

GAT NET.Lock Standalone Functional Description

Electronic, Wired RFID Locker Lock System



© 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 the manufacturer accepts no liability for the completeness or accuracy of the contents of this manual. The right is reserved to make alterations, and alterations may be made at any time without prior notice being given.

Trademarks

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

Contact

The contact information for questions regarding the GAT NET.Lock System, or for any other general enquiries, is listed below:

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 Non-safety-critical information	10
1.5.3 Instructions and results	10
2. GENERAL INFORMATION	11
2.1 Intended use	11
2.2 Special application "Standalone"	11
2.3 Functional description	11
2.4 System overview	12
2.5 Terminology	13
3. CONFIGURATION	15
3.1 Configuration with GAT Config Manager	16
3.1.1 Setup for configuration in GAT Config Manager	16
3.1.2 Viewing and editing the GAT NET.Controller S configuration settings	19
3.1.3 Uploading configuration settings to the GAT NET.Controller S	20
3.1.4 Updating the GAT NET.Controller S firmware	21
3.2 Configuration with the MoLA App	23
3.3 Configuration settings of the GAT NET.Controller S	24
3.3.1 RF standards	24
3.3.2 MASTER data carriers	25
3.3.3 Standalone mode	25
3.3.4 Operating mode	25
3.3.5 Locker number	26
3.3.6 Auto-unlock	26
3.3.7 Duration of use	27
3.3.8 Locking of personal locker without data carrier	27
3.3.9 Closing of free locker without data carrier	27
3.3.10 Configuration settings	28
3.4 Restarting a controller	33
3.5 Resetting a controller to the default settings	33
3.6 GAT NET.Lock antenna calibration	34
3.7 GAT NET.Lock signalization overview	35
3.7.1 General (applicable for all modes)	35
3.7.2 Personal locker mode	35
3.7.3 GAT Lock 5000 mode	35
4. OPERATION	37
4.1 General	37
4.2 Target group	37
4.3 Operating modes	37
4.3.1 Free locker mode (with or without duration of use function)	38
4.3.2 Free locker universal mode	39
4.3.3 Free locker unique number mode	39
4.3.4 Personal locker programming card mode	40
4.3.5 Personal locker expiry date mode	41

4.4 GAT ECO.Basic Set FD 43

4.5 Summary of the system data carriers 43

4.5.1 MASTER data carrier 43

4.5.2 DELETE MASTER data carrier 44

4.5.3 OPEN MASTER data carrier 44

4.5.4 PROGRAM data carrier 44

4.5.5 SERVICE data carrier 45

4.5.6 APP KEY data carrier 45

4.5.7 BATTERY data carrier 45

1. INTRODUCTION

1.1 About this manual

This manual contains all the information necessary to commission and configure the GAT NET.Lock wired electronic locker locks and GAT NET.Controller S sub controller in standalone mode. Furthermore, the operation for the end user is described.

The installation and technical data of the hardware components (GAT NET.Lock and GAT NET.Controller S) are described in the GAT NET.Lock system manual. Information applicable for the standalone version of this system is described in this manual.

NOTE! For both the GAT NET.Lock 7020 system and the predecessor GAT NET.Lock 7000 system, the standalone function is available from firmware version 1.9. This manual therefore uses the general terms GAT NET.Lock and GAT NET.Controller S to refer to both systems.

1.2 Chapter overview

In chapter 2 "GENERAL INFORMATION", you will find a functional description of the GAT NET.Lock system in standalone mode, a description of the most important terms used in this manual, and a system overview.

Chapter 3 "CONFIGURATION" describes how to configure a sub controller in standalone mode. In addition, you will also find a detailed description of the configuration settings available as well as instructions on how to calibrate the antenna of the GAT NET.Lock locks.

Chapter 4 "OPERATION" describes the various operating modes of the GAT NET.Controller S and GAT NET.Lock and the function of the system data carriers in the GAT ECO.Basic Set FD.

1.3 Contact & inquiries

If you have any questions concerning the GAT NET.Lock system, please contact your local sales partner or one of the GANTNER branch offices directly. The contact details are available on the last page of this manual.

1.4 Target group

This manual contains the information necessary to configure the sub controllers for standalone use and also includes notes on how to operate the GAT NET.Lock system in standalone mode. The installation, service, and maintenance of the devices used are not included in this manual. If a chapter is only intended for a specific target group, this is stated at the beginning of the chapter.

The following target groups can find information in this manual:

- Technicians responsible for putting the system into operation.
- End users of the GAT NET.Lock system (operation).

Where not explicitly stated, the information in this manual is intended for all target groups in general.

⚠ 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.

1.5 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 the device or associated equipment.

1.5.2 Non-safety-critical 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.

2. GENERAL INFORMATION

2.1 Intended use

The GAT NET.Lock is intended for the convenient electronic locking of wardrobe lockers in fitness clubs, baths, golf resorts, hotels, and other individual company applications. Identification at the GAT NET.Lock is completed using contactless RFID data carriers (Radio Frequency Identification).

The GAT NET.Lock is suitable for any type of locker material, e.g., sheet metal, wood, HPL, solid plastic, glass, and can be used with both left and right-hinged doors.

2.2 Special application "Standalone"

In standalone mode, a GAT NET.Lock system operates with only one or more sub controllers and the GAT NET.Lock locks connected to them. A main controller and the Relaxx software are not necessary. Each individual lock can be set to operate in its own operating mode. The operating modes correspond to the functions of a battery lock (see "4.3. Operating modes"). For this reason, a corresponding GAT ECO.Basic Set is also required. Special functions can be implemented using the data carriers of the Basic Set (see "4.5.4 PROGRAM data carrier").

Since the sub controllers are not networked with the main controllers in standalone mode, the configuration must be completed for each sub controller individually.

Notes on the configuration options:

- Either the GAT Config Manager (see "3.1 Configuration with GAT Config Manager") or the MoLA App (see "3.2 Configuration with the MoLA App") can be used to configure the sub controllers.
- Since the configuration with the MoLA App is partially restricted, the basic configuration must be performed with GAT Config Manager. For this purpose, an RS-485 adapter is mandatory (1102316 - GAT NET.Controller S Interface Cable USB).
- A firmware update of the sub controller is also only possible using GAT Config Manager.

2.3 Functional description

Locking a locker

Depending on the configured locker mode, the user can choose any unoccupied locker ("free locker" mode) or they must use their assigned locker ("personal locker" mode). The user closes the door of their locker and while holding the door shut, holds their data carrier next to the RFID reading center on the locker door, which is indicated by the LED of the lock. The GAT NET.Lock reads the data carrier information and communicates with the sub controller to determine whether the user is allowed to use the locker depending on their authorization. If the user is authorized to use the locker, a command is sent instructing the lock to lock the locker door.

Unlocking a locker

To unlock a locker door, the user holds their data carrier next to the reading center of their previously locked locker door. The GAT NET.Lock communicates with the sub controller and when the user is authorized to open the locker, a command is sent instructing the GAT NET.Lock to unlock the locker door.

Bookings

The sub controller logs all lock operations and status messages. These bookings can be downloaded and read via the configuration software GAT Config Manager or via the MoLA App. The GAT NET.Controller S 7000 can store 5 bookings per lock and the GAT NET.Controller S 7020 can store 50 bookings per lock.

Alarms

In case of an error or unexpected system condition, an alarm may be triggered. In this situation, a booking is recorded, and an alert on-site may be generated.

2.4 System overview

The different types of GAT NET.Lock locks and sub controllers can be combined together.

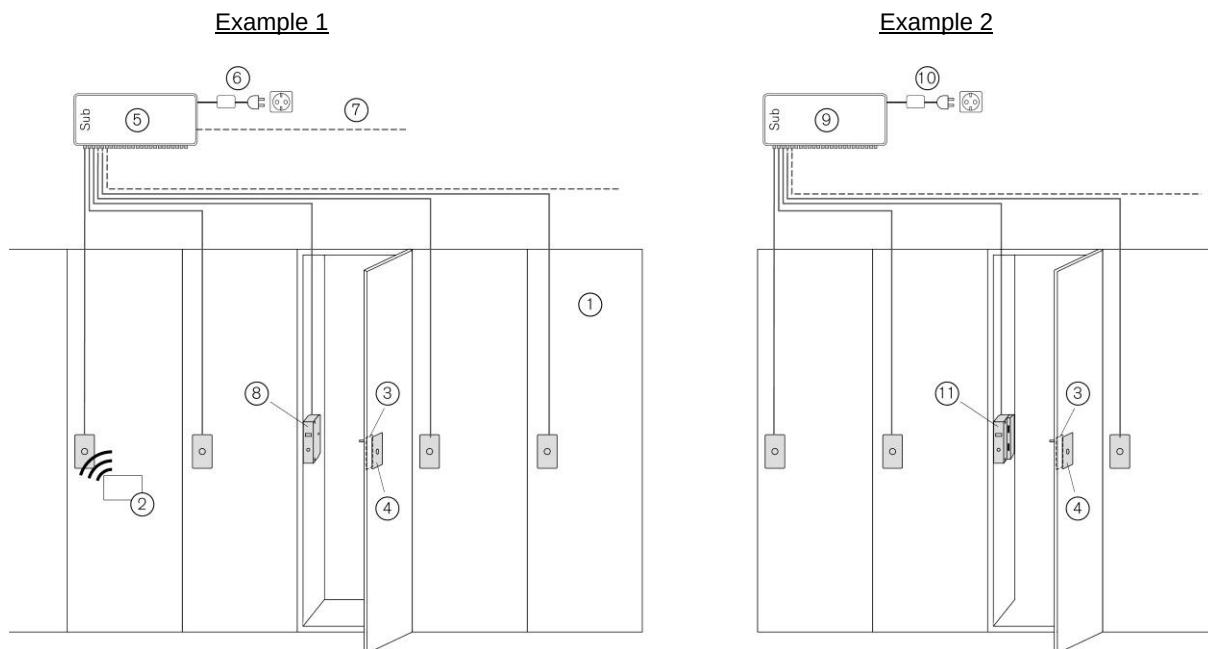


Figure 2.1 – Typical application of the GAT NET.Lock system in standalone mode

1. Lockers
2. RFID data carrier
3. Bolt set (GAT NET.Lock BoltSet 7xxx)
4. Front label

Example 1: Different variants of the GAT NET.Lock locks and controllers can operate in combination.

