13.11.2018 20:20
Authorization valid until	13.12.2019 20:20
max. allowed lockers for this authorization	controlled via authorizat
max. allowed lockers per locker group for this authorization	controlled via authorizat

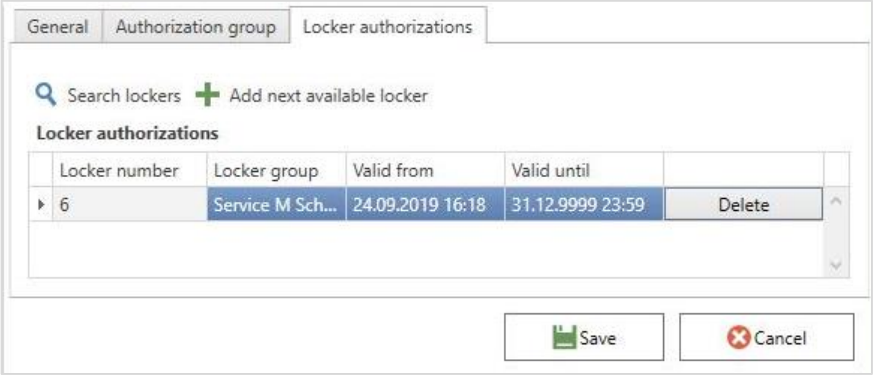
***Figure 3.63** – Authorization group tab*

3.4.6 Assigning Personal Lockers

When a locker is operating in personal locker mode, only those data carrier(s) that are assigned to the locker in the authorization list are allowed to use the locker. Multiple data carriers can be authorized for each personal locker with the maximum number configurable.

NOTE! For personal lockers the authorization groups (see register card "Authorization Group") are irrelevant, i.e., a data carrier not currently authorized according to the authorization list or one with an expired validity period, can still open and close an assigned personal locker. But keep in mind that a validity period can also be defined for each personal locker, which will, of course, be considered.

- ► To define a new locker authorization for a data carrier, first select the data carrier from the authorization list.
- ► Click on the “Locker authorizations” tab in the data carrier settings area.
- ► Click on the “Add next available locker” button.
  - o The next available personal locker, i.e., where no authorization assigned has been assigned as yet, is added to a new line.

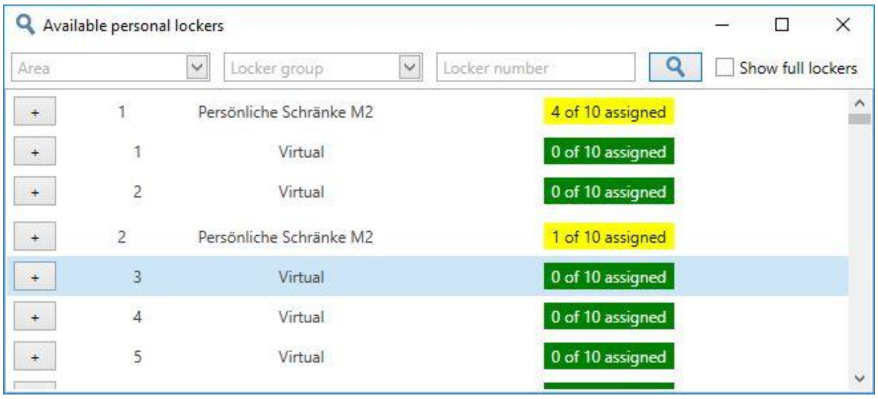


Locker authorizations

	Locker number	Locker group	Valid from	Valid until	
▸	6	Service M Sch...	24.09.2019 16:18	31.12.9999 23:59	Delete

Figure 3.64 – *Locker authorization window*

- ► Alternatively, click on “Search lockers” if you want to assign a specific personal locker.
  - o The “Available personal lockers” window opens.



+	1	Persönliche Schränke M2	4 of 10 assigned
+	1	Virtual	0 of 10 assigned
+	2	Virtual	0 of 10 assigned
+	2	Persönliche Schränke M2	1 of 10 assigned
+	3	Virtual	0 of 10 assigned
+	4	Virtual	0 of 10 assigned
+	5	Virtual	0 of 10 assigned

Figure 3.65 – *Available personal lockers window*

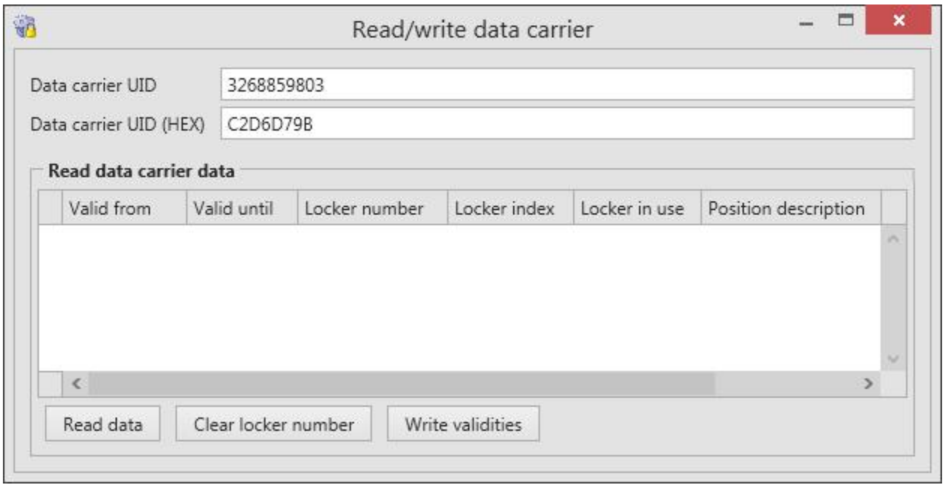
- ► Click on the search icon to display all available personal lockers in the system. You can also narrow the search by entering a locker number into the field or selecting a locker group from the drop-down menu.
  - ○ All personal lockers that match the search criteria (if used) are displayed.
  - ○ The colored bar next to the lockers show the max. allowed data carriers for each locker and how many data carriers have already been assigned. The colors symbolize the used data carriers:
    - Green: no data carriers are assigned to the locker.
    - Yellow: at least one data carrier is assigned to the locker and more data carriers can be assigned.
    - Red: no more data carriers can be assigned to the locker.
- ► Click on the “+” button next to the locker to assign it to the data carrier.
  - ○ The personal locker is added to a new line (see Figure 3.64).
- ► Define the personal locker settings:

- Locker number: The number of the locker that the data carrier will be authorized to use (cannot be changed).
- Locker group: The name of the locker group to which the locker is assigned (cannot be changed).
- Valid from / Valid until: The validity period for the data carrier. The standard values, that are used here, can be changed. You can also predefine the used standard values in the general authorization settings of Relaxx (see "2.2.6.Authorizations").

- ► Confirm the settings by clicking on "Save".
  - ○ The new locker authorization is saved in the list.
- ► To delete a personal locker authorization, select the authorization in the list then click on "Delete".
  - ○ The data carrier can no longer be used with the personal locker.

3.4.7 Read/Write Data Carriers

The "Write data carrier" icon in the “Authorizations” section allows you to read data from, or write data onto, a data carrier via a connected read/write station (GAT Writer). In addition, locker numbers and time limitations can be deleted from the data carrier, which is particularly important for data carriers used in offline applications.


Read/write data carrier

Data carrier UID: 3268859803
Data carrier UID (HEX): C2D6D79B

Read data carrier data

Valid from	Valid until	Locker number	Locker index	Locker in use	Position description

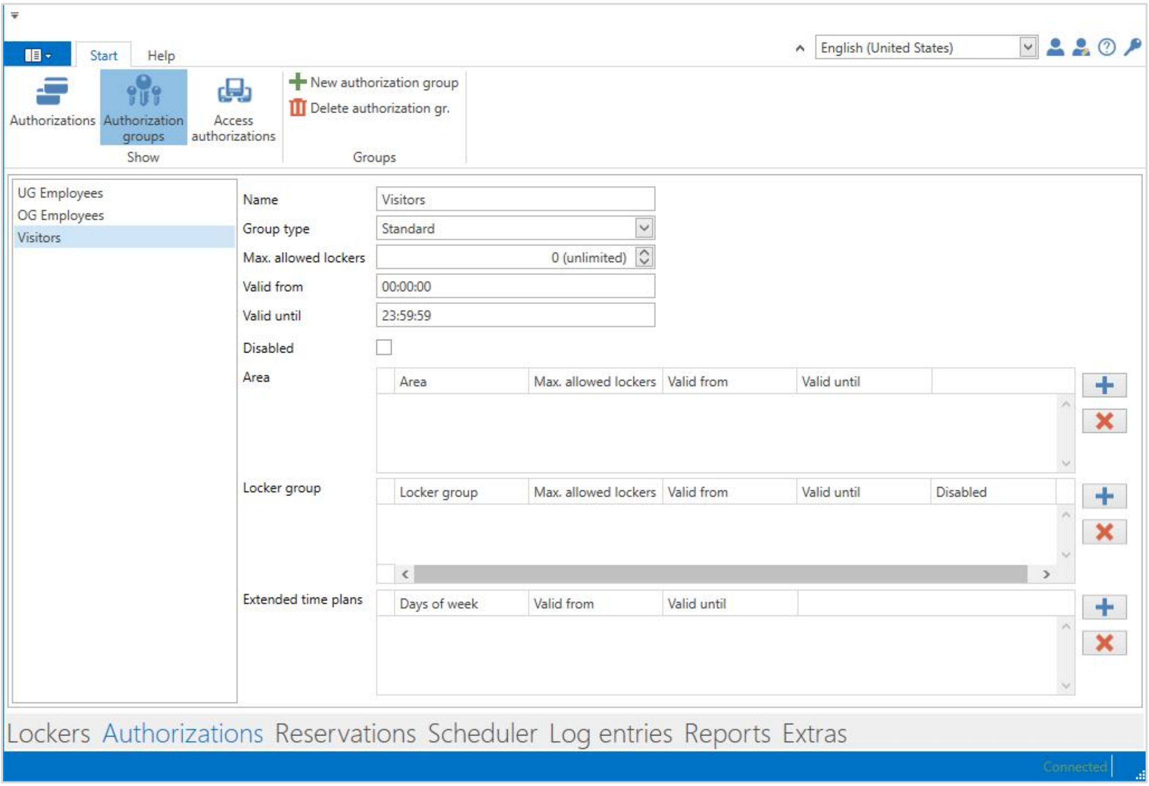
Figure 3.66 *– Read/write data carrier*

- ► Place a data carrier onto the connected read/write station.
- ► Click on "Read data".
  - ○ The data carrier unique number (UID) is displayed in standard and hexadecimal format. If any lockers are currently locked by the data carrier, this information (validity, locker number, etc.) is also displayed.
- ► To delete the locker numbers from the data carrier, so that the data carrier can be used with other lockers, click on “Clear locker number".
- ► To define a new locker validity period for the data carrier, enter the new times into the “Valid from / Valid until” fields and then click on "Write validities".

3.4.8 Authorization Groups

Authorization groups are templates that include different parameters such as time plans and locker groups. Once the authorization groups are defined, they can be assigned to data carriers in the authorization list. Authorization groups are used with lockers in free locker mode. The "Authorization list enabled" setting must also be selected to activate the authorization group functionality. Data carriers can then only use those free lockers from the locker group(s) that are assigned to the authorization group and only in the defined validity period.

- ► To view the authorization groups, click on the "Authorization groups" icon.
  - ○ All defined authorization groups are listed in the left column. The settings of the selected authorization group are displayed to the right of the list.



UG Employees
OG Employees
Visitors

Name	Visitors
Group type	Standard
Max. allowed lockers	0 (unlimited)
Valid from	00:00:00
Valid until	23:59:59
Disabled	□

Area

Area	Max. allowed lockers	Valid from	Valid until

Locker group

Locker group	Max. allowed lockers	Valid from	Valid until	Disabled

Extended time plans

Days of week	Valid from	Valid until

***Figure 3.67** – Defining authorization groups*

- ► To create a new authorization group, click on "New authorization group".
  - ○ The "Authorization group" window opens, which has the same settings as those shown in Figure 3.67.
- ► Define the authorization group settings. The following settings are available:

- Name: Name of the authorization group used to identify the group in the list.
- Group type: The following types of authorization groups for different data carrier functions are available:
  - Standard: Used for regular data carriers. An additional setting for standard data carriers is available:
    - Max. allowed lockers: This option defines how many lockers (in free locker mode) a data carrier in the group can use simultaneously. A value of “0” means an unlimited number of lockers can be used.
  - System: System data carriers can lock/unlock any locker, regardless of the operating mode, and even if the locker was locked by another data carrier. **Be aware that system data carriers function only with controllers operating in ONLINE mode**. A system group can be limited to certain times and to certain locker groups.
  - Maintenance: Maintenance data carriers allow maintenance staff to lock/unlock lockers and complete maintenance tasks, e.g., cleaning. Maintenance data carriers are also used to reset lockers from maintenance mode to normal operating mode. Additional settings for maintenance data carriers include:
    - Allow the maintenance group to open lockers: This option allows all maintenance data carriers in the group to open all lockers (regardless of operating mode) assigned to the group. When not selected, the maintenance data carriers can only lock open lockers in maintenance mode
    - Allow the maintenance group to open only lockers in maintenance: This option allows all maintenance data carriers in the group to open all lockers assigned to the group that are in maintenance mode. Lockers operating in other modes cannot be opened.
    - Clear maintenance: Define when to reset lockers in maintenance mode to their normal operating mode using a maintenance data carrier. This can occur either when the locker is unlocked (On open) or locked (On close).
- Valid from / Valid until: Define a daily timeframe when the authorization group is active. Outside of these times, data carriers assigned to the authorization group have no authorization.
- Disabled: When this option is selected, all data carriers in the authorization group are disabled from using all lockers in the system.

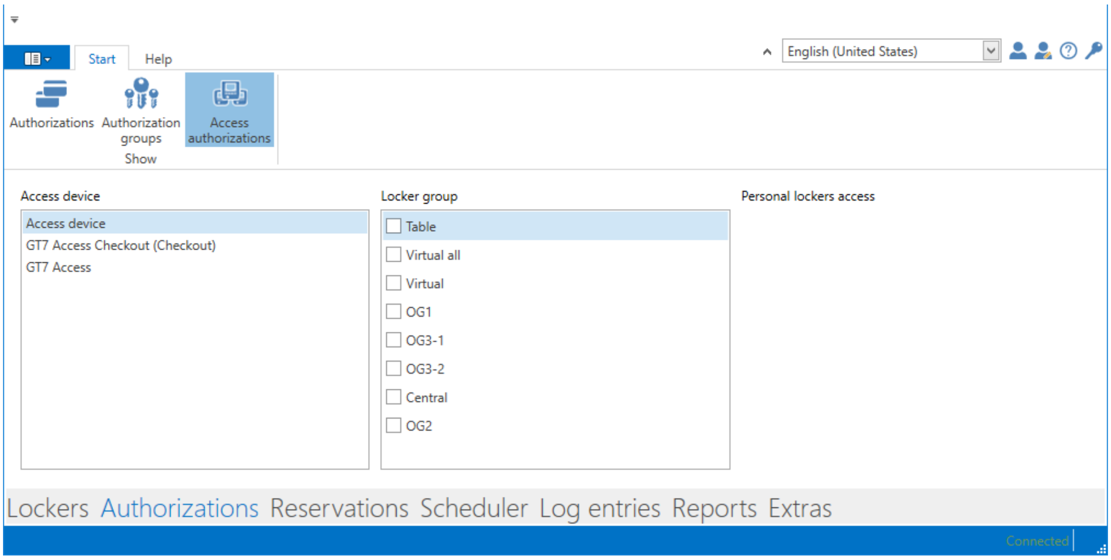
- Area: Areas can be added by clicking on the "+" icon. All data carriers assigned to the authorization group will be authorized to use all lockers in the area. If no area or locker group is selected, the data carriers are able to use all lockers in the system.
- Locker group: Locker groups can be added by clicking on the "+" icon. All data carriers in the authorization group will be authorized to use all lockers assigned to the locker group. Irrespective of the type of authorization group, all data carriers assigned to the group will have no authorization with other lockers. If no locker group is selected here, the authorization group is valid for all lockers in the system. If no area or locker group is selected, the data carriers are able to use all lockers in the system.
- Extended time plans: Additional time plans for the authorization groups can be added by clicking on the "+" icon. The extended time plan(s) defined here operate in combination with the time plan defined in the "Valid from / Valid until" fields. Extended time plans are used to make the validity period of the authorization group more specific, i.e., for specific days of the week rather than every day. For example, to create a group that is authorized only on Mondays, enter “00:00:00” in the “Valid from/ Valid until” fields then the desired times for Mondays in the "Extended time plans" fields.

► Click on “Save” to finalize the authorization group.
  - ○ The new authorization group is displayed in the list.

3.4.9 Access Authorizations

Access authorizations are used to manage access for the GAT Access devices in your system. You can define which data carriers can access specific devices and at what times. The GAT Access device grants access to a restricted area, e.g., a female locker room, based upon whether the data carrier assigned to a locker group is authorized to use the lockers or not.

► To view the access authorizations, click on the "Access authorizations" icon.
  - ○ All available access control devices in the system are listed in the left column. Click on a device to display its settings in the right column.



Access device

- Access device
- GT7 Access Checkout (Checkout)
- GT7 Access

Locker group

- □ Table
- □ Virtual all
- □ Virtual
- □ OG1
- □ OG3-1
- □ OG3-2
- □ Central
- □ OG2

Personal lockers access

Figure 3.68 *– Defining access authorizations for GAT Access devices*

The left column lists all available access devices in the facility.

- ► Select a device to display its settings in the fields to the right.

  NOTE! The word "Checkout" for a GT7 Access device indicates that this device can perform a locker checkout (see "3.2.3 d) GT7 Access and GT7 Info"). Such devices do not perform access control.
- ► In the "Locker group" section, select the locker groups that are to be considered with the GAT Access device.
  - For Access devices: The data carriers that are authorized for the selected locker groups are then also assigned access authorization for the GAT Access device.
  - For Checkout devices: When a user performs a locker checkout, the locker authorizations of the user are only deleted from the assigned locker(s) in the selected locker groups. Authorizations for lockers that are in unselected locker groups are not deleted.

NOTE! Keep in mind that a GAT Access does not grant access to a data carrier, if the data carrier:
- has locked a locker with "free locker" mode in a marked locker group
and
- the data carrier is not in the authorization list or the authorization list is not enabled.

Data carriers are assigned to locker groups while configuring the authorization groups (refer to "3.4.8. Authorization Groups").

- ► In the "Personal lockers access" field, you can define whether a data carrier is authorized for personal lockers in a locker group, and either always or only at certain times.

3.5 Locker Reservations

The reservation function in Relaxx offers the possibility of reserving lockers operating in “Reservable locker” mode for specific data carriers and for specific times.

NOTE! Locker reservations are independent of the authorization list, meaning that a locker can be reserved for and used by a specific visitor data carrier even if this data carrier does not have an authorization for the reservation timeframe according to the authorization list.

In the organization view (refer to "3.1 Software Window Elements"), reservable lockers are displayed with a light blue frame. For reservable lockers with a registered reservation, an additional blue bar is displayed in the locker field. This bar is displayed regardless whether the reservation timeframe has been reached or not.

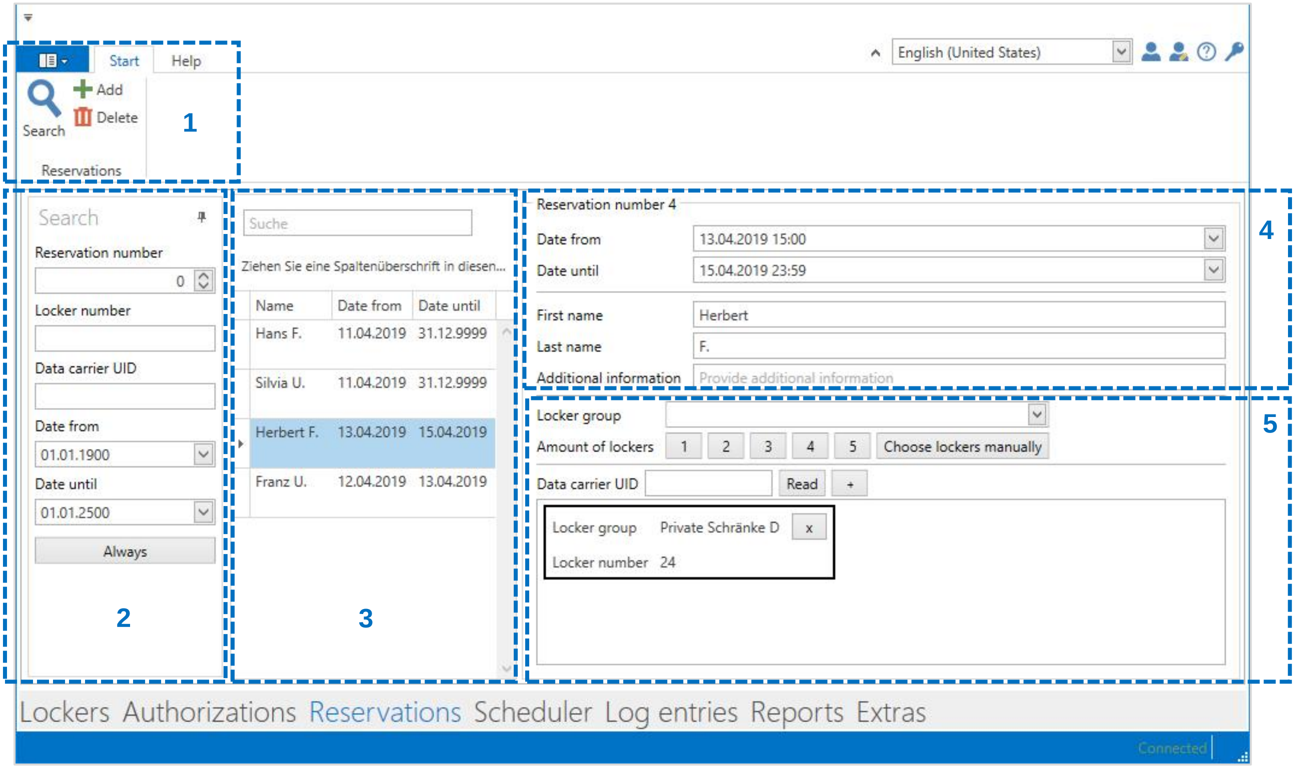
No reservation

Reservation assigned

Figure 3.69 *- Reservable lockers*

► Select the "Reservations" view.

  ○ The following screen is displayed.



Search

Reservation number: 0

Locker number:

Data carrier UID:

Date from: 01.01.1900

Date until: 01.01.2500

Always

Suche

Ziehen Sie eine Spaltenüberschrift in diesen...

Name	Date from	Date until
Hans F.	11.04.2019	31.12.9999
Silvia U.	11.04.2019	31.12.9999
Herbert F.	13.04.2019	15.04.2019
Franz U.	12.04.2019	13.04.2019

Reservation number 4

Date from: 13.04.2019 15:00

Date until: 15.04.2019 23:59

First name: Herbert

Last name: F.

Additional information: Provide additional information

Locker group:

Amount of lockers: 1 2 3 4 5 Choose lockers manually

Data carrier UID: Read +

Locker group: Private Schränke D x

Locker number: 24

Figure 3.70 *– Managing reservations*

This view is divided into several areas.

1 Multifunction bar: All functionalities available in the current view are displayed.

2 Search area: Here, the list of reservations can be searched for specific information.

3 List of reservations: All reservations are listed here, with the name of the reservation holder, the start and end dates. For every entry, underneath the name, the reserved lockers with the locker group and locker number are shown.

