

GANTNER Battery Locker Locks OSS Function Manual

GAT ECO.Side Lock



GL7p



GAT ECO.Lock



© Copyright 2023 GANTNER Electronic GmbH

Operating instructions, manuals, and software are protected by copyright. All rights are reserved. Copying, duplication, translation, installation in any electronic medium or machine-readable form in whole or in part is prohibited. The sole exception is represented by creation of a back-up copy of software for own use as a safeguard, so far as this is technically possible and recommended by us. Any infringement will render the party committing such infringement liable to compensation payment.

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

	Indicates a hazardous situation that, if not avoided, may result in minor or moderate injury.
	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.....	9
1.1	About this manual	9
1.2	Chapter overview	9
1.3	Contact & inquiries	9
1.4	Target group	10
1.5	Formatting	10
1.5.1	Safety-critical information	10
1.5.2	General information	10
1.5.3	Instructions and results	10
1.6	Terminology	11
2	GENERAL INFORMATION	13
2.1	Intended use	13
2.2	Functional description	13
2.3	System overview	14
2.4	OSS Standard Offline	15
2.5	RFID technology	15
3	COMMISSIONING	17
3.1	Target group	17
3.2	Activating the RFID reader	17
3.3	Overview of operating modes	18
3.4	Function in installation mode	18
3.4.1	Exiting installation mode	18
3.5	Standalone mode	19
3.5.1	Authorizing data carriers	19
3.5.2	Deleting a user data carrier from a lock	19
3.5.3	Deleting all user data carriers from a lock	20
3.6	GAT DL 300 Master Key Set	21
3.7	Information on the system data carriers	22
3.7.1	PROGRAMMING data carrier	22
3.7.2	DELETE data carrier	22
3.7.3	BATTERY data carrier	23
3.7.4	DEMOUNTING data carrier	23
3.7.5	COMMUNICATION data carrier	23
3.7.6	GAT Passkey Management data carrier	23
3.7.7	Authorization Card and Authorization Erase Card	23
3.8	Programming the Master Key Set into an OSS lock	24
3.9	Reader authorization for LEGIC	26
4	CONFIGURATION	27
4.1	General information	27
4.2	Setup for configuration	28
4.3	Configuring the general lock and RFID settings	30
4.4	OSS configuration	32
4.4.1	Uploading configuration data to a lock	32
4.4.2	Setting/changing the address of an OSS lock	34
4.5	Manual OSS configuration in GAT DL Analyzer	35
4.6	Saving configuration events	37
4.7	Updating the firmware of an OSS lock	37
4.8	Reading events from an OSS lock	38
4.9	Events in the protocol	39
4.9.1	Special events	44

5 OPERATION 45

5.1 Target group..... 45

5.2 Unlocking the locker door 45

5.3 Locking the door..... 45

5.4 Emergency opening of an OSS lock 46

5.5 Resetting an OSS lock..... 46

5.6 Toggle function..... 47

5.7 Passkey management and general key function 48

5.8 Signalization overview 49

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 with OSS Standard Online functionality. The following GANTNER battery locks are covered in this manual:

- GAT ECO.Side Lock 7000 NW BA OSS
- GAT ECO.Lock 7100 NW BA OSS
- GL7p.x30x OSS

In this manual, the terms "lock" and "OSS 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.



Information on the installation and commissioning of the battery locks can be found in a separate manual (see the "INSTALL" manual of the respective lock variant).



Information on the configuration and operation of the battery locks with CardNET functionality can be found in the separate CardNET manual.

1.2 Chapter overview

In chapter 2 "GENERAL INFORMATION" you will find the functional description of the OSS lock and information about the OSS Standard Offline used in the locks as well as the RFID technologies supported by the lock.

In chapter 3 "COMMISSIONING", the instructions for putting the lock into operation and additional information about the battery and the USB connection are available.

In chapter 4 "CONFIGURATION", the configuration instructions for the OSS lock are provided that describe how to configure the lock using the GAT DL Analyzer software. The most important configuration settings for the lock are explained and the configuration process via an OSS file is also described. In addition, instructions on how to update the firmware of an OSS lock and how to save configuration events are available here.

In chapter 5 "OPERATION" you will find an overview of the different operating modes of the OSS lock. The system data carriers available for the locker locking system and the alarm function are also explained in this section.

1.3 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>

1.4 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 may only be performed by the specified target group. Unqualified personnel who perform the described tasks risk personal injury or damaging property/equipment.

1.5 Formatting

1.5.1 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.

1.5.2 General information

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



The text accompanying this symbol contains interesting information relevant to the current chapter. 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.

1.5.3 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.
 - This symbol represents the result after completing the previous instruction.

1.6 Terminology

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

OSS

OSS is an open standard for access control. The standard defines how access authorizations are written to the user data carriers and evaluated at the electronic door locks. See "2.4. OSS Standard Offline" for more information.

User

In this manual, the term "user" refers to the users (persons) who operate (open or lock) a locker with a GANTNER locker lock.

Computer / PC

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

Data carrier

An identification medium (e.g., in the form of a key tag or chip card) with which the users of a system can identify themselves at the GANTNER locker locks. The data carriers are available for different identification systems (LEGIC® advant and MIFARE® DESFire) and must be encoded for use in the OSS system.

System data carrier

Various types of system data carriers are used with the OSS lock for configuration, service, and maintenance. These data carriers have special functionalities and because they are essential for the operation of the OSS lock and have security-critical functions, they must be kept in a secure place protected from unauthorized access. Most of the system data carriers are included in the GAT DL 300 Master Key Set while others can be ordered separately (if necessary or desired).

FID (Company ID) and Site Key

The company ID is a unique identifier for a specific customer installation. Data carriers are linked to the customer installation via the FID, which ensures that data carriers from one installation cannot be used in other installations. In MIFARE systems, a site key is generated from the FID and other information, which makes it possible to transport keys required for operation without knowing the keys.

In OSS systems, the company ID and the site key are only relevant for the system data carriers. All user data carriers in the system have an OSS compatible encoding that does not use the FID.

GAT DL Analyzer

PC software developed by GANTNER that is used to communicate with GANTNER devices such as the OSS locker locks, and to transfer configurations and read out event logs.

Lock / OSS 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.

2 GENERAL INFORMATION

2.1 Intended use

The OSS locker locks described in this manual are intended for the electronic locking of personal lockers in the office areas and changing rooms of company buildings as well as for other comparable applications. Identification at the OSS lock is completed via contactless RFID (Radio Frequency Identification) data carriers. The locks have been specially developed for the OSS Standard Offline in order to operate in systems and with data carriers according to the OSS Standard. For more information, see section "2.4. OSS Standard Offline".

2.2 Functional description

The OSS locker locks are suitable for almost any locker material (wood, HPL, solid plastic, sheet metal) and can be used for both right-hinged and left-hinged doors. The OSS lock is powered by a 3.6 V battery (GAT ECO.Side Lock and GL7p) or three 1.5 V batteries (GAT ECO.Lock).



Information on the installation and technical data of the OSS battery locks is provided in a separate manual (see the "INSTALL" manual of the respective lock variant).

The configuration (e.g., locker number, RFID technology, group setting for authorization check, unlocking time) of the lock is completed via a USB interface using the GAT DL Analyzer software. The configuration settings for the locks (group and individual authorizations) can either be imported via an XML file from an OSS management software or defined directly in GAT DL Analyzer. The configuration data is transferred to the lock via GAT DL Analyzer. The authorizations for the users are defined in the management software and loaded onto the data carriers using read/write stations.

The OSS management software and read/write stations are not supplied by GANTNER, however, any products from OSS compatible suppliers can be used for this purpose.

All actions (events) carried out by the OSS lock are stored internally in a log and can be read out via USB and stored in a file that can be imported into the OSS management software.

Using a locker

To begin using a locker fitted with an OSS lock, the lock must first be set from installation mode to standalone mode by programming the GAT DL 300 Master Key Set into the lock. The OSS mode can then be activated by uploading a configuration file.

To open their locked locker in standalone and OSS mode, the user must read their data carrier at the OSS lock. In the case of the GAT ECO.Side Lock by pressing the door with the data carrier in the area of the LED or, in the case of the GL7p and GAT ECO.Lock, by pressing in the lock button with the data carrier. The OSS lock checks whether the data carrier is authorized to unlock the locker and automatically opens the locker door if it is authorized. In the configuration, it can also be specified that data carriers are recognized even without pressing the door or the lock button. This convenience function reduces the battery life of the locks.

To lock a locker, the user has to read their user data carrier at the lock. Reading a data carrier is done with a GAT ECO.Side Lock by pressing the door shut while simultaneously holding the data carrier to the LED field and with a GL7p or GAT ECO.Lock by pressing the locker button with the data carrier. This can prevent the data carrier from being locked in the locker.

The lock reads the data carrier information and determines on the basis of the user's authorization data whether the user is allowed to use the locker. If the user is authorized, the lock locks the locker door.

Furthermore, the Toggle function can be used to simulate a mechanical key (see "5.6 Toggle function"). With this function, a locker can be locked or unlocked permanently during a certain time period.

2.3 System overview

The following figure shows how the OSS locks are used in an access control system and how authorization data and recorded events and messages from the locks are transmitted.