5. Sub controller 7020 or 7000
6. GAT NET.Power Supply 7020 (without "USB") or 7000
7. Configuration cable (1102316 - GAT NET.Controller S Interface Cable USB), for configuration via GAT Config Manager)
8. GAT NET.Lock 7020 / 7020 P or GAT NET.Lock 7000

Example 2: To use the USB and LED function, the GAT NET.Lock 7020 USB (P) and the following combination of controllers and power supplies must be used:

9. Sub controller 7020
10. GAT NET.Power Supply 7020 USB
11. GAT NET.Lock 7020 USB or 7020 USB P

Please note the following:

- The USB charging function and LED lighting of the GAT NET.Lock 7020 USB (P) locks are only available with the GAT NET.Controller S 7020 sub controller. In addition, only the GAT NET.Lock 7020 USB (P) locks can be connected to the sub controller. If one or more GAT NET.Lock 7020 locks without USB are connected, these functions are disabled for all locks connected to the controller.
- If the USB charging function and LED lighting are to be used, the power supply with USB function must be used to power the sub controller.

2.5 Terminology

The terms used often in this manual are defined as follows.

Lock

General term for the GAT NET.Lock 7020 and GAT NET.Lock 7000.

Locker

The term "locker" is used to generally describe all possible locker applications, e.g., a changing room locker, a depot or a private box, which can be locked by the GAT NET.Lock.

Sub controller

The GAT NET.Lock 7020 or 7000 locks are connected to a GAT NET.Controller S 7020 or GAT NET.Controller S 7000 sub controller (up to 24 locks per sub controller). The sub controllers are configured via the serial RS-485 interface and control the connected locks accordingly.

User

The term "user" in this manual refers to the person that operates, i.e., locks and unlocks, a GAT NET.Lock equipped locker.

Data carrier

A data carrier is a form of identification media that is used by staff and visitors in a facility for identification. Data carriers are available in a variety of different forms such as plastic wristbands and chip cards. Data carriers are also available to suit different RFID technologies (LEGIC, MIFARE®, ISO 15693).

FID (Company ID) and Site Key

The FID and site key are unique numbers assigned to every facility installation. The site key is a combination of the FID and the read and write keys. The site key is used in MIFARE® and ISO 15693 systems and is 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.

RFID (Radio-Frequency Identification)

Identification over short distances using radio frequency. An RFID data carrier is used as identification media.

Booster

Electronic component for amplifying the RFID reading field of the GAT NET.Lock. The bolt sets for the GAT NET.Lock are supplied with an integrated booster.

3. CONFIGURATION

To configure the system for the desired functionality, the configuration settings of the sub controller(s) must be set. There, general settings for the sub controllers as well as the modes and parameters of the locks connected to the sub controller are set individually.

NOTE! To use standalone mode, it must be activated first (see "3.3.3. Standalone mode"). Only after activation are all standalone configuration settings visible. The controller should also be reset before the initial configuration (see "3.5 Resetting a controller to the default settings").

The initial basic configuration should be carried out using GAT Config Manager. To do this, the sub controller must be connected to a USB port on the PC via the GAT NET.Controller S Interface Cable USB configuration cable (Part No. 1102316). On the sub controller, the cable must be plugged into the RJ45 socket labelled "RS 485 IN".

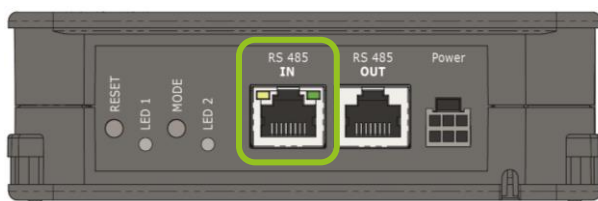


Figure 3.1 – Port for connection of the configuration cable

Another configuration option is via the MoLA app. Since not all configuration options are available with the MoLA app, it is only applicable after the first basic configuration is completed using GAT Config Manager. With this app, the most important lock settings can be configured directly on-site using a mobile device (e.g., smartphone). The MoLA app can be downloaded from the Google Play Store and be used with mobile devices with an Android operating system. The app uses NFC for configuration; therefore, the mobile device must also support NFC communication. For more information, see section "3.2 Configuration with the MoLA App".

NOTE! After completing the configuration, perform an operational test to ensure that the user and MASTER data carriers are read securely by the lock and the general lock functionality performs as expected.

The following data is imported into the sub controller during configuration:

- Site number
- Sub-site number
- Unique numbers of the MASTER data carriers

In addition, the following data is stored for each lock:

- Locker number
- Operating mode of the GAT NET.Lock ("Free Locker", "Free Locker Universal", "Free Locker unique number", "Personal Locker Programming Card", or "Personal Locker Expiry Date". See section "4.3. Operating modes")
- Free locker: Sector number of the data on the data carrier and the time setting for the "duration of use" function

i The MASTER data carriers can also be programmed into each lock directly (see section "4.5.1 MASTER data carrier"). However, the most efficient way to program the data carriers into multiple locks is via PC and GAT Config Manager.

NOTE! In general, the locker locks can be configured with the same modes and functionality as the offline locker locks from GANTNER (e.g., GAT ECO.Lock xxx).

3.1 Configuration with GAT Config Manager

3.1.1 Setup for configuration in GAT Config Manager

When a GAT NET.Controller S is connected to the PC via a configuration cable and configuration mode is activated via the SERVICE data carrier (see "4.5.5 SERVICE data carrier"), the settings can be viewed and configured using GAT Config Manager.

i There is a separate manual with detailed information on each function available in GAT Config Manager. To access the manual while the software is open, click on the "Help" drop-down menu and select "How Do I".

Complete the following steps to setup the GAT NET.Controller S for configuration in GAT Config Manager.

- ▶ After installing the software, open GAT Configuration Manager via "Start" -> "All Programs" -> "GANTNER Electronic GmbH" -> "GAT Config Manager" -> "GAT Config Manager".
 - The default start window of GAT Config Manager is displayed.
- ▶ Click on the "Open Project" icon (1 in Figure 3.2) to find an existing project.
- ▶ Alternatively, click on the "Create Project" icon (2 in Figure 3.2) to start a new project.

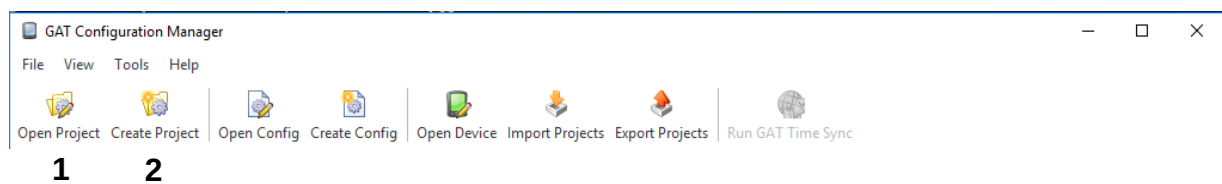


Figure 3.2 – GAT Config Manager – Project setup

- ▶ Once a project is established, locations and sub-locations for the project can be added to the "Devices" directory (2 in Figure 3.3) by clicking on the "Add location" button (1 in Figure 3.3).

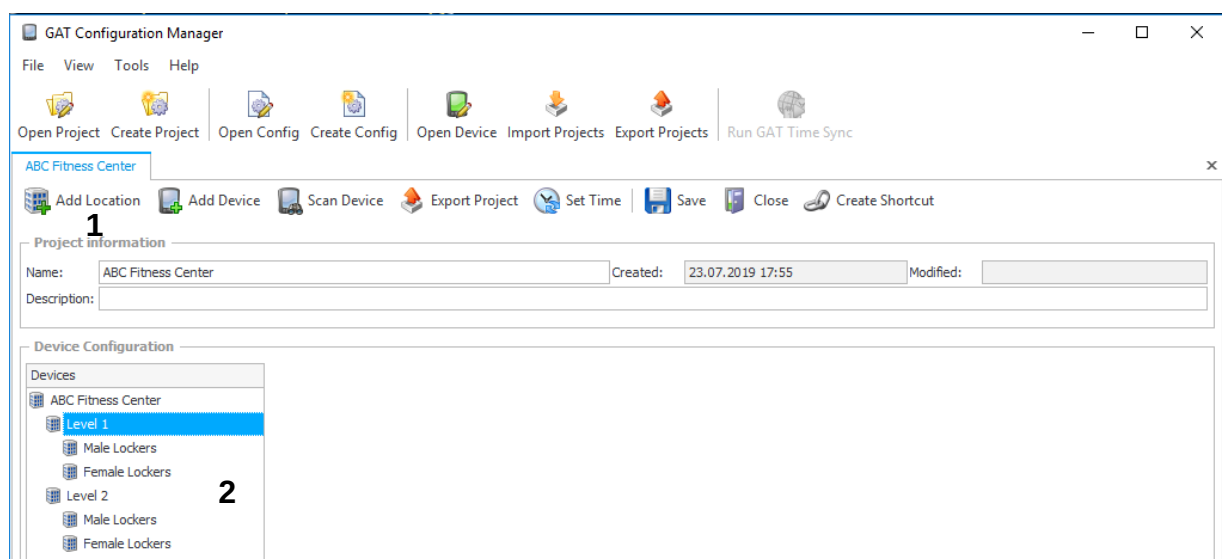


Figure 3.3 – GAT Config Manager – Add location

- To add a GAT NET.Controller S with connected GAT NET.Lock to a location, right-click on the location and select “Add Device” from the menu (Figure 3.4).