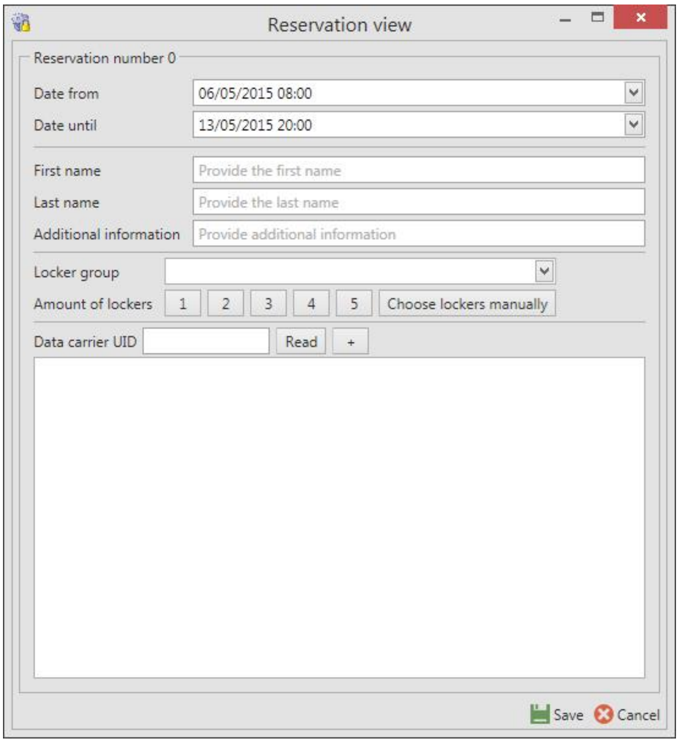
4 Reservation data: In this area, the timeframe and the name of the reservation holder are defined for the selected reservation.

5 Locker assignments: Here, the desired locker or also multiple lockers including the corresponding data carriers are assigned to the selected reservation.

3.5.1 Adding a New Locker Reservation

► In order to create a new reservation, click on the "+ Add" icon.

   ○ The following window opens.



Reservation view

Reservation number 0

Date from: 06/05/2015 08:00

Date until: 13/05/2015 20:00

***Figure 3.71** – Adding a new reservation*

► Enter the data for the new reservation. The options are described in the next section.

► Confirm the reservation by clicking "Save".

   ○ The new reservation is added to the list of reservations and you can edit the settings here anytime.

3.5.2 Reservation Settings

The same settings for a reservation can be made either at the moment of adding a new reservation or directly in the "Reservations" window. The following settings are possible.

- Date from / until: Defines the reservation timeframe. Within this timeframe, the reservation is active, and the data carrier assigned to these lockers can use the corresponding lockers during that period of time. Outside of the reservation timeframe, the data carriers have no authorization for these lockers.
- First name/Last name: Enter the names of the reservation, e.g., the name of the reservation holder. The reservations are shown with this name in the list of reservations.
- Additional information: Additional information regarding the reservation can be entered here.
- Locker group: In order to assign lockers automatically to the reservation, first select the locker group of the locker you want to assign. Lockers from different locker groups can also be assigned one after the other.
- Amount of lockers: With these buttons, one or several lockers from the locker group selected in the “Locker group” field are added to the reservation. For example, if you click on "3" and the selected locker group does not have 3 reservable lockers available, a corresponding message will be displayed.
- Choose lockers manually: With this button, a locker can be selected manually from the available locker groups.

► Click on the button.
    - A window opens in which all locker groups with reservable lockers are listed.

► The list can be sorted in increasing or decreasing order of the locker groups.

► Locate the locker for reservation within the desired locker group and check the box next to the locker number.
    - After selecting a locker, it will be added directly to the locker list.

► Additional lockers can be check in order to also assign them to the reservation.

► To close the window, click on the red “X” icon in the upper right corner of the window.

- Data carrier UID: The UID number of the data carrier is entered here (written in decimal numbers), in order to assign it to a reserved locker. The data carrier number can also be read with the "Read" button with a connected GAT Writer read/write station.

► In order to assign the entered data carrier to a locker, first check the desired locker in the locker list and then click on the "+" icon next to the data carrier UID number.

► If no locker is checked, the data carrier will assign the reservation to all lockers.

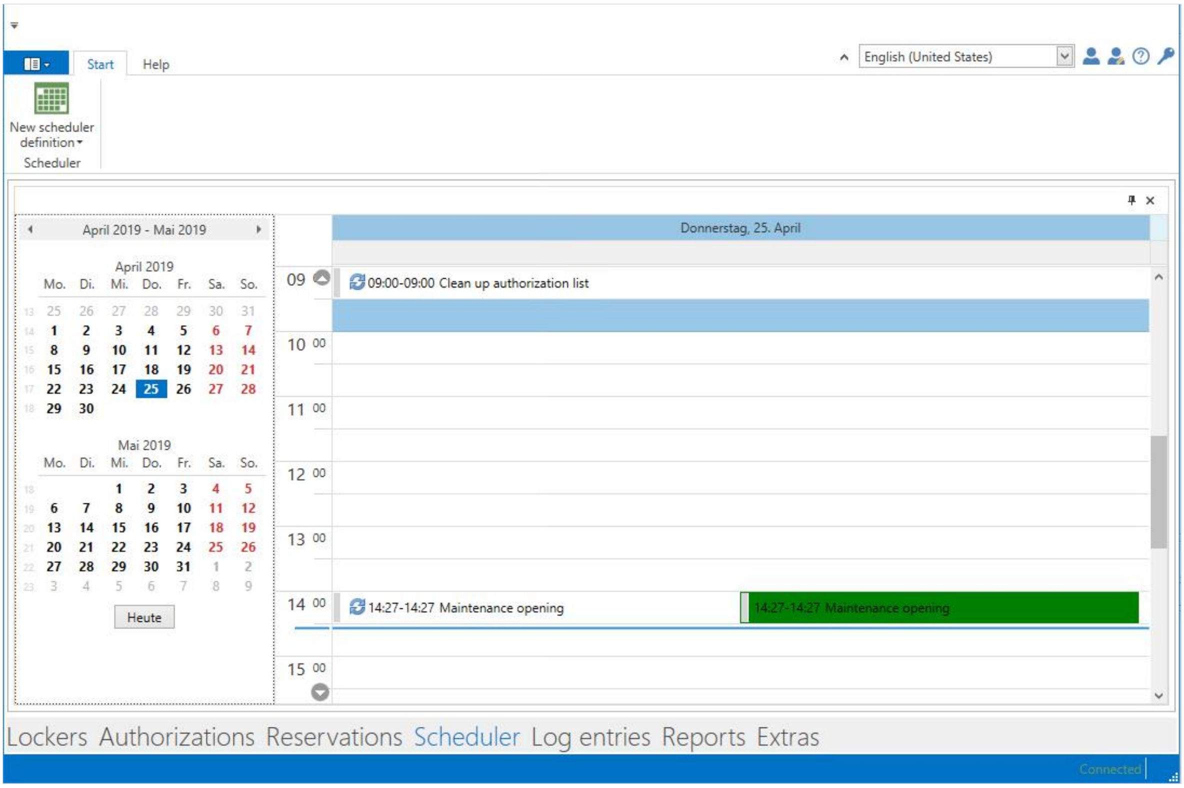
- Locker list: Here, every locker assigned to the reservation is shown in a separate frame. For every locker, the locker group, the locker number, and the data carrier are displayed.

► To delete a locker from the list, click on the "x" icon next to the locker group.

► To delete a data carrier from a locker, click on the "x" icon next to the UID number of the assigned data carrier.

3.6 Scheduler

With the scheduler functionality, regularly reoccurring actions can be scheduled, in order to have them executed automatically by Relaxx. In the calendar view, both the scheduled actions and the executed actions are displayed.



April 2019

	Mo.	Di.	Mi.	Do.	Fr.	Sa.	So.
13	25	26	27	28	29	30	31
14	1	2	3	4	5	6	7
15	8	9	10	11	12	13	14
16	15	16	17	18	19	20	21
17	22	23	24	25	26	27	28
18	29	30					

Mai 2019

	Mo.	Di.	Mi.	Do.	Fr.	Sa.	So.
18			1	2	3	4	5
19	6	7	8	9	10	11	12
20	13	14	15	16	17	18	19
21	20	21	22	23	24	25	26
22	27	28	29	30	31	1	2
23	3	4	5	6	7	8	9

09:00-09:00 Clean up authorization list

14:27-14:27 Maintenance opening

14:27-14:27 Maintenance opening

***Figure 3.72** - Scheduler view*

The white fields indicate saved, enabled actions.

- ► Right-click onto this field and select "Edit" to edit the settings of this scheduled action.
- ► Right-click onto this field and select "Delete" to delete this scheduled action.

The green fields indicate executed actions.

- ► Double-click onto this field to display status information from the executed action (as shown in Figure 3.72).

The gray fields indicate saved, disabled actions.

- ► Right-click onto this field and select "Edit" to edit the settings of this scheduled action.
- ► Right-click onto this field and select "Delete" to delete this scheduled action.

3.6.1 Scheduling a New Action

- Click on the "New scheduler definition" icon.
  - A menu with the possible actions is displayed.
- Select the desired action to be scheduled.
  - Depending on the selected functionality, the corresponding window will be displayed. The following sections describe the setting options for the actions.

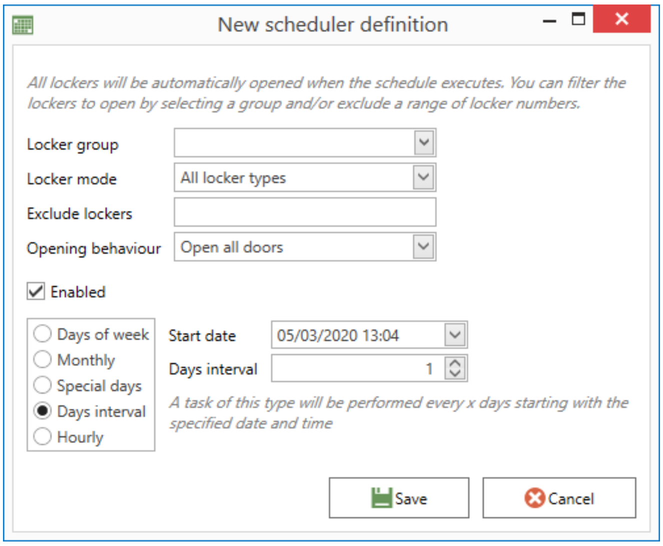
3.6.2 Actions for the Scheduler

The following actions can be scheduled.

a) Maintenance opening

With an opening for maintenance, all lockers within a selectable locker group are opened at a specific time. For example, after the facilities are closed to the public, all lockers in the system that might still be closed can be opened for inspection or cleaning purposes.

For the maintenance opening, lockers that are deactivated or have an active alarm that has not yet been acknowledged are not opened.



New scheduler definition

All lockers will be automatically opened when the schedule executes. You can filter the lockers to open by selecting a group and/or exclude a range of locker numbers.

Locker group:
Locker mode: All locker types
Exclude lockers:
Opening behaviour: Open all doors

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 05/03/2020 13:04
Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

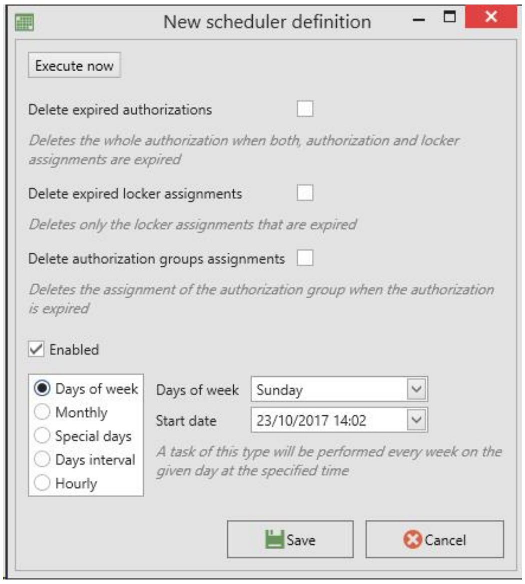
***Figure 3.73** – Scheduling an automatic opening for maintenance*

- In the "Locker group" field, select the locker group for which the action is to be created.
- In the "Locker mode" field, select which lockers shall be opened (all lockers or only free lockers).
- In the "Exclude lockers" field, the numbers of the lockers to be excluded from the automatic maintenance opening can be entered (separated by a comma). If this field is empty, all lockers in the group will be opened.
- In the "Opening behavior" field, you can choose whether all closed doors should be opened or whether lockers that are pre-locked without a data carrier should remain closed during maintenance opening in order to support the uniform appearance of always closed lockers.
- Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.
  - A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.

- ► In the list on the left, mark the time interval for the automatic action.
- ► In the fields to the right, enter the times, when the action is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the entries made by clicking "Save".
  - o The new action is added to the calendar.
- ► With the "Execute now" button, the automatic opening for maintenance based on the data entered can be executed immediately.

b) Clean up authorization list

Expired locker assignments and authorizations can be deleted automatically from the authorization list at definable intervals. For information regarding the authorization list, refer to "3.4.2. Enable or Disable the Authorization List".



New scheduler definition

Execute now

Delete expired authorizations □

Deletes the whole authorization when both, authorization and locker assignments are expired

Delete expired locker assignments □

Deletes only the locker assignments that are expired

Delete authorization groups assignments □

Deletes the assignment of the authorization group when the authorization is expired

☑ Enabled

● Days of week
○ Monthly
○ Special days
○ Days interval
○ Hourly

Days of week: Sunday
Start date: 23/10/2017 14:02

A task of this type will be performed every week on the given day at the specified time

Save Cancel

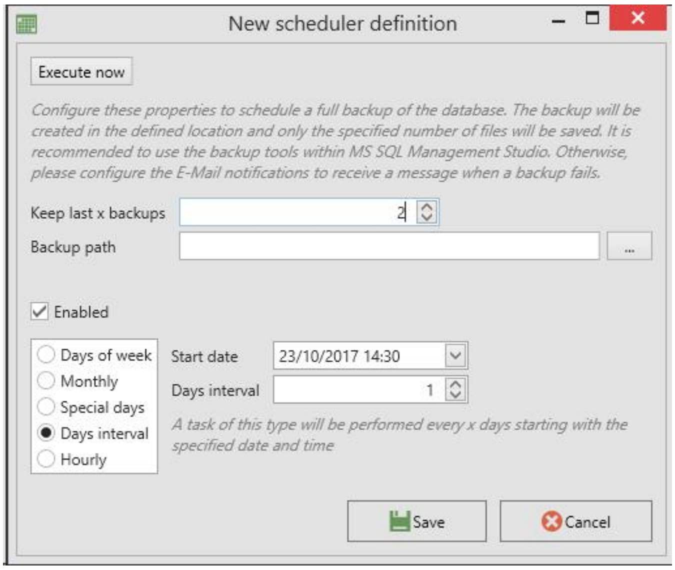
Figure 3.74 *– Scheduling the deletion of expired data in the authorization list*

- ► Check the "Delete expired authorizations" box in order to delete the data carriers from the authorization list, for which the authorization and the locker assignment have expired.
- ► Check the "Delete expired locker assignments” box in order to delete expired locker assignments of data carriers.
- ► Check the "Delete authorization groups assignments" box in order to delete the locker assignments of data carriers, where the validity of the authorization groups assignment has expired.
- ► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.
  - o A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.
- ► In the list on the left, mark the time interval for the automatic action.
- ► In the fields to the right, enter the times, when the action is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the entries made by clicking "Save".
  - o The new action is added to the calendar.
- ► With the "Execute now" button, the selected settings in the authorization list can be deleted immediately.

c) Backup database

This function allows you to automatically create backups of the Relaxx database at regular intervals. The database includes all configuration data of the locker locking system, the GAT Info and GAT Access Terminals, as well as the log data and the settings of the authorization list. This enables the importing of a database backed up previously, e.g. after an error event of or a damage to the Relaxx installation. Work can then be continued on the system with the data as of the time of the backup.

During every database backup, a new file is created. The date and time of the backup is included in the file name.



New scheduler definition

Execute now

Configure these properties to schedule a full backup of the database. The backup will be created in the defined location and only the specified number of files will be saved. It is recommended to use the backup tools within MS SQL Management Studio. Otherwise, please configure the E-Mail notifications to receive a message when a backup fails.

Keep last x backups: 2

Backup path:

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 23/10/2017 14:30

Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

Save | Cancel

Figure 3.75 *– Scheduling of an automatic database backup*

► In the "Keep last x backups" field, enter the number of backups that should be kept during the backup. In order to save space, Relaxx automatically deletes older backups when performing new ones. It is always the oldest backup that is deleted first. The “x” value entered here is the number of latest backups to always be saved. Example: If the value "5" is entered and 5 backups have already been made earlier, the oldest will be deleted, so the maximum number of backups saved will always be 5.
If backups are made frequently (e.g. on an hourly or daily basis), it is recommended not to set this value too low. Should an error not be detected immediately, more backups will be available.

► In the "Backup path", enter the name of the path, where the backups are to be saved. It is recommended to select a network path here, so the backups are not lost if the Relaxx PC / server is damaged.

► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.

  - A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.

► In the list on the left, mark the time interval for the automatic backup.

► In the fields to the right, enter the times, when the backup is to be executed. The options available here depend on the type of time interval selected in the field to the left.

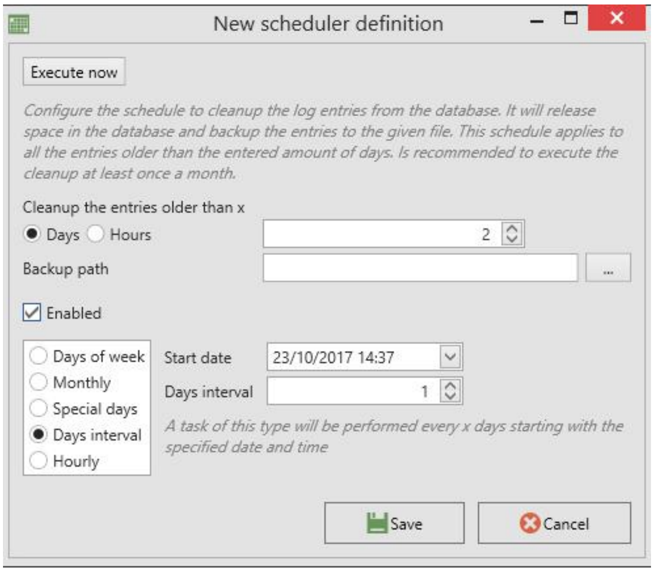
► Confirm the entries made by clicking "Save".

  - The new backup schedule is added to the calendar.

► With the "Execute now" button, a backup of the database according to the data entered (days and backup path) can be created immediately.

d) Backup log entries

The automatic log backup makes it possible to automatically create regular backups of the log data recorded by Relaxx. The oldest data is saved in external files and deleted in the Relaxx database in order to free space. The log is where the visitor actions at the lockers and terminals and the system messages are saved. During every log data backup, a new file is created. The date and time of the backup is included in the file name.



New scheduler definition

Execute now

Configure the schedule to cleanup the log entries from the database. It will release space in the database and backup the entries to the given file. This schedule applies to all the entries older than the entered amount of days. Is recommended to execute the cleanup at least once a month.

Cleanup the entries older than x

● Days ○ Hours: 2

Backup path: ...

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 23/10/2017 14:37

Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

Save Cancel

Figure 3.76 *- Scheduling of a log data backup*

- ► In the "Cleanup the entries older than x days" field, enter the number of days or hours (depending on selected option) an entry should be kept, i.e., it will be archived if it is older. At the set backup times, all log data older than the entered number of days or hours will be archived.

NOTE! In order to free space in the Relaxx database, Relaxx will delete the data from the internal database after having saved it.

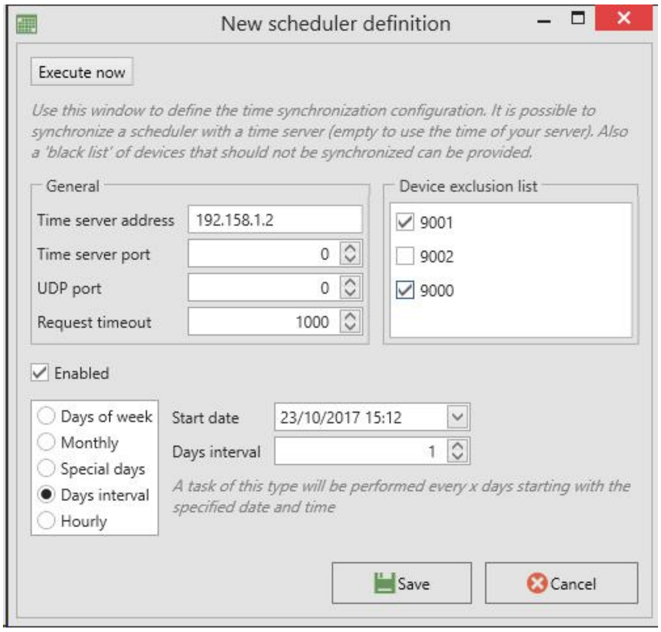
- ► In the "Backup path", enter the name of the path, where the log data backups are to be saved. It is recommended to select a network path here, so the backups are not lost if the Relaxx PC / server is damaged.
- ► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.
  - ○ A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.
- ► In the list on the left, mark the time interval for the automatic backup.
- ► In the fields to the right, enter the times, when the backup is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the entries made by clicking "Save".
  - ○ The new backup schedule is added to the calendar.
- ► With the "Execute now" button, a backup of the database according to the data entered (days and backup path) can be created immediately.

NOTE! The log data backed up can be uploaded and evaluated at a later point in time with the log view (refer to "3.7 Log Entries").

e) Time synchronization

Every controller and every GAT Info and GAT Access device is equipped with an internal clock used for time-dependent actions (e.g., authorization schedules), which is why it is important that these clocks are always in sync with the current time.

The automatic time synchronization allows all clocks in the devices to be synchronized to the current time, at a specific point in time.



New scheduler definition

Execute now

Use this window to define the time synchronization configuration. It is possible to synchronize a scheduler with a time server (empty to use the time of your server). Also a 'black list' of devices that should not be synchronized can be provided.

General

Time server address: 192.158.1.2
Time server port: 0
UDP port: 0
Request timeout: 1000

Device exclusion list

☑ 9001
□ 9002
☑ 9000

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 23/10/2017 15:12
Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

Figure 3.77 *– Scheduling of an automatic time synchronization*

► If a dedicated time server is to be used in the network for the time synchronization, enter the corresponding data of the time server in the "General" area:

- Time server address: IPv4 address of the time server. If no value is entered here, the time of the server on which the Relaxx service is running, is used for time synchronization.
- Time server port: The port used for synchronization with the time server. To use the time of the server on which the Relaxx service is running, leave this field blank ("0").
- UDP-Port: The port to be used on the devices for the time synchronization (default = 8216).
- Request timeout: Waiting time (ms) for an answer after time synchronization was requested.

► In the "Device exclusion list" check the controllers and GAT Access and GAT Info devices for which the time should not be synchronized automatically. All devices not checked here will otherwise be synchronized automatically.

► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.

○ A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.

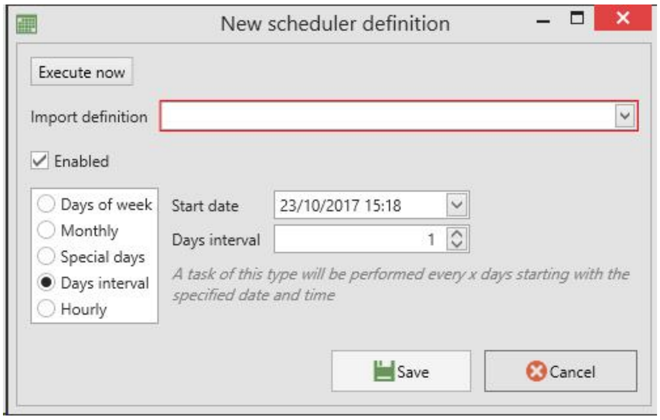
- ► In the list on the left, mark the time interval for the automatic time synchronization.
- ► In the fields to the right, enter the times, when the time synchronization is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the entries made by clicking "Save".
  - ○ The new time synchronization schedule is added to the calendar.
- ► With the "Execute now" button, a synchronization according to the data entered can be performed immediately.

f) Import data

The “Import data” action automatically imports a specific locker group at a configurable time.

