GANTNER Battery Locker Locks Function Manual

GAT ECO.Side Lock

GL7p

GAT ECO.Lock

Configuration, Operation
Document Version 1.3

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

Contact information for queries regarding this product or for general inquiries can be found on the last page of the manual, where the worldwide branches of GANTNER Electronic GmbH are listed.

Contact address of manufacturer
GANTNER Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria
www.gantner.com/locations

Important Information

Dear Customer,

Our aim is to ensure that 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.

- Pay attention to the safety messages in this manual. The messages are indicated by the signal words "DANGER", "WARNING", or "CAUTION", and inform you about hazardous situations and how to avoid them.
- Pay attention to messages indicated by the "NOTICE" signal word. These messages include important information for avoiding property damage.
- Pay attention to the symbols and safety messages on the product.
- Read all instructions in this manual carefully before installing or operating the product.
- Where not otherwise specifically documented, the appropriate installation, commissioning, operation, and maintenance of the product is the customer’s responsibility.
- Keep this manual in a safe place for quick reference.

Notation of Safety Information and Safety Symbols

This manual includes important safety messages and symbols intended to inform the user about potentially hazardous situations or important information for the safe and proper use of the described product(s). The safety messages also include directives on how to avoid hazardous situations. These safety messages and directives must be read and observed.

The structure of the safety messages and the meaning of the symbols used in this manual are described in this section.

1. Safety Messages for Personal Injury

Personal safety messages contain a signal word, describe the nature of the hazard, and indicate how to avoid the hazard.

⚠ The safety alert symbol used without a signal word always precedes important safety information that must be read carefully, and the instructions carefully observed. Not doing so may cause personal injury.

Format of safety messages that apply to an entire section:

These safety messages may be used with or without a symbol.

⚠CAUTION

Electrical shock

➔ *Touching current-conducting parts may result in injury due to electrical shock.*
- Do not remove safety protection and covers.
- Do not touch the electrical connections while power is being supplied.

Format of safety messages that are embedded in text and apply to a specific point:

⚠**CAUTION! Electrical shock.** Never remove safety protection and covers. Do not touch the electrical connections while power is being supplied.

2. Property Damage Messages

Property damage messages are used to describe potentially hazardous situations that may lead to property damage. These messages have the same layout as safety messages but use the signal word "NOTICE" instead of “CAUTION”.

Format of property damage messages that apply to an entire section:

NOTICE

Risk of damage to the device and connected devices
Risk of malfunction

- Read the following instructions carefully before installing the device.
- Always adhere to the instructions.

Format of property damage messages that are embedded in text and apply to a specific point:

NOTE! Risk of damage to the device and connected devices. Read the following instructions carefully before installing the device.

3. Definition of the Signal Words

⚠CAUTION	Indicates a hazardous situation that, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates information considered important, but not hazard-related (e.g., messages relating to property damage).

4. Definition of the Safety Symbols

⚠	**Caution: General Information** This symbol indicates general warnings or cautions that are not related to a particular type of hazard.
⚡	**Caution: Electrical Shock** This symbol indicates warnings related to electrical hazards (danger due to high voltage).
🚫	**Prohibited: Do Not Disassemble** This symbol indicates warnings about not disassembling certain components or equipment. Disassembling may lead to damage or malfunction of the device.
❗	**Mandatory Action: General Information** This symbol indicates general information that must be read and followed before proceeding with the accompanying instructions.
📖	**Mandatory Action: Read Instructions** This symbol indicates information referring to an important description in the manual, or other documentation, which must be read and followed.

⚠ Important Safety Information ⚠

- The installation, commissioning, and servicing of our products must be performed only 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.
  - ➔ Unqualified personnel may potentially perform actions that result in injury due to electrical shock.
- 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.
  - ➔ If the appliance is not disconnected from power, touching terminals or other internal parts of the appliance may lead to injury due to electrical shock.

- It is prohibited to alter the products (devices, cabling, etc.).
  - ➔ Alterations to the products may subsequently result in personal injury, property damage, or damage to the products.
- Do not remove protective shields and covers.
  - ➔ Removing protective shields and covers may result in personal injury or property damage.
- 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.

- 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 documentation. Therefore, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.
- If there are still some points that 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.
- 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.
- 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 endeavor to resolve the problem as quickly as possible.
- GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.

Although great 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.

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.

We especially look forward to hearing from you if you want to let us know that everything is functioning perfectly

CONTENTS

1 INTRODUCTION

1.1 About this manual

This manual contains the information necessary for the configuration and operation of GANTNER's battery-powered electronic locker locks. The following GANTNER battery locks are covered in this manual:

GAT ECO.Side Lock
All variants except for GAT ECO.Side Lock 7000 NW BA CardNET and GAT ECO.Side Lock 7000 NW BA OSS.

GAT ECO.Lock
All variants except for GAT ECO.Lock 7100 NW BA CardNET and GAT ECO.Lock 7100 NW BA OSS.

GL7p
All variants except for GL7p.x30x CardNET and GL7p.x30x OSS.

In this manual, the terms "battery lock" and "lock" are used to represent all lock variants. If information in the manual only applies to a specific lock, the respective product name is used.

ℹ *Information on the installation and commissioning of the battery locks is available in a separate manual (see the "Install" manual of the respective lock variant).*

ℹ *Information on the configuration and operation of the battery locks with CardNET and OSS functionality is available in separate CardNET and OSS manuals.*

1.2 Chapter overview

In chapter 2 "CONFIGURATION", you will find information on how the lock is configured with the configuration software GAT ECO Lock Configurator and with the MoLA App. The main configuration settings for the lock are explained and a table listing every setting is also available here.

In chapter 3 "OPERATION", the different operating modes of the lock are described. The system data carriers required to maintain the locker system and the LED signaling are also explained in this section.

1.3 Target group

This manual contains information relevant for the various stages in the operating life of the lock. Where not explicitly stated, the information in this manual is intended for all target groups in general. When a chapter is intended for a specific audience, this is clarified at the beginning of the chapter.

Information for the following target groups is available in this manual:

- Installation technicians (configuration)
- locker system operators (operation)

⚠**CAUTION! Injury and property/equipment damage.** The tasks described in each chapter must only be performed by the specified target group. Unqualified personnel who perform the described tasks risk personal injury or damaging property/equipment.

1.4 Formatting

1.4.1 Safety-critical information

The following formatting (with example text) is used in this manual to display important, safety-critical information that must be read and followed.

NOTE! Following on from this signal word in the manual is a reference text that must be read and followed. The reference text contains important information. Non-observance can lead to damage of the device or associated equipment.

1.4.2 General information

The following formatting (with example text) is used in this manual to display important, but not safety-critical information.

ℹ *The text accompanying this symbol contains interesting information relevant to the current chapter. You do not necessarily need to read this text; however, it will help you better understand the information in this section or provide interesting tips for the described device or the operation of the software.*

1.4.3 Instructions and results

Instructions, which must be completed by the reader, and the results of these instructions are formatted as follows.

► This symbol represents an action or instruction that that must be followed.

  o This symbol represents the result after completing the previous instruction.

1.5 Terminology

Several key terms that are used often in this manual are defined below.

Computer / PC
These terms refer to all desktop and laptop computers used to configure and maintain the locks.

Data carrier
An identification medium with electronic memory and an ID number that is used by the employees and visitors of a facility for identification. Data carriers are available in a variety of different forms (e.g., chip cards, wristbands, key tags), and to suit different RFID technologies (LEGIC, MIFARE®, ISO 15693).

System data carrier
Several types of system data carriers are used for programming, service, and maintenance tasks. These data carriers have special functions and as they are essential for operation and have security-related features, they must be kept in a secure place protected against unauthorized use. Most of the system data carriers are included in the GAT ECO.Basic Set, however, some must be ordered separately as required.

FID (Company ID) and Site Key
LEGIC systems use the FID number and in MIFARE® systems the site key is used, which is a combination of the FID and the read and write keys. The FID and site key are unique for every facility. These numbers are encoded in every data carrier and device used in the facility thereby ensuring that data carriers from one installation cannot be used in other installations.

GAT ECO Lock Configurator
A GANTNER developed PC software that is used to configure the GANTNER battery-powered locker locks.

Lock / Locker lock
General terms for all lock variants.

Locker
The term "locker" is used to describe all possible locker applications that can be fitted with a GANTNER electronic lock. Typical applications include a changing room locker, a deposit box, or a private box.

RFID (Radio-Frequency Identification)
Identification over a short distance using radio frequency. An RFID data carrier is used to identify users in GANTNER systems.

Wireless
Identification via a wireless interface in the range 2.402 to 2.48 GHz, over which identification and locker operation from a distance is possible, e.g., via a smartphone app. An additional feature is the monitoring of the lock status using an access point and the Relaxx locker management software.

User / Guest / Visitor
These general terms refer to the people in a facility who use the locker system with GANTNER locker locks, data carriers, and other GANTNER devices.

1.6 Contact & inquiries

For all inquiries concerning the GANTNER battery locker locks, please contact your local sales partner or one of the GANTNER branch offices directly. The contact details are available via the following link:
http://www.gantner.com/locations

2 CONFIGURATION

2.1 General information

The GANTNER battery-powered locker locks are configured using a PC/laptop and GAT ECO Lock Configurator software or with the MoLA app on a mobile device. For locks that use the same configuration settings, a configuration file is first created and saved in GAT ECO Lock Configurator. The configuration file can then be transferred to any lock that requires the same configuration. For locks that require a different configuration, a separate configuration must be defined in GAT ECO Lock Configurator.

When configuring the lock, always check whether the latest firmware is installed. If not, please update the firmware to the current version before the initial configuration. See chapter "2.2.3 Loading firmware into the lock".

Another option is to complete the configuration using the MoLA app, which can be downloaded from the Google Play Store and used with mobile devices with an Android operating system. The app uses NFC for configuration, which means that the mobile device must also support NFC communication. See more details in section "2.3. Configuration with the MoLA App".