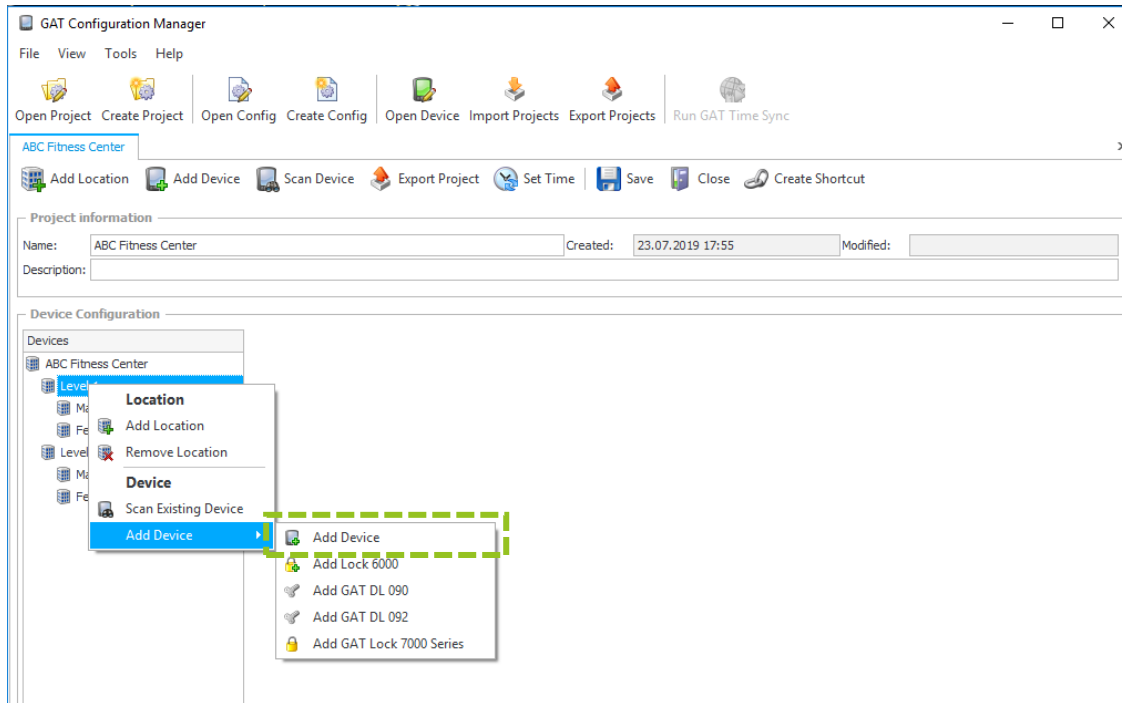


Figure 3.4 – GAT Config Manager – Adding a GAT NET.Controller S

- A window opens where you can add the controller.

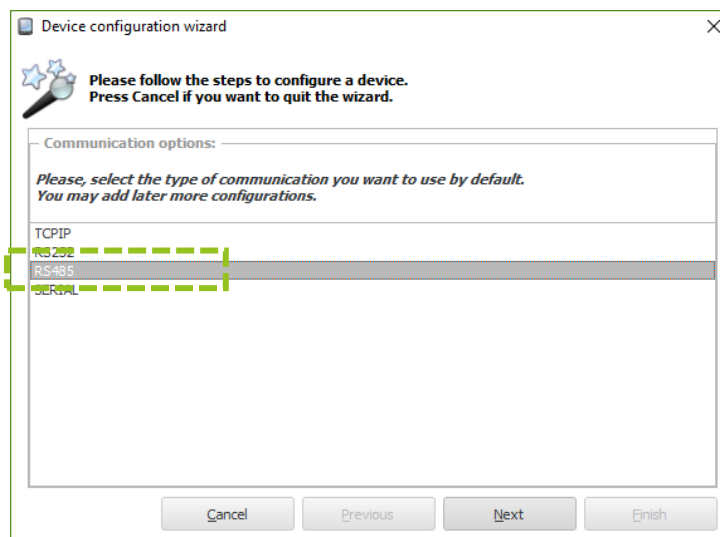


Figure 3.5 – GAT Config Manager - Selecting the sub controller interface

- Select "RS485" and click on "Next".

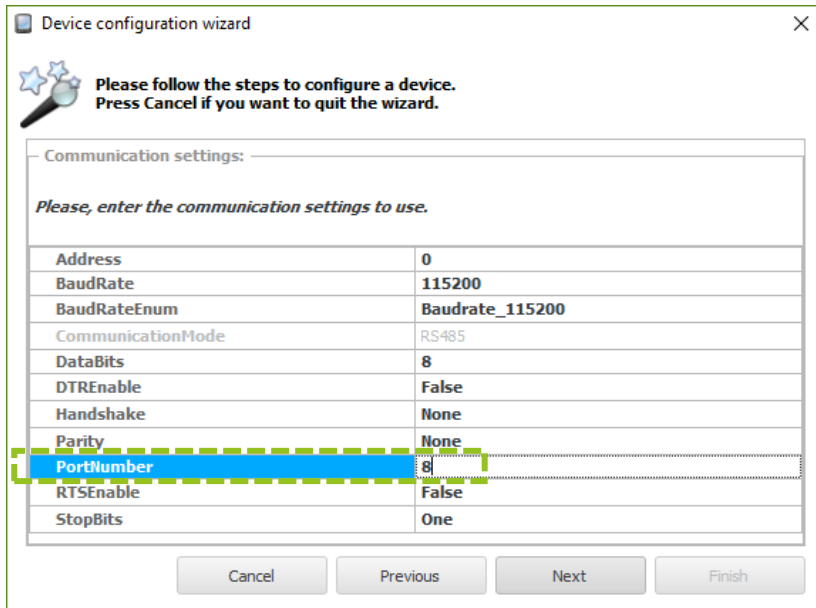


Figure 3.6 – GAT Config Manager - Setting communication parameters

- Under "PortNumber", enter the number of the COM port to which the controller is connected. You can find this in the Device Manager of Windows. In the Windows Start menu, search for "Device Manager" to open the Device Manager.

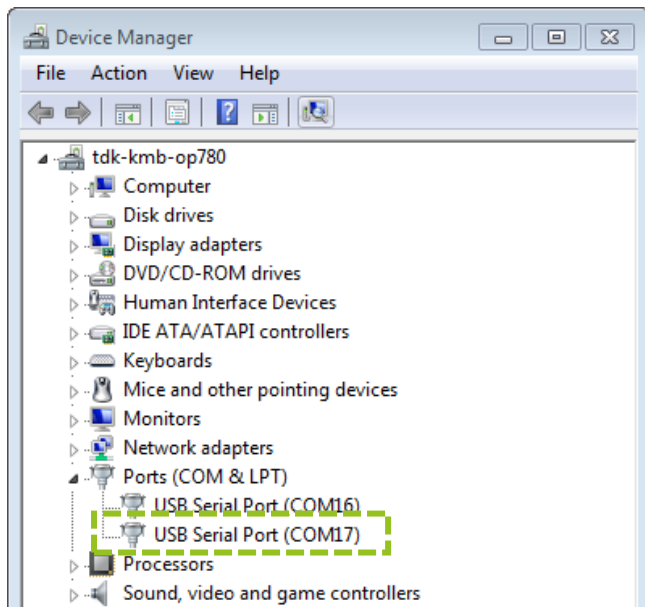


Figure 3.7 – COM port number in the Windows Device Manager

- Leave the remaining configuration parameters as their default values and click on "Next".
- In an additional window, you can enter a name for the sub controller and then confirm via "Finish".
 - The sub controller is added to the device list in GAT Config Manager and its settings are displayed to the right.

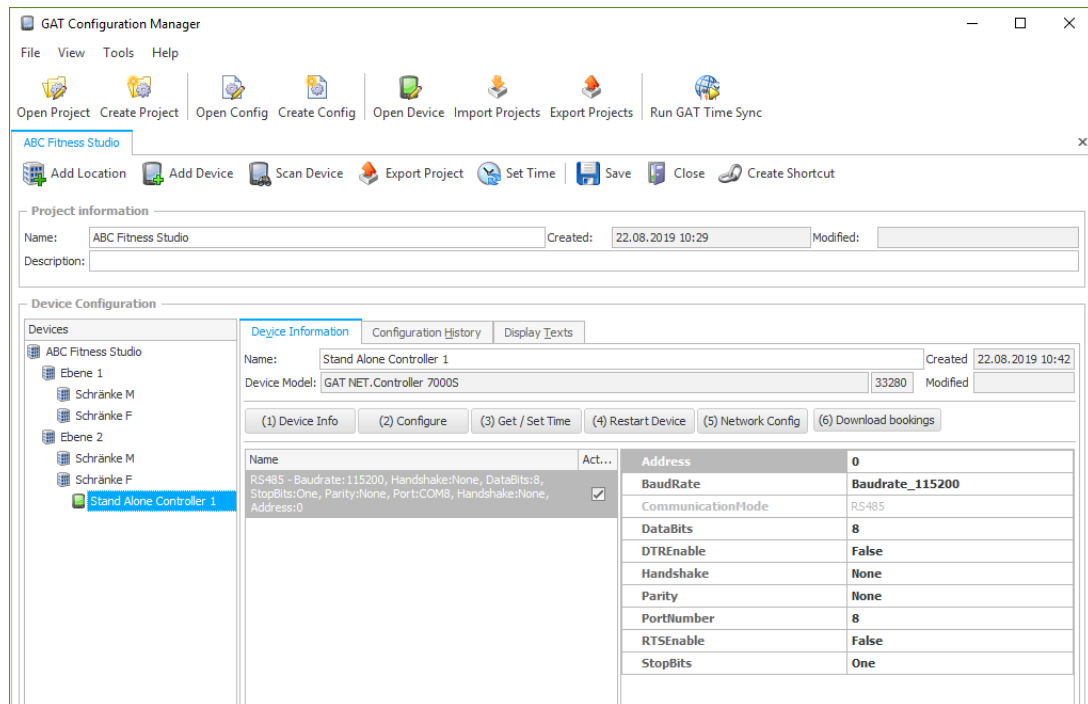


Figure 3.8 – GAT Config Manager – Display of the settings of a Standalone Controller

3.1.2 Viewing and editing the GAT NET.Controller S configuration settings

Once the GAT NET.Controller S has been added to the “Devices” directory, you can now view and configure the lock configuration settings. Complete the following steps to view the configuration settings.

- Select the GAT NET.Controller S from the “Devices” list (1 in Figure 3.9).
 - The GAT NET.Controller S is highlighted in color.

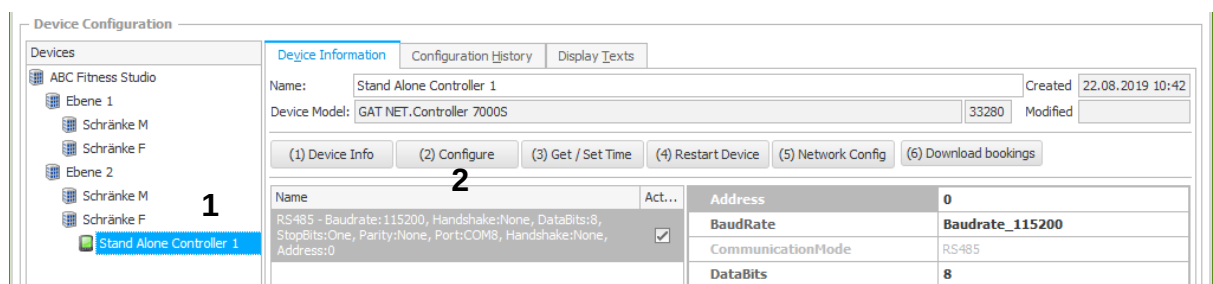


Figure 3.9 – Displaying the configuration settings

- Hold the SERVICE data carrier next to the reader of one of the locks connected to the sub controller.
 - Reading this data carrier activates the configuration mode.