NOTE! When importing data, the current data in Relaxx is overwritten with the imported data.

NOTE! During the import process, it is possible that Relaxx requests, e.g., locking/unlocking requests, cannot be completed. The effects of this issue vary depending on the hardware configuration, e.g., a locker cannot be locked during this time. For this reason, imports should be carried out at off-peak times.



Import definition:

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 23/10/2017 15:18

Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

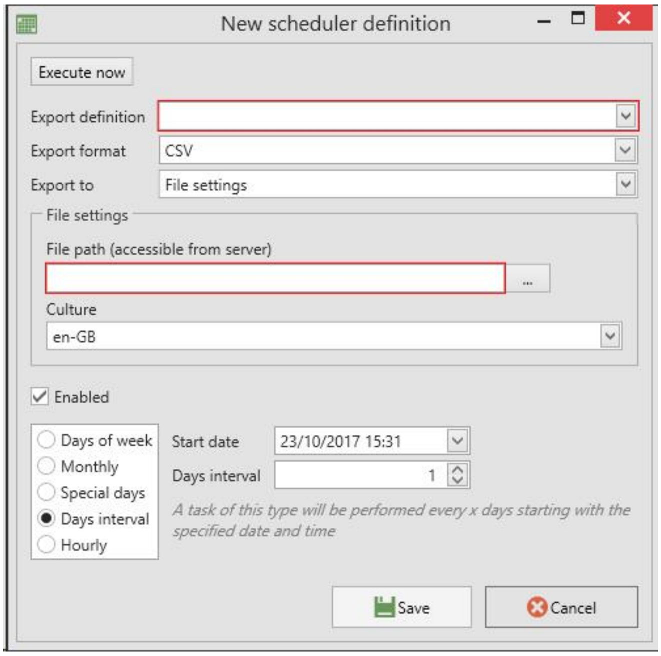
Figure 3.78 *- Scheduling of the automatic import*

- ► In the "Import definition" field, select a previously defined import definition from the menu.

  NOTE! The import definitions are defined in the "Extras" view (refer to "3.9.1 Import Definitions").
- ► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.
  - ○ A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.
- ► In the list to the left, select a time interval for the automatic import.
- ► In the fields to the right, define when the automatic import is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the settings by clicking on "Save".
  - ○ The new action is added to the calendar.
- ► With the "Execute now" button, an import action according to the data entered for the selected locker group can be performed immediately.

g) Export data

The “Export data” action automatically exports log file data at a configurable time.



New scheduler definition

Execute now

Export definition:

Export format: CSV

Export to: File settings

File settings

File path (accessible from server):

Culture: en-GB

☑ Enabled

○ Days of week
○ Monthly
○ Special days
● Days interval
○ Hourly

Start date: 23/10/2017 15:31

Days interval: 1

A task of this type will be performed every x days starting with the specified date and time

Save | Cancel

Figure 3.79 *– Schedule definition for automatic data exporting*

- ► In the "Export definition" field, select one of the preset export definitions from the drop-down menu.
  NOTE! If you need another type of export definition, contact GANTNER Electronic GmbH.
- ► Select a format for the export file (CSV or XLSX).
- ► In the "Export to" field, select how the file is to be exported. You can select to export the file to a computer directory or export the file via email.
- ► Define the file or mail settings depending on the option selected in the previous step.
  - File settings: Enter the computer directory where the export file will be exported to. In the "Culture" field, you can define country-specific formatting such as date and time.
  - Mail settings: Enter the email address(es) of the people who are to receive the email notification.

NOTE! The mail settings defined here operate in combination with the main “Email settings”, which must also be configured to ensure the file is sent. Refer to “2.2.9 Notifications” from more information.

- ► Click on the "Enabled" option to enable (field is marked) or disable (field is unmarked) the action.
  - o A disabled action remains saved in the schedule but is not executed. In the calendar view, enabled actions are displayed with a white background and disabled actions with a gray background.
- ► In the list to the left, select a time interval for the automatic export.
- ► In the fields to the right, define when the automatic export is to be executed. The options available here depend on the type of time interval selected in the field to the left.
- ► Confirm the settings by clicking on "Save".
  - o The new action is added to the calendar.
- ► With the "Execute now" button, an export action according to the data entered for the selected locker group can be performed immediately.

3.7 Log Entries

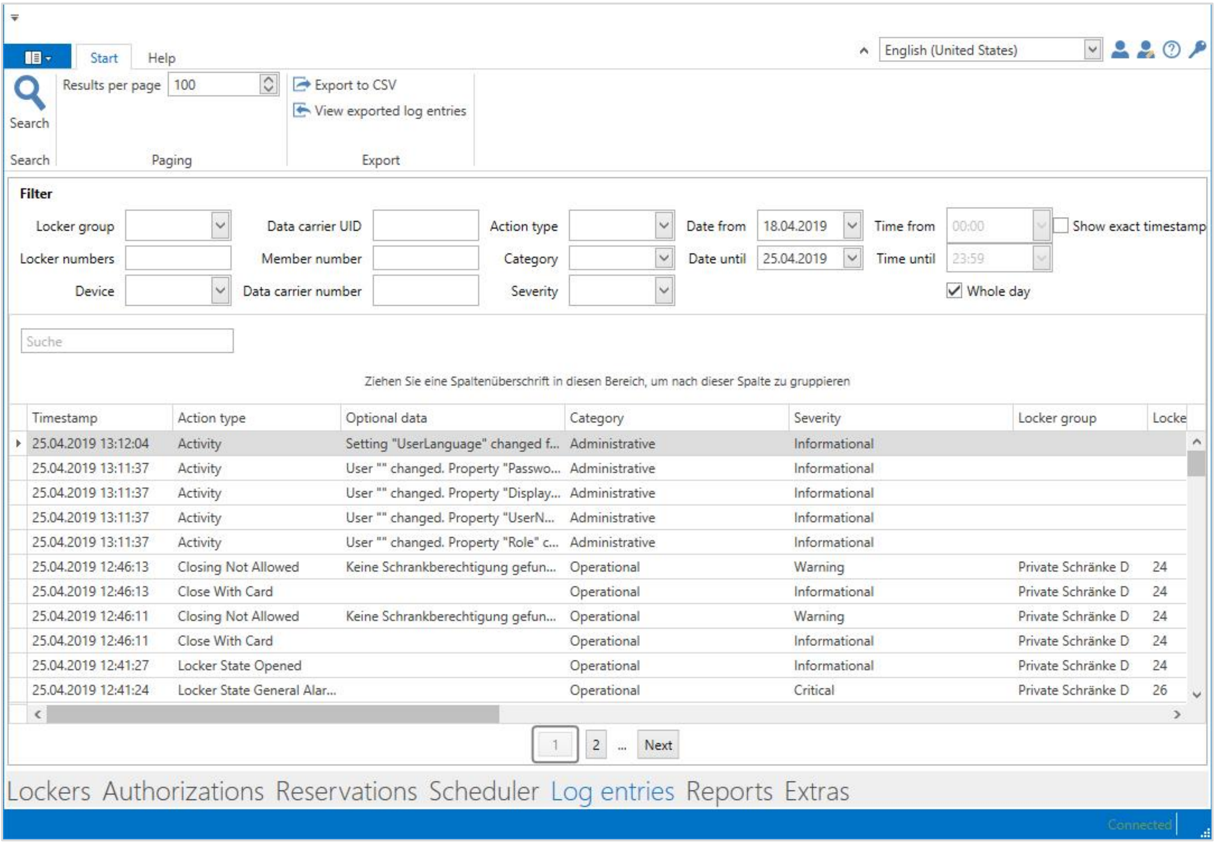
Relaxx records all system activity such as device operations, alarms, and error messages in the Relaxx database. The database can be searched according to certain criteria in Relaxx via the "Log entries" view. The data can also be exported as a CSV file for further evaluation or record keeping.

NOTE! The log data should be exported and archived regularly (recommendation: at least once a month), in order to free space in the database. Refer to "3.6.2 Actions for the Scheduler" for instructions on how to archive the log data.

An overview of the possible log entries can be found under "6. Appendix: Log entries".

► Switch to the "Log entries" view.

- This view is empty after being selected for the first time.



Filter

Locker group □ Data carrier UID □ Action type □ Date from 18.04.2019 Time from 00:00 □ Show exact timestamp

Locker numbers □ Member number □ Category □ Date until 25.04.2019 Time until 23:59

Device □ Data carrier number □ Severity □ ☑ Whole day

Suche

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser Spalte zu gruppieren

Timestamp	Action type	Optional data	Category	Severity	Locker group	Locke
25.04.2019 13:12:04	Activity	Setting "UserLanguage" changed f...	Administrative	Informational		
25.04.2019 13:11:37	Activity	User "" changed. Property "Passwo...	Administrative	Informational		
25.04.2019 13:11:37	Activity	User "" changed. Property "Display...	Administrative	Informational		
25.04.2019 13:11:37	Activity	User "" changed. Property "UserN...	Administrative	Informational		
25.04.2019 13:11:37	Activity	User "" changed. Property "Role" c...	Administrative	Informational		
25.04.2019 12:46:13	Closing Not Allowed	Keine Schrankberechtigung gefun...	Operational	Warning	Private Schränke D	24
25.04.2019 12:46:13	Close With Card		Operational	Informational	Private Schränke D	24
25.04.2019 12:46:11	Closing Not Allowed	Keine Schrankberechtigung gefun...	Operational	Warning	Private Schränke D	24
25.04.2019 12:46:11	Close With Card		Operational	Informational	Private Schränke D	24
25.04.2019 12:41:27	Locker State Opened		Operational	Informational	Private Schränke D	24
25.04.2019 12:41:24	Locker State General Alar...		Operational	Critical	Private Schränke D	26

1
2
...
Next
Lockers Authorizations Reservations Scheduler Log entries Reports Extras
Connected

Figure 3.80 *- Log entries view*

► Enter search criteria into the fields of the filter in the upper area of the screen.
NOTE! Searching for a data carrier UID or data carrier number requires entering the complete number. Entering only partial data will not return a result.

In the "Category" field, you can filter the log entries for certain personnel groups. Option "0 Administrative" lists system relevant messages that are of interest to system administrators (e.g., connection interruptions, activations of emergency modes, etc.). The setting "1 Operational" shows messages that are of interest to the operational personnel that work on a daily basis with Relaxx (e.g., locking and unlocking of lockers).

With the “Severity" field you can filter the log entries by either uncritical messages like status information messages or by critical messages like warning or error messages.

- ► When you select the "Show exact timestamp" option, the time of the log entries is also displayed to the millisecond.
- ► Click on the "Search" icon.
  - o The log is searched for the entered information and the matching entries displayed. If no search information is entered, all log entries are displayed.
  - o The number selected in the “Results per page” field determines how many entries are shown per page.
- ► To view more entries than those currently displayed, click on the number buttons below the log list to go to the following page(s).
- ► The column headers can be rearranged to the desired position via drag and drop. The list can also be sorted by a specific column, e.g., the most recent actions shown first. This setting only applies for the currently displayed page.
- ► The log entries can be exported in CSV file format by clicking on the "Export to CSV" button, in order to process the data further. Only the currently displayed log data pages are exported.
- ► Logs saved externally in CSV format can be imported into Relaxx via the "View exported log entries" button in order to edit them in the “Log entries” view.

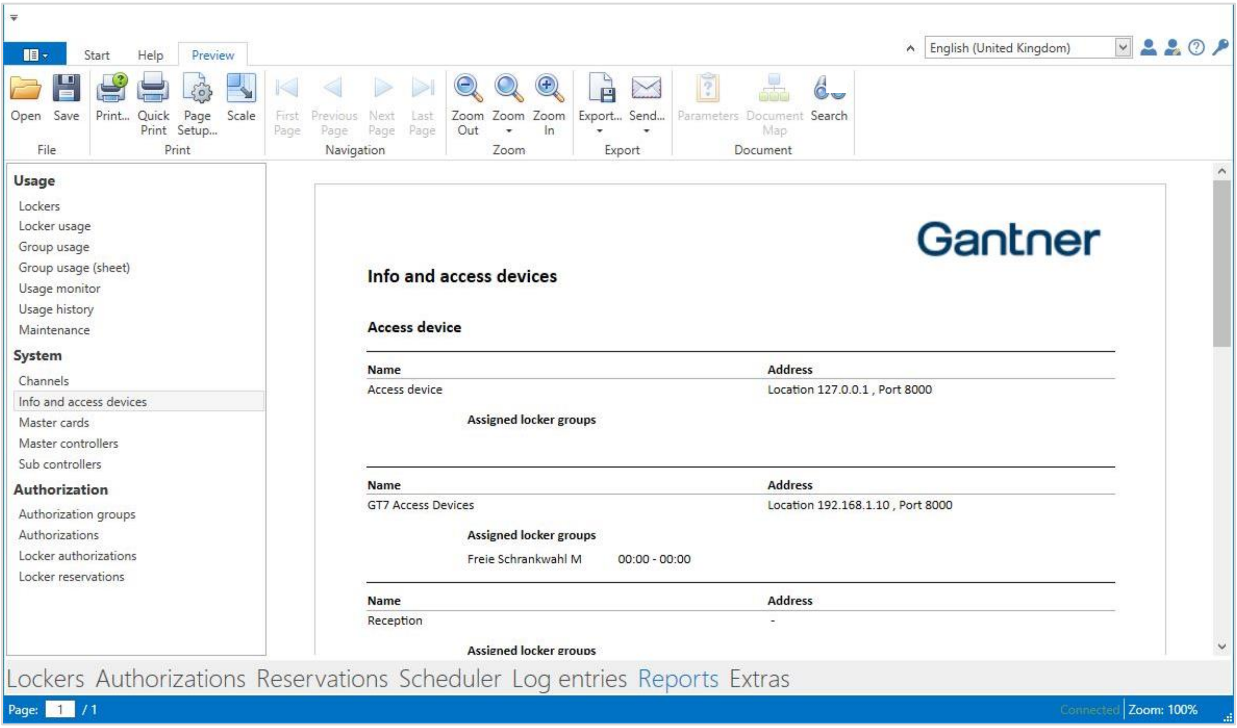
  NOTE! Imported log data is only temporarily opened in Relaxx and not added to the Relaxx database. You can view and edit the log data after importation. After a new search is made, the imported log data is blended out of the display and must be reloaded for further viewing.

In order to delete log entries, you can use the Action "Backup log entries" in the Scheduler (see "3.6.2 d) Backup log ").

3.8 Reports

Relaxx offers the possibility of creating various statistics, configuration overviews, authorization settings, etc., in report format that can be saved as PDF or printed directly.

- ► Switch to the "Reports" view.
  - ○ The following window opens.



Info and access devices

Access device

Name	Address
Access device	Location 127.0.0.1 , Port 8000

Assigned locker groups

Name	Address
GT7 Access Devices	Location 192.168.1.10 , Port 8000

Assigned locker groups

Freie Schrankwahl M 00:00 - 00:00

Name	Address
Reception	-

Assigned locker groups

Figure 3.81 *– Reports (example report showing Info and Access device information)*

- ► In the left column, all reports that can be created are listed. Click on the desired report.
  - ○ Relaxx compiles the report data based upon the current system state and displays the report to the right.
- ► Depending on the type of report selected, different functions become available in the function bar above the report. To print the displayed report, click on the "Print" icon.
- ► To save the report as a PDF, select the "Export document" icon and select "PDF".
- ► For reports where the information is arranged in columns, e.g., the “Channels” report, the column headers can be rearranged to the desired position via drag and drop. The list can also be sorted by a specific column, e.g., the most recent actions shown first.

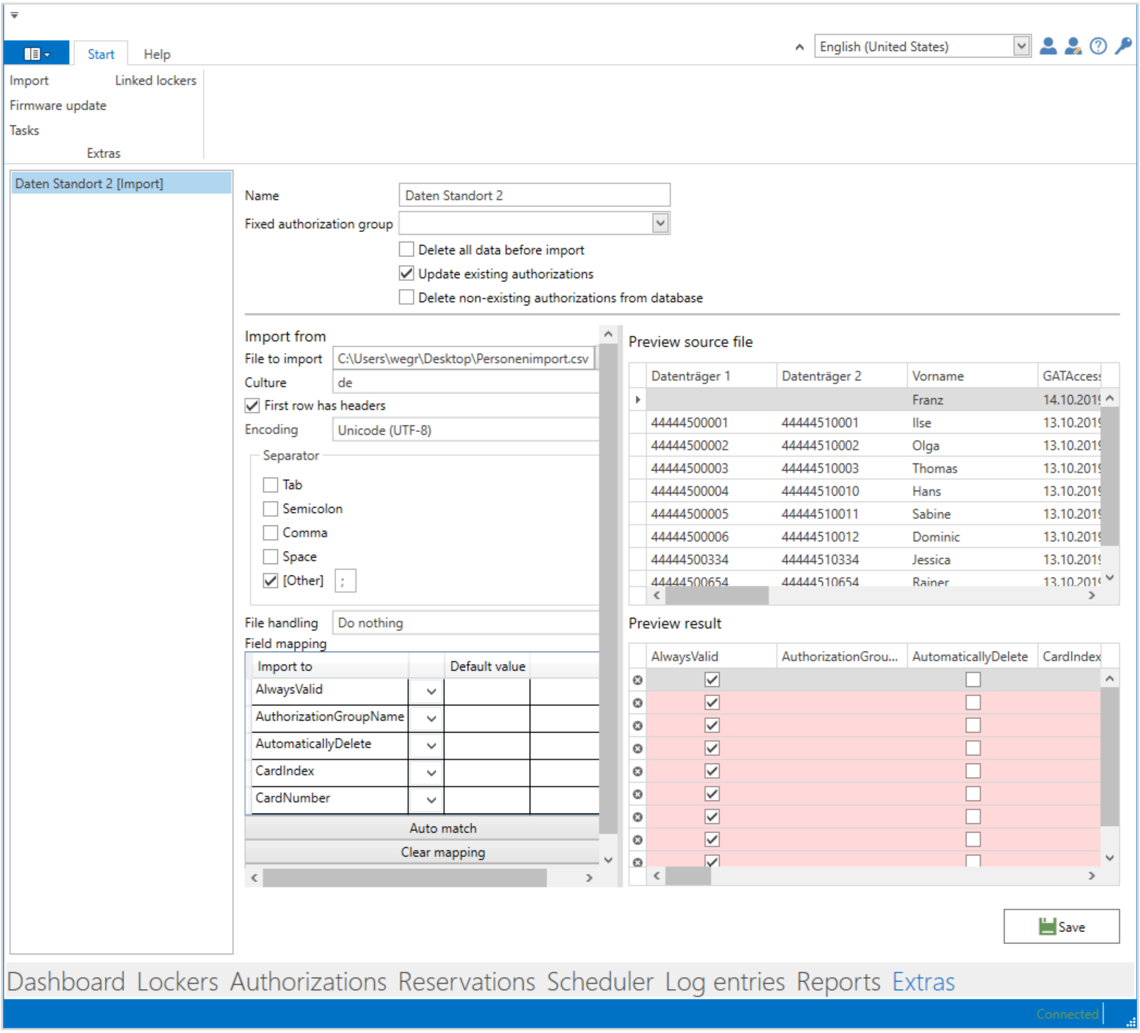
3.9 Extra Functions

In the "Extras" view, additional functions are available to define the extent of imports and exports, update devices and schedule tasks.

3.9.1 Import Definitions

Import definitions determine the content and format of the data that is to be imported into Relaxx. Multiple import definitions can be defined, which are then available for selection in the scheduler.

- ► Switch to the "Extras" view.
- ► Select an import definition from the list on the left.
  - ○ The "Import" view opens.



Name: Daten Standort 2
Fixed authorization group:
□ Delete all data before import
☑ Update existing authorizations
□ Delete non-existing authorizations from database

Import from
File to import: C:\Users\wegr\Desktop\Personenimport.csv
Culture: de
☑ First row has headers
Encoding: Unicode (UTF-8)
Separator
□ Tab
□ Semicolon
□ Comma
□ Space
☑ [Other] ;
File handling: Do nothing
Field mapping

Import to		Default value
AlwaysValid		
AuthorizationGroupName		
AutomaticallyDelete		
CardIndex		
CardNumber		

Preview source file

Datenträger 1	Datenträger 2	Vorname	GATAcces
		Franz	14.10.201
44444500001	44444510001	Ilse	13.10.201
44444500002	44444510002	Olga	13.10.201
44444500003	44444510003	Thomas	13.10.201
44444500004	44444510010	Hans	13.10.201
44444500005	44444510011	Sabine	13.10.201
44444500006	44444510012	Dominic	13.10.201
44444500334	44444510334	Jessica	13.10.201
44444500654	44444510654	Rainer	13.10.201

Preview result

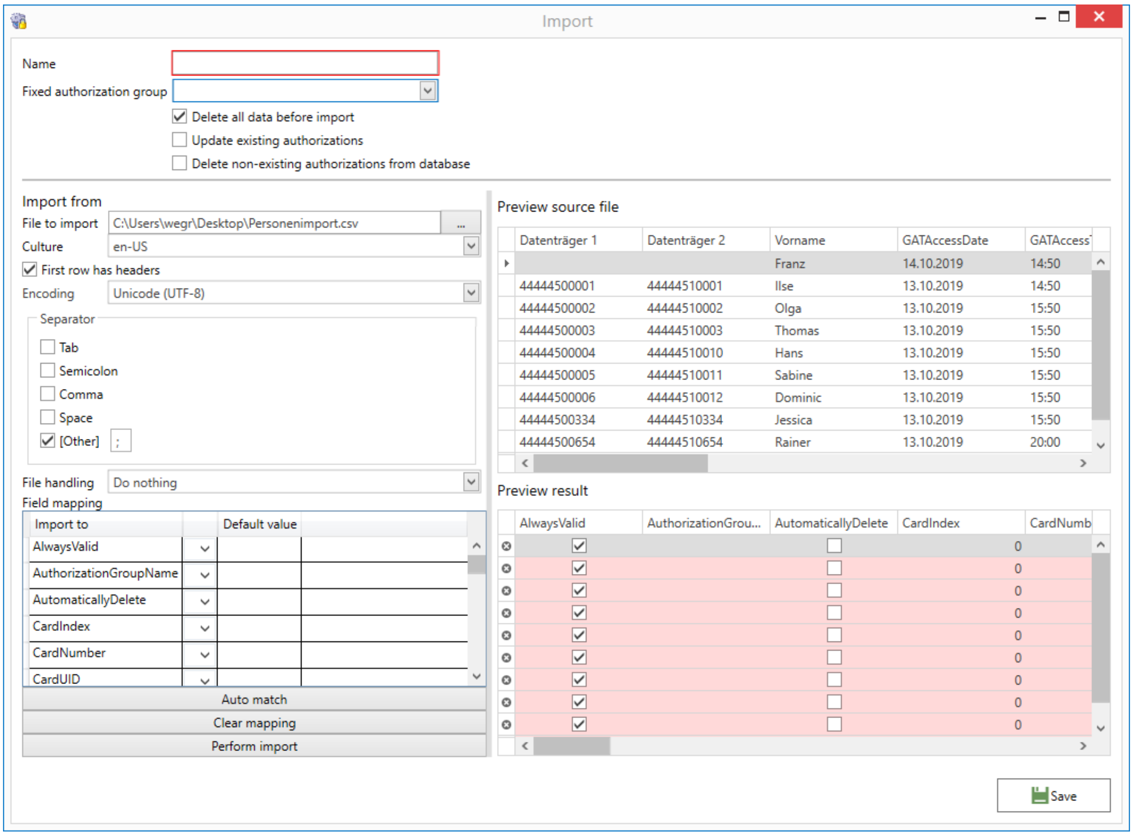
AlwaysValid	AuthorizationGrou...	AutomaticallyDelete	CardIndex
☑		□	
☑		□	
☑		□	
☑		□	
☑		□	
☑		□	
☑		□	
☑		□	
☑		□	

Figure 3.82 – *Import definition page*

All previously defined import definitions are displayed in the column to the left. Select a definition from the list to display its settings on the right.