NOTE! After configuring the first lock, perform a complete functional test to ensure that the data carriers (MASTER data carriers and standard user data carriers) are read reliably by the lock and that the lock operates according to the configured functionality before applying the configuration to the remaining locks.

The following data, among others, is imported into the lock during configuration:

- Customer-specific Site Key
- Locker number
- Lock operating mode
- Data carrier settings
- Date and time
- MASTER data carriers (and OPEN MASTER data carriers, if used)

The MASTER data carriers and OPEN MASTER data carriers can also be directly programmed into the lock (see "3.8.1 MASTER data carrier*"). However, the most efficient way to program the data carrier numbers into multiple locks is via PC using GAT ECO Lock Configurator or with the MoLA App.*

NOTE! The locks do not set the daylight-saving time automatically. Time changes due to daylight saving must be considered when evaluating bookings and also when authorizing data carriers with expiry dates/times!

2.2 Configuration with GAT ECO Lock Configurator

The GAT ECO Lock Configurator software can read the configuration of a lock. The settings can then be changed if required and uploaded to the lock. It is also possible to read out the booking data and update the firmware of the lock.

To start the configuration, the lock must be connected to the computer with the appropriate USB cable (e.g., from the GAT ECO.Basic Set) and the configuration mode must be activated using the SERVICE data carrier (see “3.8.6 SERVICE data carrier”).

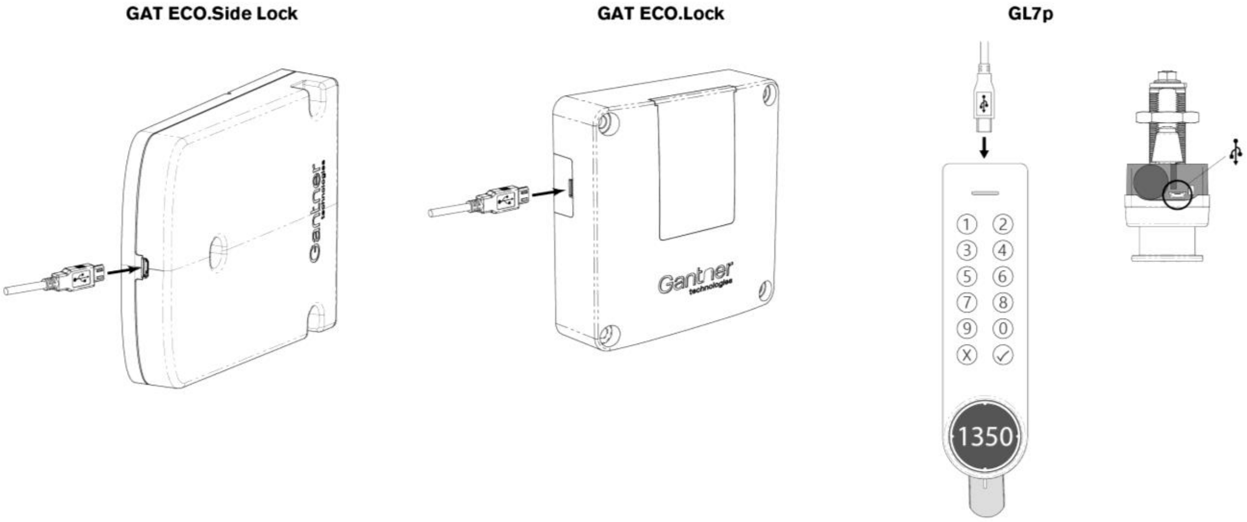


Figure 2.1 *– USB connection of the locker locks*

NOTE! The GL7p locks are powered by the USB cable, so the battery does not need to be in the lock during configuration. However, ensure that the lock is not de-energized for more than 1 minute (e.g., after disconnecting the USB cable until inserting the battery), otherwise the time and date will be deleted.

A separate manual with information on the operation of GAT ECO Lock Configurator is available to download from the GANTNER website (login required). GAT ECO Lock Configurator is currently only available in English.

2.2.1 Reading the configuration from a lock

- ► Start GAT ECO Lock Configurator. For standard installations, the link can be found in the Windows menu under “Gantner Electronic GmbH”.
  - ○ The software takes a few seconds to start. After starting, the main window is displayed.

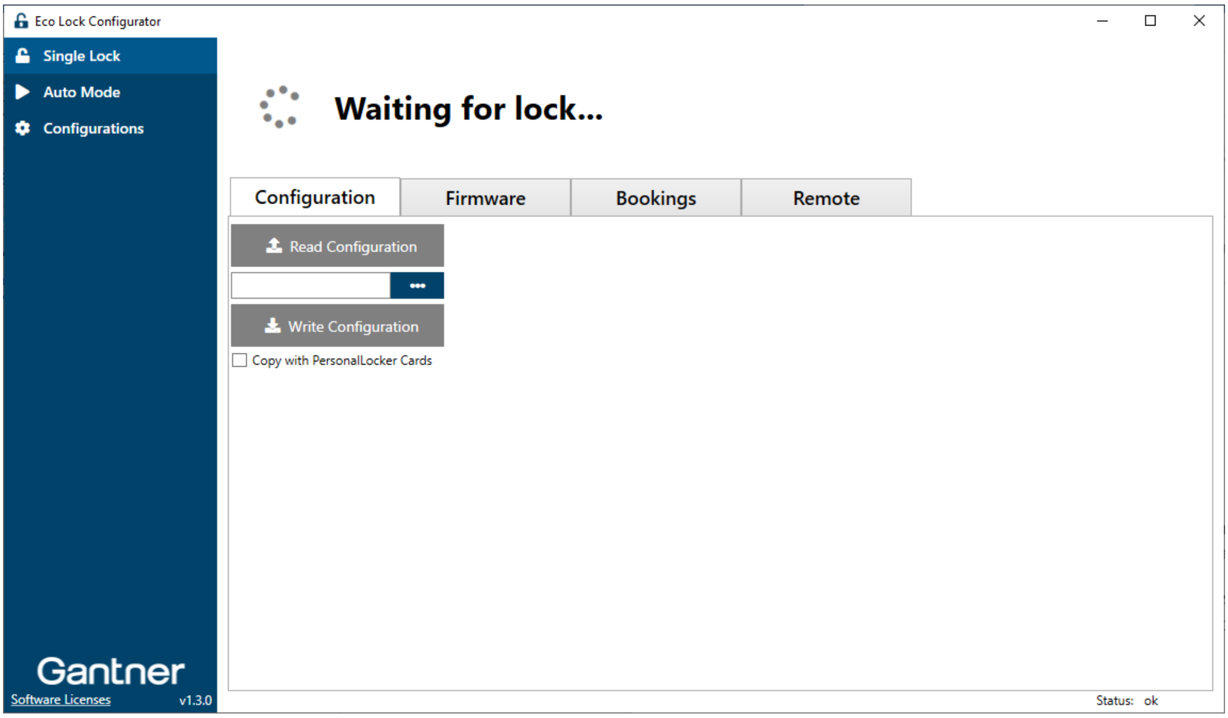
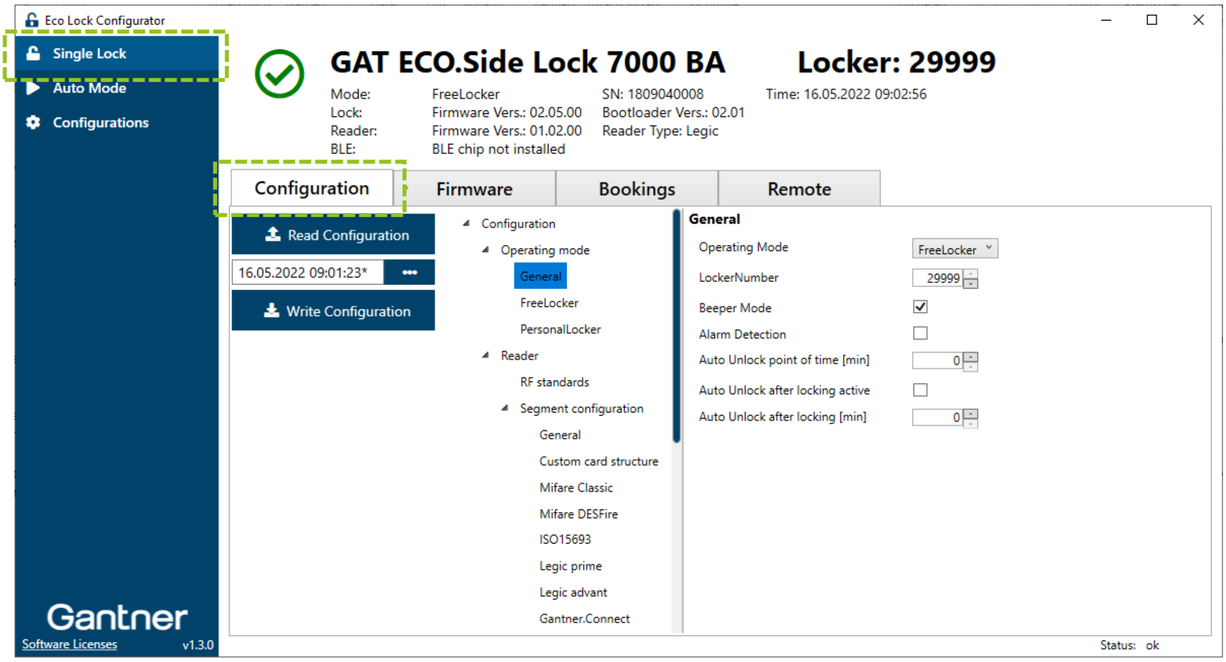


Figure 2.2 *– Main window of GAT ECO Lock Configurator*

- ► Select “Single Lock” from the menu to the left.
- ► Open the “Configuration” tab.
- ► Connect the lock to the PC via USB (see Figure 2.1).
- ► If the lock is already configured for a customer system with the specific Site Key, the LED on the lock flashes red/green. Read the SERVICE data carrier to enable communication (see “3.8.6 SERVICE data carrier”).
  If the lock has not yet been configured with a customer-specific Site Key, the LED on the lock flashes green and communication is possible without the SERVICE data carrier.
  - ○ The configuration settings are read out from the lock and displayed.