NOTE! This step is not necessary for sub controllers with default settings and the FID 9999 9999 still set.

- Click on “(2) Configure” (2 in Figure 3.9).
 - The “GAT Configurator” window opens (Figure 3.10).

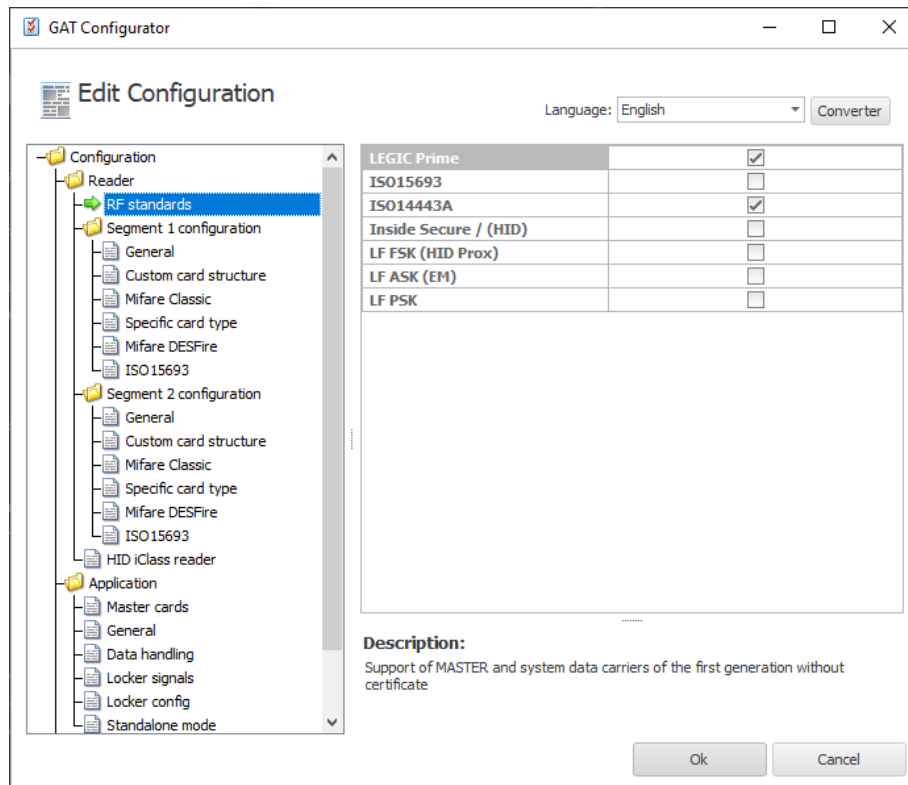


Figure 3.10 – “GAT Configurator” configuration window

3.1.3 Uploading configuration settings to the GAT NET.Controller S

When you are finished configuring the GAT NET.Controller S settings in GAT Config Manager, it is important to finalize the configuration by uploading the file. This saves the configuration settings in the GAT NET.Controller S and overwrites the default device settings. Complete the following steps to finalize the configuration.

- Click on "OK" in the GAT Configurator window (Figure 3.10).
 - A confirm upload window opens.



- Click “Yes” to apply the configuration to the controller.
 - The configuration settings are uploaded to the GAT NET.Controller S.

3.1.4 Updating the GAT NET.Controller S firmware

GANTNER periodically releases firmware updates for the GAT NET.Controller S. To take advantage of the latest features, it is recommended to update the GAT NET.Controller S to the latest firmware during configuration or at regular intervals.

NOTE! Min. firmware version 1.9 must be installed in the controller for standalone mode to be available.

- Right-click onto the GAT NET.Controller S in the “Devices” tree and select “Update Firmware”.

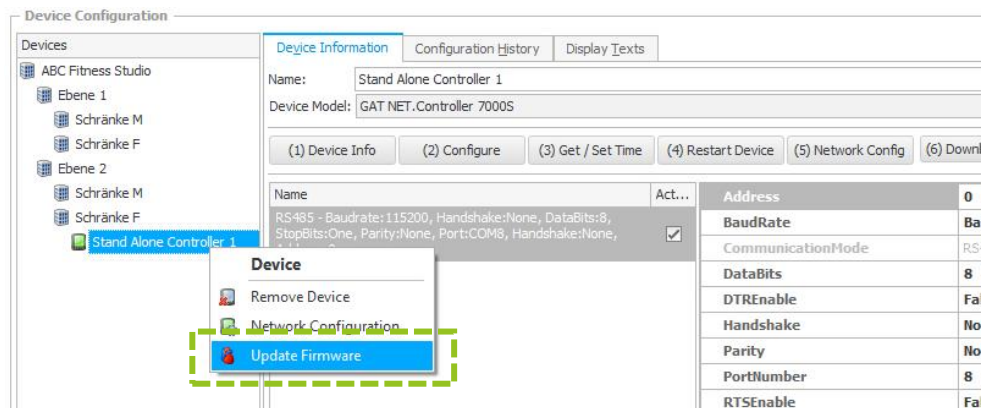


Figure 3.11 – Updating the GAT NET.Controller S firmware

- The “Device update wizard” opens where all available updates are listed.

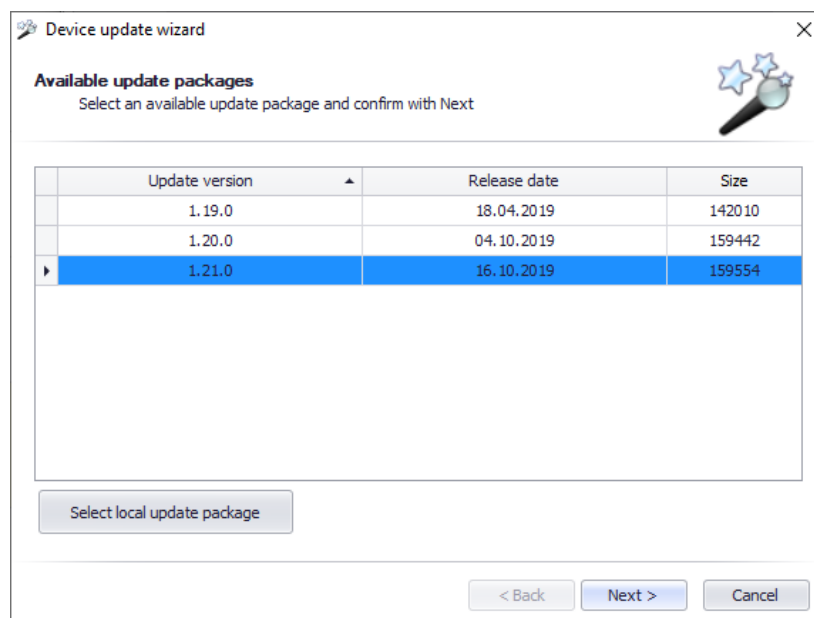


Figure 3.12 – Device update wizard – Display of the available firmware versions

- ▶ Hover over the update version with the mouse to display the new features included with the update.
- ▶ Select the most recent update then click on "Next".
- ▶ Alternatively, you can manually select a firmware update if you want to use an update file, e.g., stored locally on the PC. To do this, click on "Select local update package".
 - The "Device update wizard" downloads the update and uploads it to the GAT NET.Controller S, which usually takes around 1 minute. Do not switch the controller off or disconnect the cable during the update!
 - After uploading the update, the message "The Device has been successfully updated" should be displayed.
- ▶ Click on "Finish" when the update process is completed.

3.2 Configuration with the MoLA App

The MoLA App, which is available to download from the Google Play Store, can be used together with a mobile device (e.g., smartphone) to configure the GAT NET.Lock resp. GAT NET.Controller S.

NOTE! To use standalone mode, it must be activated first (see "3.3.3. Standalone mode"). As only the most important configuration settings can be edited with the MoLA app, we recommend using the GAT Config Manager software for the initial basic configuration. The controller should also be reset before the initial configuration (see "3.5 Resetting a controller to the default settings").

To use the MoLA app, the following requirements must be fulfilled:

- Mobile device with Android 4.4.0 or later version.
- Mobile device must be NFC enabled.
- Mobile device must not be rooted.
- The GAT NET.Controller S must have firmware version 1.9 or later version.
- A valid APP KEY data carrier is required for configuring locks on-site

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 for Apple devices.

In MoLA, you can change the same configuration settings as in GAT Config Manager (see "3.3 Configuration settings of the GAT NET.Controller S"). There are limitations, particularly with the RFID settings (segment 2) and the extended signaling. If these settings need to be changed then configuration using GAT Config Manager is necessary.

The APP KEY data carrier is a special system data carrier (see "4.5. Summary of the 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 make a new configuration.



If a GAT NET.Controller S is set to its default settings (i.e., FID is set to 9999 9999), the APP KEY data carrier is not necessary.

When the APP KEY is loaded to MoLA, it will remain valid for a certain period of time. When the validity expires, the APP KEY is automatically deleted in the mobile device by the MoLA App. This prevents the unauthorized access of the APP KEY data carrier by third-party apps, malware, etc.

3.3 Configuration settings of the GAT NET.Controller S

The important configuration settings of the GAT NET.Controller S that can be adjusted in GAT Config Manager are explained in this section. A list and brief explanation of every configuration setting available for the GAT NET.Controller S is provided in section "3.3.10. Configuration settings"

NOTE! To use standalone mode, it must be activated first (see "3.3.3. Standalone mode"). Only after activation are all standalone configuration settings visible.

3.3.1 RF standards

The GAT NET.Controller S and the GAT NET.Lock can operate with LEGIC, ISO 15693, ISO 14443A (MIFARE), and HID iCLASS data carriers. The GAT NET.Lock 7020 P locks can also read 125 kHz data carriers.