Creating a new import definition

- ► To define a new import definition, click on the "New import definition" option.
  - ○ The "Import" window opens.



Name

Fixed authorization group

☑ Delete all data before import

□ Update existing authorizations

□ Delete non-existing authorizations from database

Import from

File to import: C:\Users\wegr\Desktop\Personenimport.csv

Culture: en-US

☑ First row has headers

Encoding: Unicode (UTF-8)

Separator

□ Tab

□ Semicolon

□ Comma

□ Space

☑ [Other] ;

File handling: Do nothing

Field mapping

Import to	Default value
AlwaysValid	
AuthorizationGroupName	
AutomaticallyDelete	
CardIndex	
CardNumber	
CardUID	

Preview source file

Datenträger 1	Datenträger 2	Vorname	GATAccessDate	GATAccess
		Franz	14.10.2019	14:50
44444500001	44444510001	Ilse	13.10.2019	14:50
44444500002	44444510002	Olga	13.10.2019	15:50
44444500003	44444510003	Thomas	13.10.2019	15:50
44444500004	44444510010	Hans	13.10.2019	15:50
44444500005	44444510011	Sabine	13.10.2019	15:50
44444500006	44444510012	Dominic	13.10.2019	15:50
44444500334	44444510334	Jessica	13.10.2019	15:50
44444500654	44444510654	Rainer	13.10.2019	20:00

Preview result

AlwaysValid	AuthorizationGrou...	AutomaticallyDelete	CardIndex	CardNumb
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	
☑		□	0	

Figure 3.83 – New import definition window

- ► Enter a name for the new definition in the "Name" field.
- ► In the "Fixed authorization group" field, a group can be selected, to which the definition will apply. In this case, the import will only be performed for this group. If this field is left empty, all groups will be considered.
- ► If the "Delete data before import" option is enabled, all existing authorization data (data carriers with possible locker authorizations) is deleted in Relaxx before importation. The remaining settings, such as hardware configurations, are not deleted.
- ► If the "Update existing authorizations" option is enabled, the imported columns are updated for authorizations that are already in the database. The unique key for the identification of the authorizations is the data carrier UID number. This means that there can only be one line in the import file per data carrier. This option is therefore not possible for lockers authorizations that have a data carrier authorized for more than one locker.
- ► If the "Delete non-existing authorizations from database" option is enabled, all authorizations that are not contained in the import file are deleted from the Relaxx database during an import. The unique key for the identification of the authorizations is the data carrier UID number. Therefore, if a data carrier number is changed manually in Relaxx, this change must also be made in the import file otherwise the data carrier will be deleted after an import.
- ► In the "Import from" area, select the import file and define the formatting.

- ○ The contents of the file will be displayed on the basis of the set formatting in the upper right area “Preview source file”.

► In the area "Field mapping”, you can define which field of the import file corresponds to which Relaxx data.

NOTE: The "CardUID" is mandatory and must be assigned. All other fields are optional.

- ○ In the lower right "Preview result" area, you can see how the information will be imported and assigned to the Relaxx fields.
- ○ If cells contain errors (e.g., wrong number format for date fields) or if the card UID was not specified, this is indicated by a red background in the preview.

► To confirm the settings, click on "Save".

3.9.2 Updating Device Firmware

To update the devices (controllers and locks), the current firmware files can be uploaded to the devices. This function allows firmware updates to be performed in a time-controlled manner.

NOTE! GANTNER recommends updating the firmware of the GAT NET.Lock 7000, GAT NET.Controller S 7000, and GAT NET.Lock Controller M 7000 when you install the system. The latest firmware is available via the partner area of the GANTNER website or from your GANTNER representative.

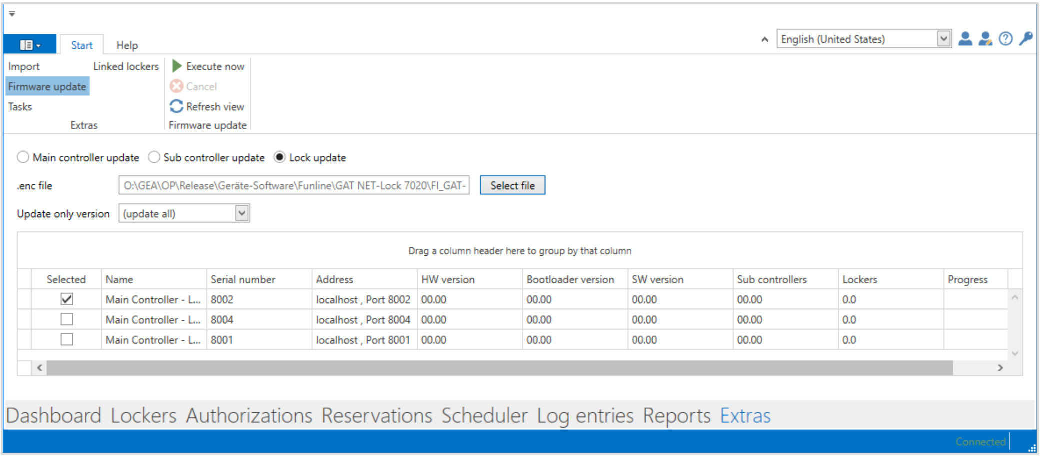
NOTE! FIRMWARE UPDATE:

- As every firmware update represents a risk to electronic devices, GANTNER recommends performing updates during non-critical operating times and by skilled employees only.
- During the firmware update process, do not complete other tasks in Relaxx, e.g., changing the hardware configuration or solving locker conflicts, etc.

► Switch to the "Extras" tab.

► Click on the "Firmware update" button.

- ○ The firmware update view is displayed with all main controllers that are currently assigned to the system listed. You can see the current hardware version (HW version) and software version (SW version) for each main controller as well as the firmware version of the sub controllers and GAT NET.Lock 7000 locks connected to them.



○ Main controller update ○ Sub controller update ● Lock update

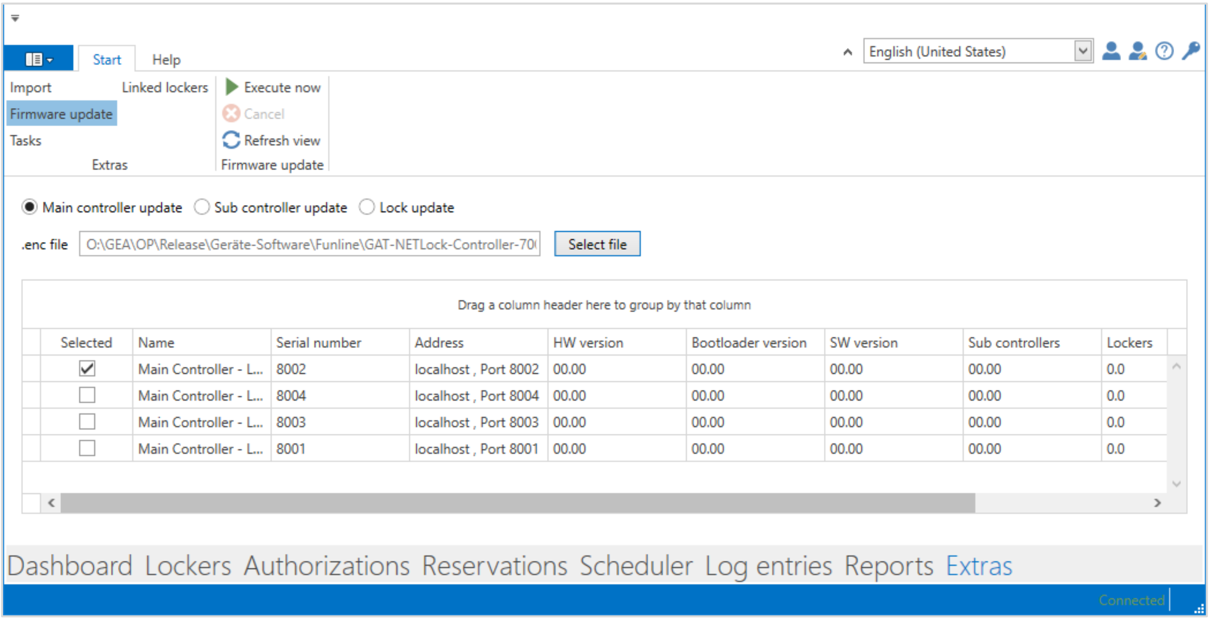
.enc file: O:\GEA\OP\Release\Geräte-Software\Funline\GAT NET-Lock 7020\FI_GAT-

Update only version: (update all)

Selected	Name	Serial number	Address	HW version	Bootloader version	SW version	Sub controllers	Lockers	Progress
☑	Main Controller - L...	8002	localhost , Port 8002	00.00	00.00	00.00	00.00	0.0	
□	Main Controller - L...	8004	localhost , Port 8004	00.00	00.00	00.00	00.00	0.0	
□	Main Controller - L...	8001	localhost , Port 8001	00.00	00.00	00.00	00.00	0.0	

Figure 3.84 *– Firmware update window*

- ► Select either “Main update”, “Sub controller update”, or “Lock update” for the type of device update to perform.
- ► When “Lock update” is selected, an additional “Update only version” option is displayed, which allows you to update all locks or a specific firmware version. This is helpful, e.g., when one lock is exchanged with another lock that has outdated firmware. Rather than updating all locks, which can take some time, you can update only those locks with outdated firmware.



● Main controller update ○ Sub controller update ○ Lock update

.enc file O:\GEA\OP\Release\Geräte-Software\Funline\GAT-NETLock-Controller-70(

Selected	Name	Serial number	Address	HW version	Bootloader version	SW version	Sub controllers	Lockers
☑	Main Controller - L...	8002	localhost , Port 8002	00.00	00.00	00.00	00.00	0.0
□	Main Controller - L...	8004	localhost , Port 8004	00.00	00.00	00.00	00.00	0.0
□	Main Controller - L...	8003	localhost , Port 8003	00.00	00.00	00.00	00.00	0.0
□	Main Controller - L...	8001	localhost , Port 8001	00.00	00.00	00.00	00.00	0.0

***Figure 3.85** – Device firmware updating options*

- ► In the ".enc file" field, select a firmware file for the update. Click on “Select file” to locate the file via the computer directory or you can simply drag and drop the file onto the field.
- ► In the controller list, mark the “Selected” box next to the main controller requiring an update. Multiple controllers can be selected for the update. To select all controllers, right-click onto a controller and select “Select all” from the pop-up menu.
- ► When updating sub controllers or locks, select the applicable main controller(s) to which the sub controllers/locks are connected.

  NOTE! If a main controller is not shown in the list, click on the “Refresh view” button or check that the main controller is still communicating with Relaxx (green icon in the hardware view).
- ► Click on the "Execute now" button to execute the firmware update.
  - o The update process for the selected device(s) may take several minutes to complete. Once completed, the new firmware version is displayed in the corresponding column.

3.9.3 Tasks

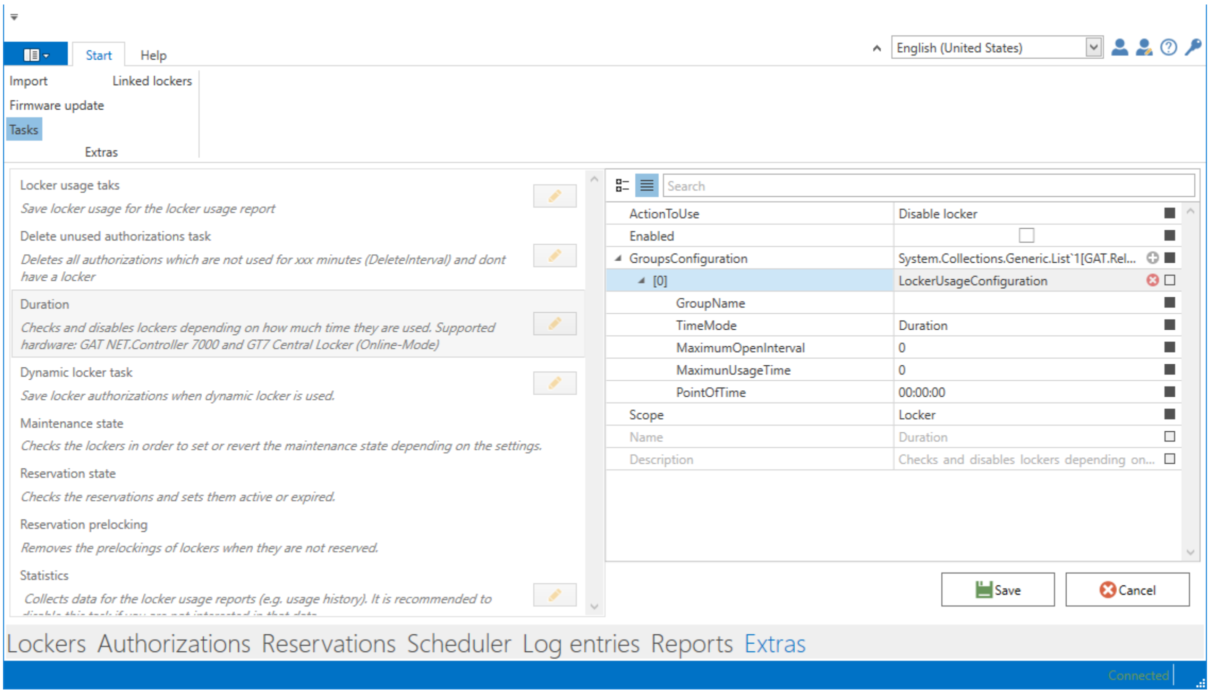
Using the "Tasks" function, tasks can be defined that Relaxx executes automatically. A pen icon next to the task name indicates that the task can be edited. All other tasks cannot be edited and are permanently active.

NOTE! Please note that the settings for the scheduling of tasks may only be modified by skilled staff or in cooperation with GANTNER.

► Switch to the "Extras" view.

► Select the "Tasks" functionality,

  ○ The "Tasks" view is displayed.



Locker usage taks

Save locker usage for the locker usage report

Delete unused authorizations task

Deletes all authorizations which are not used for xxx minutes (DeleteInterval) and dont have a locker

Duration

Checks and disables lockers depending on how much time they are used. Supported hardware: GAT NET.Controller 7000 and GT7 Central Locker (Online-Mode)

Dynamic locker task

Save locker authorizations when dynamic locker is used.

Maintenance state

Checks the lockers in order to set or revert the maintenance state depending on the settings.

Reservation state

Checks the reservations and sets them active or expired.

Reservation prelocking

Removes the prelockings of lockers when they are not reserved.

Statistics

Collects data for the locker usage reports (e.g. usage history). It is recommended to disable this task if you are not interested in that data.

ActionToUse	Disable locker
Enabled	□
◢ GroupsConfiguration	System.Collections.Generic.List`1[GAT.Rel...
◢ [0]	LockerUsageConfiguration
GroupName	
TimeMode	Duration
MaximumOpenInterval	0
MaximunUsageTime	0
PointOfTime	00:00:00
Scope	Locker
Name	Duration
Description	Checks and disables lockers depending on...

Figure 3.86 *– Scheduling tasks*

The tasks and their descriptions are shown in the left column. The tasks are defined as follows:

- Locker usage task: Here you can activate the saving of locker usage data by selecting "Enabled". This data is required for the locker usage report (see “3.8 Reports”).
  - RetentionDays: Define how long (in days) the data will be retained for.
  - WriteInterval: Time interval (in minutes) for writing data to the database. A larger interval requires less database space but reduces the precision in the data.
- Delete unused authorizations task:

  With this function, all locker authorizations that no longer have a locker assigned and that have not been used for a certain period of time can be deleted in order to clear the authorization list and minimize legacy issues.

- DeleteAuthorizationsAfterInactivity: Select this option to enable the task.
- DeleteInterval: A locker authorization must be used within the time entered here (in minutes), otherwise it will be deleted.

- Duration: This is an editable task that executes a locker action depending on locker usage. For example, a user has exceeded their permitted locker usage time; the duration task is therefore activated, and the locker is disabled.
  - ActionToUse: From the drop-down menu, select the type of locker action to activate once the "Maximum Usage Time" or "Point Of Time" time has expired.
  - Enabled: Select this option to enable the task.
  - GroupsConfiguration: Click on the plus symbol to add a group and define the following configuration settings:
    - GroupName: The name of the group that the task will apply to. Enter a * character in this field to apply the task to all groups.
    - TimeMode: Select either "Duration" or "Point Of Time" from the menu:

      Duration: In this mode, a usage period is set in the "Maximum Usage Time" field. The usage period begins at the point when the locker is first locked by the user and it must be unlocked again within the period or the "Action To Use" command is activated.

      PointOfTime: For this mode, a time is defined up to which the locker can be used every day. After locking a locker, the locker must be unlocked before the defined time or the "Action To Use" command is activated. The usage period starts from the configured time after midnight.
    - MaximumOpenInterval: The maximum time in minutes that a locker can remain open before the duration task is cancelled.
    - MaximumUsageTime: When "Time Mode" is set to "Duration", enter the locker usage period in minutes here.
    - PointOfTime: When "Time Mode" is set to "Point Of Time", enter here the time of day before which the locker must be opened.
  - Scope: From the menu, select one of the following settings to define the scope of the duration task:

    Locker: The user's locker usage time is reset if the user switches to another locker.

    Locker Group: The user's locker usage time continues to be counted if the user switches to another locker within the same locker group.

    System: The user's locker usage time continues to be counted if the user switches to another locker within any of the locker groups configured in the duration task.

- Dynamic locker task: When "DeleteLockerAuthorizationsOnOpen" is enabled, locker authorizations are deleted from lockers in dynamic locker mode after being unlocked.

- Maintenance state: This task checks the lockers in order to set or automatically revert the maintenance state depending on the settings.

- Reservation state: This task checks the reservation status of lockers and updates the information to either active or expired.
- Reservation prelocking: This task manages locked lockers (reserved) and reverts them to their default operating mode if the reservation is not saved within 15 minutes.
- Statistics: This is an editable task that collects the data required for the locker usage reports every x number of minutes. It is recommended to disable this task if you are not interested in the locker usage data.
  - Enabled: Select this option to enable the task.
  - WriteInterval: In this field you can define the number of minutes.

► Select a task.

  ○ The settings of the task are displayed in the left column.

► To edit a task, click on the icon with the pen symbol.

  ○ The settings can now be edited on the right.

► After editing, click on "Save".

3.9.4 Linked Lockers

The "Linked lockers" function, two or more lockers can be linked so that they can be operated together.

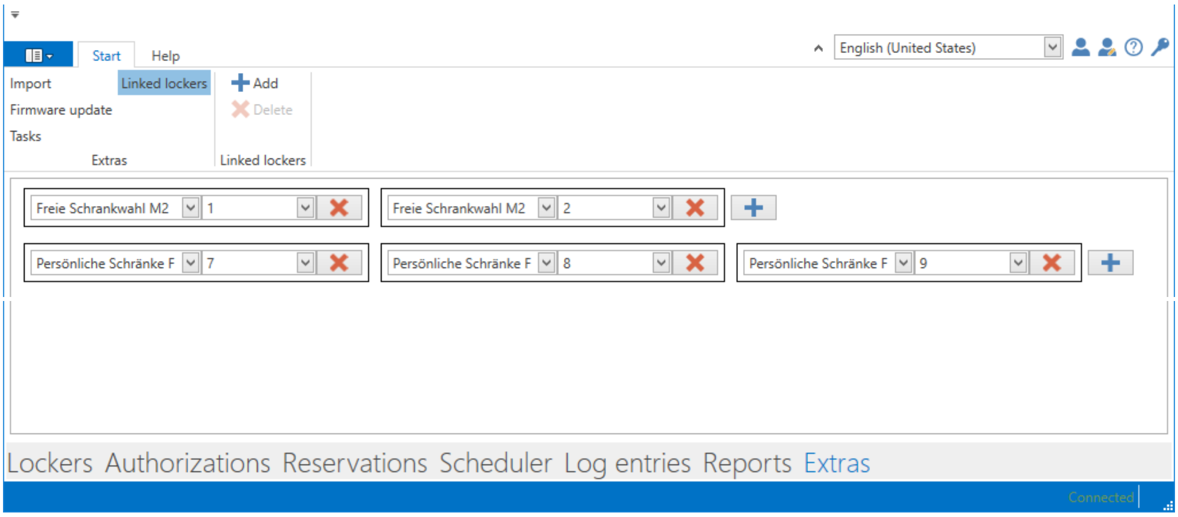
For the "Linked lockers" function, only the GAT NET.Lock 70x0 operating in "Free Locker" mode and with the "Pre-close free lockers" function enabled can be linked.

To link lockers, proceed as follows:

► Open the "Extras" area.

► Click on "Linked lockers".

  ○ The overview of the defined, linked lockers is displayed.



Freie Schrankwahl M2 | 1 — Freie Schrankwahl M2 | 2

Persönliche Schränke F | 7 — Persönliche Schränke F | 8 — Persönliche Schränke F | 9

***Figure 3.87** – Linked lockers*

Each row shows two or more lockers that are linked.

- ► You can insert a new line via the "+ Add" symbol.
- ► Select a locker in each column by selecting a locker group and a locker number.
- ► Another locker can be inserted via the “+” sign at the end of a line.
- ► Click on the "Save" button to save the settings.

The functionality of the linked lockers is as follows (example of 2 linked lockers).

- When both doors are closed and the locker is unoccupied, the LEDs on both doors are green.

Occupy locker:

- When the user opens one door, the LED on the other door turns red.
- The user puts their belongings into the locker.
- The user now pushes the locker door shut; the LEDs on both doors remain red for the defined linked lockers "Release time" (see “Advanced” tab under "2.2.3 Devices").
- The user holds their data carrier near the lock LED -> both locker doors are locked (if the data carrier is not read by the lock within the release time, the locker will be available again -> both LEDs will turn green).

Open locker:

- The user holds their data carrier near the lock LED -> one door opens, the other remains closed and the LED remains red.
- The user empties the locker.
- Close the locker door again -> both LEDs remain red for the defined linked lockers "Release time" (see “Advanced” tab under "2.2.3 Devices").
- If no data carrier is read by the lock, both LEDs turn green after the release time and the locker is available again.

3.9.5 Manual

In the “Help” tab, the “Manual” icon contains a link to the Relaxx documentation. The following files are available:

- Relaxx.chm:	This is the help file for Relaxx and describes every feature and function available in the software. Main topics can be accessed using the menu structure on the left side of the window. The file also contains a search function under the “Search” tab where specific keywords can be entered. Another option is to use the context-sensitive help by pressing the “F1” key while working within Relaxx. This will access the help topic for the window that is currently open.
- Relaxx_Installation.pdf:	This document contains all the information required to install and setup Relaxx.
- Relaxx_Handbook.pdf:	This is the user manual for Relaxx and contains all the relevant information required to operate and manage Relaxx.

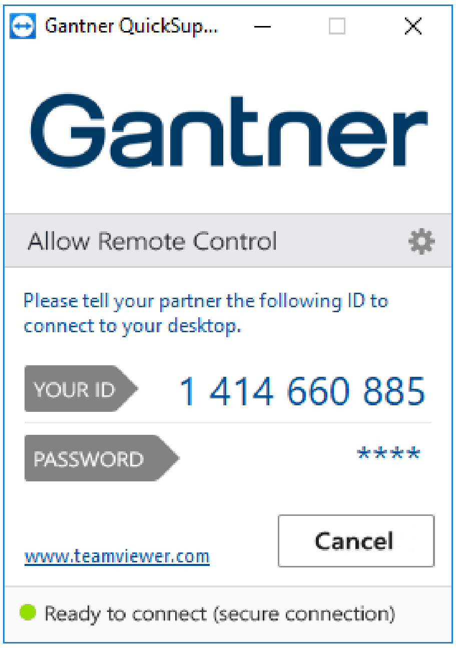
3.9.6 TeamViewer

TeamViewer is a software program that allows persons to view and control your computer remotely. This tool is useful if you have an operational issue and require assistance from the GANTNER support team. The support team uses TeamViewer to see your desktop configuration and provide an effective solution.