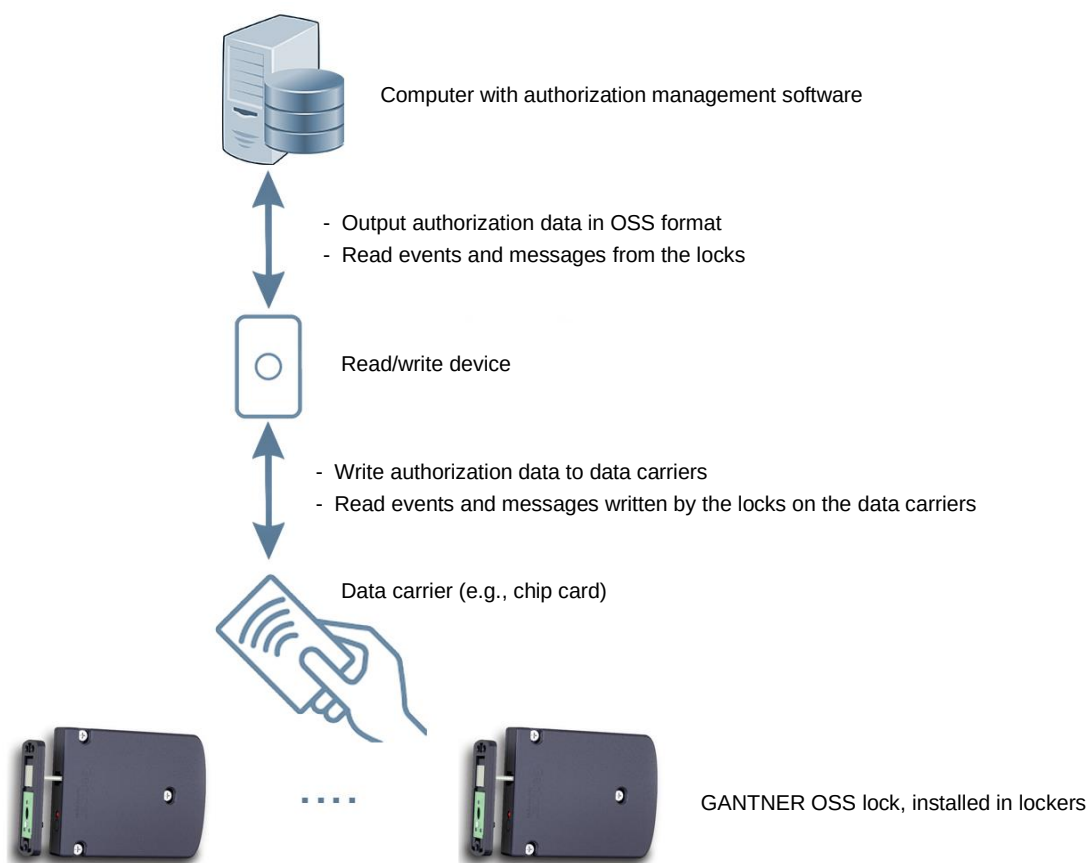


Figure 2.1 – System overview of the OSS locks

2.4 OSS Standard Offline



The OSS Standard Offline is a widely used open standard in access control and defines the format of authorization data for access control using electronic offline locks. The standard is defined by the OSS Association (<https://www.oss-association.com>). This is an open industry forum for manufacturers in the security market and it ensures a permanent exchange between users, security consultants, specialists and executives by providing cooperation platforms for its members.

With the implementation of the OSS Standard Offline, the GANTNER battery locker locks with OSS functionality can be used in many systems with a wide range of OSS compliant authorization management software.

The authorization data is defined in an authorization management software and written to the user data carriers in OSS standard. This means that these data carriers can be read and interpreted by the OSS lock independently of the software used. The lock is then unlocked and locked autonomously on the basis of the read authorizations.

The OSS standard offline data on the data carrier is specified in such a way that the flexibility of access rights in online systems is largely retained. In this way, it is possible to assign many different access rights regardless of the storage space on the data carrier. These access rights are rewritten to the data carrier each time the data carrier is read by an online reader with an "updater" function.

In offline systems, the access rights are stored on the data carriers. To increase security, limited validity periods can be assigned to the access rights. In addition, if a data carrier is lost, it is also possible to restrict the data carrier from using the OSS locks (block list).

The OSS standard allows the storage of numerous access rights for one person. Larger systems can also be divided into sites with the possibility to configure different access rights on the data carrier for each site.

2.5 RFID technology

The reader of the OSS lock is a multi-technology RFID reader that enables data carriers with OSS coding of the RFID technologies LEGIC advant and MIFARE DESFire to be used. These two technologies can be used simultaneously with the OSS lock without the need to reconfigure the lock to use one or the other technology.

In addition to the different RFID technologies, data carriers are available in a variety of shapes and sizes. The OSS locks are designed to operate with a broad range of media types. It must be ensured however that the range of the selected data carrier is large enough for it to be read and written to securely by the lock through the closed locker door.

3 COMMISSIONING

3.1 Target group

This chapter contains information for the technicians responsible for commissioning the OSS lock. A basic understanding of electrical engineering is assumed. Previous knowledge of the OSS lock is not required.

3.2 Activating the RFID reader

To save battery power, the RFID reader of the OSS lock is deactivated in the idle state. In order to read a data carrier, the lock electronics must be activated. Depending on the configuration of the **RFID Wake Up** option, this is completed as follows:

- **RFID Wake Up** enabled: by holding a data carrier in front of the LED or the lock button.
- **RFID Wake Up** disabled:
 - o GAT ECO.Side Lock: by pressing the locker door in.
 - o GAT ECO.Lock and GL7p: by pressing the button of the lock in.

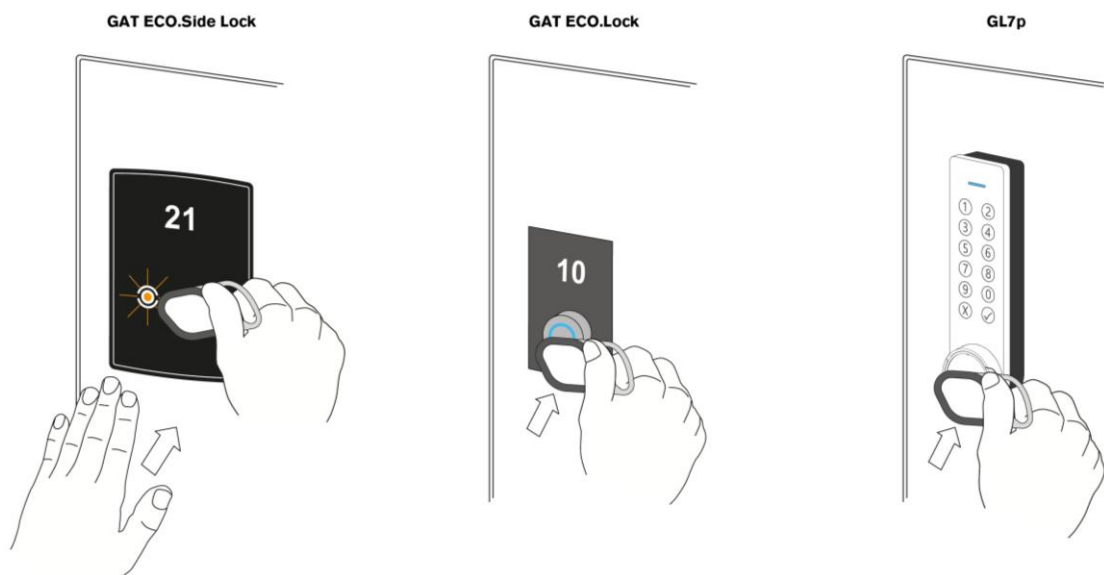


Figure 3.1 – Activating the electronics and RFID reader of the lock



The **RFID Wake Up** option is enabled or disabled during lock configuration in GAT ACE 7000 (see “4.3 Configuring the general lock and RFID settings” for instructions).

3.3 Overview of operating modes

The OSS locks can operate in different modes:

- Installation mode: This is the default operating mode of the lock upon delivery. See "3.4 Function in installation mode".
- Standalone mode: The process of programming the Master Key Set into the lock switches the lock from installation mode to standalone mode. In this mode, only the unique number of the data carriers is used for the authorization check. Programming and authorization assignment are performed directly at the lock.
- OSS mode: From standalone mode, the lock can be set to OSS mode by configuring the lock via the USB interface and the GAT DL Analyzer software. This manual specifically describes OSS mode and the configuration can be found in chapter "4 CONFIGURATION".
- CardNET mode: The OSS lock can also be set from stand-alone mode to CardNET mode by configuring the lock via the USB interface. In this mode, the lock can be operated with GANTNER data carriers in CardNET mode. A detailed description of this mode can be found in the manual "GANTNER Battery Locker Locks CardNET Function".

3.4 Function in installation mode

In the default state, the lock is set to 'installation mode'. In this mode, the lock can be locked by simply pressing it shut and unlocked again with any data carrier (provided a suitable RFID technology is used).

NOTE! Installation mode is intended for installation and commissioning but not for regular use!

In order to configure the lock, it must be first set to standalone mode

3.4.1 Exiting installation mode

To end the installation mode of a lock, the Master Key Set must be programmed into the lock. The exact process is described in section "3.8. Programming the Master Key Set into an OSS lock". After the Master Key Set is programmed into the lock, the lock is in standalone mode (see "3.5 Standalone mode").



The Master Key Sets are only valid for the matching installation.

The lock can then still be locked by pressing the locker door shut or pressing the lock button in. To open the locker, an authorized data carrier or the "PROGRAMMING" and "DEMOUNTING" system data carriers are required (see "3.7. Information on the system data carriers").

3.5 Standalone mode

In standalone mode, user data carriers can be programmed into the lock using the "PROGRAMMING" system data carrier, after which the data carriers can open and lock the locker. The only requirement is that the data carriers are of one of the supported RFID types. Special programming is not necessary.



The OSS lock can continue to operate with the basic functionality in standalone mode.

3.5.1 Authorizing data carriers

To authorize user data carriers in standalone mode, proceed as follows.

- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - Two short beeps are emitted and the LED flashes green and red alternately.
- ▶ Remove the PROGRAMMING data carrier from the reading field, wait 1 second, and then hold the PROGRAMMING data carrier in front of the reading field again.
 - Two short beeps are emitted and the LED flashes green.
- ▶ Remove the PROGRAMMING data carrier from the reading field.
- ▶ Hold the data carrier to be authorized in front of the reading field.
 - One short beep is emitted and the LED continues to flash green.
 - The data carrier has now been authorized for the lock.
- ▶ To authorize another data carrier, hold it in front of the reading field as in the previous step. In this way, several data carriers can be authorized for the lock.
- ▶ To complete the programming, hold the PROGRAMMING data carrier in front of the reading field again.
- ▶ Two short beeps are emitted and the LED switches off.
 - Programming mode ends, and the data carriers can now be used to open and lock the locker.