The data carrier settings of the GAT NET.Lock or sub controller respectively are found here:

Configuration > Reader > RF Standards

- ▶ Select / deselect the desired options.
- ▶ In addition to the standard used, other settings must be configured for the data carriers. These settings are found via the following configuration paths:

Configuration > Reader > Segment 1 configuration

Configuration > Reader > Segment 2 configuration

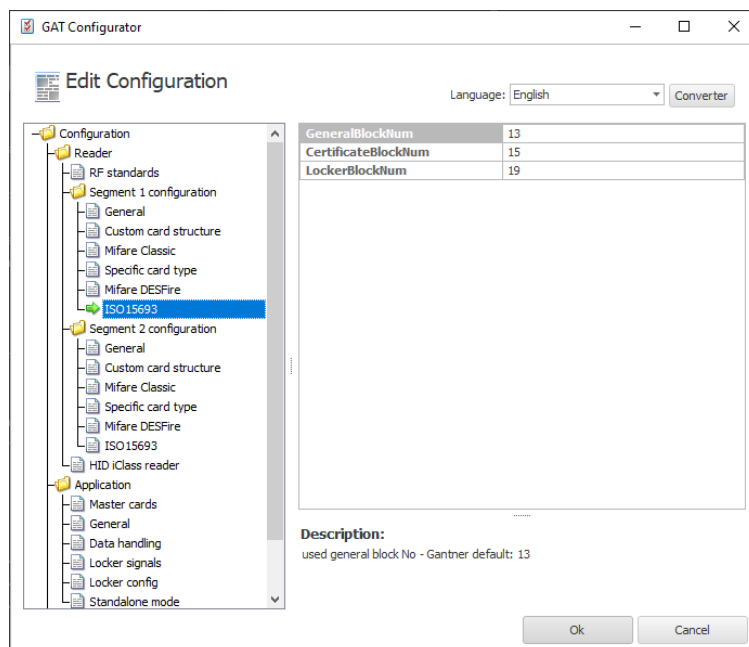


Figure 3.13 – Configuration settings

Two different segment definitions for the data carriers can be configured for a sub controller ("Segment 1 configuration" and "Segment 2 configuration").

3.3.2 MASTER data carriers

Up to 10 MASTER data carriers (also called MASTER cards in the configuration) can be assigned to a sub controller. Using one of these MASTER data carriers, each locker connected to the sub controller can be opened under special circumstances, e.g., if a user has lost their data carrier. The MASTER data carriers are assigned to the sub controller here:

Configuration > Application > Master cards > MasterCard1 - 10

- ▶ Enter the number of each MASTER data carrier into the respective fields.

NOTE! The MASTER data carrier numbers must be entered in hexadecimal format.

i The MASTER data carriers can also be programmed directly at any lock connected to the sub controller using the DELETE MASTER data carrier. See "4.5.2 DELETE MASTER data carrier".

3.3.3 Standalone mode

In order to use standalone mode, it must be enabled in the configuration:

Configuration > Application > General > OperatingMode

- ▶ Select "STANDALONE" here to enable standalone mode.
- ▶ Confirm by clicking on "OK".
 - The configuration is transferred to the sub controller and standalone mode is enabled.
- ▶ Now open the configuration page again.
 - An additional configuration option "Locker config" for the individual setting of the lock functions is displayed (see "3.3.4 Operating mode").

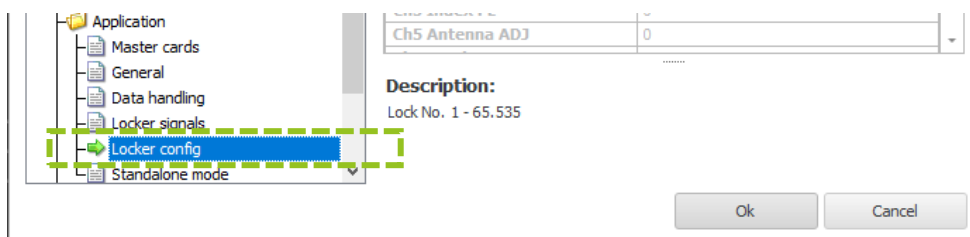


Figure 3.14 – Edit locker configurations

3.3.4 Operating mode

Each GAT NET.Lock connected to a sub controller in standalone mode can be individually set to operate in one of five different operating modes. See "4.3 Operating modes" for a detailed description of each mode. This setting is found here:

Configuration > Application > Locker config

There are four settings per lock (or channel Chx) available here. The locks are automatically detected and only the channels to which GAT NET.Lock is connected can be edited.

- The operating mode is set via the "Chx Mode" setting.
 - "Free locker"
 - "Free locker universal"
 - "Personal locker programming card"
 - "Personal locker expiry date" or
 - "Free locker unique number"

3.3.5 Locker number

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

Configuration > Application > Locker config > Chx Number

- Enter the locker number for the GAT NET.Lock into the "Chx Number" field of the desired locker.

The "x" in "Chx" stands for the channel number on the sub controller where the lock is connected. The channel number is written on the front of the sub controller above the lock connection sockets.

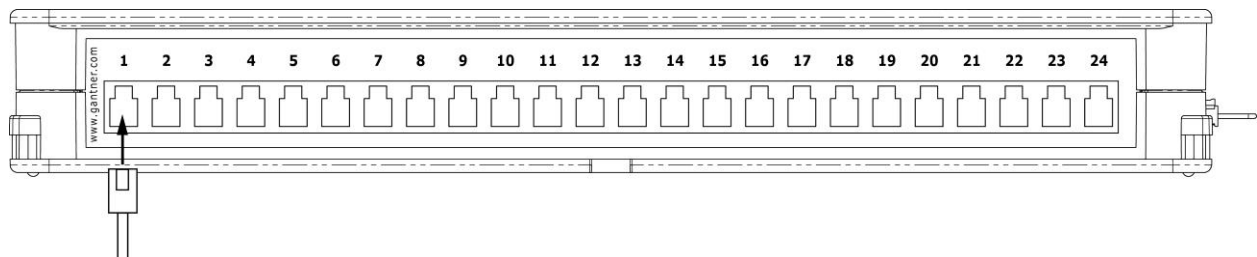


Figure 3.15 – Channel numbering on the sub controller

3.3.6 Auto-unlock

The auto-unlock function automatically unlocks the GAT NET.Lock at a defined point in time. The time must be set correctly once via software.

NOTE! When this function is activated, the lock will always unlock at the defined point of time regardless of the operating mode (see "4.3 Operating modes"). Please be aware that the lock does not automatically switch between daylight saving time and standard time. This means that the automatic open time points are different during daylight saving and standard time.

The auto-unlock function is found here:

Configuration > Application > Standalone mode > 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.

It is also possible to automatically unlock a lock after a certain locking time:

Configuration > Application > Standalone mode > Auto Unlock after locking [min]

- ▶ Enter the time for how long a lock may max. be locked before it gets automatically unlocked.

3.3.7 Duration of use

Lockers operating in free locker mode can be configured to limit the user to a defined period of use. See section "4.3.1. Free locker mode (with or without duration of use function)" for detailed information. The duration of use function is found here:

Configuration > Application > Standalone mode > Use Time Limit

- ▶ 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.

3.3.8 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 is unlocked again using the data carrier(s) authorized to use the personal locker. The function is found here:

Configuration > General > AutoLock-PersonalLocker

- ▶ Select / deselect the desired option to enable / disable the lock without data carrier function.

3.3.9 Closing of free locker without data carrier

The function of closing lockers in free locker mode allows a locker to be closed just by pressing the locker door shut (without data carrier). A locker closed in this way can be re-opened by pressing the door in again. The function is found here:

Configuration > General > AutoClose-FreeLocker

NOTE! A locker closed using this function is NOT locked! The locker can be opened again without a data carrier by pressing the locker door.

3.3.10 Configuration settings

The following table contains all the configuration settings for a GAT NET.Controller S that can be edited in GAT Config Manager.

i The parameter "Locker config" is only displayed when the sub controller is operating in standalone mode (see "3.3.3. Standalone mode").

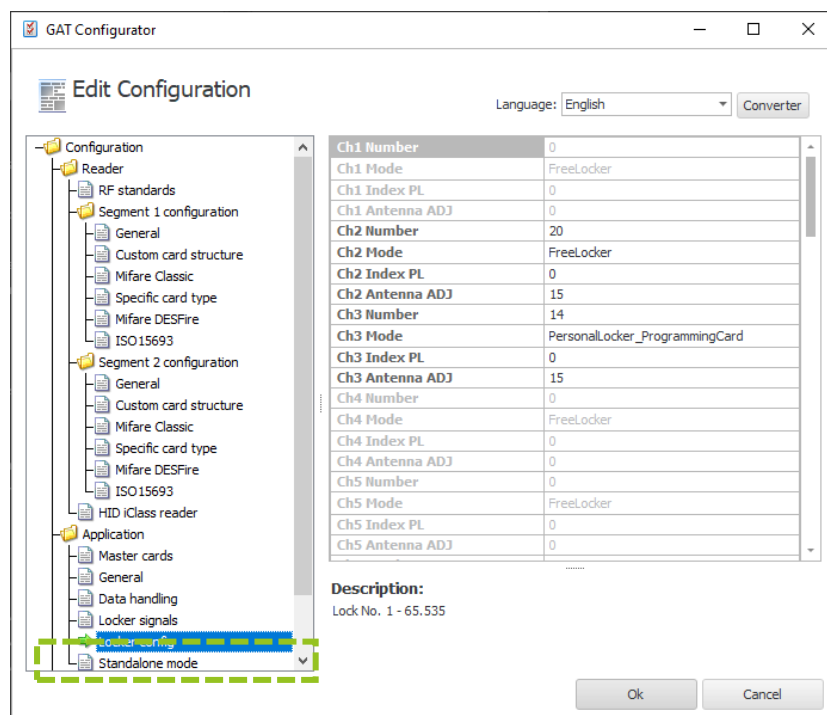


Figure 3.16 – Configuration settings

Options	Description	Format	Default
Reader			
RF Standards			
LEGIC Prime	When set to "True", LEGIC prime data carriers can be read by the device. Only for LEGIC controllers (GAT NET.Controller S 7020 BA (NU)).	Boolean	True
ISO15693	When set to "True", ISO 15693 data carriers can be read by the device.	Boolean	False
ISO14443A	When set to "True", ISO 14443 (MIFARE) data carriers can be read by the device.	Boolean	True
Inside Secure / (HID)	When set to "True", HID iCLASS data carriers can be read by the device (UID number only).	Boolean	False
LF FSK (HID Prox)	When set to "True", 125 kHz HID data carriers can be read by the device.	Boolean	False
LF ASK (EM)	When set to "True", 125 kHz EM data carriers can be read by the device.	Boolean	False
LF PSK	When set to "True", 125 kHz PSK data carriers can be read by the device.	Boolean	False
Segment 1 configuration			
General			