Eco Lock Configurator

GAT ECO.Side Lock 7000 BA **Locker: 29999**

Mode: FreeLocker
Lock: Firmware Vers.: 02.05.00
Reader: Firmware Vers.: 01.02.00
BLE: BLE chip not installed
SN: 1809040008
Bootloader Vers.: 02.01
Reader Type: Legic
Time: 16.05.2022 09:02:56

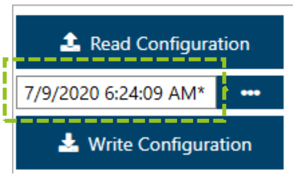
General

Operating Mode: FreeLocker
LockerNumber: 29999
Beeper Mode: ☑
Alarm Detection: □
Auto Unlock point of time [min]: 0
Auto Unlock after locking active: □
Auto Unlock after locking [min]: 0

Status: ok

Figure 2.2 *– Configuration settings*

In the left area of the window, the configuration categories are displayed as a tree structure. When you select a category ("General" in the example above), the configuration settings of the category are displayed on the right.



To the left of the configuration tree, the name of the currently displayed configuration is displayed in the text field. After a configuration is read from a lock, the current date and time is displayed here. When you save the configuration, you can change this name. If you have loaded a previously saved configuration, the name of the saved configuration is displayed here.

2.2.2 Editing and loading the configuration settings into the lock

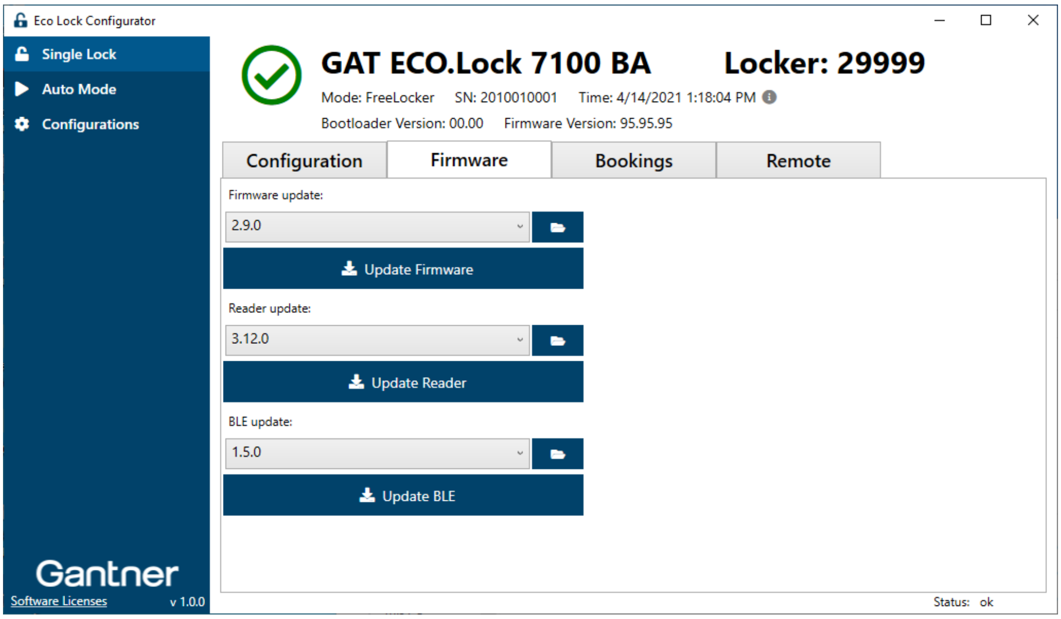
A description of each configuration setting is provided in chapter “2.4.12 Configuration settings table”.

- Edit the desired settings.
  - Changes are saved automatically.
- To transfer the settings to the lock, click on the "Write Configuration" button.
  - The changes are loaded into the lock. The LED on the lock flashes red briefly.
  - During the transfer, the Windows loading indicator (default = loading circle as mouse pointer) is displayed.
- Click on "Read Configuration" to read the configuration from the lock again.
- To save the currently displayed configuration, click on the ••• button and select "Save/Load Configuration" in the pop-up menu.
  - The “Configurations” page is displayed. Here, you can save the configuration and organize it into the configuration library.

2.2.3 Loading firmware into the lock

The firmware is the "operating system" of a lock and by loading a new firmware version, new functionalities for the lock can be added or also possibly occurring problems can be solved.

NOTE! Always check that the latest firmware is installed in the lock and update to the current version if required. The latest firmware is only updated with an active FTP connection to the Internet when GAT ECO Lock Configurator is started.



GAT ECO.Lock 7100 BA Locker: 29999
Mode: FreeLocker SN: 2010010001 Time: 4/14/2021 1:18:04 PM
Bootloader Version: 00.00 Firmware Version: 95.95.95

Firmware update: 2.9.0
Reader update: 3.12.0
BLE update: 1.5.0

Status: ok

__Figure 2.3__ – Selecting the firmware

- ► Ensure that the lock is connected via USB to the PC.
- ► In the "Single Lock" menu of GAT ECO Lock Configurator, open the "Firmware" tab.
  - ○ The possible firmware types are detected, and you can select the desired versions.
- ► If you only select the version, the matching firmware from GAT ECO Lock Configurator is used.
- ► If you want to use a special firmware, click on the 📁 symbol and select the desired firmware files.
- ► Click on "Update Firmware", "Update Reader", or "Update BLE" to load the desired component with the selected firmware.
  - ○ A graphic displays the loading progress, which may take a few seconds.
  - ○ The lock LED flashes red while the firmware is being loaded.
  - ○ A corresponding message is displayed indicating a successful update.

2.3 Configuration with the MoLA App

The MoLA app, which is available for download via Google Play Store, can be used with a mobile device, e.g., a smartphone, to configure the lock. To use the MoLA app, the following requirements must be fulfilled:

- Mobile device with Android 4.4.0 or later
- Mobile device must be NFC enabled
- Mobile device must not be rooted
- The lock must have the latest firmware version installed
- A valid APP KEY data carrier is required for configuring on-site locks

The MoLA app can be downloaded with this link from Google Play Store:

https://play.google.com/store/apps/details?id=com.gantner.mola

Due to technical limitations in iOS, the MoLA app is currently not available on Apple devices.

In MoLA, you can change the same configuration settings as those available in GAT ECO Lock Configurator (see "2.4. Configuration settings"). A detailed description about the operation of the app is available directly in MoLA.

The APP KEY data carrier is a special system data carrier (see "3.8. Summary of system data carriers") and is included in the GAT ECO.Basic Set. This data carrier is required to change the configuration of a lock or to create a new configuration.

When the lock is in factory mode (default, unconfigured state), the lock is operating in “DEMO” mode and the APP KEY is not needed.

Once the APP KEY data carrier is loaded into MoLA, it remains valid for a certain time period. When the session expires, the APP KEY is automatically deleted from the device. This prevents the unauthorized use of the APP KEY data carrier by third-party apps, malware, etc.

2.4 Configuration settings

The important configuration settings that can be defined in GAT ECO Lock Configurator are explained in this section. A list and brief explanation of every configuration setting available for the locks is provided in section “2.4.12 Configuration settings table”.

The configuration settings available depend on which lock variant is being configured. For example, the PIN code settings are only relevant for the GL7p.

2.4.1 Operating mode

The lock can operate in one of five different operating modes. See “3.6 Operating modes" for a detailed description of each mode. The operating mode setting is found here:

Configuration > Operating mode > General > Operating mode

► In the “Operating Mode” menu, select either:
- “Free locker”
- “Free locker universal”
- “Personal locker programming card”
- “Personal locker expiry date”, or
- “Free locker unique number”

2.4.2 Locker number

The number of the locker where the lock is installed can be defined. The locker number setting is found here:

Configuration > Operating mode > General > Locker number

► Enter the locker number for the lock into the “Locker number” field.

2.4.3 Sound signals

The lock has an integrated beeper that generates a sound for each lock operation or for signaling different states. The beeper can be activated or deactivated, and the setting is found here:

Configuration > Operating mode > General > Beeper mode

► Select / deselect the “Beeper mode” option to turn the sound signals on / off.

NOTE! If this setting is deactivated, a sound signal will still be generated if an alarm is triggered and if a system data carrier is used with the lock, e.g., to unlock the locker door with a MASTER data carrier.

2.4.4 Auto-unlock

There are two auto-unlock functions available for the locks. The first option automatically unlocks the locker at a defined point in time each day. The second option automatically unlocks the locker a definable number of minutes after being locked. For both options, the time must be set correctly once via software.

NOTE! If either of these functions is enabled, the lock will always unlock at the defined time regardless of the operating mode.

NOTE! The locks always operate according to UTC time and do not adjust to seasonal time changes automatically. Therefore, select a time that is suitable for the lock to open at any time of the year!

The point in time auto-unlock function is found here:

Configuration > Operating mode > General > Auto Unlock point of time [min]

► Enter a value representing the number of minutes into the field. The countdown time for unlocking begins at 00:00 (24 h). For example, a value of “300” means that the lock will unlock at 05:00 am. A value of “0” means that the function is inactive.

The auto-unlock after locking function is found here:

Configuration > Operating mode > General > Auto Unlock after locking active [min]

► Select / deselect the “Auto Unlock after locking active” option to turn the function on / off.