If you are asked to start a TeamViewer session:

► Go to the “Extras” page, click on the “Help” tab then click on the “TeamViewer” icon.

  ○ The following window opens.



Gantner QuickSup...

Gantner

Allow Remote Control

Please tell your partner the following ID to connect to your desktop.

YOUR ID 1 414 660 885

PASSWORD ****

www.teamviewer.com

Cancel

● Ready to connect (secure connection)

Figure 3.88 *– TeamViewer window*

Your desktop is shared only when the support team logs into TeamViewer using your "Your ID" number.

Configuration settings for the TeamViewer session, e.g., video or audio settings, can be viewed and changed by clicking on the settings icon. There are three configuration options available in the "TeamViewer options" window – “General”, “Audio conferencing” and “Video”. Please visit the TeamViewer website for further information on configuring and operating the software.

3.9.7 Diagnostics

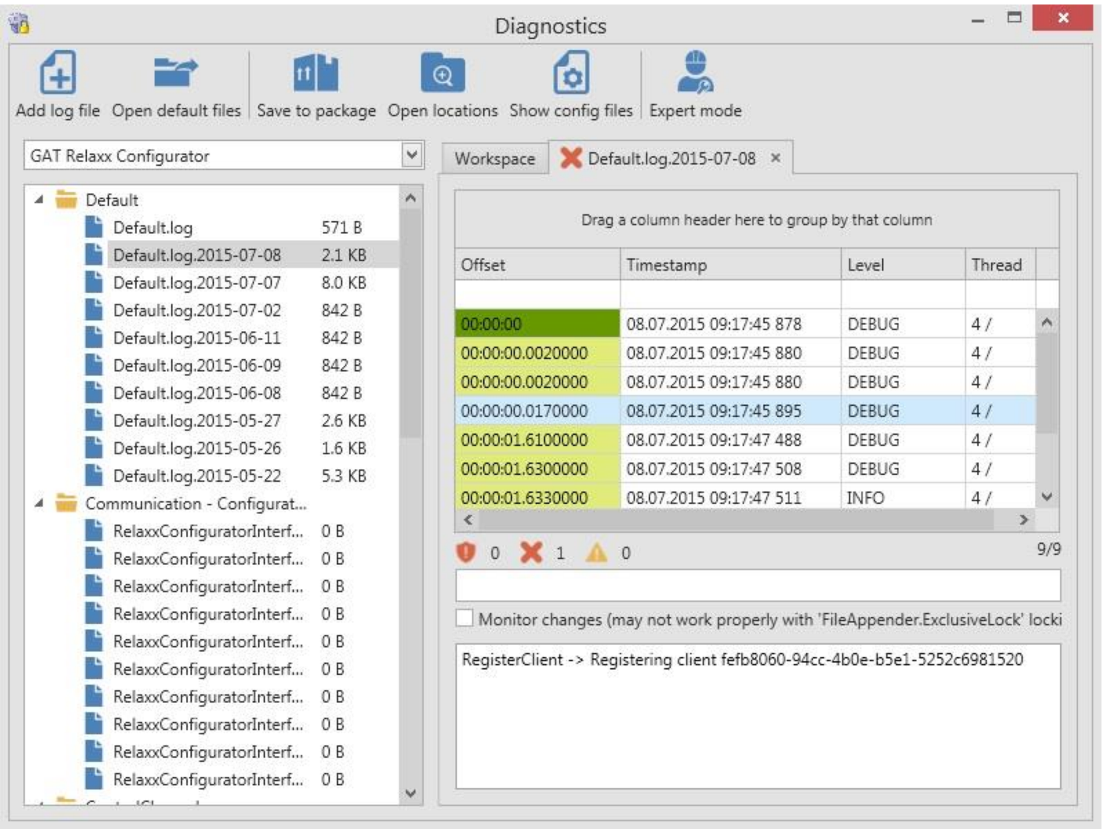
Relaxx records all system events and activity as log files. Using the integrated diagnostics tool, you have the ability to view and evaluate the log files and, if required, to save them as a package that can be sent to GANTNER or your partner for further analysis.

► The drop-down menu in the upper left corner contains a "collection" of log files. Select a collection type:

- “Relaxx Service” contains the log files of the Relaxx service.
- "Relaxx Configurator" contains the log files of the user interface.
    - ○ All the log files that are included in the selected collection are listed beneath the collection menu.

► Double-click on a log file in the left column to view the details.

- ○ The log file entries are displayed in the right column. If multiple log files are opened, these can be selected via tabs.



Default	
Default.log	571 B
Default.log.2015-07-08	2.1 KB
Default.log.2015-07-07	8.0 KB
Default.log.2015-07-02	842 B
Default.log.2015-06-11	842 B
Default.log.2015-06-09	842 B
Default.log.2015-06-08	842 B
Default.log.2015-05-27	2.6 KB
Default.log.2015-05-26	1.6 KB
Default.log.2015-05-22	5.3 KB
Communication - Configurat...	
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B
RelaxxConfiguratorInterf...	0 B

Offset	Timestamp	Level	Thread
00:00:00	08.07.2015 09:17:45 878	DEBUG	4 /
00:00:00.0020000	08.07.2015 09:17:45 880	DEBUG	4 /
00:00:00.0020000	08.07.2015 09:17:45 880	DEBUG	4 /
00:00:00.0170000	08.07.2015 09:17:45 895	DEBUG	4 /
00:00:01.6100000	08.07.2015 09:17:47 488	DEBUG	4 /
00:00:01.6300000	08.07.2015 09:17:47 508	DEBUG	4 /
00:00:01.6330000	08.07.2015 09:17:47 511	INFO	4 /

0 ✖ 1 ⚠ 0 9/9

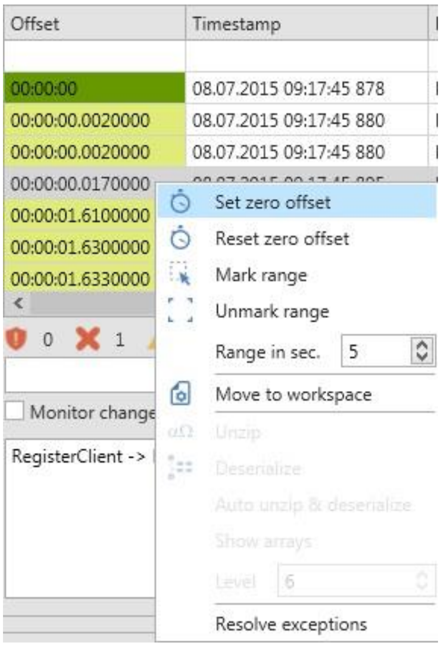
□ Monitor changes (may not work properly with 'FileAppender.ExclusiveLock' locki

```
RegisterClient -> Registering client fefb8060-94cc-4b0e-b5e1-5252c6981520
```

Figure 3.89 *– Diagnostics window*

► Right-click on a specific log file entry.

- ○ A pop-up window with various settings opens.



Offset	Timestamp
00:00:00	08.07.2015 09:17:45 878
00:00:00.0020000	08.07.2015 09:17:45 880
00:00:00.0020000	08.07.2015 09:17:45 880
00:00:00.0170000	
00:00:01.6100000	
00:00:01.6300000	
00:00:01.6330000	

***Figure 3.90** – Log file diagnostics options*

► Via the options in this menu you can filter the log files, so they are arranged in a time-specific way. The log file in the list can be reset so that the time-reference point (= green marker in the log entries) begins with the chosen log entry.

Other functions in the diagnostics window include:

- Open default files: This option opens all commonly used log files at once.
- Save to package: Click on this icon if you want to save the log files or send them for analysis. You have the option to save just the files currently displayed in the list or to save all files in the collection. This function saves the data in a ZIP file that can be sent directly via email.
- Open locations: This icon activates Windows File Manager, which automatically opens each folder where the log files are located.
- Expert mode: Some log files (e.g., "Communication - ConfiguratorInterface") are saved in compressed format. To view these files, click on the “Expert mode” icon. For security reasons, a password is required to activate expert mode.

3.9.8 General Feedback

Use this window to send us your general thoughts on how the system is working for you. You can use the five-star rating system at the bottom of the window to rate the software. Hover over each star for a detailed description of each star's value.

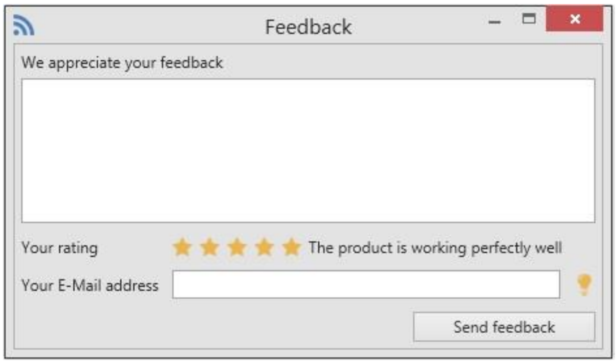

Feedback
We appreciate your feedback
Your rating
★★★★★ The product is working perfectly well
Your E-Mail address
Send feedback

***Figure 3.91** – General feedback window*

Please include your email address so that we can contact you again. Click on "Send Feedback" at the bottom of the window to finalize your feedback.

3.9.9 Report a Bug

Use this window to inform us of any errors in Relaxx. It helps us greatly if you can reproduce the error and document the system configuration when the error occurs. The more information we have about the error, the more efficient we can be at developing a solution.

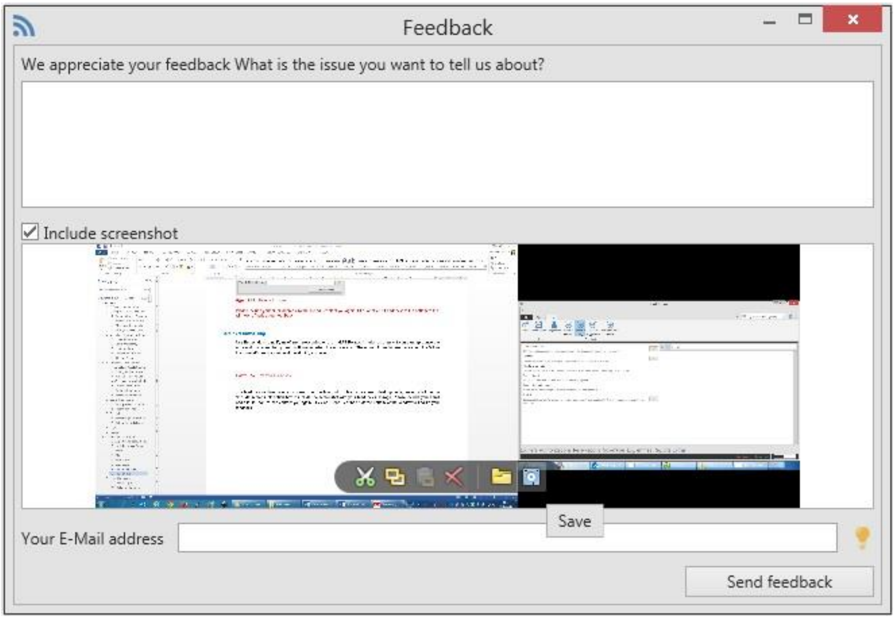

Feedback
We appreciate your feedback What is the issue you want to tell us about?
☑ Include screenshot
Save
Your E-Mail address
Send feedback

***Figure 3.92** – Report a bug feedback window*

The feedback window includes a screenshot function that displays your current desktop configuration. The screenshot is sent with the feedback form when the "Include screenshot" option box is selected. Please include your email address so that we can contact you again. Click on "Send Feedback" to send the information.

3.9.10 Make a Suggestion

Use this window to offer suggestions for the Relaxx system. Perhaps you have encountered a situation during the day-to-day operation of the software that can be improved, any ideas that can help enhance the usability of our software are welcomed.

The feedback window is similar to Figure 3.92 and includes a screenshot function that displays your current desktop configuration. The screenshot is sent with the feedback form when the "Include screenshot" option box is selected. Please include your email address so that we can contact you again. Click on "Send Feedback" to send the information.

3.9.11 Request a New Feature

Use this window to send us your ideas about features you would like to see included in future versions of Relaxx. The end users of our software are in the best position to see market or technological trends developing in the industries that Relaxx serve. We welcome the chance to develop new market-driven features and improve our software.

The feedback window is similar to Figure 3.92 and includes a screenshot function that displays your current desktop configuration. The screenshot is sent with the feedback form when the "Include screenshot" option box is selected. Please include your email address so that we can contact you again. Click on "Send Feedback" to send the information.

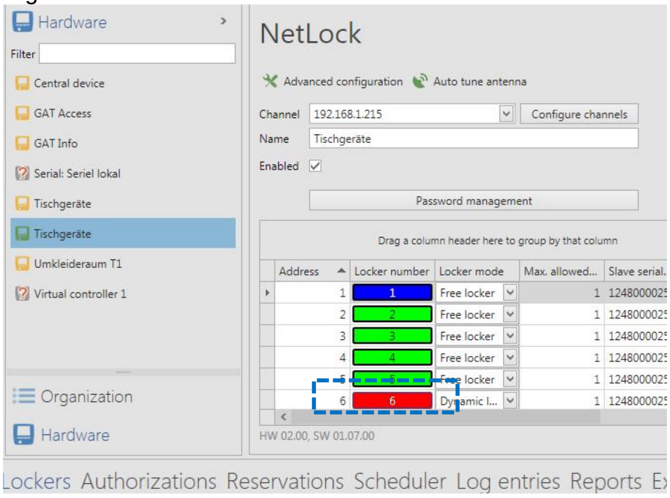
3.10 Handling Alarms

Various alarms can be triggered in the locker system, e.g., when a locker is opened without the use of a data carrier (i.e., illegal break-in).

3.10.1 Alarm Display

If an alarm is triggered at a locker, this is displayed at various points in Relaxx:

- Lockers, where an alarm was triggered, are displayed with a red background both in the hardware view and the organization view.



Channel 192.168.1.215
Name Tischgeräte
Enabled ☑

Drag a column header here to group by that column

Address	Locker number	Locker mode	Max. allowed...	Slave serial.
1	1	Free locker	1	124800002
2	2	Free locker	1	124800002
3	3	Free locker	1	124800002
4	4	Free locker	1	124800002
5	5	Free locker	1	124800002
6	6	Dynamic l...	1	124800002

HW 02.00, SW 01.07.00

Figure 3.93 *– Alarm displayed in the hardware view*

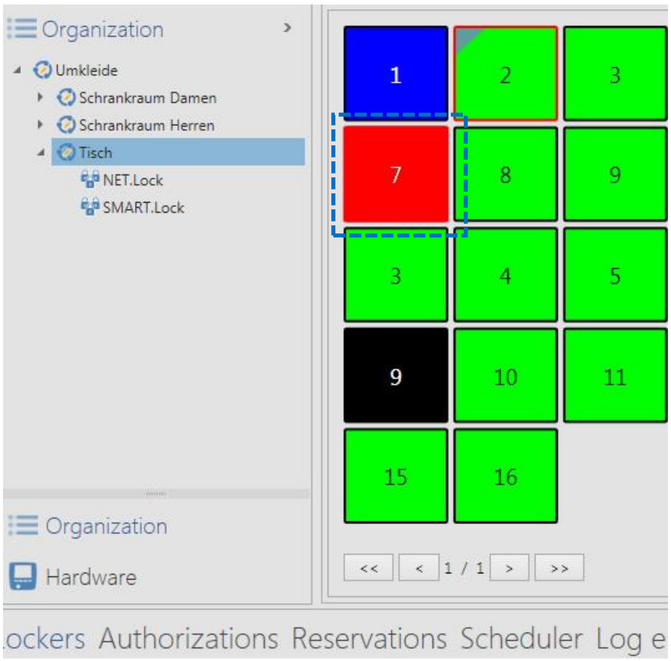
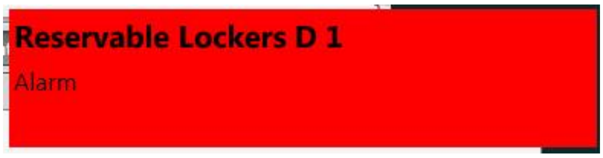


Figure 3.94 *– Alarm displayed in the organization view*

An alarm is also displayed with a small, red pop-up window and an alarm window on the screen.



Reservable Lockers D 1

Alarm

Figure 3.95 *- Alarm pop-up window*

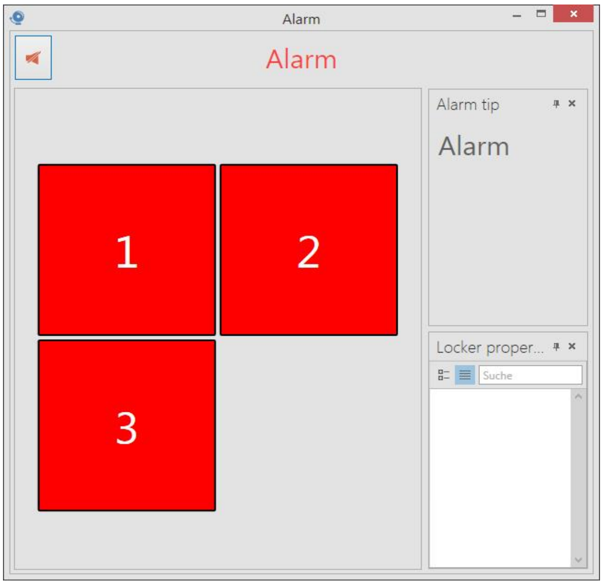


Figure 3.96 *– Alarm window of the Alarm Viewer*

The configuration of which alarm sounds to use and which texts to display with the alarms in the "Alarm tip" area is set in the “Alarm” area of the general software settings (refer to "2.2.2 Alarm").

NOTE! To cancel the alarm sound (if enabled), click on the loudspeaker icon in the upper left corner of the alarm window.

3.10.2 Acknowledging Alarms

In order to acknowledge an alarm, the cause of the alarm must first be removed otherwise the alarm is activated again. Proceed as follows.

► Check the locker and the system to find out the reason for the alarm.

NOTE! For locker systems with the GAT NET.Lock 70x0, the integrated LED on this lock can show the various locking states, e.g. alarm enabled. Refer to the GAT NET.Lock 70x0 manual for further information.

- ► Take the appropriate action to eliminate the reason of the alarm.
- ► In the organization of Relaxx, select the locker that triggered the alarm and click on the icon "Deactivate alarm" in the multifunction bar. Alternatively, this point can also be selected in the pop-up menu of the AlarmViewer (right-click onto the locker).
  - o The "Locker actions" window opens, if this is defined in the user administration for the current user (refer to option "Login for locker commands" in "4.3.2. Default ").

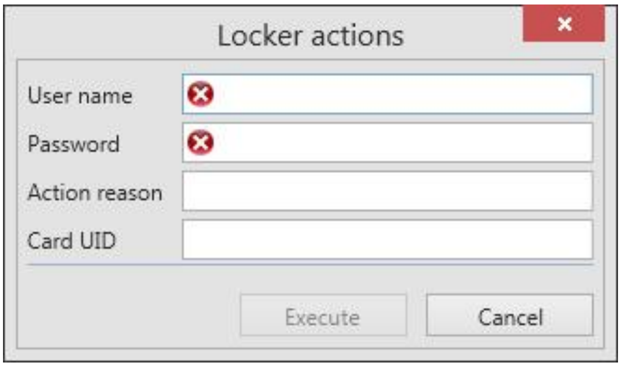


***Figure 3.97** – Accepting locker actions*

- ► Enter your username and password.

  NOTE! This step is necessary for safety reasons, so unauthorized persons cannot acknowledge (accept) alarms. This also enables following up who acknowledged (accepted) the alarm.
  A username and password must always be entered in the AlarmViewer window for acknowledgment, even if the "Login for locker commands" option has been deactivated in the user settings for the user who is logged in when the AlarmViewer is opened (see "4.3.2 Default Users").
- ► For better follow-up, a reason can be entered for the accepting.
- ► Click "Execute".
  - o The alarm is deactivated and is not displayed in the hardware and organization views by a red background any longer.
  - o After deactivating the alarm, the locker is deactivated and shown with a black background. If the reason for the alarm has not been remedied, the alarm will be triggered again.
- ► Once the reason for the alarm has been identified and remedied (e.g. a new locker has been installed after break-in), the locker can be enabled for use, by right-clicking with the mouse on the locker and selecting the “Locker enable” option in the pop-up menu. Identification is also required for this locker action.

3.10.3 Relaxx AlarmViewer

The Relaxx AlarmViewer is software that can be installed via the Relaxx installation package in addition to the Relaxx Service and Client (see the Relaxx Installation Manual). Relaxx AlarmViewer can be started manually in order to activate it. To do so, you will find the corresponding entry in the Windows Start menu.

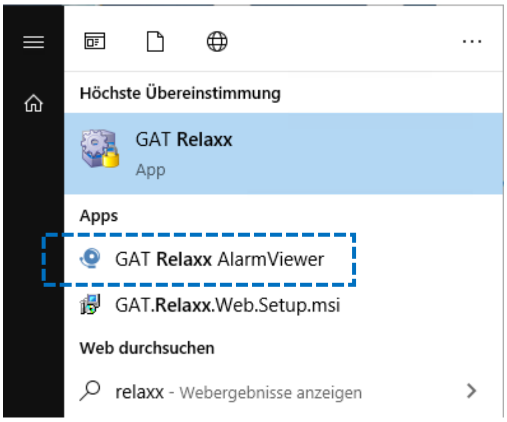


***Figure 3.98** – Starting the Relaxx AlarmViewer*

By default, AlarmViewer is added to the Windows auto-startup function after installation so that the software automatically starts every time Windows is started.
If the encrypted TLS communication is activated (see Relaxx Installation Manual), the username and password must be entered when AlarmViewer is started. If TLS communication is deactivated, AlarmViewer starts automatically and runs in the background.

When Relaxx AlarmViewer is started, the following icon is displayed in the Windows status bar.

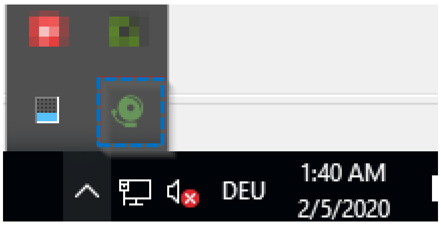


***Figure 3.99** - Relaxx AlarmViewer icon in the Windows status bar*

Right-clicking on the icon opens a menu where you can configure settings for the Relaxx AlarmViewer.