3.5.2 Deleting a user data carrier from a lock

If you want to remove the authorization of a user data carrier from a lock (i.e., to withdraw the user's authorization for the locker), complete the following steps.



To delete an individual data carrier from a lock, it must be physically available. If not, all data carriers must be deleted (see next section).

- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - Two short beeps are emitted and the LED flashes green and red alternately.
- ▶ Remove the PROGRAMMING data carrier from the reading field, wait 1 second, and then hold the PROGRAMMING data carrier in front of the reading field again.
 - Two short beeps are emitted and the LED flashes green.
- ▶ Remove the PROGRAMMING data carrier from the reading field and hold the DELETE data carrier in front of the reading field.
 - Two short beeps are emitted and the LED flashes red.
 - Delete mode is now active.
- ▶ Hold the data carrier to be deleted in front of the reading field.

- One short beep is emitted, and the data carrier is deleted. It is now no longer authorized for the lock.
- ▶ You can delete further data carriers if necessary. To do this, hold the additional data carrier(s) briefly in front of the reading field in delete mode until a beep can be heard.
- ▶ To end delete mode, hold the PROGRAMMING data carrier in front of the reading field again.
- ▶ Two short beeps are emitted, and the LED switches off.
 - Delete mode ends, and the data carriers are now no longer authorized to open and lock the locker.

3.5.3 Deleting all user data carriers from a lock

It is possible to delete all authorized data carriers from a lock in one step, after which they no longer have authorization. This step is helpful or necessary if one or more data carriers have been lost and are no longer physically available to be deleted individually. Complete the following steps.

- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - Two short beeps are emitted and the LED flashes green and red alternately.
- ▶ Remove the PROGRAMMING data carrier from the reading field, wait 1 second, and then hold the PROGRAMMING data carrier in front of the reading field again.
 - Two short beeps are emitted and the LED flashes green.
- ▶ Remove the PROGRAMMING data carrier from the reading field and hold the DELETE data carrier in front of the reading field.
 - Two short beeps are emitted and the LED flashes red.
 - Delete mode is now active.
- ▶ Remove the DELETE data carrier from the reading field, wait 1 second, and then hold the DELETE data carrier in front of the reading field again.
 - Two short beeps are emitted and the LED continues to flash red.
- ▶ Remove the DELETE data carrier from the reading field, wait 1 second, and then hold the DELETE data carrier near the reading field again.
 - A long beep will sound and the LED is switched off.
 - All previously authorized user data carriers are now deleted from the lock and can no longer use the locker. You can now authorize new user data carriers in the lock as described previously.

3.6 GAT DL 300 Master Key Set

The GAT DL 300 Master Key Set contains the following system data carriers in the form of RFID chip cards. These system data carriers can be used to perform important system functions on a OSS lock.

System data carriers:

- PROGRAMMING data carrier



- BATTERY data carrier



- DELETE data carrier



- WINET data carrier



- DEMOUNTING data carrier



Optionally available data carriers:

- COMMUNICATION data carrier



The GAT DL 320 340 demo kit also contains these system data carriers.

3.7 Information on the system data carriers

The system data carriers are intended for the configuration and maintenance of a locker system equipped with OSS locks from GANTNER. The system data carriers (PROGRAMMING, DELETE, BATTERY, DEMOUNTING) required for operation are included in the GAT DL 300 Master Key. Further system data carriers are optionally available.



The system data carriers are system-specific and therefore only function with the respective system.

NOTE! The system operator must ensure secure storage of the system data carriers, protected against unauthorized usage!

3.7.1 PROGRAMMING data carrier

The PROGRAMMING data carrier can be used to perform important actions on an OSS lock. These include:

- Program system data carriers into a lock
- Program the GAT Passkey Management Card into a lock
- Exit installation mode and activate standalone mode
- Authorize user data carriers in a lock in standalone mode
- Reset lock
- Reset battery warning after battery change
- Unlock or lock the lock (in combination with the DEMOUNTING data carrier)

In addition, the PROGRAMMING data carrier can be used to set a lock to communication mode as soon as the lock is connected to a computer via USB (see "4.2 Setup for configuration"). The settings of the lock are configured using the GAT DL Analyzer software while the lock is in communication mode (see chapter "5 OPERATION").

NOTE! The PROGRAMMING data carrier must be available for service personnel configuring the locker system. Without the PROGRAMMING data carrier, system configuration is not possible!

A COMMUNICATION data carrier can also be used to operate a fully configured OSS system. This allows the PROGRAMMING data carrier to remain in a secure environment.

3.7.2 DELETE data carrier

The DELETE data carrier can be used to reset a lock. This resets the lock address to zero and deletes the data in the lock. See section "5.5. Resetting an OSS lock".

In addition, this data carrier can be used to delete all authorized data carriers in the lock.

The DELETE data carrier is also required to exit installation mode and activate standalone mode.

3.7.3 BATTERY data carrier

After a battery change, the lock is in battery change mode and must be reset to the normal operating mode using the BATTERY data carrier. The battery warning is reset with the BATTERY data carrier. For instructions, please refer to the installation manual of the respective lock.



When the battery of a lock is changed, the authorizations stored in the lock are not lost.

The BATTERY data carrier is also required to exit installation mode and activate standalone mode.

3.7.4 DEMOUNTING data carrier

The DEMOUNTING data carrier can be used to unlock any lock in the associated system in order to unlock the locker in question. To do this, proceed as follows:

- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - The LED flashes alternately red/green.
- ▶ Remove the PROGRAMMING data carrier from the reading field and read the DEMOUNTING data carrier.
 - The LED lights up green briefly and the lock is unlocked, allowing the locker door to be opened.

3.7.5 COMMUNICATION data carrier

With the optional COMMUNICATION data carrier, a lock can be set to communication mode (see "4.2 Setup for configuration"). This has the advantage that the PROGRAMMING data carrier, which has security-relevant functions and must be stored securely, does not have to be used and can remain in a secure storage location.

In order to use the COMMUNICATION data carrier, it must be programmed into the lock using a PROGRAMMING data carrier.

3.7.6 GAT Passkey Management data carrier

This is an optional data carrier available from GANTNER (Part No. 496738), which is used to program the master data carriers and fire brigade data carriers into a lock. For more details on this function, see "5.7. Passkey management and general key function".

3.7.7 Authorization Card and Authorization Erase Card

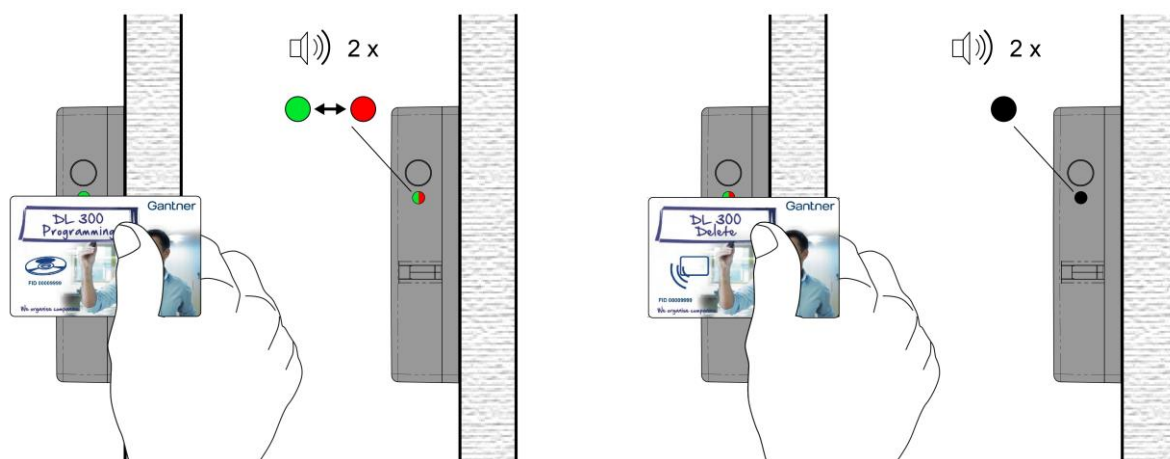
The Authorization Card is an optional data carrier that is used to authorize the reader of a lock for LEGIC operation so that LEGIC data carriers can be used. The optional Authorization Erase Card can be used to cancel this authorization. For more details on this function, see "3.9. Reader authorization for LEGIC".

3.8 Programming the Master Key Set into an OSS lock

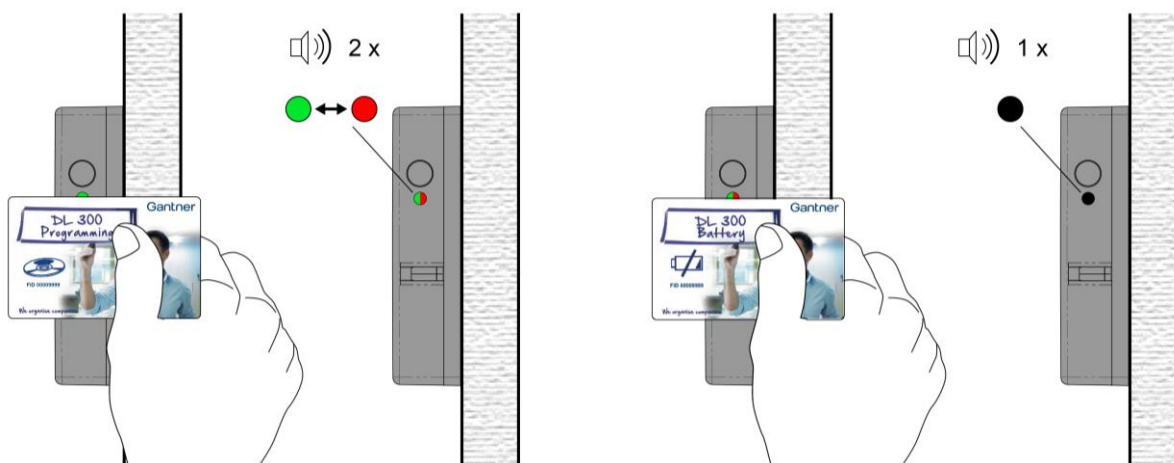
In order to use the data carriers of the Master Key Set with an OSS lock, they must be programmed once into the lock after delivery. This process is described below using a GAT ECO.Side Lock OSS. The procedure is identical for the GAT ECO.Lock and GL7p.