► In the “Auto Unlock after locking active [min]” field, enter a value representing the number of minutes. The countdown time for unlocking begins after the locker is locked. For example, if a value of “300” is entered and the locker is locked at 8:00 a.m., the lock will unlock at 1:00 p.m. A value of “0” means that the function is inactive.

2.4.5 Duration of use

Lockers operating in free locker mode can be configured to limit the user to a defined period of use. See section “3.6.1. Free locker mode (with or without duration of use function)” for detailed information. The duration of use function is found here:

Configuration > Operating mode > Free Locker

► Select either “Duration” or “Point of time” from the “Use time limit” menu for the type of time limit.

► Define the time limit in minutes in the “Time limit (min)” field.

2.4.6 Locking of personal locker without data carrier

The functionality of locking personal lockers without data carriers allows the locker to lock automatically when the locker door is pushed shut, without needing to use a data carrier. The locker can be unlocked again using the data carrier(s) authorized to use the personal locker. The function is found here:

Configuration > Operating mode > PersonalLocker

► Select / deselect the “PreLock Personal Locker” option to turn the function on / off.

2.4.7 RF standards

The GANTNER battery locker locks can operate with data carriers that use different RFID technologies. The RFID technologies supported by the lock depends upon the lock variant, as different RFID readers are operating in the variants. Some of the settings for the lock to operate with RFID technologies can be enabled/disabled and are found here:

Configuration > Reader > RF standards

► Select / deselect the desired technology to turn the setting on / off.

NOTE! Please note that disabling “ISO 14443” deactivates the NFC communication and configuration using the MoLA app is not possible anymore.

2.4.8 MASTER data carriers

Up to 10 MASTER data carriers (also called MASTER cards) can be assigned to the lock to allow the locker to be opened in special circumstances, e.g., if a user has lost their data carrier. For this functionality, the MASTER data carriers must be first entered, which is done here:

Configuration > Application > Master cards > Master Card 1 - 10

► Enter the number of each MASTER data carrier in decimal format into the respective fields.

NOTE! The “Read” button in GAT ECO Lock Configurator is used to read the data carrier directly at the connected lock and enter the number into the respective field. To do this, the RFID settings must be set correctly, and the data carrier must be a valid MASTER or OPEN MASTER data carrier.

ℹ *There are OPEN MASTER data carriers (not included in the GAT ECO.Basic set). Similar to the MASTER data carriers, these special data carriers can open all lockers, but can no longer lock them. To program an OPEN MASTER data carrier, enter its number into one of the "MasterCard" fields. A total of 10 MASTER or OPEN MASTER data carriers can be configured.*

2.4.9 Wireless interface

For lock variants with a wireless interface, the identification can also be transmitted wirelessly, e.g., via smartphone. Another function is the ability to monitor the lock status using an access point and the Relaxx locker management software. The wireless interface can be enabled via the following option.

Configuration > Reader > BLE > General > BLE enabled

- ► Select the option if you want to use the wireless interface.
- ► You can configure the wireless interface as required via the other fields in this window.

2.4.10 Alarm mode (GAT ECO.Side Lock)

The GAT ECO.Side Lock is designed to detect when somebody attempts to force open a locker door. The lock emits a loud, intermittent alarm tone and the status LED flashes red when an alarm is triggered. The alarm mode function is found here:

Configuration > Operating mode > General > Alarm detection

- ► Select / deselect the “Alarm detection” option to turn the function on / off.

2.4.11 PIN-code keypad (GL7p)

For GL7p variants with a PIN-code keypad, the identification can also be completed using a PIN code. To allow identification via PIN code, the following option must be enabled.

Configuration > Reader > KeyPad > General > KeyPad enabled

- ► Select the option if you want to allow the PIN-code keypad to be used.
- ► Via the other fields in this window, you can specify the time within which a PIN code must be entered and set the permitted length of the PIN code. You can also define whether the time limit function should be activated when entering the PIN code.

2.4.12 Configuration settings table

The following table lists all the configuration information available for the GANTNER battery locker locks.
NOTE! Not all settings are available for all lock variants. Settings that are specific to one type of lock only are identified as such in the table.

Options	Description	Format	Default
Operating mode			
General			
Operating Mode	Select the operating mode (see "3.6 Operating modes") of the lock: - FreeLocker - PersonalLocker_ProgrammingCard - PersonalLocker_ExpiryDate - FreeLocker_UniqueNumber - FreeLockerUniversal	List option	Free Locker
Locker Number	The locker number of the lock. Max. Number = 29,999 (BA locks) or 65,535 (F/ISO locks)	Integer	29,999 (BA) 65,535 (F/ISO)
Beeper Mode	Enable/disable the integrated beeper.	Boolean	True
Alarm Detection (GAT ECO.Side Lock only)	Switch on/off the alarm function	Boolean	False
Auto unlock point of time [min]	Unlock locker at a defined point in time (input in minutes after midnight), "0" = inactive.	Integer	0
Auto unlock after locking active	Enable/disable the automatic unlocking of a locked locker	Boolean	False
Auto unlock after locking [min]	After it is locked, the locker will unlock automatically after the number of minutes entered here. "0" = inactive.	Integer	0
Free Locker			
Use Time Limit	Select the type of time limit for the locker (see "3.6.1. Free locker mode (with or without duration of use function)"): "Duration" or "Point of time"	List option	Duration
Time Limit [min]	Define the time limit. Value must be entered in minutes (if the most significant bit is not set) or in hours (if the most significant bit is set). Examples: Dec. value 1 up to 32767 -> 1 up to 32767 minutes Dec. value 32768 to 65535 -> 1 up to 32766 hours "0" = inactive	Integer	0
Time Limit Interrupt Timeout [min]	Minimum waiting time from the end of a locker usage period until the next usage period can begin.	Integer	60
Card Validity Date Required	When enabled, a valid expiration date must be set on the data carriers for them to be used (default: 1.1.2007 is not valid).	Boolean	False
Ignore Card Validity Date	If this option is enabled, the expiration date on the data carriers will be ignored.	Boolean	False
Personal Locker			
Index Personal Locker	Define the index of the personal locker.	Integer	0
PreLock Personal Locker	Enable/disable the automatic lock function without data carrier for personal lockers.	Boolean	False
Personal Locker Secure Flag	When enabled, a new index or validity date can only be transferred from a data carrier to the lock when the locker is open. When this option is deactivated, transferal is possible even when the locker is locked (see "3.6.5. Personal locker expiry date mode").	Boolean	False

	Last Open At Expired Date	When enabled, a locker can be reopened after the expiration of its useful life using the data carrier with which it was locked (see "3.6.5. Personal locker expiry date mode").	Boolean	True
	Write Locker Data PL ExpDate	When enabled, the lock status is written to the data carrier when the data carrier is read.	Boolean	
Reader				
	RF standards			
	LEGIC Prime **(only for LEGIC locks)**	When enabled, LEGIC prime data carriers can be read by the lock.	Boolean	True
	ISO15693	When set to "True", ISO 15693 data carriers can be read by the lock.	Boolean	False
	ISO14443A	When set to "True" ISO 14443 (MIFARE) data carriers ca be read by the lock. This setting is not configurable.	Boolean	True
	HID	When set to "True", the device can read HID iCLASS data carriers (UID / CSN number only).	Boolean	False
	Segment configuration			
	General			
	Site Key	Site key of the lock. Each data carrier must be encoded with the same site key in order to function with the lock.	Hex	xxx
	DESFire KeySet	Custom DESFire AES key, encrypted. This key is only required for customer-specific encrypted DESFire data carriers.	Hex	00000…
	Use Custom Card	Enable/disable the ability to use a custom card (see the following settings).	Boolean	False
	Custom card structure	Settings for reading customer-specific data carriers		
	DataOffset	Start position of the data on the data carrier (byte).	Integer	0
	DataLen	Length of the data on the data carrier (bytes).	Integer	0
	CRCDataStartAdr	Start address of the CRC checksum (byte).	Integer	0
	CrcAdr	Address of the CRC checksum (byte).	Integer	0
	CrcMode	CRC checksum mode: NONE, LRC, LRC_UID_B0, LEGIC_CRC8, LEGIC_CRC16	List option	NONE
	Format	Format of the data: BIN_LSB, BIN_MSB, BCD, ASCII	List option	BIN_LSB
	MIFARE Classic	Options for MIFARE Classic data carriers		
	Sector Number	The MIFARE Classic sector where the locker information is stored on the data carrier.	Integer	4
	Read Key	Select the “Read Key” (Key A or Key B)	List option	KEY A
	Write Key	Select the “Write Key” (Key A or Key B)	List option	KEY B
	MIFARE DESFire	Options for MIFARE DESFire data carriers		
	Read Key Num	Number of the “Read Key”	Integer	1
	Write Key Num	Number of the “Write Key”	Integer	2
	Application ID	ID of the desired DESFire application	Hex	DF8405
	Encryption Mode	Select the type of encryption mode	List option	AES
	File Number	DESFire Locker File in which the locker information is stored	Integer	1
	File Comm Mode	File communication mode: “Plain”, “Maced”, “Enciphered”	List option	ENCIPHERED
	File Type	Type of file: “Standard”, “Backup”	List option	BACKUP
	File Data Offset	Data offset in the DESFire locker file	Integer	0
	ISO15693	Options for ISO 15693 data carriers		
	General Block Num	The segment where general data is stored	Integer	13