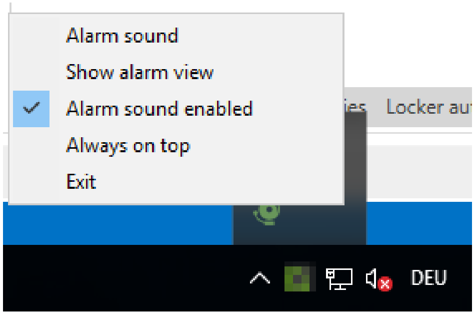
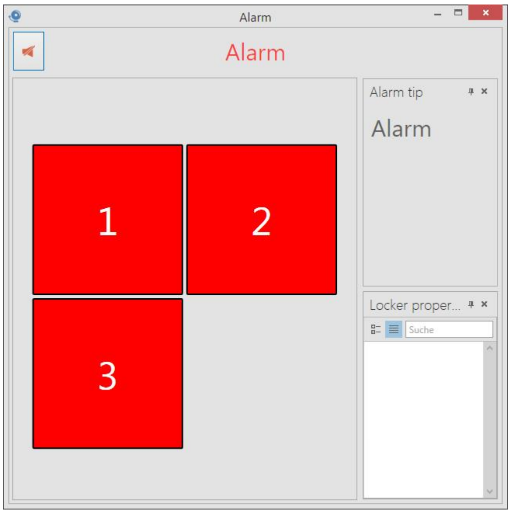


***Figure 3.100** - Relaxx AlarmViewer settings menu*

The following settings are available here:

- Alarm sound: This menu item opens a file selection window where you can select a .wav file that contains the desired alarm sound. This tone is played when an alarm occurs.
  The alarm tone can also be selected globally in Relaxx via the alarm settings (see "2.2.2 Alarm"). However, the sound in the AlarmViewer has priority.
- Show alarm view: This option displays the alarm window where you can see information about the pending alarm(s).



- Alarm sound enabled: Here, you can switch the alarm sound on and off.
- Always on top: If this option is selected, the alarm window is always displayed as the top window in Windows. If the function is deactivated, it can also be overlaid in the background or by other windows.
- Exit: This closes the AlarmViewer.

3.11 Remote-Controlled Locker Operation via Mobile Device (REST API)

Relaxx 4.0 offers the possibility to access the software via a REST API over the network. This allows the locker system to be controlled remotely, for example, to lock and unlock an authorized locker via a mobile app such as LockPal.

To enable a user to use the remote control function, e.g., via an app, a corresponding data carrier, authorized in Relaxx, is always required for the user for security reasons.

The following figure shows the operation of the remote control function via the REST API.

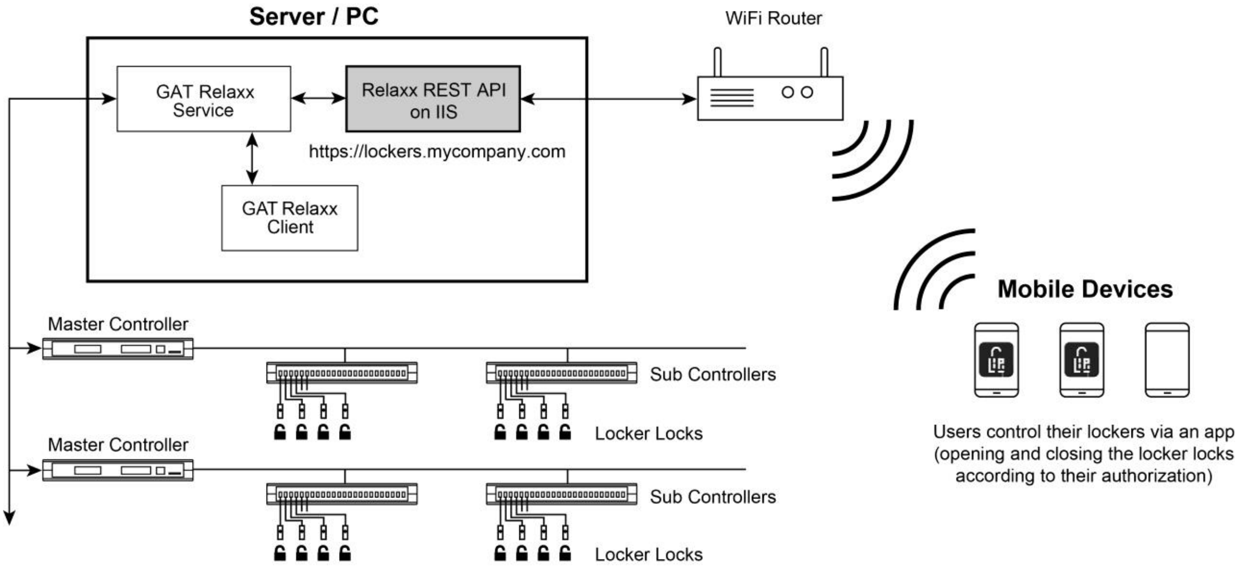


__Figure 3.101__ - Authentication for locker actions

The Relaxx REST API is included in the installation package of Relaxx and can be installed via the installation wizard (see the Relaxx Installation Manual).

It is also possible, by using the REST API interface, to integrate other software packages into the locker system and to enable remote control. Please contact GANTNER for more information regarding the REST API or the LockPal app.

4 AUTHORIZATION MANAGEMENT

Relaxx offers the possibility to assign individual users with different levels of system control. This is done using a simplified “role” based access system. Each user is assigned to one role, the user’s system control being inherited from this role. A role represents a collection of permissions to modify certain functions within the application. Furthermore, the system allows overriding of the permissions at user level.

4.1 Function Blocks

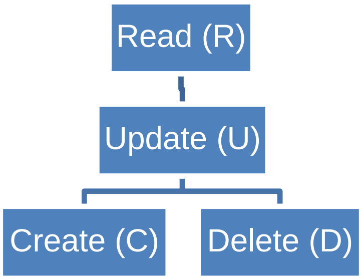
A function block is a group of simple actions (e.g. Hardware view manipulations, scan devices, open lockers) in the application for which permission to modify can be granted instantly. Depending on the function block, you can assign Create (C), Read (R), Update (U), Delete (D), Execute (E) and Grant (G) permissions.

Execute permissions are assigned to allow a user to execute an action or not. An example for this is the “Start/Stop service” function block. It is not logical to define RUCD permissions for this function block since nothing can be created or deleted.

Alternatively, RUCD permissions can be assigned for the “Hardware view management” function block. It is possible to specify the users who are permitted to view the hardware configuration on the Hardware View page and other users who are permitted to modify or delete the hardware configuration.

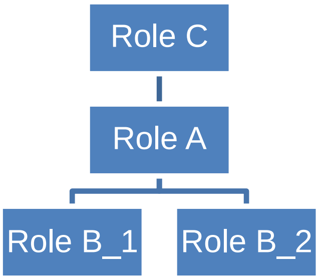
The RUCD permissions are organized in a hierarchical way. This means that it is not possible to give Update permission without having Read permission. The diagram to the right shows the hierarchy of access levels.

The "User Management" and "Role Management" function blocks are used to give users the possibility to manage users and roles.



In addition to RUCD and Execute permissions, Grant (G) permission can also be assigned. Grant permission allows the user to assign their permission for a certain function block to another user. To achieve this, the user must have Grant permission for this function block. Any future users who are assigned function block permission from another user become a child role of the user granting permission.

The diagram to the right represents a permission hierarchy. The user in Role A has Grant permission for a certain function block and is allowed to assign this permission on to Roles B_1 and B_2. The maximum permissions that can be passed on are the permissions currently assigned to Role A. For example, RUCD permissions cannot be assigned if Role A only has RU permissions.



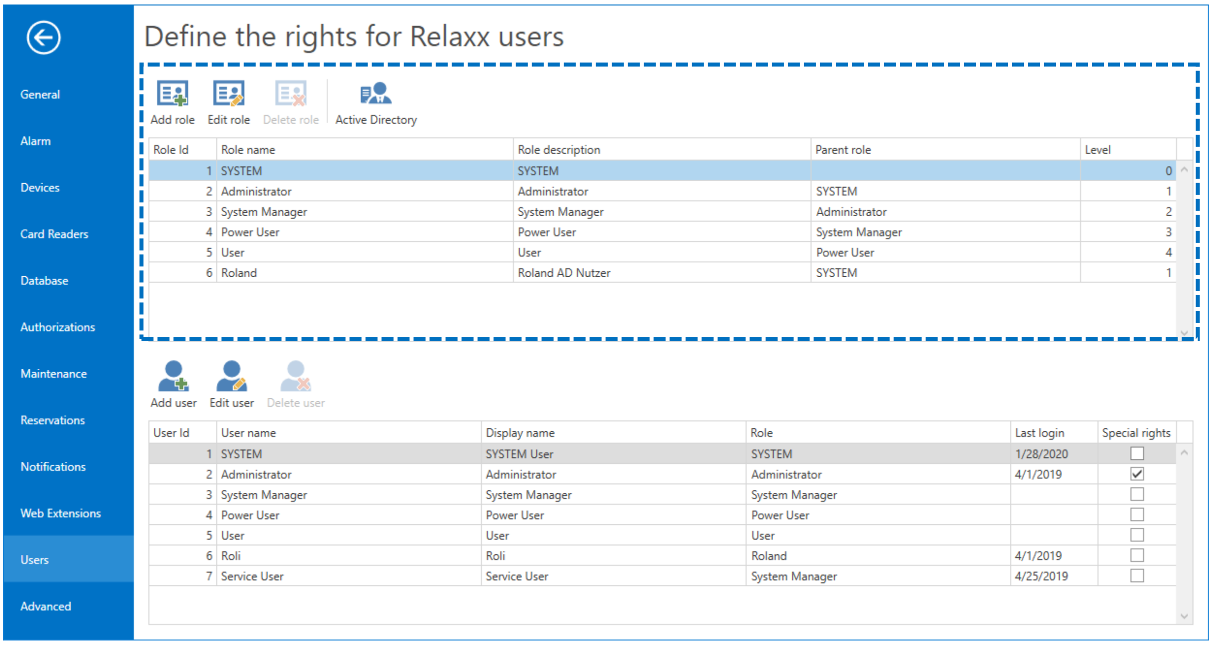
4.2 Role Management

A role represents a collection of permissions for the function blocks defined in the software. Roles are organized in a hierarchical way. Every role is assigned to exactly one parent role and has multiple child roles. The hierarchical structure defines who is allowed to manage which roles and therefore which users. Users of a role can only manage descendant roles and the users of these roles (provided the user has been assigned "User Management" and "Role Management" permission).

Relaxx starts with one superior role called the SYSTEM role. The SYSTEM role contains exactly one user, the SYSTEM user who is allowed to do anything within the application. Every following role is therefore a descendant of the SYSTEM role.

The maximum rights a role can have are the rights of its parent role. Removing a right from a parent role will also delete the right from any descendant.

► To define a new role, open the "Users" page in the system settings menu.
  - The user management page opens.



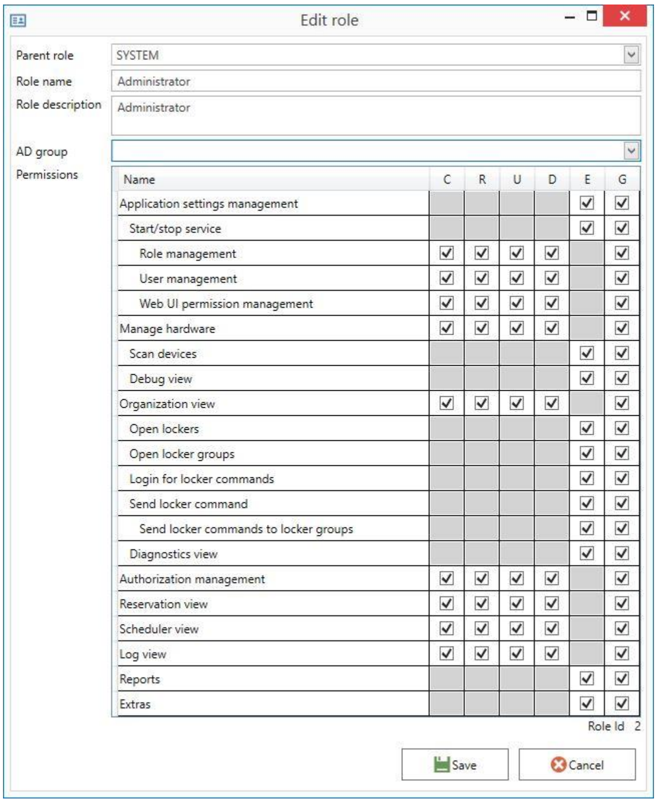
Define the rights for Relaxx users

Role Id	Role name	Role description	Parent role	Level
1	SYSTEM	SYSTEM		0
2	Administrator	Administrator	SYSTEM	1
3	System Manager	System Manager	Administrator	2
4	Power User	Power User	System Manager	3
5	User	User	Power User	4
6	Roland	Roland AD Nutzer	SYSTEM	1

User Id	User name	Display name	Role	Last login	Special rights
1	SYSTEM	SYSTEM User	SYSTEM	1/28/2020	☐
2	Administrator	Administrator	Administrator	4/1/2019	☑
3	System Manager	System Manager	System Manager		☐
4	Power User	Power User	Power User		☐
5	User	User	User		☐
6	Roli	Roli	Roland	4/1/2019	☐
7	Service User	Service User	System Manager	4/25/2019	☐

***Figure 4.1** – Role overview*

► Click on "Add role" to define the new role.
  - The “Edit role” window opens in which the role settings are defined.



Edit role

Parent role	SYSTEM
Role name	Administrator
Role description	Administrator
AD group	
Permissions	

Name	C	R	U	D	E	G
Application settings management					☑	☑
Start/stop service					☑	☑
Role management	☑	☑	☑	☑		☑
User management	☑	☑	☑	☑		☑
Web UI permission management	☑	☑	☑	☑		☑
Manage hardware	☑	☑	☑	☑		☑
Scan devices					☑	☑
Debug view					☑	☑
Organization view	☑	☑	☑	☑		☑
Open lockers					☑	☑
Open locker groups					☑	☑
Login for locker commands					☑	☑
Send locker command					☑	☑
Send locker commands to locker groups					☑	☑
Diagnostics view					☑	☑
Authorization management	☑	☑	☑	☑		☑
Reservation view	☑	☑	☑	☑		☑
Scheduler view	☑	☑	☑	☑		☑
Log view	☑	☑	☑	☑		☑
Reports					☑	☑
Extras					☑	☑

Role Id 2

Figure 4.2 *– Role settings (for “Administrator” user)*

- ► In the "Parent role" field, enter a parent role from which the new role inherits.

  NOTE! New roles must not use the “SYSTEM” role for the parent role. Any other role may be selected from the menu for the parent role.
- ► Enter the name of the role in the "Role name" field. Each role must have a unique name.
- ► In the "Role Description" field, you can enter a more detailed description for the role.
- ► The "AD group" field is only displayed when an Active Directory is used for user authorization (see "4.3.1 Active Directory”). In this case, select the applicable Active Directory group for the user.

Depending on the selected parent role, different permissions are available to assign to the selected role. In the figure above, it is possible to set permissions for every function available in Relaxx. This is because the logged-in user is the SYSTEM user who has grant permission for every function block. Clicking on the option boxes next to the functions define which permissions are valid for each function. The definition for each abbreviation is as follows:

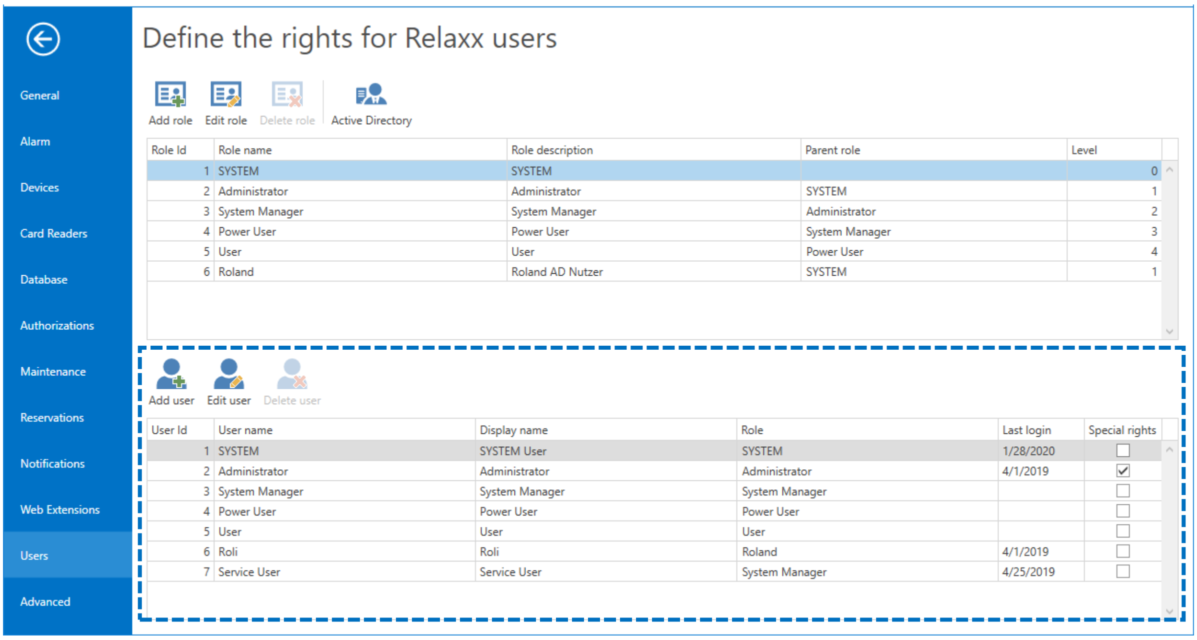
- C: "Create" permission - Generate new data records for the function
- R: "Read" permission - Display data records for the function
- U: "Update" permission - Changing existing data records for the function
- D: "Delete" permission - Deleting data records for the function
- E: "Executing" permission - Execute actions concerning the function
- G: "Grant" permission - Passing on the permissions of this function to other users

4.3 User Management

Each user has their own user account. With this account a user is identified by a unique username and password which is used to prevent other people from logging in under this user account. Every user in Relaxx must be assigned to exactly one role (see “4.2. Role Management”). It is impossible to have users that are not assigned to a role. The user will inherit their system permissions from that role.

There is also the possibility to override permissions inherited from a role by explicitly configuring permissions for a certain function block for the user. These user permissions will also exist, if the permissions for the function block are changed at role level.

► To define a new user account, open the "Users" page in the system settings menu.
    ○ The user management page opens.



Define the rights for Relaxx users

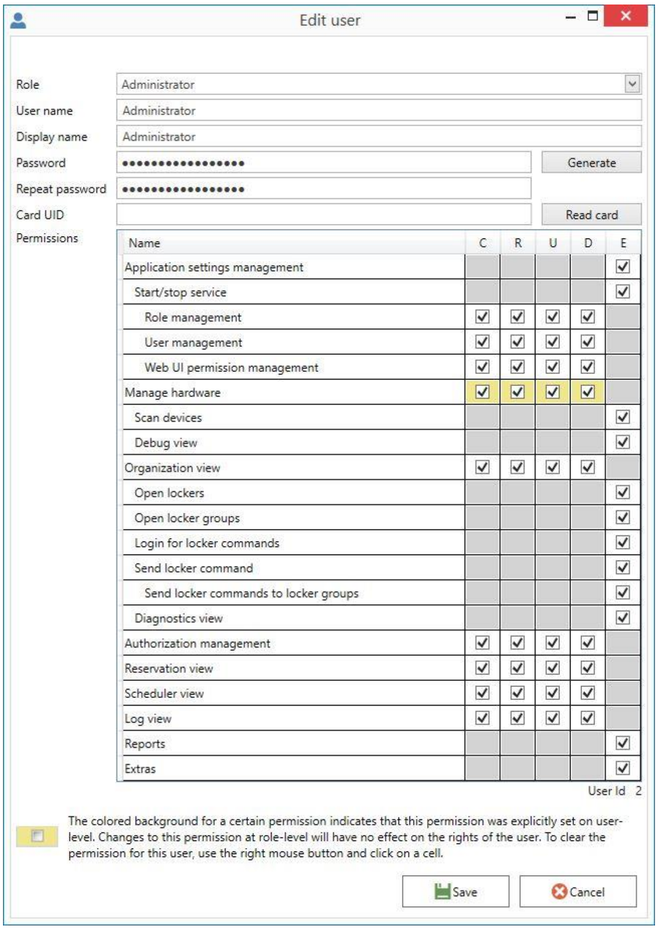
Role Id	Role name	Role description	Parent role	Level
1	SYSTEM	SYSTEM		0
2	Administrator	Administrator	SYSTEM	1
3	System Manager	System Manager	Administrator	2
4	Power User	Power User	System Manager	3
5	User	User	Power User	4
6	Roland	Roland AD Nutzer	SYSTEM	1

User Id	User name	Display name	Role	Last login	Special rights
1	SYSTEM	SYSTEM User	SYSTEM	1/28/2020	☐
2	Administrator	Administrator	Administrator	4/1/2019	☑
3	System Manager	System Manager	System Manager		☐
4	Power User	Power User	Power User		☐
5	User	User	User		☐
6	Roli	Roli	Roland	4/1/2019	☐
7	Service User	Service User	System Manager	4/25/2019	☐

***Figure 4.3** – User overview*

Listed at the bottom of the page are all current user accounts. The figure above shows the default users, which are included with Relaxx, as described in section "4.3.2. Default ". To edit a user account, select the user from the list and click on the "Edit user" icon.

► To create a new user, click on "Add user".
    ○ The "Edit user" window opens.



Role: Administrator
User name: Administrator
Display name: Administrator
Password: •••••••••••••••••
Repeat password: •••••••••••••••••
Card UID:
Permissions

Name	C	R	U	D	E
Application settings management					☑
Start/stop service					☑
Role management	☑	☑	☑	☑	
User management	☑	☑	☑	☑	
Web UI permission management	☑	☑	☑	☑	
Manage hardware	☑	☑	☑	☑	
Scan devices					☑
Debug view					☑
Organization view	☑	☑	☑	☑	
Open lockers					☑
Open locker groups					☑
Login for locker commands					☑
Send locker command					☑
Send locker commands to locker groups					☑
Diagnostics view					☑
Authorization management	☑	☑	☑	☑	
Reservation view	☑	☑	☑	☑	
Scheduler view	☑	☑	☑	☑	
Log view	☑	☑	☑	☑	
Reports					☑
Extras					☑

User Id 2

☐ The colored background for a certain permission indicates that this permission was explicitly set on user-level. Changes to this permission at role-level will have no effect on the rights of the user. To clear the permission for this user, use the right mouse button and click on a cell.

***Figure 4.4** – User settings*

- ► Enter a unique name for the user in the "Username" field. The user will use this name to log in.
- ► In the "Display name" field, enter a display name for the user. Relaxx uses this name to represent the user in the application, e.g., in the log files.
- ► Enter a password for the user. This must be entered twice for verification.
- ► The "Read card" button allows you to save the UID of data carrier that is read by a connected read/write station. The user can log into Relaxx using this data carrier.

NOTE! Use a strong password. The password must be at least 7 characters long and contain at least one uppercase letter, one lower case letter and one number. Click on "Generate" to automatically generate a strong password.

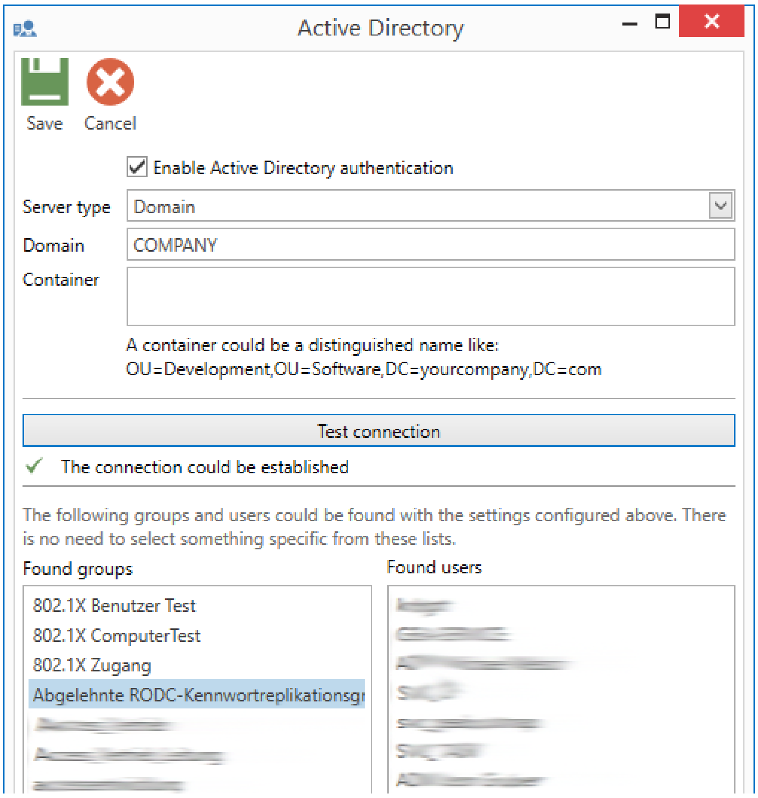
- ► In the “Role” field, assign a role to the user from the drop-down menu.
  - o The authorization of the user to use specific Relaxx functions is directly linked to the selected role.
- ► If desired, role permissions can be overridden by explicitly setting user permissions in the table.
  - o Permissions that are set explicitly on user level are marked with an ochre background. In Figure 4.4 for example, all available permissions for the “Manage hardware” function have been set explicitly for the user and will override the inherited settings.
- ► To revoke a set permission, left click onto the appropriate field.