	SiteKey	Site key of the device. All data carriers must have the same site key to be used with the device.	Hex	
	SubFID	Sub-site number, for the subdivision of a facility. If not used = 0.	Hex	0
	SegId	Type of segment used.	Menu	NOT_USED LOCKER1 LOCKER2 CUSTOM1 CUSTOM2
	SendToHost	Not used in standalone mode.	Boolean	False
	HandleLockerGroupId	Not used in standalone mode.	Integer	0
	KeySet	DESFire AES key, encrypted.	Hex	
	Flip UID	If enabled, the unique numbers read from the data carriers are reversed (MSB -> LSB).	Boolean	False
	Enable segment	Enables the segment configuration.	Boolean	False
	FreelockerUniversalMode	Enables/disables the free locker universal mode (see "4.3.2 Free locker universal mode").	Boolean	False
	Custom card structure	Settings for reading MIFARE Classic data carriers		
	DataOffset	Starting point of the data to be read.	Integer	0
	DataLength	Data length of the data to be read.	Integer	0
	CRCDataStartAdr	Start address of the checksum calculation.	Integer	0
	CRCAdr	Address of the checksum	Integer	0
	CRCMode	Mode of the checksum	Menu	NONE LRC LRC_UID_B0 LEGIC_CRC8 LEGIC_CRC16
	Number format	Format setting for the card numbers on the data carriers (binary, BCD, or ASCII coding)	Menu	BIN_LSB BIN_MSB BCD ASCII
	Use number as UID	If this option is enabled, the card number is used as a unique number	Boolean	False
	MIFARE Classic	Settings for reading MIFARE Classic data carriers		
	SectorNum	The segment where UID data is stored	Integer	4
	ReadKey	Select the "Read Key" (Key A or Key B)	Menu	Key A
	WriteKey	Select the "Write Key" (Key A or Key B)	Menu	Key B
	Specific card type	Data carrier types		
	LegicPrime	Activation of LEGIC prime data carriers	Boolean	False
	LegicAdvant	Activation of LEGIC advant data carriers	Boolean	False
	MifareUltralight	Activation of MIFARE Ultralight data carriers	Boolean	False
	MifareClassic	Activation of MIFARE Classic data carriers	Boolean	False
	MifarePlus	Activation of MIFARE Plus data carriers	Boolean	False
	MifareDESFire	Activation of MIFARE DESFire data carriers	Boolean	False
	Generic ISO15693	Activation of ISO 15693 data carriers	Boolean	False
	GantnerConnect	Activation of GANTNER Connect	Boolean	False
	Generic ISO14443A	Activation of data carriers according to ISO14443A standard	Boolean	False
	Generic ISO14443B	Activation of data carriers according to ISO14443B standard	Boolean	False
	FeliCa	Activation of FeliCa data carriers	Boolean	False
	Prox-125kHz	Activation of proxy (125 kHz) data carriers	Boolean	False
	Mifare DESFire	Settings for reading MIFARE DESFire data carriers		
	ReadKeyNum	Number of the "Read Key"	Integer	1
	WriteKeyNum	Number of the "Write Key"	Integer	2
	ApplicationId	ID of the target DESFire application	Text	DF8405

	EncryptionMode	Select the type of encryption mode	Menu	AES
	FileNum	File number to read data from	Integer	1
	FileCommMode	File communication mode: "PLAIN", "MACED", "ENCIPHERED"	Menu	ENCIPHERED
	FileType	File type: "STANDARD", "BACKUP"	Menu	Backup
	File Data Offset	Offset of the data in the DESFire locker file	Integer	0
	ISO15693	Settings for reading ISO 15693 data carriers		
	GeneralBlockNum	The segment where general data is stored	Integer	13
	CertificateBlockNum	The segment where certificate data is stored	Integer	15
	LockerBlockNum	The segment where locker data is stored	Integer	19
	HID Prox	Settings for reading HID iClass data carriers		
	CheckFacilityCode	This setting is used to check the company ID number of the data carriers and controllers. These must match when enabled, which means that no non-system data carriers can be used.	Boolean	True
	Use all PACS Bits as UID	If this option is enabled, the entire HiD PACS data (incl. parity bits) is used as UID. There is no interpretation of the bit format.	Boolean	False
	Segment 2 configuration	Same settings as for segment 1		
Application				
	Master cards			
	MasterCard1 - 10	Fields to enter number for MASTER data carrier 1-10	Hex	00000....
	General			
	Emergency Mode	Function for emergency operation. Not used in standalone mode.	Menu	LOCKER_MODE
	Send Alive Requests	Not used in standalone mode.	Boolean	False
	Auto Close - FreeLocker	When set to "True", a user can close a locker in free locker mode by pushing the locker door shut (door is not locked, only held shut) and reopen it by pressing again. NOTE! The door is not locked. It can be opened by anyone without a data carrier.	Boolean	False
	Auto Lock - PersonalLocker	When set to "True", a user can lock their personal locker without a data carrier, just by pressing the door shut.	Boolean	False
	Locker Manipulation Detection	Not used in standalone mode.	Boolean	True
	Locking Timeout At Host Command	Not used in standalone mode.	Integer	10
	Operating Mode	Select the mode of the sub controller here: - ONLINE: The sub controller connects via a main controller to a server via which it is controlled by management software. - STANDALONE: The sub controller operates autonomously without connection to a main controller or server (this feature is described in this manual). When this mode is selected, an additional configuration option is displayed for each sub controller lock (Configuration > Application > Locker config). After selecting STANDALONE, the configuration must be transferred to the sub controller with "OK" and the configuration window reopened.	Menu	STANDALOLNE
	Alarm Mode	Select this option to enable the alarm surveillance for the lockers.	Boolean	True
	Push to Open - Personal Locker	Not used in standalone mode.	Boolean	False
	Push to Open - Dynamic Locker	Not used in standalone mode.	Boolean	False
	Push to Open - Free Locker	Not used in standalone mode.	Boolean	False
	Push to Open timeout	Not used in standalone mode.	Integer	30

Data handling			
Reading sequence	Setting for reading data carriers: - FIRST_AND_SECOND_SETTING: Up to two segments can be read on one data carrier. FIRST_OR_SECOND_SETTING: Two differently coded data carriers can be read.	Menu	FIRST_AND_SECOND_SETTING FIRST_OR_SECOND_SETTING
Locker signals			
Beeper	Defines whether the acoustic signal transmitter of the sub controller / locks should be used or not.	Boolean	True
AcousticAlarm	Switches on / off an acoustic signal on the GAT NET.Lock in the event of an alarm.	Boolean	False
GAT Lock 5000 Compatibility	The LED of the GAT NET.Lock is used as with the predecessor GAT Lock 5000 system.	Boolean	False
Show Rented Status	Indicates whether a person has been assigned to the locker when in personal locker programming card mode.	Boolean	False
Color unlocked / not reserved	Defines the LED color of the connected GAT NET.Lock 7020 displayed when the locker is free, i.e., the locker door is not locked and not reserved (e.g., GREEN = LED is green, BLACK_OFF = LED is off).	Menu	GREEN
Intensity unlocked / not reserved	Brightness of the LED display in percent. E.g., "70" = 70% of the maximum brightness. Refers to the "Color unlocked / not reserved" setting.	Integer	70
Color locked / reserved	Defines the LED color of the connected GAT NET.Lock 7020 displayed when the locker is occupied, i.e., the locker door is locked or reserved (e.g., GREEN = LED is green, BLACK_OFF = LED is off).	Menu	GREEN
Intensity locked / reserved	Brightness of the LED display in percent. E.g., "70" = 70% of the maximum brightness. Refers to the "Color locked / reserved" setting.	Integer	70
Advanced Acoustic Signaling Mode	If this setting is enabled, low-high and high-low tones are emitted. The signaling is analogous to the GAT ECO.Lock 7xxx lock.	Boolean	False
One time signaling (Eco.Lock compatibility)	Similar to the GAT ECO.Lock locks, this option sets the LED to switch on only briefly (e.g., when the locker door is pressed or after opening/locking) and is otherwise switched off.	Boolean	False
Beeper loudness	Volume level of the GAT NET.Lock beeper in percent.	Integer	100
Locker config	Configuration of the individual locks on the sub controller. Only visible when the mode is set to STANDALONE (Configuration > Application > General > OperatingMode)		
Chx Number	Locker number	Integer	0
Chx Mode	Operating mode of the lock: - FreeLocker: Any unoccupied locker can be selected. - PersonalLocker_ProgrammingCard: Personal locker in which several data carriers can be programmed using a programming card. - PersonalLocker_ExpiryDate: Personal locker with expiration date - FreeLockerUniqueNumber: Free locker with UID mode - FreeLockerUniversal: Free locker universal mode	Menu	FreeLocker
Chx Index PL	Index number for personal locker mode. See "4.3.5 Personal locker expiry date mode".	Integer	0
Chx Antenna ADJ	Value for antenna adjustment. Only displayed and cannot be changed.	Integer	0
Standalone mode			
Auto Unlock point of time [min]	Unlock locker at a defined point in time (minutes after midnight). 0 = inactive	Integer	0