NOTE! The process of programming the Master Key Set into a lock after delivery disables the default installation mode and sets the lock to standalone mode.

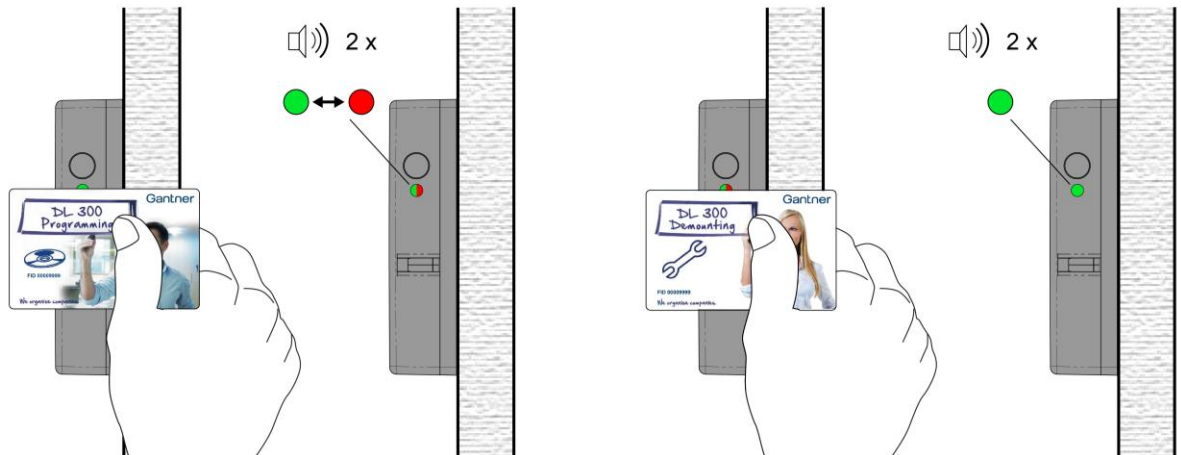
- ▶ Activate the lock. If the toggle function is not enabled, keep the door pressed shut.
 - The lock is activated and the LED lights up.
- ▶ Hold the PROGRAMMING and DELETE data carriers against the reading field (LED) in the following order:



- The PROGRAMMING and DELETE data carriers are now stored in the lock.
- ▶ Release the locker door.
 - The locker door remains locked.
- ▶ Press the locker door in and keep it pressed.
 - The lock is activated and the LED lights up.
- ▶ Hold the PROGRAMMING and BATTERY data carriers against the reading field (LED) in the following order:



- The BATTERY data carrier is now stored in the lock.
- ▶ Release the locker door.
 - The locker door remains locked.
- ▶ Press the locker door in and keep it pressed.
 - The lock is activated and the LED lights up.
- ▶ Hold the PROGRAMMING and DEMOUNTING data carriers in front of the reading field (LED) in the following order:



- The locker door is then unlocked.
- ▶ The other optional system data carriers (e.g., COMMUNICATION data carrier, GAT Passkey Management data carrier) can be programmed into the lock in the same way.

3.9 Reader authorization for LEGIC

In order for an OSS lock to use LEGIC data carriers, the LEGIC reader in the lock must be authorized. This enables the reading of authorizations from the data carriers and the writing of events and battery warnings to the data carriers. The authorization process requires the authorization card ("GAT Authorization Tag 400 BA"), which can be ordered from GANTNER when using GANTNER data carriers. When using data carriers from other manufacturers, please contact the corresponding manufacturers.



No reader authorization is required for reading and writing MIFARE and MIFARE DESFire data carriers.

The authorization process is possible from firmware version 2.0 or higher (GAT ECO.Side Lock) or version 1.0 or higher (GAT ECO.Lock and GL7p) and functions as follows:

Authorizing the reader

- ▶ Activate the lock (see Figure 3.1) with the authorization card. Depending on the **RFID Wake Up** setting, the lock reads the card automatically or must be activated by briefly pressing the locker door or the lock button in.
 - The LED flashes 5 x red/green alternately and 5 ascending tone signals are emitted.
 - After this signalization (approx. 3 seconds), the authorization data is stored in the lock and the authorization is thus completed.

Deleting the authorization of the reader

To cancel an authorization and delete the authorization data, the OSS lock must be reset to the default settings.

- ▶ Activate the lock (see Figure 3.1) with the PROGRAMMING data carrier and then the DELETE data carrier five times to reset the lock to the default settings (see "5.5. Resetting an OSS lock").
 - The authorization of the LEGIC reader is deleted.

NOTE! This process also deletes all authorizations and configurations from the lock!

4 CONFIGURATION

4.1 General information

Before the main configuration of the OSS locks can be completed, the system data carriers must be programmed into the lock as explained in chapter “3 COMMISSIONING”. For further information, see section “3.7 Information on the system data carriers”.

In general, there are 2 possibilities for configuring an OSS lock:

1. Configuration via an OSS file: A configuration file in XML format containing the configuration settings according to the OSS specifications. This file can be loaded into a lock using GAT DL Analyzer.
2. Manual configuration. Here the settings for a lock can be defined manually in GAT DL Analyzer and uploaded to the lock. The configuration also corresponds to the OSS format.



After configuring the first lock, carry out a test to confirm that the data carriers (system data carriers and standard user data carriers) are read by the lock successfully and that the lock operates as expected.

During configuration, the following data is transferred to the lock:

- System number (SiteID)
- ID number (lock address)
- Option “RFID wake up” enabled or disabled
- Automatic summer/winter time changeover enabled or disabled
- Beeper on/off
- Option “break-in alarm” enabled or disabled
- Operating mode: OSS
- Date and time (automatically set)
- Settings for the RFID reader (read/write keys, LEGIC stamps, etc.)
- Unlocking time
- Group authorizations

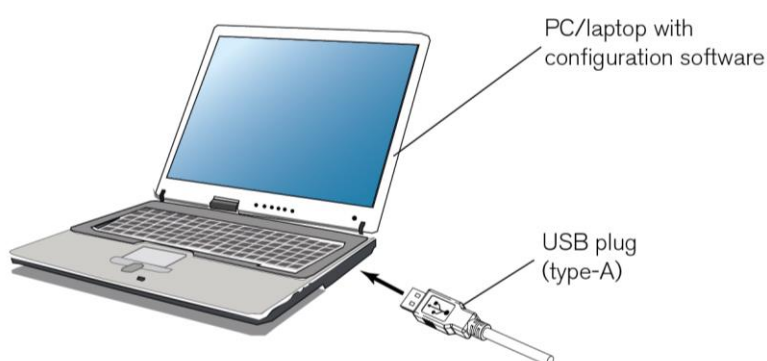
NOTE! The OSS lock can automatically switch between summertime and wintertime! This option can be enabled or disabled when configuring the OSS lock. Whether the summer/wintertime changeover is carried out must be considered when evaluating the bookings as well as when authorizing data carriers that have a validity date.

4.2 Setup for configuration

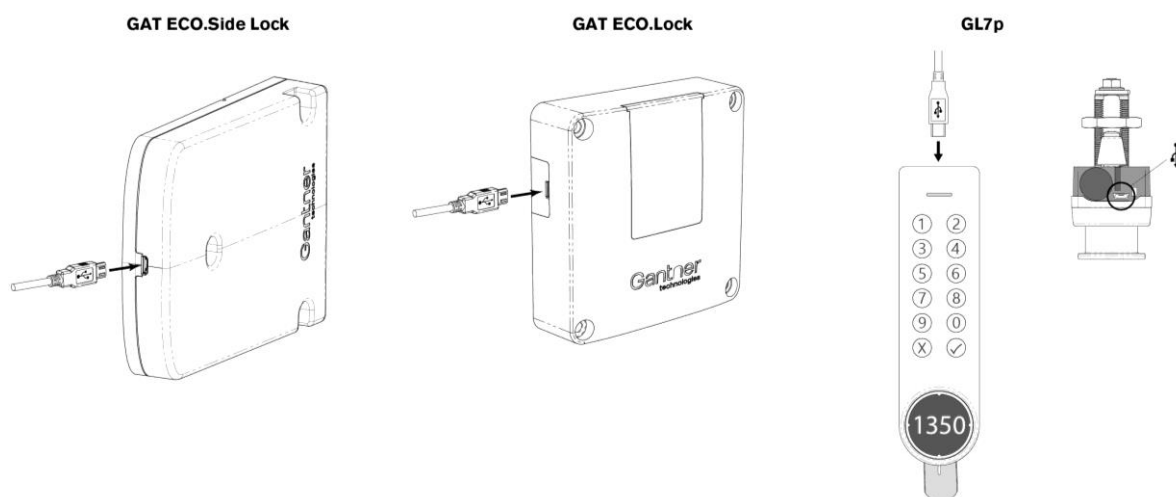
The GAT DL Analyzer software is used to configure an OSS lock. To connect to a computer with a Windows® operating system (Windows® 7 and higher) there is a Micro-B USB port on the lock.

i GAT DL Analyzer is only available in German; however, the operation is straightforward using the translations provided in the following sections. Only the menus **Analyse**, **OSS Sync**, and **Firmware Update** are required for configuring an OSS lock.

- ▶ Start the GAT DL Analyzer software on the PC/laptop (the software is portable and does not have to be installed).
- ▶ Plug the end of the USB cable (plug type A) into a free USB port on the computer.