	Certificate Block Num	The segment where certificate data is stored	Integer	15
	Locker Block Num	The segment where locker data is stored	Integer	19
	LEGIC prime **(only for LEGIC locks)**	Options for LEGIC prime data carriers		
	SearchStr	LEGIC prime stamp. Structure as follows: 1. ID: GANTNER standard = 1A2200 2. FID: Default = 9999 3. Segment ID: Default = 03	Text	1A2200 999903
	Search String Length	Length of the stamp	Integer	6
	Legic Locker	Select here the LEGIC locker number (1 or 2) in the locker information coded on the data carrier.	List option	Locker1
	LEGIC advant **(only for LEGIC locks)**	Options for LEGIC advant data carriers		
	Stamp	Value of the stamp for LEGIC advant. Structure: 1. ID: GANTNER default = 1A24 2. FID: Default = 00009999 3. Segment ID: default = 0008 4. 00000000	Text	1A240000 99990008
	Stamp String Length	Length of the LEGIC advant stamp in bytes	Integer	8
	Gantner.Connect			
	File ID	ID number for GANTNER.Connect.	Integer	1
	Basic Set configuration			
	General			
	Site Key	System number of the Basic Set used.	Hex	xxx
	DESFire KeySet	Custom DESFire AES key, encrypted. This key is only required for customer-specific encrypted DESFire data carriers.	Hex	
	Use user card settings	Use the settings of the generally defined data carriers (see "Segment configuration"). If this option is enabled, the remaining Basic Set settings are ignored!	Boolean	True
	BLE (only for lock variants with a wireless interface)			
	General			
	BLE enabled	Setting to enable/disable the wireless interface.	Boolean	False
	KeySet BLE	Custom key for the wireless interface. GANTNER standard = 0	Hex	
	BLE advertise timeout idle mode	Duration for how long the information packets (BLE Advertise) are sent in idle mode (deep sleep mode of the lock). Idle mode begins after activation mode has expired. If you enter "0", idle mode is active indefinitely.	Integer	0
	BLE pulse period idle mode	Period between the sending of information packets (BLE Advertise) in idle mode. Input in 100 ms (e.g., 600 = 1 min.). As each pulse requires energy, the period should be set so large, depending on the application, that the information packets are still detectable.	Integer	100
	BLE advertise timeout activation	Duration how long the information packets (BLE Advertise) are sent in activation mode (after pressing the button). Input in 100 ms (e.g., 600 = 1 min.). When activation mode ends, idle mode starts. If you enter "0", activation mode is active indefinitely and idle mode is not used.	Integer	150

	BLE pulse period activation	Period between the sending of information packets (BLE Advertise) in activation mode. Input in 100 ms (e.g., 600 = 1 min.). As each pulse requires energy, the period should be selected so that wireless signals are still quickly detectable in activation mode.	Integer	5
	BLE PreLock Timeout	Time period (in seconds) for locking the lock after receiving the locking command via wireless interface.	Integer	10
	BLE Advertising Format	Type that is used for the BLE advertising data. Type 1 is required for networking via BLE gateways.	List option	TYPE1
	KeyPad (only for GL7p variants)			
	General			
	KeyPad enabled	When set to "True", operation via PIN code is possible for the locks with a keypad.	Boolean	True
	PIN code timeout	Max. input time between 2 digits of the PIN code. If no additional key is pressed during this time and the entry is not confirmed with (✓) or button, the entry is cancelled. Input in 100 ms (e.g., default value 40 = 4 seconds).	Integer	40
	Minimum PIN length	Minimum required PIN code length.	Integer	4
	Maximum PIN length	Maximum required PIN code length.	Integer	7
	Activate PIN code UseTimeLimit	When set to "True", the usage duration is used for PIN code entry, analogous to the operation with data carriers. See "3.6.1. Free locker mode (with or without duration of use function)".	Boolean	False
Application				
	General			
	Legacy BasicSet Coding	When set to "True", data carriers in the Basic Set are coded for a predecessor system (previous coding).	Boolean	False
	Master cards			
	MasterCard1 .. 10	Fields to enter the numbers for MASTER or OPEN MASTER data carrier 1-10.	Integer	
	License			
	License Certificate Check	When "installed" is displayed here, the certificate check can be switched on/off.	Info	installed
	Certificate Check enabled	Switch on/off the certificate check for data carriers.	Boolean	False
Read only parameter				
	Production	Production-specific information		
	ArticleNum	Part number of the lock	Integer	
	SerialNum	Serial number of the lock	Integer	
	ManufacturerNum	Manufacturer number of the lock	Integer	
	ProductionYear	Production year of the lock	Integer	
	ProductionWeek	Production week of the lock	Integer	
	HardwareUidNum	Unique ID number of the lock	Integer	
	ControllerType	Type number of the lock		
	HardwareVers	Hardware version of the lock	Integer	
	BootloaderVers	Bootloader version of the lock	Integer	
	FirmwareVers	Firmware version of the lock	Integer	
	LockEngineVers	Version of the lock logic	Integer	
	Internal	Internal data for service purposes		
	Antenna matching	Antenna calibration	Integer	
	CNT Activation	Number of button actuations since resetting the counter	Integer	

	CNT Locking	Number of valid locks (with data carrier or PIN) since resetting the counter	Integer	
	CNT Activation ABS	Total number of button actuations	Integer	
	CNT Locking ABS	Total number of locks (with data carrier or PIN)	Integer	
	Temp. int.	Internal temperature of the lock in °C	Integer	
	BV	Information for service technicians		
	TL	Information for service technicians		
	MC	Information for service technicians		
	BM	Information for service technicians		
	ReaderChip			
	FW	Firmware of the RFID reader electronics		
	BL	Information for service technicians		
	PT	Product type of the reader electronics		
	HW	Hardware version of the reader electronics		
	AC	Information for service technicians		
	Telemetry	Status information about the operation of the lock		
	Duration Locked [min.]	Counter that shows how long the lock has been locked for (in minutes)	Integer	
	CNT activations last locking	Number of button presses since the last locking of the lock	Integer	
	CNT door released while locking	Number of cancelled locking operations	Integer	
	CNT write on card failed 1	Number of write errors to data carriers, first attempt	Integer	
	CNT write on card failed 2	Number of write errors to data carriers, second attempt	Integer	
	CNT write on card failed card removed	Number of write errors to data carriers because the data carrier was removed too soon from the reading field	Integer	
	BLE			
	BLE Module FW Version	Firmware of the wireless interface electronics		
BatteryMgt				
	Settings			
	Batt Idle MA	Information for service technicians	Integer	
	Batt Idle	Information for service technicians	Integer	
	Supply Reg OFF	Information for service technicians	Integer	

Table 2.1 *– Configuration settings*

3 OPERATION

RF exposure statement

The users must keep at least 20 cm separation distance from the lock, except during the identification and operation process at the lock, which must be performed as described in this manual.

3.1 Target group

This chapter contains information for the technicians responsible for commissioning the lock and performing service work in case of operational problems.

3.2 General

The GANTNER battery locker locks can operate in "free locker" mode or "personal locker" mode. In free locker mode, the user can select any unoccupied locker; in personal locker mode, the user is assigned a specific locker that only they can use.

When free lockers and personal lockers are used together in one system, it is recommended that the locker numbers are unique for both functions. This means that the same locker number should never be used for both a personal locker and a free locker.

To operate the lock (e.g., to lock or unlock a locker), the user must identify themselves at the lock using their RFID data carrier or via PIN code (GL7p only). To save battery power, the lock is deactivated in its normal state and the lock electronics must be activated before identification or operation can occur. For the GL7p and GAT ECO.Lock, this is done by pressing the lock button in using the data carrier. For the GAT ECO.Side Lock, the locker door must be pressed in while holding the data carrier in front of the lock LED. Through his process, the RFID reader is activated, and the data carrier is read.

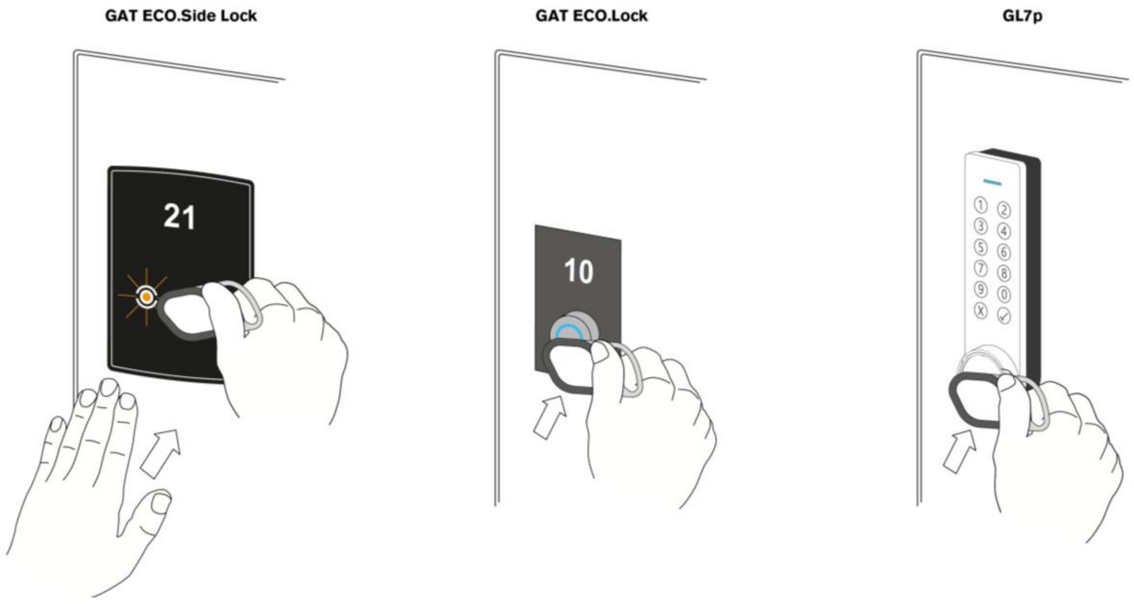


***Figure 3.1** – Activating the RFID reader of the lock*

3.3 PIN-code operation (GL7p)

For the GL7p locks with a keypad (GL7p.**1**xxx and GL7p.**3**xxx), operating the lock, i.e., locking and unlocking, can be completed by entering a PIN code instead of reading a data carrier.

See section “2.4.11 PIN-code keypad (GL7p)” for information on how to enable the keypad for PIN-code operation.