	Auto Unlock after locking active	Activating or deactivating the automatically open function after a certain locking duration of a lock.	Boolean	False
	Auto Unlock after locking [min]	Time to wait after locking a lock until the lock is automatically unlocked again. Value in minutes.	Integer	0
	Use Time Limit	Select the type of time limit for the locker (see "4.3.1. Free locker mode (with or without duration of use function)") "DURATION" or "POINT_OF_TIME"	Menu	DURATION
	Time Limit [min]	Time limit for locker usage. When using "DURATION", this value means the usage time in minutes. When using "POINT_OF_TIME" this value means the time point after midnight.	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	If set to "true", a valid expiry date must be set on the data carriers in order to be used (standard value of 1.1.2007 is not valid).	Boolean	False
	Last Open At Expired Date	When this option is enabled, a locker can be unlocked one more time using the data carrier that locked it (see "4.3.5. Personal locker expiry date mode").	Boolean	True
	Write Locker Data PL ExpDate	This setting is applicable for lockers in personal locker mode. When enabled, the status of the lock is written to the data carrier when a data carrier is read at a lock.	Boolean	False
	System data carrier	Settings for the SYSTEM data carriers		
	Read from	This setting defines which segment/area the data is to be read from the SYSTEM data carriers	Menu	IDENT 1 IDENT 2 SPECIAL
	LegicPrime	If the SYSTEM data carriers used are of the type LEGIC prime, enable this setting.	Boolean	False
	LegicAdvant	If the SYSTEM data carriers used are of the type LEGIC advant, enable this setting.	Boolean	False
	MifareClassic	If the SYSTEM data carriers used are of the type MIFARE Classic, enable this setting.	Boolean	False
	MifareDESFire	If the SYSTEM data carriers used are of the type MIFARE DESFire, enable this setting.	Boolean	False
	ISO15693	If the SYSTEM data carriers used are of the type ISO 15693, enable this setting	Boolean	False
	MOLA	If this setting is enabled, the MoLA App can be used for configuration (comparable to the GANTNER battery locks)	Boolean	False
	SiteKey	Enter the Site Key of the SYSTEM data carriers here	Hex	
Read only parameter				
	Production			
	ProductionData	Internal production data	Integer	
	ArticleNum	Part number of the lock	Integer	
	SerialNum	Serial number of the lock	Integer	
	HardwareVers	Hardware version 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 identification number of the hardware	Integer	
	ControllerType	Controller type of the lock		
	NumLockerChannels	Number of locks / locker channels on the sub controller	Integer	
	FirmwareVers	Version number of the firmware in the controller	Integer	
	BootloaderVers	Version number of the bootloader software in the controller	Integer	

Table 3.1 – Configuration settings of the GAT NET.Controller S in GAT Config Manager

3.4 Restarting a controller

In certain situations, e.g., after a network problem, it can be helpful to restart a controller. This means that the software in the controller is restarted.

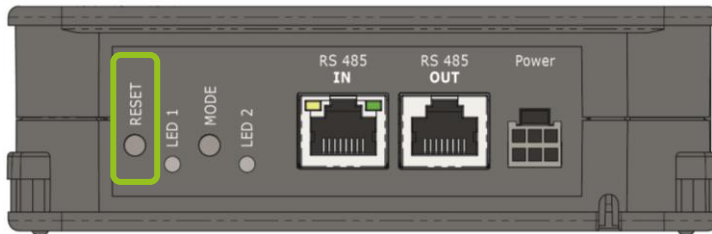


Figure 3.17 – RESET button to restart the controller

Complete the following steps:

- ▶ Press the RESET button for 5 seconds.
 - LED 2 flashes red and green.
- ▶ Release the RESET button.
 - The controller restarts after approx. 5 seconds. The configuration settings remain unchanged.

3.5 Resetting a controller to the default settings

Resetting a main or sub controller to the default settings deletes all configuration parameters saved in the controller and returns it to that same state it was in at the time of delivery.

NOTE! The resetting of a controller must only be performed by an authorized service technician. After resetting the controller, the entire locker system must be reconfigured via software.

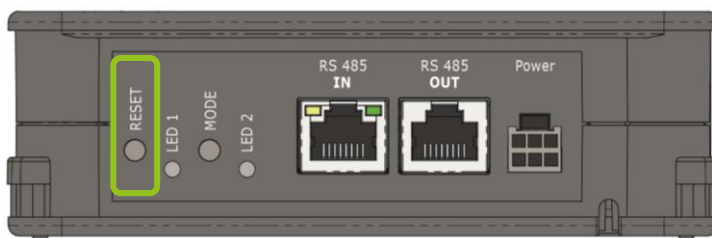


Figure 3.18 – RESET button to reset a controller

Complete the following steps:

- ▶ Press the RESET button for approx. 12 seconds.
 - LED 1 flashes blue.
- ▶ Release the RESET button and press it again within 3 seconds.
 - The configuration settings are reset to the default settings. The LEDs of the connected locks flash red/green while the controller restarts.

3.6 GAT NET.Lock antenna calibration

The antenna of the GAT NET.Lock must be calibrated so that an optimal reading range for the RFID data carriers is obtained. The antenna calibration process for the GAT NET.Lock is completed using the SERVICE data carrier.

NOTE! The locker door must be locked during antenna calibration to ensure the test conditions meet the operating conditions.

When?

- After installation of the locks.
- If reading of the data carrier takes a long time or does not work consistently.

How?

To calibrate the antenna of a lock using the SERVICE data carrier, follow these instructions.

- ▶ Lock the locker door.
 - The LED is red, and the door is closed.
- ▶ Hold the SERVICE data carrier next to the lock LED.
 - The LED flashes green.
- ▶ Hold the SERVICE data carrier next to the lock LED again.
 - A short beep is emitted and the LED flashes green. The antenna calibration is completed automatically, which takes about 1 second.
- ▶ When the SERVICE data carrier is read by another locked locker, the antenna calibration is immediately completed at this locker as well (beep tone).
- ▶ Wait approx. 20 seconds to complete the antenna calibration function.
 - The LED of the locker flashes red again and the locker remains locked.

3.7 GAT NET.Lock signalization overview

The GAT NET.Lock displays current status information via an integrated multi-colored status LED. The status LED is designed to remain visible through a hole in the locker door even when the locker door is closed. The following tables show the different LED signals and their corresponding lock states.

3.7.1 General (applicable for all modes)

LED signal (each field = 0.5 second)								Status	Configurable
1	2	3	4	5	6	7	8		
Green	Red	Green	Red	Green	Red	Green	Red	Not configured (default setting on delivery)	
Green	Green	Green	Green	Green	Green	Green	Green	Door is open, lock is unlocked (also when pre-closed)	
Green		Green		Green		Green		Door is closed, ready to lock	
Red	Red	Red	Red	Red	Red	Red	Red	Door is closed and locked	
Red		Red		Red		Red		Door is closed and locked, data carrier not valid	
			Red		Red		Red	ALARM (recommended with beeper)	X (beeper)
						Red		Door is closed and locked, lock is disabled	
						Green		Door is open, lock is disabled	
Green	Green	Green	Red	Red	Red			Door is open, lock is in cleaning mode	X
Red	Red	Red	Green	Green	Green			Door is closed and locked, lock is in cleaning mode	X

Table 3.1 - LED status signals of the GAT NET.Lock – Valid for all modes

3.7.2 Personal locker mode

LED signal (each field = 0.5 second)								Status	Configurable
1	2	3	4	5	6	7	8		
Green	Green	Green	Green	Green	Green	Green	Green	Door is open, lock is unlocked, no data carrier assigned	
Green	Green	Green	Green	Green	Green	Green	Red	Door is open, lock is unlocked, min. 1. data carrier assigned	X
Red	Red	Red	Red	Red	Red	Red	Red	Door is closed, lock is locked, min. 1. data carrier assigned	
Red	Red	Red	Red	Red	Red	Red	Green	Door is closed, lock is locked, no data carrier assigned	X

Table 3.2 - LED status signals of the GAT NET.Lock - Personal locker mode

3.7.3 GAT Lock 5000 mode

To operate in this mode, the GAT NET.Lock must be configured accordingly.

LED signal (each field = 0.5 second)								Status	Configurable
1	2	3	4	5	6	7	8		
								Door is open, lock is unlocked	
Red	Red	Red	Red	Red	Red	Red	Red	Door is closed and locked	
Red	Red		Red	Red		Red	Red	Door is closed, ready to lock	
Red		Red		Red		Red		Door is locked, data carrier not valid	

Table 3.3 - LED status signals of the GAT NET.Lock - GAT Lock 5000 mode

4. OPERATION

4.1 General

In general, the GAT NET.Lock supports the same modes as the battery-powered offline locks from GANTNER (GL7p series, GAT ECO.Lock 7000 series, GAT ECO.Side Lock 7000 series).

The operating modes "free locker" and "personal locker" are supported in standalone mode. In free locker mode, the user can choose any unoccupied locker they want to use. In personal locker mode, the user is assigned a specific locker and only they have access to use this locker.

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 not be used for both a personal locker and a free locker.

4.2 Target group

This chapter contains information for the technicians responsible for commissioning the GAT NET.Lock Standalone and for servicing it in case of operational problems.

4.3 Operating modes

The GAT NET.Lock Standalone can function in one of the following operating modes:

- Free locker **NOTE!** The duration of use function is not available for LEGIC prime systems.
- Free locker universal
- Free locker unique number **NOTE!** This mode is only available for MIFARE or ISO 15693 systems.
- Personal locker programming card
- Personal locker expiry date



The operating modes of the locks can be set in the controller configuration (see "3.3.4 Operating mode").

Requirements for MIFARE and ISO 15693 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 coded accordingly
Free locker universal	The locker segment must be unused (encoded with all zeros) and the access keys must be correct
Free locker unique number	All MIFARE and ISO 15693 data carriers are possible
Personal locker programming card	All MIFARE and ISO 15693 data carriers are possible
Personal locker expiry date	Data carrier must be coded accordingly

Figure 4.1 – Requirements for data carriers

4.3.1 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 GAT NET.Controller. If the date has passed, the locker cannot be used.

NOTE! The GAT NET.Lock and GAT NET.Controller do not automatically adjust to daylight saving time changes. This must be considered when defining the validity or expiry date.

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.

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 release their data carrier at an Info Terminal, e.g., a GAT Info 6100 F (Part No. 776891) or a GAT Info 6800 F (Part No. 765687).

NOTE! This function is only possible with MIFARE systems, and the data carrier must be coded accordingly for the duration of use function (the corresponding config bits on the data carrier must be set). In addition, the GAT NET.Lock or GAT NET.Controller respectively must be configured in GAT Config Manager for the function (see section "3.3.10. Configuration settings"). 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 "3.3.10 Configuration settings") 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 is set to 360 minutes. If the locker is locked at 17:00, it can be unlocked until 23:00. If the locker is locked at 21:00, it can be unlocked until 03:00 of the next day. The duration of use time is reset after the locker remains open for 60 minutes.

- 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.

Locking and unlocking lockers

- ▶ Close the locker door and hold it shut.
- ▶ Hold the data carrier next to the LED on the locker door for approx. 1 second.
 - The information on the data carrier is read.
- ▶ a) Valid data carriers: The LED flashes green and the locking action is carried out.
- ▶ b) Invalid data carriers: The LED flashes red briefly and the locker is not locked. A possible reason for this is that 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.
- ▶ Release the locker door.