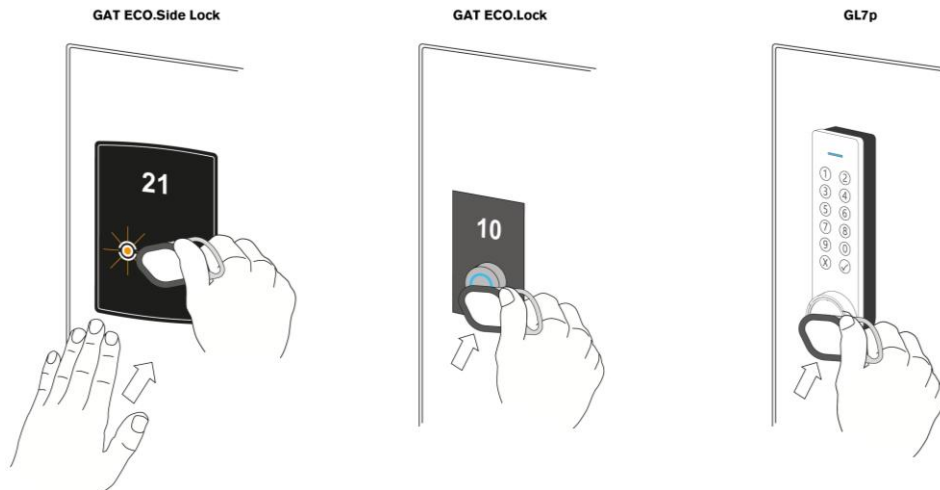
- ▶ Plug the Micro-B connector of the USB cable into the USB port of the lock. This is done as follows for the different OSS locks:



- ▶ When a lock is connected to the computer for the first time, the driver is installed and the lock is then detected correctly in Windows.

i If the automatic driver installation does not work and you need the driver, you can download it from the GANTNER website (login required) by searching for "USB driver".

- To set the lock into communication mode, activate the lock using the PROGRAMMING data carrier or COMMUNICATION data carrier. See section “3.6. GAT DL 300 Master Key Set”.



- The lock switches to communication mode and the status LED pulses green every 2 seconds.
- The COM port to which the lock is connected is displayed with green text at the bottom of the GAT DL Analyzer window in the status bar.

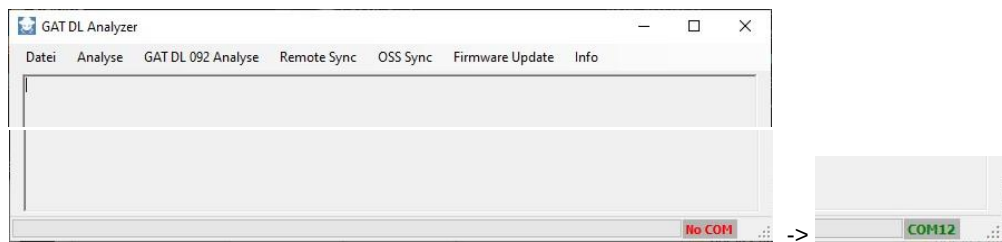


Figure 4.1 – GAT DL Analyzer – Connection to a lock

ATTENTION!

- **GAT ECO.Side Lock / GAT ECO.Lock:** Because the battery of these locks is discharged when connected via USB, unplug the USB cable as soon as the configuration is finished. The battery life is greatly reduced if the lock remains connected via USB for an extended time.
- **GL7p:** The GL7p locks are powered by the USB cable so the battery does not need to be inserted in the lock during configuration. However, ensure that the lock is not without power for more than 1 minute (e.g., after disconnecting the USB cable until the battery is inserted).

4.3 Configuring the general lock and RFID settings

The following settings can be configured in GAT DL Analyzer and then used for all locks that require the same configuration.

i The GAT DL Analyzer software is only available in German; however, the operation is straightforward using the translations provided in the following instructions.

- In GAT DL Analyzer, click on the **Einstellungen** (settings) option in the **OSS Sync** menu.
 - The OSS settings window opens.

Oss Einstellungen

Allgemeine Einstellungen

Automatische Beladung	☒ Ja
RFID Wake Up	☒ Ja
Automatische Sommer-/Winterzeitschaltung	☒ Ja
Silent Mode	☐ Ja
Break-In Alarm (nur bei ECO Side Locks unterstützt)	☐ Ja

RFID Technologien

Legic Prime	☒ Aktiviert	ISO 14443B	☐ Aktiviert
ISO 15693	☒ Aktiviert	Inside	☐ Aktiviert
ISO 14443A	☒ Aktiviert	FelCa	☐ Aktiviert

Legic RFID Einstellungen

Stamp	00000000000000000000000000000000
Stamp Länge	0

DESFire RFID Einstellungen

Application Id	000000
Read Key Number	0
Write Key Number	0
Encryption Mode	2K3DES_DF4
File Communication Mode	Plain
Key Source	Gantner Key Set
Gantner Key Set	

Abbrechen Übernehmen

Figure 4.2 – General OSS settings for the configuration of the locks

The following settings are available here.

Allgemeine Einstellungen (General settings)

- Automatische Beladung (Automatic loading):

Automatic loading can be enabled here. This allows previously selected configurations to be transferred automatically when a lock is connected (see "4.4.1. Uploading configuration data to a lock").

- RFID Wake Up:

If this option is enabled, the lock continuously checks whether a data carrier is within the reading field. As soon as a data carrier is held in front of the lock, it is read. If this option is not enabled, the locker door or the lock button (depending on the lock type) must be pressed in to activate the lock and read the data carrier.

- Automatische Sommer-/Winterzeitschaltung (*automatic summer-/wintertime change*):
If this option is enabled, the lock automatically switches internally between summertime and wintertime.
- Silent Mode:
When this option is enabled, the acoustic signal generator (beeper) in the lock is switched off. No more acoustic signals are then emitted.
- Break-In Alarm:
Note: This option is only possible with the GAT ECO.Side Lock.
If enabled, an alarm is generated if the locker door is opened without a valid identification occurring before. With the option disabled, no alarm is activated for this case. An activated break-in alarm can be deactivated using the PROGRAMMING data carrier.
Note: Deactivating the break-in alarm function extends the battery life.

RFID Technologien (RFID technologies)

Here you can select the technologies to be read by the lock.



Only the settings ISO 14443A (MIFARE DESFire and LEGIC) and ISO 15693 (LEGIC) are relevant for OSS mode.

Legic RFID Einstellungen (Legic RFID settings)

Note: This information must be provided by the data carrier supplier.

- Stamp: This is the segment identifier for LEGIC systems.
Example: 1A22000A0B0B0B
- Stamp Länge (*Stamp length*): Length of the stamp in bytes.

DESFire RFID Einstellungen (DESFire RFID settings):

Note: This information must be provided by the data carrier supplier.

- Application Id: The system- and application-specific ID number for reading MIFARE data carriers is entered here.
Example: F48B20
- Read/Write Key Number: Number of the read and write keys.
- Encryption Mode: Encryption method used for reading data carriers.
- File Communication Mode: Encryption mode for communication:
 - Plain: No encryption
 - MACed: MAC encrypted
 - Enciphered: encrypted
- Key Source: Here you can select how the key is used for reading and writing the data carriers:
 - Gantner Key Set: The Gantner Key Set is a method for storing the keys for accessing the data of a data carrier in an encrypted way in the lock. Please contact GANTNER or your sales partner for this information. It can then be entered in the **Gantner Key Set** field.
 - AES Key: If this setting is used, the read or write key can be entered directly in the **AES Key** field.

- After entering the information, click on **Apply**.
 - The window closes and the settings are transferred to the locks when configuring locks in the future. The settings can always be changed later if required.

4.4 OSS configuration

A configuration in OSS format is created, for example, in your OSS authorization management software, in which the lock authorizations of the users are managed. The XML file containing the OSS configuration can be transferred to a lock as follows to apply the configuration data.

If your OSS authorization management software cannot create this file, you can also manually create a configuration for one or more locks in GAT DL Analyzer (see "4.5. Manual OSS configuration in GAT DL Analyzer") and save it as an OSS file. This file can then also be loaded into the corresponding locks as described below.

4.4.1 Uploading configuration data to a lock

- Click on **Konfiguration einspielen** in the **OSS Sync** menu.

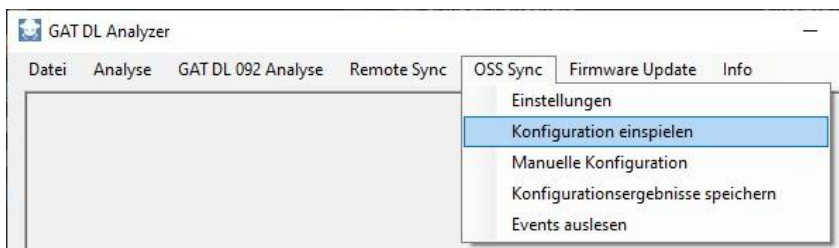


Figure 4.3 – Menu item for loading the OSS configuration into a lock

- A file explorer window opens.
- Select the XML file with the desired OSS configuration in the window.
- The loading window opens.