After entering the PIN code, it must be confirmed by pressing the "✓" key or by pressing the push button. An RFID data carrier is then not necessary. An entered PIN code can be deleted by pressing the "X" button.

The length of the PIN code is configurable (see “2.4.12 Configuration settings table”). So that the personal PIN codes remain protected, the PIN codes entered into the lock are not logged in the lock bookings and cannot be read.

3.4 Alarm and handling (GAT ECO.Side Lock)

The GAT ECO.Side Lock is designed to detect when somebody attempts to force open a locker door. To alert facility staff to the break-in, a loud, intermittent alarm signal is emitted, and the status LED flashes red.

The alarm function is deactivated by default. See section “2.4.10. Alarm mode (GAT ECO.Side Lock)” for information on how to enable the function.

To deactivate a locker alarm:

- ► Close the locker door and hold it shut.
- ► Hold a MASTER data carrier next to the RFID reading field (see section “3.8.1. MASTER data carrier”).
    - o The alarm sound signal is deactivated and the LED stops flashing.
- ► If the locker door is still locked, hold a MASTER data carrier or the data carrier previously used to lock the locker next to the RFID reading field.
    - o The locker door opens.

NOTE! The GAT ECO.Side Lock, bolt set, and door shackle must all be replaced following a break-in.

3.5 Automatic antenna adjustment (GAT ECO.Side Lock)

The antenna of the GAT ECO.Side Lock can be calibrated to ensure the optimal reading range for the RFID data carriers. The lock is equipped with an automatic antenna adjustment function, which can be activated with the SERVICE data carrier or via the configuration software.

3.5.1 Antenna adjustment with the SERVICE data carrier

The SERVICE data carrier is included in the GAT ECO.Basic Set (see "3.7 GAT ECO.Basic Set"). Complete the following steps to activate the antenna adjustment function.

- ► Press the locker door shut with one hand.
- ► Hold the SERVICE data carrier next to the RFID reading field. Remove the data carrier immediately after activating the antenna adjustment.
    - o The antenna adjustment process starts, and the status LED flashes red for 5 seconds. The process is complete when the LED flashes green for 1 second and the lock emits a beep.

ℹ *It is possible to activate the antenna adjustment function even when the locker door is locked.*

3.5.2 Antenna adjustment via GAT ECO Lock Configurator

- ► In the GAT ECO Lock Configurator software, click on "Adjust Antenna" in the "Remote" tab.

3.6 Operating modes

In the following instructions, the process of “activating” the lock in order to carry out an operation is described for all lock variants in general. Refer to Figure 3.1 for a demonstration of how the activation process is performed for each lock variant.

The following operating modes are possible:

“Free Locker” mode

- Free locker selection with or without duration of use function (default)
- Free locker universal

  NOTE! The “Free locker universal” mode is only available with MIFARE data carriers.
- Free locker unique number

“Personal Locker” mode

- Personal locker programming card
- Personal locker expiry date

Requirements for LEGIC prime, LEGIC advant, MIFARE, ISO 15693, and HID iClass data carriers
All MIFARE and ISO 15693 data carriers that are used in the system must meet the operating mode requirements as specified in the following table.

Operating mode	Requirements for data carriers
Free locker	Data carriers must be encoded with the GANTNER locker information accordingly.
Free locker universal	The set data area of the MIFARE data carriers must be unused (encoded with zeros) and the read/write rights must be available and configured.
Free locker unique number	The data carriers do not have to be encoded. All LEGIC, MIFARE, ISO 15693 and HID iClass data carriers can be used provided that no random UID is available.
Personal locker programming card	The data carriers do not have to be encoded. All LEGIC, MIFARE, ISO 15693, and HID iClass data carriers can be used provided that no random UID is available.
Personal locker expiry date	Data carriers must be encoded with the GANTNER locker information accordingly.

***Table 3.1** – Requirements for data carriers*

3.6.1 Free locker mode (with or without duration of use function)

In free locker mode, the user has the option of selecting any unoccupied locker and locking it using their data carrier. After the locker has been locked, the user cannot occupy any additional lockers within the same locker group. Only once the original locker has been unlocked can the user lock another locker in the locker group.

Locker groups are used to organize the locks within a system into certain functional blocks, e.g., changing room lockers, safe-deposit boxes, etc. Different sector numbers are used on the data carriers to distinguish between the locker groups, which allows two or more lockers from different groups to be used with the same data carrier, depending on the data carrier storage space.

For data carriers that are configured with an expiry date, the date is checked by the lock. If the date has passed, the locker cannot be used.
NOTE! The lock does not automatically adjust to seasonal time changes. This must be considered when defining the validity or expiry date.

Locking and unlocking lockers with a data carrier

► Activate the lock using a data carrier for approximately 1 second.

  o The information on the data carrier is read.

  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.

  b) Invalid data carrier: The LED flashes blue briefly and then red and the lock switches off without completing the locking action. Possible reasons for this include:

  - Another locker has already been locked using the data carrier. In this case, the first locker must be unlocked before the data carrier can be used with the new locker.

► When locking the locker, check that it is locked by pulling the locker door.

Locking and unlocking lockers with a PIN code (GL7p only)

► Enter your PIN code.

NOTE! The length of the PIN code can be defined in the configuration.

► To confirm the PIN code, press the OK button (✓) and then the lock button or simply press the lock button directly.

  o The PIN code is checked.

  a) Valid PIN code: The LED flashes green briefly, and the action (lock/unlock) is carried out.

  b) Invalid PIN code: The LED flashes red briefly and the lock switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

Duration of use function

Free locker mode also offers the possibility to define a duration of use for each locker. If a locker with this function is locked with a data carrier, the current time is written onto the data carrier and the time subsequently checked when the user attempts to open the locker again. With PIN code entry, this function is also possible. The timer resets after a new PIN code has been entered. It should be noted that each new PIN entry restarts the maximum usage time.

The locker can be locked/unlocked as often as required during the duration of use period. If the duration of use period is exceeded, the data carrier can no longer unlock the locker. In this case, the user must recode their data carrier at a central station, e.g., a GT7 with G7 Info App. If the maximum usage time is exceeded when using a PIN, the lock must be opened with a valid MASTER data carrier.

NOTE! The data carriers must be coded accordingly for the duration of use function (the corresponding config bits on the data carrier must be set). This feature is not available with LEGIC prime data carriers. When used with a PIN code, the duration-of-use function must be activated separately in the configuration (see section "2.4.11 PIN-code keypad (GL7p)"). The lock must also be configured for the function (see section “2.4.5. Duration of use ”). There are two configuration modes for the function:

- Absolute duration of use (“Duration” function)
  In this mode, a usage period (depending on the “Time limit” parameter in minutes or hours, see "2.4.12 Configuration settings table") is configured. After locking a locker, the user must unlock the locker again within the defined period. The period begins from when the locker was first locked.
  Example:
  The time of use has been set (Time Limit [min] parameter) to 360 minutes (3 hours). If the locker is locked at 10:00, it can be opened again until 13:00. If the locker is locked at 14:00, it can be opened until 17:00. The duration time is reset if the locker is open for more than 60 minutes (Time Limit Interrupt Timeout [min] parameter). If any locker with an active duration function is locked again within the defined interrupt timeout, the previously active duration continues to run.
  If a locker can no longer be opened because the duration has been exceeded, the user must have their data carrier reset at a central location, e.g., at a GT7 terminal with G7 Info App.

- Use up to a specific time after midnight (“Point of time” function)
  In this mode, a time is configured up to which the locker can be used every day. After locking a locker, the locker must be unlocked before the defined time. The usage period starts from the configured time after midnight.
  Example:
  The time is set to 120 minutes. As the calculation begins at midnight, the locker can be used until 02:00 the following day regardless of when the locker was locked. If the locker is locked, e.g., at 01:00, it can be unlocked until 02:00 of the following day. If the locker remains locked past this time, the data carrier can no longer unlock the locker. In this case, the user must release the data carrier at a central station, e.g., a GT7 with G7 Info App.

<u>Locking and unlocking lockers with a data carrier</u>

► Activate the lock using a data carrier for approximately 1 second.

  o The information on the data carrier is read.

  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out. The time on the data carrier is checked and the current time written onto the data carrier.

  b) Invalid data carrier: The LED flashes blue briefly and then red and the lock switches off without completing the locking action. Possible reasons for this include:

    - Another locker has already been locked using the data carrier. In this case, the first locker must be unlocked before the data carrier can be used with the new locker.
    - The duration of use period has been exceeded and the locker cannot be opened anymore. In this case, the data carrier must be reset at a central station.

► When locking the locker, check that it is locked by pulling the locker door.

3.6.2 Free locker universal mode

The “free locker universal” operating mode differs from the standard free locker mode in the following ways:

- Free locker universal mode allows the use of data carriers that have not been encoded with the GANTNER locker information.
- There is no validity date with free locker universal mode.
- It is not possible to use a duration of use time with free locker universal mode.
- The following requirements for the data carriers apply:
    1. They must use a MIFARE Classic or DESFire technology.
    2. The locker segment or file must be unused and "empty", i.e., coded with all zeros.
    3. The Access Keys must be correct.

ATTENTION! If "free locker universal" mode is activated and encoded data carriers are used at the same time, all data from the defined data carrier area will be deleted when the locker is opened! As a result, these data carriers can no longer be used with locks in "free locker" or "personal locker expiry date" mode. To be able to use these data carriers again, the corresponding data areas must be recoded!

Locking and unlocking lockers with a data carrier

► Activate the lock using a data carrier for approximately 1 second.

  ○ The information on the data carrier is read.

  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.

  b) Invalid data carrier: The LED flashes blue briefly and then red and the lock switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

3.6.3 Free locker unique number mode

“Free locker unique number” operating mode differs from the standard free locker mode in the following ways:

- All LEGIC, MIFARE, HID iClass, and ISO 15693 data carriers can be used with the lock provided that they do not use random unique numbers (Random UID).
- The data carrier can have a GANTNER locker segment, however the segment is not used for this mode.
- When a locker is locked with a data carrier, the locker usage information is not written onto the data carrier.
- Every data carrier can use (lock) any number of lockers at the same time.