4.3.1 Active Directory

An Active Directory (AD) domain controller authenticates and authorizes all users and computers in a Windows domain type network. When a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted login details to confirm the validity. The Active Directory group is assigned to a user in the settings window when assigning a role to the user (see "4.2 Role Management").
Relaxx offers the possibility for users to log in to Relaxx by using their Windows account information (user name and password).

When GAT Active Directory is enabled, users can log into the Relaxx WEB User Interface using their Windows login data.

On the “Users” software settings page, click on the Active Directory icon. The following window opens after clicking on the icon.



☑ Enable Active Directory authentication

Server type: Domain

Domain: COMPANY

Container:

A container could be a distinguished name like:
OU=Development,OU=Software,DC=yourcompany,DC=com

✓ The connection could be established

The following groups and users could be found with the settings configured above. There is no need to select something specific from these lists.

Found groups:
802.1X Benutzer Test
802.1X ComputerTest
802.1X Zugang
Abgelehnte RODC-Kennwortreplikationsgr

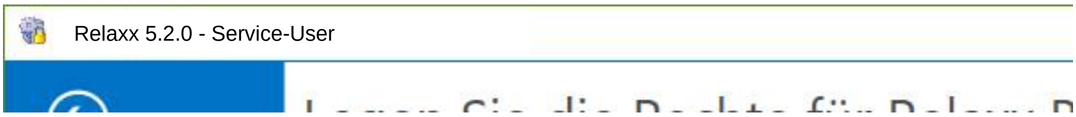
Found users

__Figure 4.5__ – Settings window for authentication via Active Directory

- Enable Active Directory authentication:
  If this option is selected, the users must use their Windows login details for authentication in Relaxx (for Single Sign On see “2.1 Login”).
- Server type: Select the location of the Active Directory to be used.
  - Machine: Select this option to use the authentication system of the local Windows installation. The “Test connection” button searches the computer and lists groups and users that can be used for authorization. There is no need to select a specific group or user from the list.

- Domain: Select this option to use an Active Directory located on a server. Enter the "Domain" and "Container" details (see Figure 4.5) then press "Test connection" to display a list of groups and users that can be used for authorization.

If a user has logged in using Active Directory, the role of the user is displayed in the header of Relaxx ("Service-User" in the example). If an AD group is assigned to several roles in Relaxx, the role with the highest rights is used and displayed.



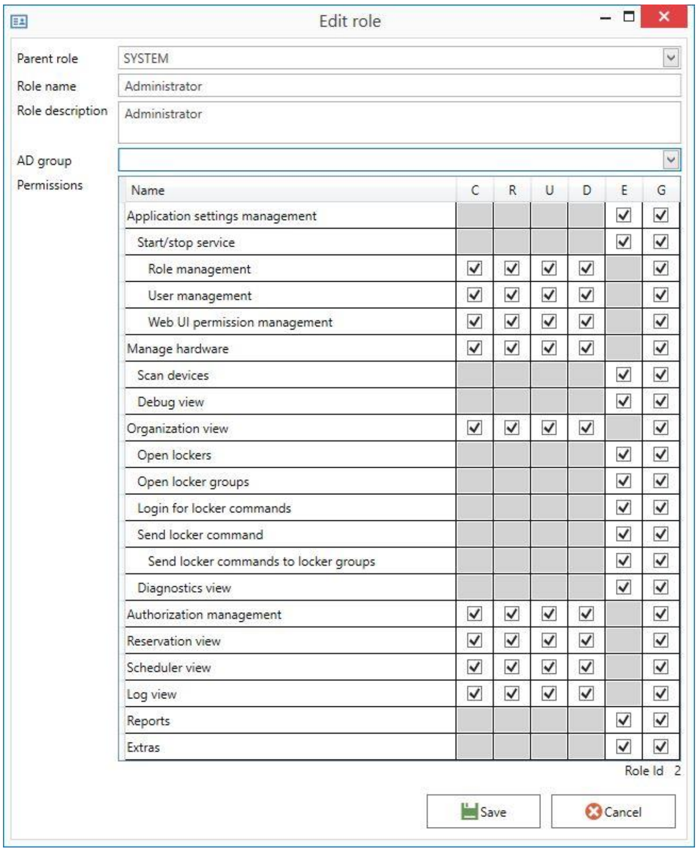
Relaxx 5.2.0 - Service-User

Legen Sie die Rechte für Relaxx R

4.3.2 Default Users

After the installation of Relaxx, the following default users and their login passwords are available. The permissions set by default in Relaxx for each user (inherited from their role) are shown. The permissions that can be selected or deselected for each user are shown in the edit window with a selection box. The permissions where a selection box is not shown are not available for the user.

User:	**Administrator**
Role:	Administrator
Password:	Mirone59



Edit role

Parent role: SYSTEM

Role name: Administrator

Role description: Administrator

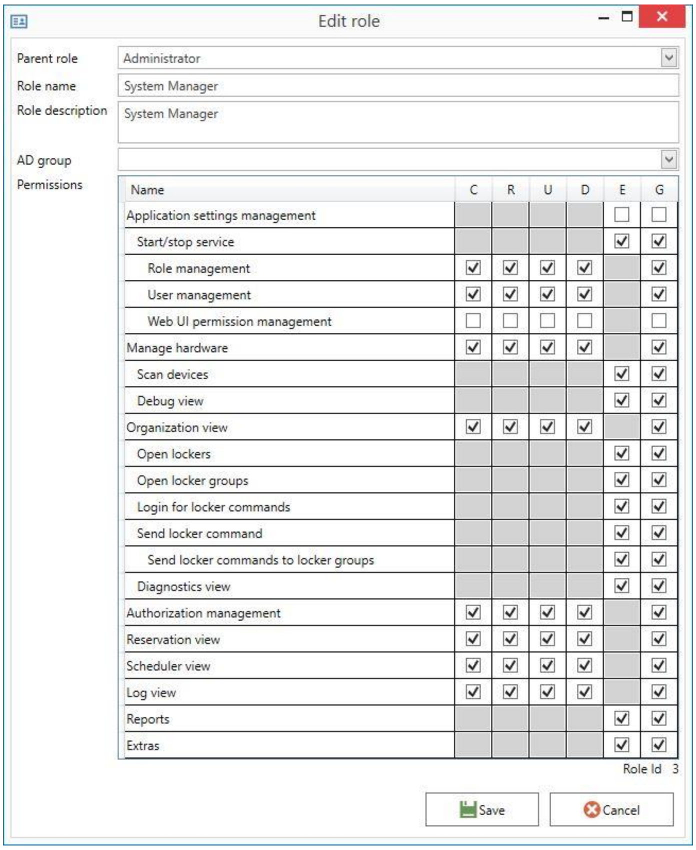
AD group:

Permissions

Name	C	R	U	D	E	G
Application settings management					☑	☑
Start/stop service					☑	☑
Role management	☑	☑	☑	☑		☑
User management	☑	☑	☑	☑		☑
Web UI permission management	☑	☑	☑	☑		☑
Manage hardware	☑	☑	☑	☑		☑
Scan devices					☑	☑
Debug view					☑	☑
Organization view	☑	☑	☑	☑		☑
Open lockers					☑	☑
Open locker groups					☑	☑
Login for locker commands					☑	☑
Send locker command					☑	☑
Send locker commands to locker groups					☑	☑
Diagnostics view					☑	☑
Authorization management	☑	☑	☑	☑		☑
Reservation view	☑	☑	☑	☑		☑
Scheduler view	☑	☑	☑	☑		☑
Log view	☑	☑	☑	☑		☑
Reports					☑	☑
Extras					☑	☑

Role Id 2

User:	**System Manager**
Role:	System Manager
Password:	Nekiwi70

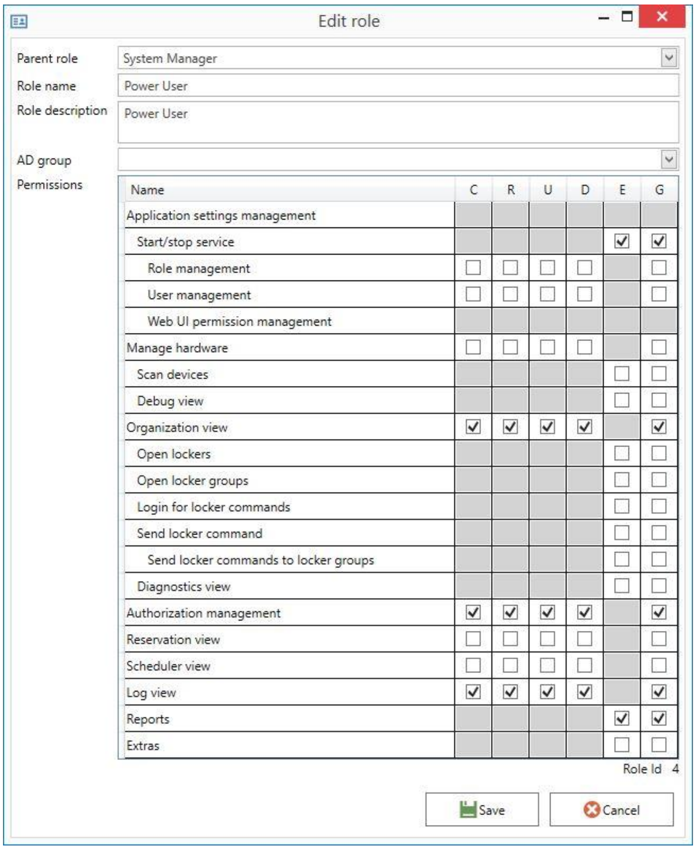


Parent role: Administrator
Role name: System Manager
Role description: System Manager
AD group:
Permissions

Name	C	R	U	D	E	G
Application settings management					□	□
Start/stop service					☑	☑
Role management	☑	☑	☑	☑		☑
User management	☑	☑	☑	☑		☑
Web UI permission management	□	□	□	□		□
Manage hardware	☑	☑	☑	☑		☑
Scan devices					☑	☑
Debug view					☑	☑
Organization view	☑	☑	☑	☑		☑
Open lockers					☑	☑
Open locker groups					☑	☑
Login for locker commands					☑	☑
Send locker command					☑	☑
Send locker commands to locker groups					☑	☑
Diagnostics view					☑	☑
Authorization management	☑	☑	☑	☑		☑
Reservation view	☑	☑	☑	☑		☑
Scheduler view	☑	☑	☑	☑		☑
Log view	☑	☑	☑	☑		☑
Reports					☑	☑
Extras					☑	☑

Role Id 3

User:	**Power User**
Role:	Power User
Password:	Roliba59

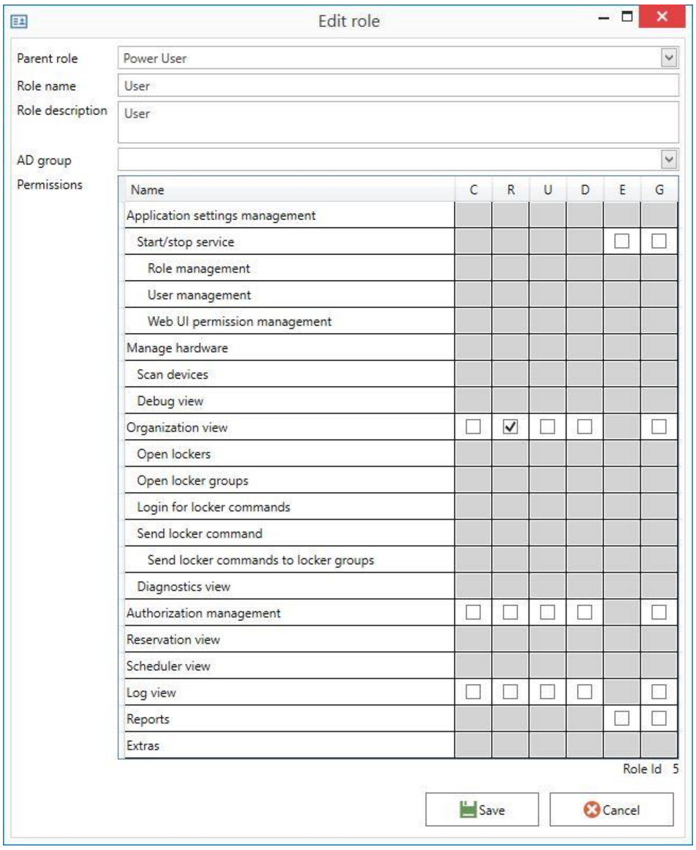


Parent role: System Manager
Role name: Power User
Role description: Power User
AD group:
Permissions

Name	C	R	U	D	E	G
Application settings management						
Start/stop service					☑	☑
Role management	□	□	□	□		□
User management	□	□	□	□		□
Web UI permission management						
Manage hardware	□	□	□	□		□
Scan devices					□	□
Debug view					□	□
Organization view	☑	☑	☑	☑		☑
Open lockers					□	□
Open locker groups					□	□
Login for locker commands					□	□
Send locker command					□	□
Send locker commands to locker groups					□	□
Diagnostics view					□	□
Authorization management	☑	☑	☑	☑		☑
Reservation view	□	□	□	□		□
Scheduler view	□	□	□	□		□
Log view	☑	☑	☑	☑		☑
Reports					☑	☑
Extras					□	□

Role Id 4

User:	**User**
Role:	User
Password:	Bubaka49



Edit role

Parent role: Power User

Role name: User

Role description: User

AD group:

Permissions

Name	C	R	U	D	E	G
Application settings management						
Start/stop service					□	□
Role management						
User management						
Web UI permission management						
Manage hardware						
Scan devices						
Debug view						
Organization view	□	☑	□	□		□
Open lockers						
Open locker groups						
Login for locker commands						
Send locker command						
Send locker commands to locker groups						
Diagnostics view						
Authorization management	□	□	□	□		□
Reservation view						
Scheduler view						
Log view	□	□	□	□		□
Reports					□	□
Extras						

Role Id 5

5 LICENSE MANAGEMENT

The functions available for use within Relaxx are differentiated through the two types of base licenses available – Professional and Enterprise. The functions available with each license are defined as follows:

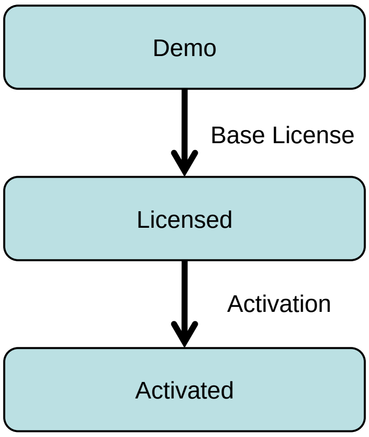
Function	Professional	Enterprise
Advanced card reader features can be used	No	Yes
Relaxx WEB Info Screen	No	Yes
Relaxx WEB Locker Usage Screen	No	Yes
Relaxx WEB Floorplan	No	Yes
Relaxx REST API	No	Yes
Online JSON Clients	No	Yes

Maximum number of licensed locks

The maximum number of locks that can be used in your system is defined when purchasing the Relaxx “Managed Locks” license. Such a license must be purchased together with a basic license. When ordering the Managed Locks license, the desired maximum number of locks can be specified. If you add more than the maximum number of licensed locks in the system, a warning is displayed in the locker overview (see "3.2.6. Setting up the Organization System") and all lockers are set to emergency mode, i.e., they continue to function autonomously according to the configuration. The following restrictions also apply in this case:

- Inquiries from GAT SMART.LockAxx 6xxx devices are generally rejected.
- The "transparent" mode, in which locker inquiries are answered by third-party software, is deactivated.
- No personal lockers are loaded into the controller.
- Lock requests via the LockPal app are always allowed. Therefore, any number of locks can be locked.

Licensing process



After installing Relaxx, the software is set to run in demo mode. Only certain functions can be used in this mode. The default settings of the functions that are included in the license will apply. A valid license for Relaxx must be activated within 14 days of demo mode use. If not activated, Relaxx will not function after this time.

Licensing the software is achieved by purchasing a Professional or Enterprise license from GANTNER Electronic GmbH or your reseller. After licensing the software with the Professional or Enterprise license, the final step is to activate Relaxx via an activation code within 14 days. To activate, contact your sales partner, who will provide you with an activation code for your installation, or carry out the activation yourself online via the Internet. The activation code is linked to the Hardware ID, which allows the unique identification of a Relaxx installation.

NOTE! The Hardware ID does not contain any data about the configuration of your computer.

Besides the Professional and Enterprise Relaxx licenses, GANTNER offers the following support and upgrade licenses:

- Relaxx Upgrade 1 + 1 (Part No.: 1103702) Mandatory for new installations. Eligible for updates to the latest major version. Valid for 2 years (including free start year). The annual fee is 12% of the list price of the basic license + Relaxx Managed Locks at the time of billing. The contract is automatically renewed annually (termination possible). Software updates within a major version (e.g. V5.1 to B 5.2) are free of charge.
- Relaxx Support Contract (Part No.: 1103703): Remote support available Mo. to Fr., 9 am to 5 pm (CET / CEST).

5.1 License Overview

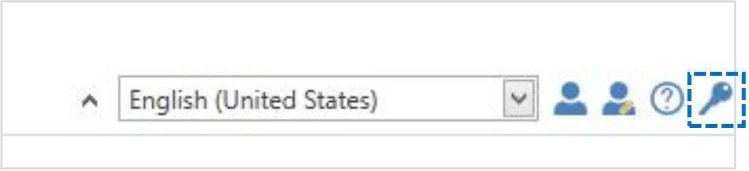
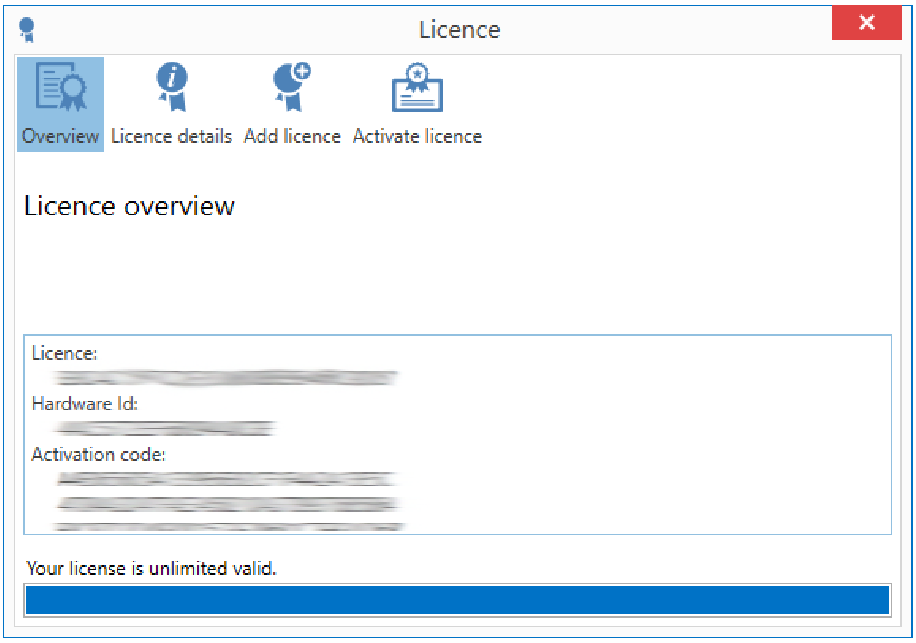


Figure 5.1 *- Icon to open the license overview*

To display the license window, click on the key symbol in the top right of the program window. The window as shown in Figure 5.2 opens. The window shows the base license, the hardware ID of your computer and the activation code. Displayed at the bottom of the window is the time remaining until licensing / activation of Relaxx is required.



Licence overview

Licence:
[redacted]

Hardware Id:
[redacted]

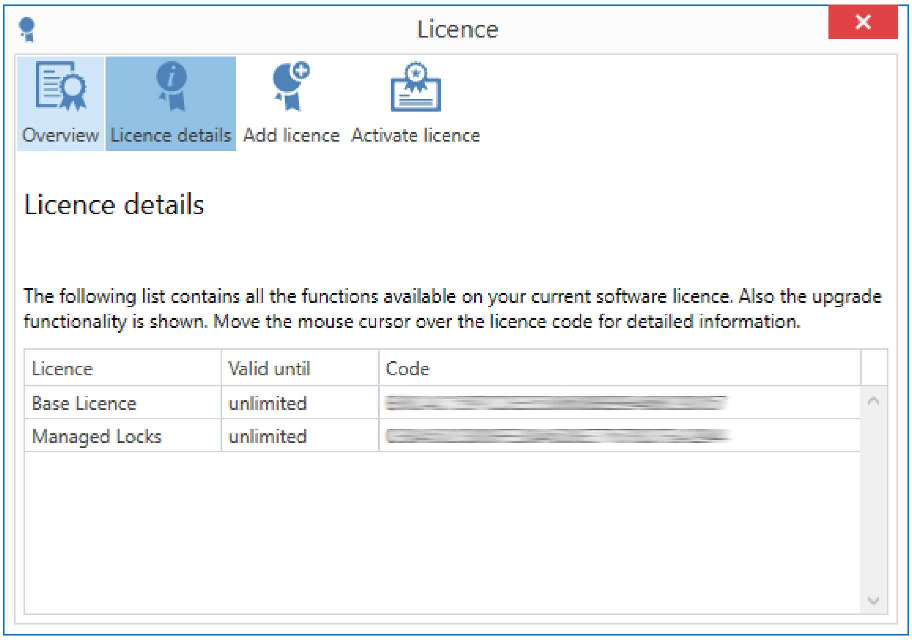
Activation code:
[redacted]

Your license is unlimited valid.

Figure 5.2 *- License overview*

5.2 License Details

Choosing "License details" from the toolbar will display the following window where each acquired license is shown.



Licence details

The following list contains all the functions available on your current software licence. Also the upgrade functionality is shown. Move the mouse cursor over the licence code for detailed information.

Licence	Valid until	Code
Base Licence	unlimited	[redacted]
Managed Locks	unlimited	[redacted]

Figure 5.3 *- License details*

For every function that can be licensed, the corresponding license code and validity date are shown on a single line in the table. The column named "Functionality" stands for a collection of simple functions that can be licensed by a single license code.