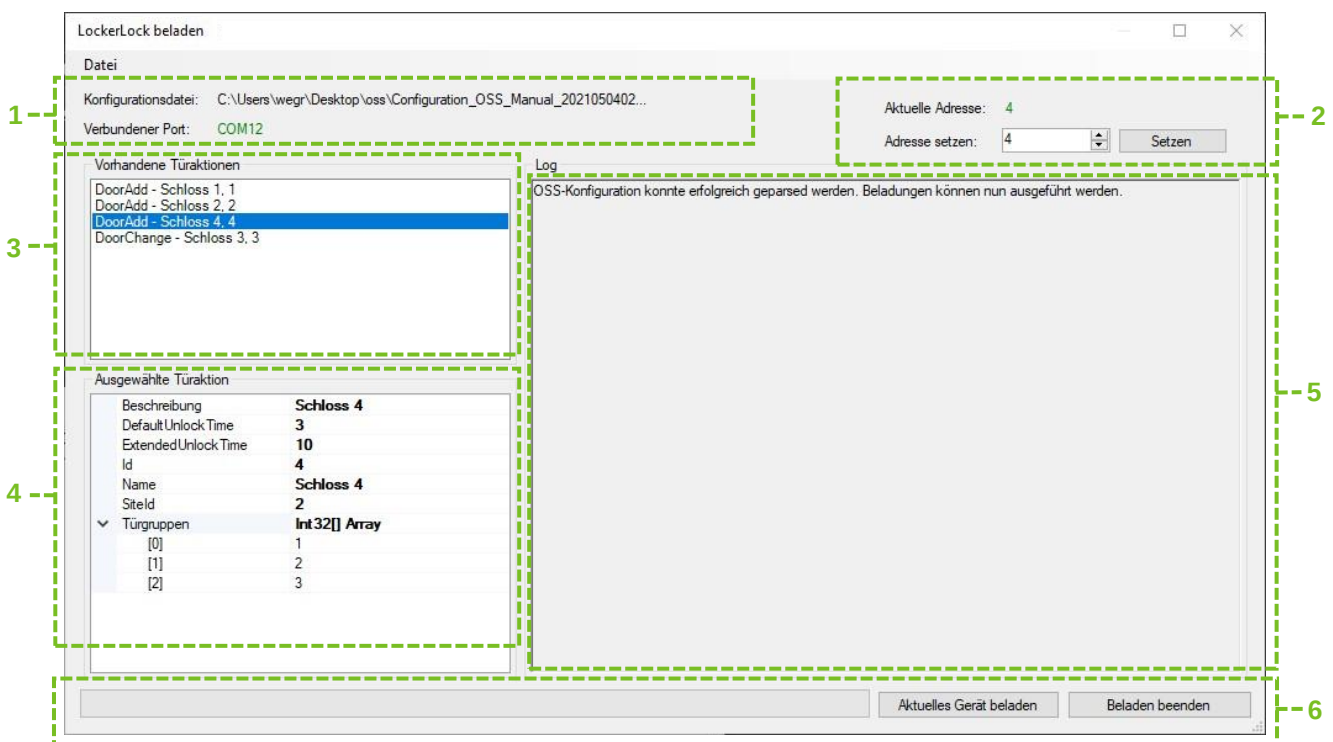


Figure 4.4 – Loading window

The content of the loaded configuration file is displayed here. The window is divided into the following areas:

- | | | |
|---|--|---|
| 1 | Info: | Here you see the opened configuration file and the serial COM port to which the lock is connected below. A COM port number in green color indicates that the lock is connected and ready for communication. |
| 2 | Adresse (Address): | Here you can see the address or locker number of the currently connected lock. You can also change the number directly here (see below). |
| 3 | Vorhandene Türaktionen:
(Existing door actions) | All locks contained in the opened configuration file are listed here. Behind each lock is the number of the lock. Here you can also see whether the configuration for a lock has been newly created (DoorAdd) or whether the configuration for an existing and configured lock has been changed (DoorChange). |
| 4 | Ausgewählte Türaktion:
(Selected door action) | <p>The configuration data of the lock selected in the above list is displayed.</p> <ul style="list-style-type: none"> - Beschreibung (Description): Designation of the lock in the configuration (only for info - text is not transferred to the lock). - DefaultUnlockTime: Unlocking time in seconds. - ExtendedUnlockTime: Extended unlocking time in seconds. - Id: Address or locker number of the lock. - Name: Display name of the lock (only for information - text is not transferred to the lock). - SiteId: Site number stored in the lock. Must match the site numbers of the data carriers used. - Türgruppen (Door groups): The data carriers of the users can be authorized for individual locks or also for groups of locks. Click on the > symbol to display the numbers of the door groups to which the lock is assigned. |
| 5 | Log: | This window displays all actions performed by the software. |
| 6 | Footer: | <p>Here you can see the status bar with progress display, e.g., of a loading process.</p> <p>You can use the buttons to manually start (Aktuelles Gerät beladen) and stop (Beladen beenden) the transfer of data to a lock.</p> <p>NOTE! If automatic loading is enabled (see "4.3. Configuring the general lock and RFID settings"), the Aktuelles Gerät beladen button is not displayed.</p> |

If automatic loading is enabled

- The configuration data is automatically sent to a lock as soon as it is connected and recognized by GAT DL Analyzer. The configuration with the matching address (same number as the lock) is then automatically used and transferred to the lock.

If automatic loading is not enabled, complete the following steps

- To transfer a configuration to the connected lock, select the lock in the list (2) **Vorhandene Türaktionen**.
- Click on **Aktuelles Gerät beladen** or double-click on the lock in the lock list (2).

NOTE! To load the configuration into an existing lock, select the lock with the same address/number that is currently connected. If you select a lock with a different address, the configuration is transferred and at the same time the address of the connected lock is also set to the selected address.

- The configuration data is sent to the lock.
- You can see the actions carried out in the **Log** window (5).

- All locks that have been uploaded with a configuration are marked with a tick and displayed in green.

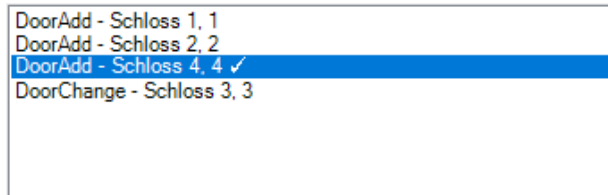


Figure 4.5 - Configuration upload complete for lock no. 4

- Click on **Beladen beenden** to end the loading process.

4.4.2 Setting/changing the address of an OSS lock

In the default state, the address, i.e., the locker number, of an OSS lock is set to zero. To set the address, proceed as follows. You can also use these instructions to change the address of a lock that has already been set.

- In the **OSS Sync** menu, click on **Konfiguration einspielen**.
 - A file explorer window opens.
- Select the XML file with the OSS configuration in the window.
 - The loading window opens.
- Connect the lock to the PC.
 - If the connection is active, the serial COM port is displayed in green on the left under **Verbundener Port** and the current address of the connected lock is displayed on the top right next to **Aktuelle Adresse**.



Figure 4.6 – Loading window

- To change the address, enter the desired new address into the **Adresse setzen** field and click on **Setzen**.
 - The address is changed in the lock and the new address is displayed next to **Aktuelle Adresse**. In the **Log** window you can see notifications indicating whether the setting was successful.

4.5 Manual OSS configuration in GAT DL Analyzer

GAT DL Analyzer offers the possibility to define the configuration settings of an OSS lock and to transfer them directly to the locks. However, the settings can also be saved in an OSS file, which is then transferred to the locks in a second step (see previous section).

i The recommended procedure is to first save the configuration in an OSS file and then transfer it to a lock.

- In the **OSS Sync** menu, select the option **Manuelle Konfiguration** (manual configuration).



Figure 4.7 – Option for manual configuration

- The window **OSS Schlösser manuell beladen** opens.

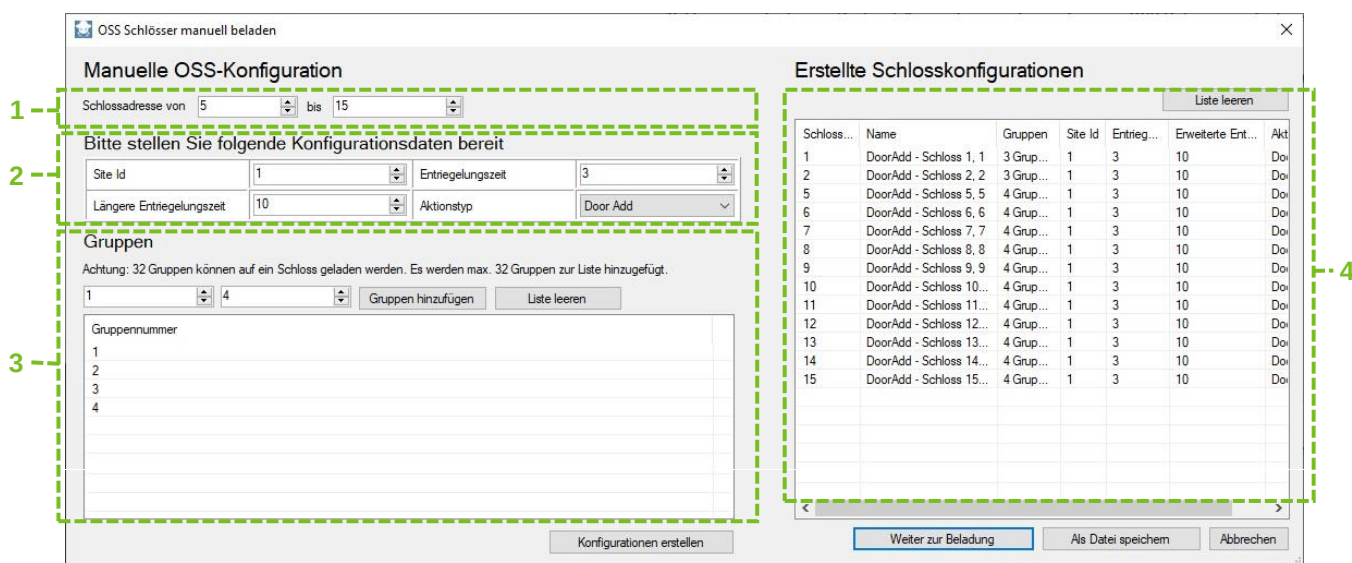


Figure 4.8 – Manual OSS configuration

Configuration is done on the left and the configurations created are listed on the right:

- | | | |
|---|--|--|
| 1 | Schlossadresse:
(Locker address) | Start and end addresses of the locks for which the configuration is being created. |
| 2 | Konfigurationsdaten:
(Configuration Data) | Configuration settings for the locks (see below). |
| 3 | Gruppen:
(Groups) | Numbers of the groups that are loaded into the lock. With groups, the authorizations of the data carriers or users can be determined according to the settings in the authorization management software. |
| 4 | Schlosskonfigurationen:
(Lock Configurations) | The locks for which a configuration has been created are listed here. |

- ▶ In the fields **Schlossadresse von** and **bis** (*lock address from - to*), enter the start and end addresses of the locks that will share the same configuration settings.
 - ▶ Edit the settings for the locks:
 - Site Id: Site number where the locker locks are operating. Only data carriers with the same SiteID can be used.
 - Entriegelungszeit (*Unlocking Time*): Duration in seconds that the lock unlocks the locker after a valid identification.
 - Längere Entriegelungszeit (*Longer Unlocking Time*): The longer unlocking time allows longer releases of a lock to enable persons with a handicap to open the door. Due to the design of the GANTNER OSS locks, this time is not relevant.
 - Aktionstyp (*Action type*): Here you can define whether to configure the settings for a new lock (**Door Add**) or to change an existing lock configuration (**Door Change**).
 - ▶ Add the group numbers to be loaded into the locks in the **Gruppen** (*groups*) area. To do this, define the number range by entering the first number in the left field and the last number of the number range in the second field and click on **Gruppen hinzufügen** (*add group*). You can add a single group number by entering the same number in both fields.
- Note:** A total of 32 groups can be authorized per lock.
- ▶ To add different number ranges and individual numbers, repeat the previous step accordingly.
 - Data carriers authorized for the group numbers in the list can then unlock/lock the locks.
 - ▶ Click on **Liste leeren** (*empty list*) to delete the entered numbers again.
 - ▶ Click on **Konfigurationen erstellen** (*create configurations*).
 - A configuration with the defined settings is created for each of the locks with the selected lock addresses and added to the list on the right (4).
 - ▶ To configure additional locks, enter the lock address or the address range into the **Schlossadresse von - bis** fields, define the settings as described in the previous steps, and add these locks to the lock configuration list via the **Konfigurationen erstellen** button.