Locking and unlocking lockers with a data carrier

► Activate the lock using a data carrier for approximately 1 second.

  ○ The information on the data carrier is read.

  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.

  b) Invalid data carrier: The LED flashes blue briefly and then red and the lock switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

Locking and unlocking lockers with a PIN code (GL7p only)

► Enter your PIN code.

NOTE! The length of the PIN code can be defined in the configuration.

► To confirm the PIN code, press the OK button (✓) and then the lock button or simply press the lock button directly.

- The PIN code is checked.

a) Valid PIN code: The LED flashes green briefly, and the action (lock/unlock) is carried out.

b) Invalid PIN code: The LED flashes red briefly and the lock switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

3.6.4 Personal locker programming card mode

For locks operating in “personal locker programming card” mode, up to 32 data carriers or 32 PIN codes (GL7p only) per lock can be authorized for use. The max. 32 authorizations can be used with the locker as often as required and share the same authorization access, e.g., for use as family cards.

The authorizations are programmed into the lock using the PROGRAM data carrier (included in the GAT ECO.Basic Set, see section “3.7 GAT ECO.Basic Set”).

Authorizing data carriers

► Activate the lock using the PROGRAM data carrier for approximately 1 second.

- The information on the data carrier is read and the LED flashes green briefly.

► The lock enters into programming mode.

- The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready to program data carriers.

► Within 5 seconds, hold the data carrier being authorized in front of the lock (the lock does not need to be activated).

a) Successful authorization: The LED flashes green for approximately 3 seconds. When the data carrier is removed, the LED flashes red/green alternately again and another data carrier can be authorized in the same way. Repeat this process until all the data carriers are authorized.

b) Unsuccessful authorization: The LED flashes red. A possible reason for this is that the data carrier could not be read correctly, e.g., because the data carrier is damaged.

► You can repeat the last step using different data carriers to program these data carriers successively. To do this, each data carrier being authorized must be read by the lock within 5 seconds after removing the previous data carrier. If you wait longer than 5 seconds, the reading process is terminated, and the read data carriers are saved in the lock.

Authorizing PIN codes (GL7p only)

► Activate the lock using the PROGRAM data carrier for approximately 1 second.

   o The information on the data carrier is read and the LED flashes green briefly.

► The lock enters into programming mode.

   o The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready to program data carriers.

► Within 5 seconds, enter the PIN code being authorized and to confirm, press the OK button (✓) and then the lock button or simply press the lock button directly.

a) Successful authorization: The LED flashes green for approximately 3 seconds. When the data carrier is removed, the LED flashes red/green alternately again and another PIN code can be authorized in the same way. Repeat this process until all the PIN codes are authorized.

b) Unsuccessful authorization: The LED flashes red 3 times. A possible reason for this is that the PIN code was not entered correctly, e.g., the PIN code was too short or long or an invalid PIN code was entered.

► You can repeat the last step using different PIN codes to program these successively. To do this, the PIN code must be entered within 5 seconds after confirming the previous PIN code. If you wait longer than 5 seconds, the reading process is terminated, and the PIN codes are saved in the lock.

Deleting data carriers or PIN codes (= removing authorization)

It is only possible to delete all authorizations from the lock at once.

► Activate the lock using the PROGAM data carrier for approximately 1 second.

   o The information on the data carrier is read and the LED flashes green briefly.

► The lock enters into programming mode.

   o The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready for the next step.

► Within 5 seconds, hold the PROGRAM data carrier in front of the lock for approximately 1 second.

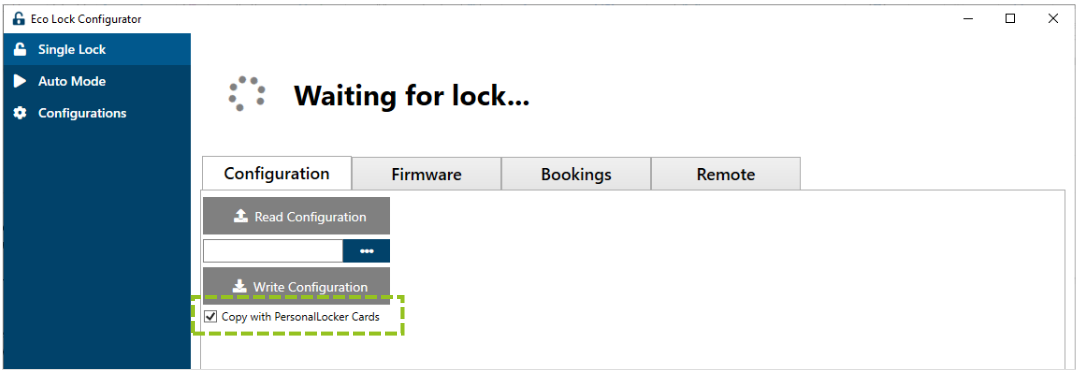
► When the action is successful, the LED flashes red 3 times and 2 beeps are emitted. The lock then switches off.

   o All data carriers / PIN codes are now deleted from the lock and no longer have the authorization to use the locker.

Transferring authorizations to a new lock

If a lock operating in personal locker programming card mode is being replaced with a new lock, the existing settings and data carrier authorizations can be transferred to the new lock in GAT ECO Lock Configurator.

- ► Before connecting the existing lock to the PC, select the “Copy with Personal Locker Cards” option in GAT ECO Lock Configurator.

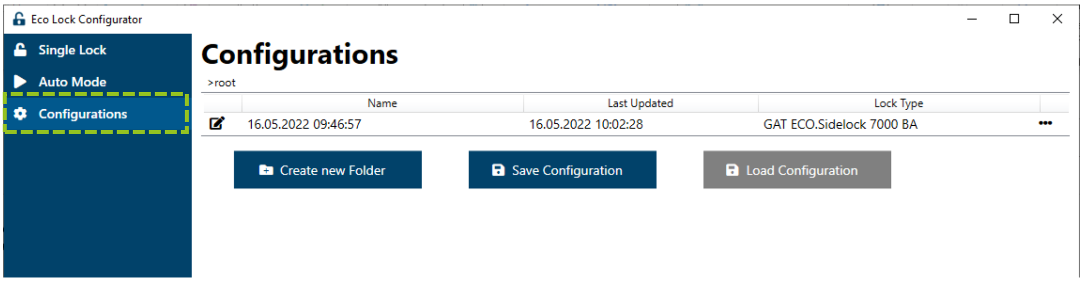


Waiting for lock...

☑ Copy with PersonalLocker Cards

Figure 3.2 *– “Copy with Personal Locker Cards” option*

- ► Connect the existing lock to the PC and select “Read Configuration”.
  - ○ The configuration of the lock as well as the stored data carriers are read.
- ► Open the “Configurations” page of GAT ECO Lock Configurator via the sidebar.



Configurations

>root

	Name	Last Updated	Lock Type	
	16.05.2022 09:46:57	16.05.2022 10:02:28	GAT ECO.Sidelock 7000 BA	•••

Figure 3.3 *– “Configurations” page*

- ► Here you can save the lock configuration via the “Save Configuration” button.
- ► Now connect the new lock to the PC and load the configuration file into the lock via the “Load Configuration” button.

See the GAT ECO Lock Configurator manual for further information.

3.6.5 Personal locker expiry date mode

Information for GL7p locks
As PIN codes cannot be used to save a validity date, this mode is only possible with RFID data carriers and not with PIN-code operation.

Information for LEGIC prime systems
For systems with LEGIC prime, the index value is omitted for data carriers.

The customer receives a data carrier encoded with GANTNER locker information. The customer's personal locker number and the expiration date ("valid from" and "valid until") are written onto the authorized data carrier. In addition, an index value is written in the locker information. The "valid from" date must always be valid, i.e., equal to or after the date set in the lock.

Upon first use of a lock, the expiry date ("valid to" date) and the current index value of the data carrier are stored in the lock. The guest can lock and unlock the locker as required, starting from the "valid from" date and for as long as the expiry date is not reached or exceeded.

NOTE! The lock does not adjust to daylight saving time automatically. This must be considered when evaluating events and authorizing data carriers with an expiry date.

An unlimited number [1] of data carriers (users) can use the same locker. The following conditions apply to the data carriers in this mode:
- The same locker number must be stored on the data carriers.
- The same expiry date must be stored on the data carriers.
- The same index value must be stored on the data carriers.[2]

[1] For LEGIC prime systems, the number of usable data carriers is limited to 32, since the lock also stores the unique number of the authorized data carriers.
[2] Not included in LEGIC prime systems. The data carriers are recognized via the locker number and the validity date.

When one of the data carriers assigned to a user is used at the locker for the first time, the expiry date and the index value of the data carrier are transferred to the lock.

NOTE! For LEGIC prime systems, the authorizations are deleted from the data carrier after being transferred to the lock.

Locking and unlocking lockers

► Close the locker door.

► Activate the lock using the data carrier for approximately 1 second.
  - ○ The information on the data carrier is read. The locker number on the data carrier must correspond with the locker number in the lock.

► The following situations are possible. The data carrier ...
  1) … is the first data carrier used at the locker:
     - ○ The index value and the "valid to" date of the data carrier are saved in the lock. The data carrier can lock and unlock the locker until the end of the validity period.
  2) …has the same index value and "valid to" date as stored in the lock:

   - The data carrier is now authorized to lock and unlock the locker like the previously authorized data carriers.

3) …has a higher index value than in the lock:
   - The new index value and the "valid to" date of the data carrier are saved in the lock. The data carriers previously authorized in the lock lose their validity, i.e., they are no longer authorized to use the locker.