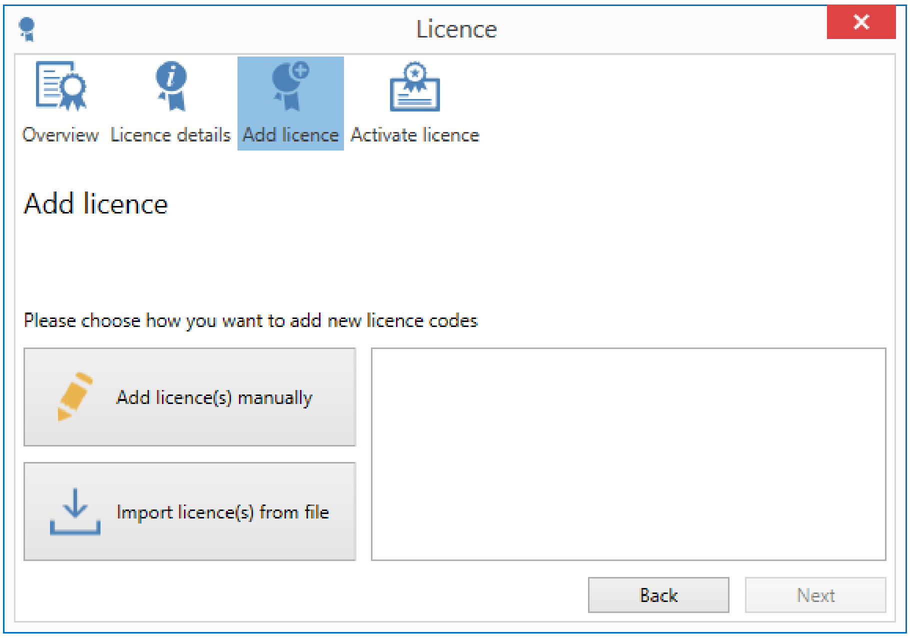
When you keep the mouse over a license code, the individual functions, e.g., Professional or Enterprise license, number of controllers, certificate check, etc., activated with this license are displayed.

In the last two columns the license code and the validity date are shown. If a license for a specific function has not been acquired yet, these fields are marked with a "-" to represent this.

See the following page for instructions on adding a new license.

5.3 Adding Licenses

The "Add license" button is used to add new license codes for Relaxx.



Please choose how you want to add new licence codes

Figure 5.4 *- Adding a license*

There are two ways to add a license:

- ► Add a license code manually by clicking on "Add license(s) manually" and entering the code in the textbox to the right.
- ► Using a license file. In this case, click on "Import license(s) from file" and select the license file received from your reseller.

To work with Relaxx, a base license (Professional or Enterprise) as a minimum is required. For this license, please contact GANTNER or your local sales partner. The following information is needed to generate a base license:

- Number of locks: Each license is issued for a specific max. number of locks (see also "3.2.6. Setting up the Organization System"). If the max. number of locks is increased later, e.g., when the system is expanded with new locks, a new base license with the new max. number of locks must be ordered. Reactivation of the base license is not necessary in this case.
- Version of Relaxx: Professional or Enterprise (see "5. LICENSE MANAGEMENT" for included functions).
- Certificate check: Information whether the certificate check on GAT NET.Controller 70xx should be activated or deactivated. For Relaxx version 1.2.0 and later.

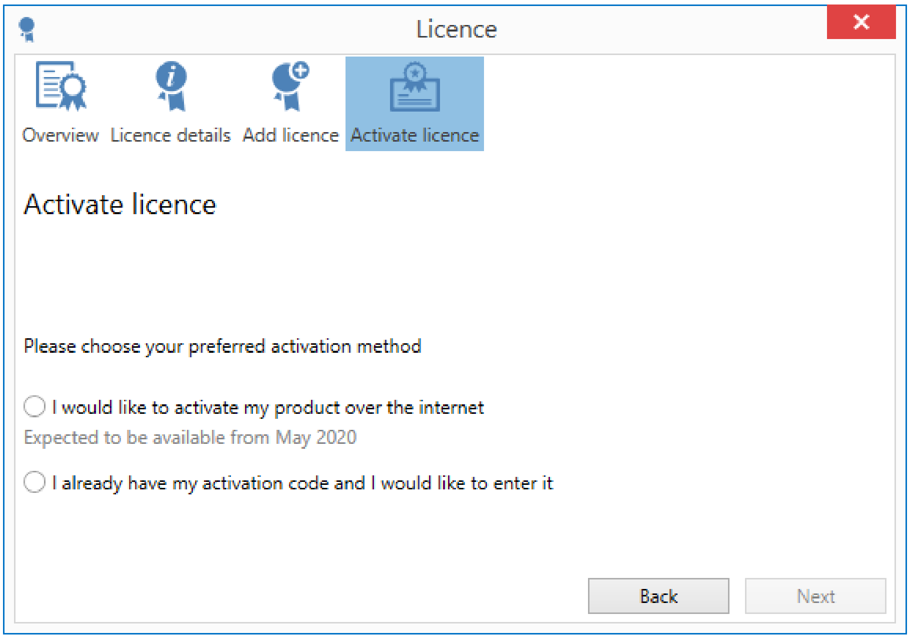
For some expansion licenses, it is possible that the license is only valid for a certain period (e.g., until the end of 2022). This information is shown in the license overview window (see Figure 5.3).

5.4 Product Activation

The "Activation" button is used to activate Relaxx.

NOTE! It is no longer possible to work with Relaxx if it is not activated within 14 days. When Relaxx is not activated, a corresponding message is displayed each time you start Relaxx.

To activate Relaxx, you can either contact GANTNER or your sales partner to receive an activation code for the activation or to carry out the activation autonomously via the Internet.



Activate licence

Please choose your preferred activation method

○ I would like to activate my product over the internet
Expected to be available from May 2020

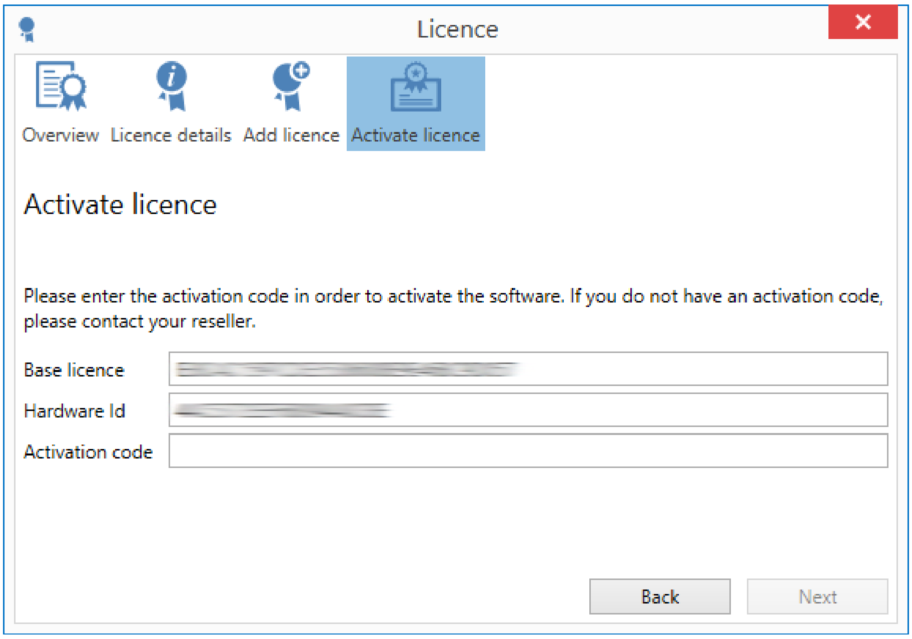
○ I already have my activation code and I would like to enter it

***Figure 5.5** – Select the type of software activation*

- ► Select the first option if you want to complete the activation autonomously via the Internet.
- ► Click on "Next".
  - o See chapter "5.4.2. Autonomous activation via the Internet" for instructions.
- ► Select the second option if you already have an activation code or would like to request this from your sales partner via telephone.
- ► Click on "Next".
  - o See chapter "5.4.1. Request activation key, manual entry" for instructions.

5.4.1 Request Activation Code, Manual Entry

You can use this type of software activation if you already have the activation code or want to inquire directly with your sales partner or GANTNER to receive it.



Activate licence

Please enter the activation code in order to activate the software. If you do not have an activation code, please contact your reseller.

Base licence
Hardware Id
Activation code

Figure 5.6 *- Software activation using activation code*

The "Base licence" and the "Hardware ID" are displayed in the first two fields of this window.

► To receive an activation code, please send the base license and the hardware ID (first two fields) to your sales partner or GANTNER Electronic GmbH.
  - Currently, the activation codes can only be transmitted by phone.

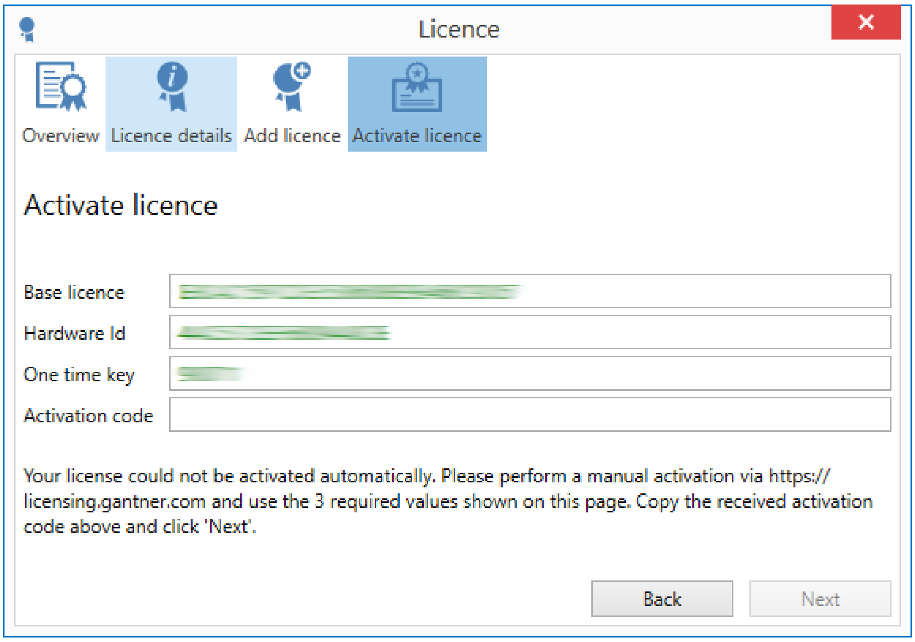
► After receiving the activation code, enter it into the third "Activation code" field and click "Next".

► If the code has been entered correctly, Relaxx is activated.

5.4.2 Autonomous Activation via the Internet

With this type of activation, you can create an activation key yourself. You only need internet access.

- ► If you have Internet access from your Relaxx computer, select the "I would like to activate my product over the internet" option. After clicking on "Next", the activation is carried out automatically.
- ► If there is no Internet connection, the following window is displayed.



Activate licence

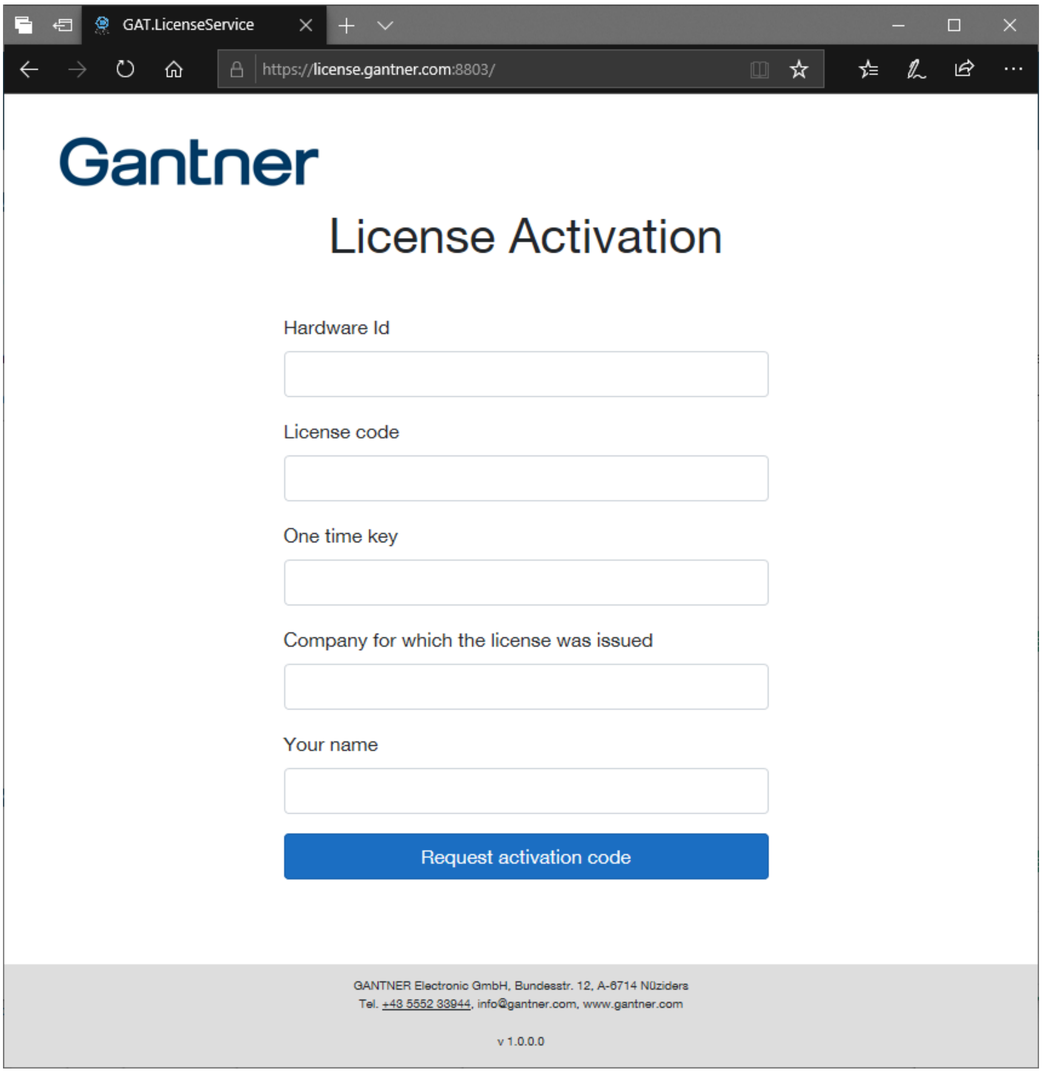
Base licence [redacted]
Hardware Id [redacted]
One time key [redacted]
Activation code

Your license could not be activated automatically. Please perform a manual activation via https://licensing.gantner.com and use the 3 required values shown on this page. Copy the received activation code above and click 'Next'.

Figure 5.7 *- Software activation over the Internet*

The "Base licence" and the "Hardware ID" are displayed in the first two fields in this window. Use these codes together with the "One time key" to get an activation key as follows.

- ► Enter the website address https://license.gantner.com:8803 into a web browser on a computer or mobile phone with an Internet connection.
  - ○ The following page is displayed.



Gantner

License Activation

Hardware Id

License code

One time key

Company for which the license was issued

Your name

GANTNER Electronic GmbH, Bundesstr. 12, A-6714 Nüziders
Tel. +43 5552 33944, info@gantner.com, www.gantner.com

v 1.0.0.0

Figure 5.8 *- Website for software activation*

- Enter the “Hardware ID”, “License code”, and “One time key” from the Relaxx window.
- Next, enter your company name ("Company for which the license was issued") and your name ("Your name"). You had to provide this information when creating the license.
- Click on "Request activation code".
  - When all the information has been entered correctly, the activation code is generated and displayed on the screen.
- In Relaxx, enter the activation code into the "Activation code" field and click on "Next".
  - When the code has been entered correctly, Relaxx is activated.

6 APPENDIX: LOG ENTRIES

The following entries are possible in the Relaxx event log (see "3.7 Log Entries").

No.	Name	Source	Event Category	Event Severity	Description	Example
0	-	-	A	C		
1	Locker State Closed	Device	O	I	The device reports that the lock is closed.	
2	Locker State Opened	Device	O	I	The device reports that the lock is open. Notes for GAT Lock Controller 5010: If a data carrier that currently has the locker in use wants to open it again, the GAT Lock Controller 5010 no longer asks Relaxx and opens it autonomously. The UID data carrier in the event log is empty for this event. Additionally in this case, you will not get the events “11 Open With Card” and “13 Opening Allow”. If the GAT Lock Controller 5010 is connected to a GAT NET.Controller M 7000, you will get the event again (but with the data carrier UID) and with the reference to "booking entry" in the optional data due to the autonomous opening.	GAT Lock Controller 5010 and NET.Controller M 7000:
3	Locker State Closed With Master Card		O	W		
4	Locker State Opened With Master Card		O	W		
5	Locker State General Alarm	Device	O	C		
6	Locker State Disabled	Device	O	W		
7	Locker State Blocked	Device	A	W	The controller reports that the lock is blocked. The status is open, but the bolt is still pressed. Usually a mechanical problem, the bolt does not drive properly into the lock, the door does not fit exactly, check door.	
8	Locker State Not Found	Relaxx	A	W	The lock assigned and stored in Relaxx is not found on the device.	
10	Close With Card	Device	O	I	The device requests from Relaxx whether a user may close this locker with the given data carrier. Typically, this is done by holding a data carrier to the reader of the lock.	
11	Open With Card	Device	O	I	The device requests from Relaxx whether a user may open this locker with the given data carrier. Typically, this is done by holding a data carrier to the reader of the lock.	
12	Closing Allowed	Relaxx	O	I	Relaxx reports back to the device that closing is permitted.	

13	Opening Allow	Relaxx	O	I	Relaxx reports back to the device that opening is permitted. Remarks for GAT Lock Controller 5010: Will never be triggered, because a valid opening will be performed by the controller autonomously, without asking Relaxx.	
14	Closing With Master Allow		O	W		
15	Opening With Master Allow		O	W		
16	Closing Not Allowed	Relaxx	O	W		
17	Opening Not Allowed	Relaxx	O	W		
18	Closed With Card Failed	Device	A	W	Trigger: A user tried to close the locker but the controller reports that locking of the lock was not successful. Remarks: No alarm is raised. Caused either by operating error (door was not closed properly) or there is a mechanical problem --> check the lock. This event for GAT NET.Lock 7000 is available in Relaxx 2.9.0 or higher. Notes for GAT Lock 5020 (GAT Lock Controller 5010): Locker State Opened is the next expected action. Please note, that if connected to a GAT NET.Controller M 7000, this event is not triggered.	
19	Open With Card Failed	Device	A	W		
20	Master Card Deleted		A	I		
21	Master Card Not Deleted		A	E		
22	Master Card Loaded		A	I		
23	Master Card Not Loaded		A	E		
24	User Action Requested	Relaxx	A	I	A Relaxx operator has requested an action via a Relaxx client, e.g., open a locker or set it to maintenance mode.	
25	User Action Executed		A	I		
26	User Action Not Executed		A	E		
27	Locker Maintenance Set		O	W		
28	Locker Maintenance Reverted		O	W		
31	Card Identification Received	Device	O	I		
32	Card Identification Rejected	Relaxx	O	W		

33	Card Identification Granted	Relaxx	O	I		
34	Scheduler Action Executing	Relaxx	A	I		
35	Scheduler Action Executed	Relaxx	A	I		
36	NET Lock70xx Start Emergency Mode	Device	A	I		
37	NET Lock70xx End Emergency Mode	Device	A	I		
38	Firmware Update	Device	A	I		
39	Authentication Rejected Not Ready Hardware	Relaxx	A	E	Trigger: GAT NET.Controller M 7000 is not licensed GAT NET.Controller M 7000 channel is currently being started by Relaxx Relaxx has to refresh locker states of a specific sub controller. In all cases, opening and closing requests are processed by the controller (like in emergency mode) and not by the Relaxx.	
40	Connection Lost	Relaxx	A	E	Connection to the device has been lost.	
41	Connection Recovered	Relaxx	A	I	Connection to the device has been recovered.	
42	Permission Loaded		A	I		
43	Permission Not Loaded		A	E		
44	Permission Deleted		A	I		
45	Permissions Not Deleted		A	E		
46	Start Service	Relaxx	A	I	The Relaxx Windows service has been started.	
47	Stop Service	Relaxx	A	W	The Relaxx Windows service has been stopped.	
48	Task Action	Relaxx	A	I	An event from a Relaxx Task has been triggered (see Extras / Tasks).	

49	Replace Card In use		A	I	Configuration: Locker Mode: Free Locker / Authorization List enabled Trigger: A user has closed the locker and you change the data carrier UID of the related authorization. Remarks: Event is not triggered in Personal- , Dynamic or Reservable Locker mode as the locker authorization itself is updated. Event is not triggered when related controller was not started by the time performing the action. When controller was not reachable by the time sending the command, there is no mechanism that will resolve the resulting inconsistency automatically.	Optional Data: Card UID 3897729132 replaced by 2337370869 in locker 1 Office NorthA b3c84b3e-e95d-4e75-a462-776d50280f47
50	Mail Sent	Relaxx	A	I	An email notification has been sent by Relaxx. This can be configured in the application settings.	
51	Manipulation detected	Device	A	W		
52	Locker State Inconsistent	Relaxx	A	W	Trigger: The controller sends an unexpected request, which is usually an indicator that the locker states of Relaxx and controller are out of sync: the locker has the status "closed" in Relaxx, but the controller is requesting "10 Close With Card" the locker has the status "open" in Relaxx, but the controller is requesting "11 Open With Card" Remarks: available in Relaxx 2.7.0 or higher You can use "Synchronize Device" to force to update the current locker status. Relaxx answers with "?" to let the GAT NET.Controller M 7000 decide autonomously. (introduced in Relaxx 2.8.0) Example: {"TID":13581,"GRAuthRequestResult":{"State":"?"}}	Optional Data: Current locker state: Open / Controller requesting: Open locker Current locker state: Closed / Controller requesting: Close
53	Lock overcurrent detected	Device	A	C	Occurs if an overcurrent was detected (works for NET.Lock only)	
54	Disconnected Cabling Resolved	Device	A	E	Occurs if all cables are connected again (works for NET.Lock only)	
55	Disconnected Cabling Detected	Device	A	E	A manipulation event is fired, if - The Ethernet cable is disconnected - Any sub controller is disconnected - The power source of any sub controller is disconnected - Any locker is disconnected	
56	Activity	Relaxx	A	I	Records the most important changes to the configuration. This includes important application settings, security-related changes to authorizations and scheduled tasks.	
57	Opening With System/Maintenance Card Allowed	Relaxx	O	W		

58	Opening With System/Maintenance Card Not Allowed	Relaxx	O	W		
59	Closing With System/Maintenance Card Allowed	Relaxx	O	W		
60	Closing With System/Maintenance Card Not Allowed	Relaxx	O	W		
61	Locker State Opened With System/Maintenance Card	Device	O	W		
62	Locker State Closed With System/Maintenance Card	Device	O	W		
63	Login failed	Relaxx	A	W	When a user logs in with wrong credentials for his/her Relaxx authorization via - REST API - JSON Interface - Relaxx Configurator (Desktop) - Relaxx WEB Introduced in Relaxx 2019	
	Licensing (Not enough licensed locks)	Relaxx	A	C	This event is saved if there are not enough licenses for all locks managed in Relaxx. Introduced in Relaxx 2019 (4.0)	
1077	Access terminal door opened	Device	O	I		
1078	Access terminal door not opened	Device	O	W		

Event category:

- A	Administrative
- O	Operational

Event severity:

- I	Informational
- W	Warning
- E	Error
- C	Critical

***Table 6.1** - Overview of the possible log entries*

Note:
This manual is valid as of 5th August 2020. It is subject to change.
Amendments can be made without prior notice at any time.
Information in this manual is valid for version 5.2.0 of Relaxx.

Austria/Headquarters
Los Angeles/USA
Ahmedabad/India
Bochum/Germany
London/GB
Sydney/Australia
Ypern/Belgium
Würzburg/Germany
Houten/Netherlands
Dubai/U.A.E.

GANTNER operates in over 60 countries worldwide. **Please visit www.gantner.com**

Nüziders, Austria
info@gantner.com

Houten, the Netherlands
info@gantner.nl

Sydney, Australia
info-aus@gantner.com

London, United Kingdom
info-uk@gantner.com

Bochum, Germany
info-de@gantner.com

Los Angeles, USA
info-us@gantner.com

Ypern, Belgium
info@gantner.be

Dubai, UAE
info-me@gantner.com

Ahmedabad, India
info@gantnerticketing.com

Current contact information: www.gantner.com/locations