Saving the configuration as file

- ▶ It is recommended to save the configurations of the locks displayed in the list in OSS format to an XML file. To do so, click on **Als Datei speichern** (*save as file*).
 - A file explorer window opens where you can specify the folder to which the file is to be saved.
- ▶ The OSS file can be loaded into the locks as described in "4.4.1. Uploading configuration data to a lock".

Uploading the configuration directly to locks

- ▶ The list of configurations can be loaded directly to the locks by clicking on **Weiter zur Beladung** (*continue to loading*).
 - The **Schloss beladen** (*load lock*) window opens. Here you can upload the configuration to the locks as described in section "4.4.1. Uploading configuration data to a lock".

4.6 Saving configuration events

All configuration settings loaded into a lock are logged in GAT DL Analyzer. These logs can be saved in any folder for backup purposes or evaluation, and to re-synchronize the events with the management software.

- In GAT DL Analyzer, select the option **Konfigurationsergebnisse speichern** (save configuration events) from the **OSS Sync** menu.



Figure 4.9 – Option for saving configuration events

- The logs are moved as XML files to the directory of the GAT DL Analyzer software.
- The actions performed, e.g., the path that the files were moved to, are displayed in the application window.

4.7 Updating the firmware of an OSS lock

Updating the firmware in a lock can add new functions or solve issues. Ask your sales partner or GANTNER for a new firmware version.

NOTE! The firmware update is only supported in open locker state.

- Connect the respective lock to the PC (see "4.2 Setup for configuration").
- Ensure that the locker door is open, i.e., the lock is unlocked. The door bolt must not be engaged in the lock.
- Select the option **GAT Locker Lock > Firmware laden** from the **Firmware Update** menu.

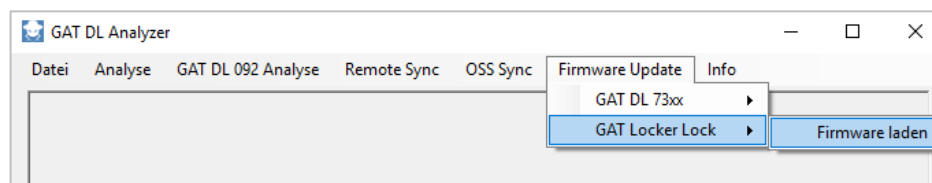


Figure 4.10 – Option for updating the firmware

- A file explorer window opens
- Select the firmware file (file extension. enc) for the respective lock variant.
 - The firmware file is uploaded to the lock. The progress of the loading process is displayed in the window of GAT DL Analyzer.

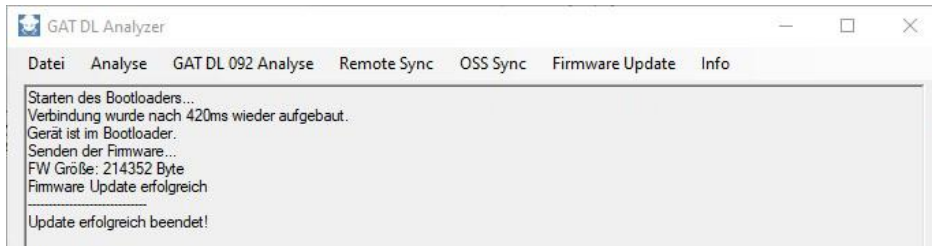


Figure 4.11 – Results of the firmware update

- During the update, the lock LED illuminates red.
- When the firmware has been successfully loaded, the message "Update erfolgreich beendet!" (*update successfully completed*) is displayed in the info window of GAT DL Analyzer.
- The LED continues to pulse green as long as the lock remains connected to the PC.

4.8 Reading events from an OSS lock

An OSS lock internally stores events such as the setting of the date and time, a change of configuration, and also the locking or unlocking of the locker. Using GAT DL Analyzer, these events can be read out and stored on the computer.

Note that events can also be synchronized with the OSS management software by users via their data carriers. However, it is possible that not all events are sent to the software (e.g., if a data carrier is lost or defective). In such a case, the events can be downloaded from the lock.

- ▶ Connect the respective lock to the PC (see "4.2 Setup for configuration").
- ▶ In GAT DL Analyzer, select **Events auslesen** (*read events*) from the **OSS Sync** menu.

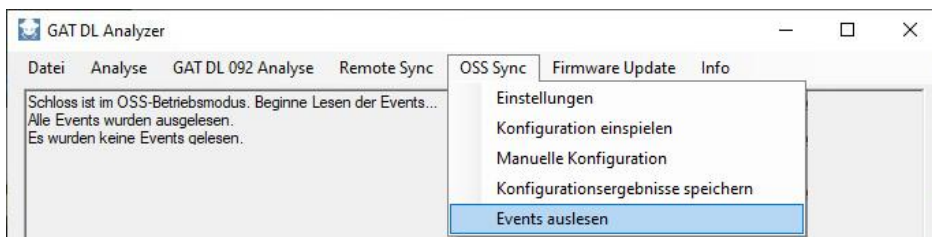


Figure 4.12 – Option for downloading the events

- The events are downloaded from the lock.
- A file dialogue opens.
- ▶ Specify the location (folder) where the events are to be saved.
 - The events are saved as an XML file in the selected folder.

There are different event types, which are identified with an event ID and associated event info. A table of all available events with their ID and info values is provided in section "4.9 Events in the protocol".

4.9 Events in the protocol

The following table shows an overview of the possible events that can be stored by a lock. The **Event IDs** indicate the type of an event. The **Event Info Code** shows extended information about an event.

Notice for the described firmware versions ("FW Version"):

⁽¹⁾ Valid for the GAT ECO.Lock and the GL7p.

⁽²⁾ Valid for the GAT ECO.Side Lock.

OSS defined	Event ID (hex / dec)	Designation of the Event ID	Event Info Code (hex / dec)	Designation of the Event Info Code	FW Version	Implemented	Comment
yes	h: 00 d: 0	No event	-	-	-	-	No event occurred
yes	h: 01 d: 1	Battery charge low	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Battery charge in the lock is low (little remaining capacity) / time to replace the battery. The timestamp of the event indicates when the low battery charge level was reached. If the battery was successfully replaced, the lock does not report this event.
yes	h: 02 d: 2	Battery replaced	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Battery in lock has been successfully replaced.
yes	h: 03 d: 3	Lock jammed	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	Lock could not lock and the mechanism is stuck, typically due to a mechanical fault. In most cases, this means that the locker door is not locked/locked. When the error is corrected, this event is no longer reported.
yes	h: 04 d: 4	System event	h: 00 d: 0	-	-	-	General placeholder for locker events not recognized as errors by the lock. Intended use for troubleshooting. A manufacturer-specific

OSS defined	Event ID (hex / dec)	Designation of the Event ID	Event Info Code (hex / dec)	Designation of the Event Info Code	FW Version	Implemented	Comment
							event code is provided in the 'Event Info' field.
yes	h: 04 d: 4	System event	h: 00 d: 0	Undefined	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	Information missing. Shall not be used. Event Info Code must be non-zero.
yes	h: 04 d: 4	System event	h: 01 d: 1	SystemRestart	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	The lock electronics have been restarted but are still ready for operation. The restart was triggered, e.g. by a battery change or an intended software restart.
yes	h: 04 d: 4	System event	h: 02 d: 2	SystemConfigured	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	A configuration of the lock firmware was carried out (group, ID or keys changed).
yes	h: 04 d: 4	System event	h: 03-7F d: 03-127	Reserved	1.0 ⁽¹⁾ 2.0 ⁽²⁾	-	Reserved OSO area.
no	h: 04 d: 4	System event	h: 91 d: 145	SYSTEM_TIME_SET	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Date / time set
no	h: 04 d: 4	System event	h: 92 d: 146	SYSTEM_FACTORY_RESET	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Configuration and permissions reset
no	h: 04 d: 4	System event	h: A0 d: 160	SYSTEM_PRG_CARD_USED	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	System data carrier read – PROGRAMMING data carrier
no	h: 04h d: 4	System event	h: A1 d: 161	SYSTEM_COM_CARD_USED	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	System data carrier read – COMMUNICATION data carrier
no	h: 04 d: 4	System event	h: A3 d: 163	SYSTEM_PASSKEY_MANAGEMENT_USED	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	System data carrier read – PASSKEY MANAGEMENT data carrier

OSS defined	Event ID (hex / dec)	Designation of the Event ID	Event Info Code (hex / dec)	Designation of the Event Info Code	FW Version	Implemented	Comment
no	h: 04 d: 4	System event	h: A4 d: 164	SYSTEM_PASSKEY_USED	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	System data carrier read – valid PASSKEY data carrier used
yes	h: 05 d: 5	Internal error	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	Lock internal error detected. Several internal event types can be signaled by this event (memory error, test error at start-up, etc.). A manufacturer-specific event code is provided in the 'Event Info' field.
yes	h: 06 d: 6	Error while unlocking	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	An error occurred when unlocking the locker door with the lock.
yes	h: 07 d: 7	Manipulation detected	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Security breach detected by the lock. The signals sent by the integrated tamper sensors of some locks can be logged with this event.
yes	h: 08 d: 8	Blocklist entry detected	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	The lock has recognized an identification entered in the blocklist.
yes	h: 09 d: 9	Blocklist full	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Blocklist is full, no further entries possible
yes	h: 0A d: 10	Opening allowed	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	The lock allows access for the current identification. For more information, see the Event Info field.
yes	h: 0A d: 10	Opening allowed	h: 00 d: 0	Undefined	1.0 ⁽¹⁾ 2.0 ⁽²⁾	-	Not valid. Decision missing. General code for allowed or denied opening should be used even if no further info is given.