4) …has the same index value and a newer "valid to" date than in the lock:
   - The index value and the new "valid to" date of the data carrier are saved in the lock. The data carriers previously authorized in the lock lose their validity, i.e., they are no longer authorized to use the locker.

NOTE! Situation 2) is possible when the locker is locked or unlocked. Situations 3) and 4) are possible with a locked or unlocked locker except when the "PersonalLockerSecureFlag" option is set (see "2.4.12 Configuration settings table"). With this option set, the procedure is only possible with an open (unlocked) locker.

► Release the locker door.

a) Valid data carriers: The locker state will switch, i.e., the locker will open if it was locked or will lock if it was open.

b) Invalid data carriers: The LED flashes red briefly and the lock switches off without carrying out an action.

There is also no unlimited usage period for the locker, i.e., the expiry date must be a valid date (not "0"). If the "valid to" date is exceeded, the locker can no longer be opened using the data carrier except when the "LastOpenAtExpiredDate" option is enabled (see "2.4.12 Configuration settings table"). With this option enabled, the locker can be opened one more time using the data carrier.

NOTE! The PROGRAM data carrier can be used for the setting “Personal locker mode - Expiry date” to reset the index of the lock to 0.

NOTE! The PROGRAM data carrier deletes all stored authorizations from the lock in LEGIC prime systems.

3.7 GAT ECO.Basic Set

The GAT ECO.Basic Set is intended for all GANTNER battery locker locks without CardNET function and OSS Standard Online function. Two GAT ECO.Basic Sets are available to suit the required RFID technology:
- For LEGIC advant: GAT ECO.Basic Set B BA (Part No. 958131)
- For MIFARE DESFire: GAT ECO.Basic Set FD (Part No. 1100550)

The following items are included in the GAT ECO.Basic Set.

System data carriers
- MASTER data carrier (3 pieces, red)
- DELETE MASTER data carrier (orange)
- PROGRAM data carrier (black)
- BATTERY data carrier (blue)
- SERVICE data carrier (yellow)
- APP KEY data carrier (purple)

<u>Additional items included in the Basic Set</u>

- 3 m USB programming cable
- GANTNER USB stick with configuration software
- GANTNER lanyard
- Battery compartment key “GL7p Battery Cover Key”
- Battery compartment key “GAT ECO.Lock 7000 - Battery Key GEA”
- Emergency power adapter “GAT ECO.EPS 7000” (only for the GAT ECO.Lock 7xxx and GAT ECO.Side Lock 7xxx)

<u>Optional data carriers</u>

- OPEN MASTER data carrier

3.8 Summary of system data carriers

The data carriers included in the GAT ECO.Basic Set are required to configure and maintain a locker system equipped with GANTNER battery locker locks.

NOTE!

- The system data carriers are coded to function with specific installations and will only function with the respective system.
- To maintain the security of the locker system, ensure that all system data carriers included in the GAT ECO.Basic Set are kept in a secure location protected from unauthorized use.

3.8.1 MASTER data carrier

With a MASTER data carrier, all locks in a system can be unlocked and locked. If a user's data carrier has been lost, an emergency opening of the corresponding locker can be carried out using a MASTER data carrier. Three MASTER data carriers are included in the GAT ECO.Basic Set, and they are only valid for the respective system.

If a MASTER data carrier is lost, a new MASTER data carrier can be ordered from GANTNER Electronic GmbH. Before using the new MASTER data carrier with a lock for the first time, all "old" MASTER data carriers must first be deleted from the lock using the DELETE MASTER (RESET) data carrier and then all new (or still valid) MASTER data carriers must be saved in the lock. Complete the following procedure:

► Activate the lock using the DELETE MASTER data carrier for approximately 1 second.
  - The information on the data carrier is read and the LED flashes red until the DELETE MASTER data carrier is removed.

► Remove the DELETE MASTER data carrier from the lock.
  - All MASTER data carriers are now deleted from the lock. Next, the LED flashes green and red alternately and the new MASTER data carriers can be programmed.

► Within 5 seconds, activate the lock using the first MASTER data carrier for approximately 1 second.
  - When the data carrier is read correctly, the LED flashes green for 2 seconds.

► Remove the MASTER data carrier from the lock.
  - The LED flashes green and red alternately. The second MASTER data carrier can now be programmed.

► Repeat the process until all MASTER (or also OPEN MASTER) data carriers are programmed.

► If no action occurs after 5 seconds during programming of the MASTER data carriers, the lock automatically returns to the normal operating mode and the new MASTER data carriers are saved in the lock.

3.8.2 OPEN MASTER data carrier (optional accessory)

The OPEN MASTER data carriers can unlock any lock in a system. If a user's data carrier is lost, an emergency opening of the corresponding locker can be carried out using an OPEN MASTER data carrier. Compared to the MASTER data carrier, the OPEN MASTER data carrier cannot lock the locker after it has been opened.

The OPEN MASTER data carrier is not included in the Basic Set and must be ordered separately as required. This data carrier is only valid for the respective system.

An OPEN MASTER data carrier can be used instead of an original MASTER data carrier. To program the OPEN MASTER data carrier into a lock, read the data carrier at the lock. If the max. number of MASTER data carriers (10) are already programmed into the lock, the MASTER data carriers must first be deleted, and the OPEN MASTER data carrier must be programmed together with the required MASTER data carriers (max. total amount of 10).

3.8.3 DELETE MASTER data carrier

The DELETE MASTER data carrier is used to delete all the MASTER data carriers stored in the lock. See section "3.8.1. MASTER data carrier".

3.8.4 PROGRAM data carrier

For locks operating in personal locker mode, the PROGRAM data carrier is used to authorize data carriers so that they can be used with the locker. The PROGRAM data carrier is also used to delete the existing authorizations of personal lockers and can be used for the "Personal locker mode - Expiry date" setting to reset the index of the lock to 0. See section "3.6.4 Personal locker programming card mode".

3.8.5 BATTERY data carrier

After the batteries are replaced in the lock, the lock must be reset to the normal operating mode using the BATTERY data carrier. The internal action counter is reset to zero when the BATTERY data carrier is used. See the "INSTALL" manual of the respective lock for instructions.

NOTE! After replacing the battery of a lock in personal locker mode, all settings stored in the lock remain as previously configured.

3.8.6 SERVICE data carrier

The SERVICE data carrier is used to put the lock into configuration mode after the lock is connected to a computer via USB. See the "INSTALL" manual of the respective lock for instructions. While the lock is in configuration mode, the settings of the lock are configured using GAT ECO Lock Configurator (see "2 CONFIGURATION").

NOTE! The SERVICE data carrier must be available for service technicians who are required to configure the locker system. Without the SERVICE data carrier, system configuration is not possible!

3.8.7 APP KEY data carrier

The APP KEY data carrier is required to configure the lock using the MoLA app. This app can be installed on mobile devices with an Android operating system. When the lock is in factory mode and is being configured for the first time, the APP KEY is not needed. For subsequent configuration changes, the APP KEY data carrier is required (see also "2.3. Configuration with the MoLA App").

ℹ *The APP KEY data carrier is not required to configure a lock using GAT ECO Lock Configurator.*

3.8.8 BLOCKING data carrier (optional accessory)

This data carrier is used to block a locker that has been locked by a user. After reading the BLOCKING data carrier at the lock, the user cannot open the locker anymore. To open the locker, a MASTER or OPEN MASTER data carrier must be used. After the BLOCKING data carrier is read, the automatic open function is also disabled until the lock is opened again using a MASTER or OPEN MASTER data carrier.

The BLOCKING data carrier is not included in the scope of supply but can be ordered as an accessory.

3.9 Signalization overview

Each lock has an LED and an integrated beeper that are used to indicate the following information. Signals that are specific to a lock variant are shown at the end of the table.

LED	Signalization	Meaning
🔵	1 x brief blue flash	Lock activated, ready to read a data carrier
🔵	Permanently on	• Lock has been activated via USB cable but USB communication is not possible • The status remains active for approx. 1½ minutes • Check USB cable, check USB interface on the PC
🔴	• 1 x red flash • Descending signal tone	• No authorization • No data carrier read • Error
🟢	• 1 x green flash • Ascending signal tone	• Data carrier accepted • Operation successful
🟢	• 1 x long green flash • Rising melody	• Battery change confirmed successfully with BATTTERY data carrier • Battery warning reset
🔴 🟢 🔴 🟢 🔴	Fast red / green flashing	Lock is waiting for a data carrier for programming or release (SERVICE, MASTER, user data carrier, etc.)
🔴 🔴 🔴 🔴	• 4 x red flashes • 5 x beeps	Battery change required
🟢 🟢 🟢	Several brief green flashes in succession	Locking activated via app, lock locks automatically when operated
🟢 ◌ 🟢 ◌	Pulsing green LED	USB communication mode active
🔴 🔴 🔴 🔴 🔴	Fast red flashing	• Bootloader active • Firmware can be loaded
🔴 • 🔴 • 🔴 • 🔴	Red flickering	• Firmware is being loaded • Communication to the lock active
GL7p		
✸	• 1 x brief white flash • 1 x beep	Pressing of a PIN-code key detected
GAT ECO.Side Lock		
🔴 🔴 🔴 🔴 🔴	• Continuous red flashing • Continuous high / low tone interval	• Break-in alarm triggered • Acknowledge the alarm using a valid MASTER data carrier

***Table 3.4 –** Overview of signaling*

Note:

This manual is valid as of February 7, 2024. It is subject to change.
Amendments can be made without prior notice at any time!

GLOBAL
PARTNER NETWORK

40+
OFFICES

40,000+
PROJECTS WORLDWIDE

40+ MILLION
USERS DAILY

SCAN FOR CONTACT

Gantner
A SALTO GROUP COMPANY

www.gantner.com

GANTNER reserves the right to change technical specifications,
designs and services without prior notice.

Photos: GANTNER, shutterstock, IMSinteriors, SALTO Systems