OSS defined	Event ID (hex / dec)	Designation of the Event ID	Event Info Code (hex / dec)	Designation of the Event Info Code	FW Version	Implemented	Comment
yes	h: 0A d: 10	Opening allowed	h: 01 d: 1	Granted	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	General code for permitted opening. Used when none of the following codes can be applied or when the reason is not to be displayed.
yes	h: 0A d: 10	Opening allowed	h: 02 d: 2	GrantedDefaultTime	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Opening allowed with standard unlocking time.
yes	h: 0A d: 10	Opening allowed	h: 03 d: 3	GrantedExtendedTime	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Opening allowed with extended unlocking time.
yes	h: 0A d: 10	Opening allowed	h: 04 d: 4	GrantedToggleUnlock	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Opening allowed with toggle authorization (see "5.6. Toggle function").
yes	h: 0A d: 10	Opening allowed	h: 05 d: 5	GrantedToggleLock	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Locking allowed with toggle authorization (see "5.6. Toggle function").
yes	h: 0A d: 10	Opening allowed	h: 06-7F d: 6-127	Reserved	1.0 ⁽¹⁾ 2.0 ⁽²⁾	-	Reserved value range
yes	h: 0B d: 11	Opening allowed	-	-	-	-	
yes	h: 0B d: 11	Opening denied	h: 80 d: 128	Denied	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	General code for denied opening without further info. This typically means an invalid DoorInfo or DTSchedule. Can also be used if the lock is set to not display the reason for a denial. "Denied" can be used for all reasons that lead to a refusal to open.
yes	h: 0B d: 11	Opening denied	h: 80 d: 130	DeniedBlocklisted	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Opening denied because data carrier on blocklist.
yes	h: 0B d: 11	Opening denied	h: 83 d: 131	DeniedValidity	1.0 ⁽¹⁾ 2.0 ⁽²⁾	yes	Opening refused due to expired validity.

OSS defined	Event ID (hex / dec)	Designation of the Event ID	Event Info Code (hex / dec)	Designation of the Event Info Code	FW Version	Implemented	Comment
yes	h: 0B d: 11	Opening denied	h: 87-FF d: 135-255	Reserved	1.0 ⁽¹⁾ 2.0 ⁽²⁾	-	Reserved value range.
yes	h: 0C d: 12	CRC error	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	No MIFARE Classic CRC error.
yes	h: 0C-FF d: 12-265	Reserved	-	-	1.0 ⁽¹⁾ 2.0 ⁽²⁾	no	Reserved for future applications.

Table 4.1 – Event overview

i System events can be displayed in the OSS management software but cannot be configured more precisely there because they are product-specific.

4.9.1 Special events

Toggle processing

If the OSS lock is set to **Permanently Open** by a toggle data carrier, the events are still handled the same. Depending on whether the authorization is valid or not, the data carrier receives an **AccessGranted** or **AccessDenied** event.

The following signaling is indicated by the lock:

- LED: Green -> red
- Beeper: Long signal tone



For a description of the toggle function, see chapter "5.6. Toggle function".

5 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.

5.1 Target group

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

5.2 Unlocking the locker door

To unlock a locker door, hold your data carrier in front of the reading field of the lock. Depending on whether the **RFID Wake Up** option is enabled or not, the lock reads the data carrier automatically or it must be activated by briefly pressing the locker door or the lock button in (see "3.2 Activating the RFID reader").

The lock checks the authorization of the data carrier and unlocks the door if the authorization is valid. The authorization check is carried out differently by the lock depending on the operating mode used.

- Installation mode: Every readable data carrier is authorized to use the OSS lock.
- Standalone mode: Each user data carrier must be manually programmed into the lock on-site using the PROGRAMMING data carrier. Only the authorized data carriers are then allowed to use the lock.
NOTE! In this mode, a maximum of 200 data carriers can be authorized per lock.
- OSS mode: The authorization of the users is done in an access management software. There, the users' data carriers can be authorized for certain locks or also lock groups. Time-limited authorizations are also possible. The authorizations are written to the data carriers when the data carrier is read by an online reader. The OSS lock then checks the authorization data and unlocks the locker door accordingly.

i If the toggle function is activated by reading a toggle data carrier when the locker door is locked (see "5.8. Toggle Function"), the locker door will be unlocked and will remain unlocked until the lock is locked again using a toggle data carrier or when the time period (if defined) expires.

5.3 Locking the door

The locker door will lock automatically when the locker door is pushed shut (GAT ECO.Side Lock) or when the lock button is pushed in (GL7p and GAT ECO.Lock).

i For the GL7p locks that are equipped with a keypad, the keypad currently has no function. It is reserved for future use.

5.4 Emergency opening of an OSS lock

You can use the data carriers of the Master Key Set to open any locker in a system for which the Master Key Set is valid.

ATTENTION! Since the Master Key Set can be used to open any locker, the system data carriers must be kept in a secure place protected from unauthorized access.

- ▶ Press the locker door closed and keep it pressed.
- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - The information on the data carrier is read and the LED flashes alternately red and green.
- ▶ Remove the PROGRAMMING data carrier from the reading field again while continuing to hold the locker door closed.
- ▶ Within the next 5 seconds, hold the DEMOUNTING data carrier on the RFID reading field.
 - The LED lights up green briefly and the locker door is unlocked.
- ▶ Remove the DEMOUNTING data carrier from the reading field and release the locker door.
 - The locker door opens.

5.5 Resetting an OSS lock

An OSS lock can be reset to the default settings, which resets the address of the lock to zero and deletes the configuration in the lock. To do this, proceed as follows.

- ▶ Press the locker door closed and keep it pressed.
- ▶ Activate the lock with the PROGRAMMING data carrier (see Figure 3.1).
 - The information on the data carrier is read and the LED flashes alternately red and green.
- ▶ Remove the PROGRAMMING data carrier from the reading field again while continuing to hold the locker door closed.
- ▶ Within the next 5 seconds, hold the DELETE data carrier on the RFID reading field.
 - 2 long beeps are emitted and the LED flashes red in rapid succession.
- ▶ Remove DELETE data carrier from the reading field and hold it to the reading field a second time after approx. 1 second.
 - 3 short beeps are emitted and the LED flashes red in rapid succession.
- ▶ Remove DELETE data carrier from the reading field and hold it towards the reading field a third time after approx. 1 second.
 - 2 short beeps are emitted and the LED flashes red in rapid succession.
- ▶ Remove DELETE data carrier from the reading field and hold it towards the reading field a fourth time after approx. 1 second.
 - 1 short beep is emitted and the LED flashes red in rapid succession.

- ▶ Remove DELETE data carrier from the reading field and hold it towards the reading field a fifth time after approx. 1 second.
 - 2 long beeps are emitted.
 - If the DELETE data carrier is removed from the reading field after the fifth time, the LED flashes continuously red for a few seconds and the lock is reset to address 0. Data carriers that were authorized are no longer valid. The lock is reset to the default installation mode.

5.6 Toggle function

With the toggle function of the OSS standard it's possible to simulate the functionality of a mechanical key, which means that the OSS lock can be switched between continuously open (depending on the time schedule) and continuously locked. If a toggle data carrier is read at a locked lock and opening is possible according to the schedule, the toggle function is activated and the lock is unlocked and remains unlocked. It is not possible to lock the locker with another user data carrier or by pushing the door shut. It can only be locked again by reading a toggle data carrier again. If during active toggle function the current time schedule window expires, then the lock can also be locked with a normal, valid data carrier or by pushing the locker door shut.

The OSS standard stipulates that if the door is unlocked by means of the toggle function, the lock is automatically locked when the current time schedule window expires. This is not possible with GANTNER OSS locks due to their design. After the toggle time has elapsed, the lock remains unlocked until it is locked again by pressing the locker door shut or by means of a data carrier.

If the lock has been unlocked by means of a toggle data carrier, events such as closing attempts etc. that occur at the lock are still processed (see "4.9.1. Special events").

5.7 Passkey management and general key function

The Passkey Management System is a convenient way of authorizing and managing general and fire brigade data carriers in access systems equipped with offline terminals or offline locks. General data carriers have a general key function and can be used to lock and unlock any locker in a system with an OSS lock provided that the respective passkey management data carrier has been programmed into the lock.

The passkey management data carrier (GAT Passkey Management Card - Part. No. 496738) can be ordered from GANTNER. After the order is placed, 1 to 9 general and fire brigade data carriers suitable for the respective system are then coded onto the passkey management data carrier. These stored data carriers are programmed into an OSS lock by reading the PROGRAMMING data carrier and then the GAT Passkey Management Card at the lock.

The advantage is that the general data carrier or the fire brigade data carrier is not necessary for programming and can remain, e.g., in the fire brigade safe.

NOTE! A loss of the GAT Passkey Management Card is not immediately critical to security because the PROGRAMMING data carrier is always additionally required for the programming and use of the data carriers stored on it. Nevertheless, the GAT Passkey Management Card should be kept in a secure place.



For further information and the exact programming of the GAT Passkey Management Card, please refer to the Passkey Management Quick Start Guide ("DK_GAT-PasskeyManagementCard_Bedienung-EN").

5.8 Signalization overview

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

LED	Signalization	Meaning
	Blue LED	Lock activated, ready to read a data carrier
	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 - Tones with rising pitches	- Battery change confirmed successfully with BATTERY 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

Table 5.13 – Overview of signaling

Note:

This manual is valid as of 11th May 2023. It is subject to change.
Amendments can be made without prior notice at any time!



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

www.gantner.com