4.3.2 Free locker universal mode

Free locker universal mode differs from the standard free locker mode in the following ways:

- Free locker universal mode allows the use of data carriers that are also used for other applications.
- No validity date in free locker universal mode
- The duration of use function is not possible
- The following requirements for the data carriers apply:
 1. The locker segment must be unused and "empty", i.e., coded with all zeros.
 2. The access keys must be correct.

Locking and unlocking lockers

- ▶ Close the locker door and hold it shut.
- ▶ Hold the data carrier next to the LED on the locker door for approx. 1 second.
 - The information on the data carrier is read.
- ▶ a) Valid data carriers: The LED flashes green and the locking action is carried out.
- ▶ b) Invalid data carriers: The LED flashes red briefly and the locker is not locked/unlocked.
- ▶ Release the locker door.

4.3.3 Free locker unique number mode

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

- All MIFARE and ISO 15693 data carriers can be used with the lock.
- There must be no GANTNER locker segment on the data carrier.
- When a locker is locked with a data carrier, the locker number is not written onto the data carrier.
- A data carrier cannot lock more than one lock per controller at the same time.

Locking and unlocking lockers

- ▶ Close the locker door and hold it shut.
- ▶ Hold the data carrier next to the LED on the locker door for approx. 1 second.
 - The information on the data carrier is read.
- ▶ a) Valid data carriers: The LED flashes green and the locking action is carried out.
- ▶ b) Invalid data carriers: The LED flashes red briefly and the locker is not locked/unlocked.
- ▶ Release the locker door.

4.3.4 Personal locker programming card mode

For the personal locker programming card mode, up to 32 data carriers per lock for the GAT NET.Controller S 7020 or up to 10 data carriers per lock for the GAT NET.Controller S 7000 can be authorized. Each data carrier can lock and unlock the locker as often as required and all share the same authorization access, e.g., family cards. The data carriers are authorized for use in the GAT NET.Controller S using the PROGRAM data carrier (included in the GAT ECO.Basic Set, see section "4.4 GAT ECO.Basic Set FD").

Authorizing data carriers

- ▶ Close the locker door and hold it shut.
 - The LED flashes green.
- ▶ Hold the PROGRAM data carrier next to the LED on the locker door for approx. 1 second.
 - The information on the data carrier is read.
- ▶ The GAT NET.Lock enters into programming mode.
 - The LED flashes red/green and the lock is ready to program data carriers.
- ▶ Within 5 seconds, hold the data carrier to be authorized next to the lock.
 - a) Successful authorization: The LED switches off for approx. 2 seconds and then the LED flashes red and green again. The data carrier is programmed, and the next data carrier can be programmed in the same way. Repeat this process until all the data carriers are programmed.
 - b) Unsuccessful authorization: The LED flashes red and a long beep is emitted. Possible reasons for this include:
 - The maximum of 32 (or 10) data carriers are already authorized for use with the lock.
 - The data carrier was not read by the lock correctly, e.g., the data carrier was not read for long enough or the data carrier is damaged.

You can repeat the last step using different data carriers to program these data carriers successively. To do this, hold the data carrier next to the LED within 5 seconds after removing the previous data carrier. If you wait longer than 5 seconds, the reading process is terminated, and the previously read data carriers are saved in the lock.

Deleting data carriers (removing authorization)

It is only possible to delete all data carriers in the GAT NET.Lock at once.

- ▶ Close the locker door and hold it shut.
 - The LED flashes green.
- ▶ Hold the PROGRAM data carrier next to the LED on the locker door for approx. 1 second.
 - The information on the data carrier is read.
- ▶ The GAT NET.Lock enters into programming mode.
 - The LED flashes red/green.
- ▶ Within 5 seconds, hold the PROGRAM data carrier again next to the LED for approx. 1 second.
 - The LED switches off for approx. 2 seconds. All previously authorized data carriers are now deleted from the GAT NET.Lock are no longer authorized to lock/unlock the locker anymore.

4.3.5 Personal locker expiry date mode

During check-in, the user receives a data carrier encoded with GANTNER data blocks. The FID is written onto the "general" data block and the guest's personal locker number together with the expiry date ("valid from" and "valid to") are written onto the "locker" data block of the data carrier. Furthermore, an index value is written onto the "locker" data block. The "valid from" date must always be valid, i.e., equal to or later than the data set in the GAT NET.Lock.

Upon first use of a locker, the expiry date ("valid to" date) and the current index value of the data carrier are stored in the lock. The user can use (lock / unlock) the lock beginning at the "valid to" date as often as he likes until the expiry date is not reached.

NOTE! The GAT NET.Controller does not automatically switch between daylight-saving or standard time. This must be taken into consideration when evaluating the recorded bookings or when authorizing data carriers for certain validity dates and times.

An unlimited number of data carriers (persons) can use the same locker. The following conditions apply for 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.

NOTE! The index of a lock can be reset to 0 using the PROGRAM data carrier from the GAT ECO.Basic Set. To do this, the PROGRAM data carrier must be held in front of the lock until the LED switches off briefly for confirmation.

Locking and unlocking lockers

- ▶ Close the locker door and hold it shut.
 - The LED flashes green.
- ▶ Hold an authorized data carrier next to the LED on the locker door for approx. 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 then lock and unlock the locker.
 - 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 previously authorized data carriers 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 previously authorized data carriers 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 and if the option "PersonalLockerSecureFlag" ist not set (see "3.3.10. Configuration settings").

- Release the locker door.
 - a) Valid data carriers: The information on the data carrier is saved in the lock. The locker state will switch, i.e., the locker will open when it was locked or will lock when it was open.
 - b) Invalid data carriers: The LED flashes red briefly and the locker state is not changed.

There is also no unlimited usage period for the locker, i.e., the expiry date must be a valid date (not "0"). After the "valid to" date the locker cannot be unlocked with the data carrier anymore.

4.4 GAT ECO.Basic Set FD

The following system data carriers are included in the GAT ECO.Basic Set FD (Part No. 1100550).

- 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)

Optional:

- OPEN MASTER data carrier



The Basic Set contains other items, e.g., a USB programming cable and a battery compartment key for the GAT ECO.Lock series. These items are not required for the GAT NET.Lock system.

4.5 Summary of the system data carriers

The data carriers included in the GAT ECO.Basic Set are required to configure and maintain a GAT NET.Lock locker system.



The system data carriers are coded to function with specific installations and will only function with the respective system.

4.5.1 MASTER data carrier

The MASTER data carriers can lock and unlock any GAT ECO.Lock 7xxx F/ISO in a system. If a user's data carrier is 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.

NOTE! The system operator must ensure that the MASTER data carriers are stored in a safe and secure location.

If one or multiple MASTER data carriers are lost, new MASTER data carriers can be ordered from GANTNER. Before the new MASTER data carriers can be used, all previous MASTER data carriers must be deleted from the lock and the new MASTER data carriers programmed in. Complete the following procedure:

- ▶ Press the locker door shut with one hand.
- ▶ Hold the DELETE MASTER (RESET) data carrier next to the GAT NET.Lock LED for approx. 1 second.
 - The information on the data carrier is read and the LED flashes red/green alternately.
- ▶ Remove the DELETE MASTER (RESET) data carrier from the LED.
 - All MASTER data carriers have been deleted. The LED continues to flash red/green alternately. The new MASTER data carriers can now be programmed in.
- ▶ Within 5 seconds, hold the first MASTER data carrier next to the LED for about 1 second.
 - The LED switches off for approx. 2 seconds. The MASTER data carrier is now programmed in.
- ▶ Remove the MASTER data carrier from the LED.

- The LED flashes red/green alternately again. The second MASTER data carrier can now be programmed. Hold it next to the LED.
- ▶ Repeat the process until all MASTER data carriers are programmed.
- ▶ If a MASTER data carrier is read for longer than 5 seconds during programming, the GAT NET.Lock automatically returns to the normal operating mode and the new MASTER data carriers are saved in the lock.

In addition, the MASTER data carriers can be entered in the configuration of the GAT NET.Controller S (see "3.3.2 MASTER data carriers"). Up to 10 MASER data carriers per sub controller can be added here.

4.5.2 DELETE MASTER data carrier

The DELETE MASTER data carrier deletes all MASTER data carriers stored in a GAT NET.Controller S. In addition, new MASTER data carriers can be programmed using the DELETE MASTER data carrier (see "4.5.1 MASTER data carrier").

NOTE! The system operator must ensure that the DELETE MASTER data carrier is stored in a safe location that is secured against unauthorized access!

4.5.3 OPEN MASTER data carrier

The OPEN MASTER data carriers can unlock any GAT NET.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 can unlock a locker but cannot lock the locker. The OPEN MASTER data carrier is not included in the Basic Set and must be ordered separately if required. This data carrier is only valid for the respective system.

NOTE! The system operator must ensure that the OPEN MASTER data carriers are stored in a secure location that is protected against unauthorized access!

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 maximum amount 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).

4.5.4 PROGRAM data carrier

For lockers operating in "Personal Locker Programming Card" mode, the PROGRAM data carrier is used to authorize user data carriers or to delete (block) already authorized data carriers (see "4.3.4. Personal locker programming card mode"). For lockers operating in "Personal Locker Expiry Date" mode, the PROGRAM data carrier is used to reset the index of the lock (see "4.3.5 Personal locker expiry date mode").

NOTE! The system operator must ensure that the PROGRAM data carrier is stored in a safe location that is secured against unauthorized access!

4.5.5 SERVICE data carrier

The GAT NET.Controller S settings are configured using the GAT Config Manager software while the sub controller is in configuration mode. To do this, the sub controller must be connected to the computer via the RS-485 programming cable (see "3.1 Configuration with GAT Config Manager") and be in configuration mode.

- ▶ To activate configuration mode in the sub controller, the SERVICE data carrier must be read at one of the locks connected to the sub controller.
 - The respective lock LED pulses green slowly.
- ▶ When the SERVICE data carrier is read twice in succession at a lock, the antenna of the lock is calibrated. See "3.6 GAT NET.Lock antenna calibration".

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!

 In the default state when the controller is still set to FID 9999 9999, communication can also be completed without having to activate configuration mode with the SERVICE data carrier.

4.5.6 APP KEY data carrier

The APP KEY data carrier is required to configure a GAT NET.Lock or GAT NET.Controller S with the MoLA App. This app operates on mobile devices with an Android operating system. When the controller is in factory mode and being configured for the first time, the APP KEY is not required. For later configuration changes however, the APP KEY data carrier is required (see also "3.2. Configuration with the MoLA App").

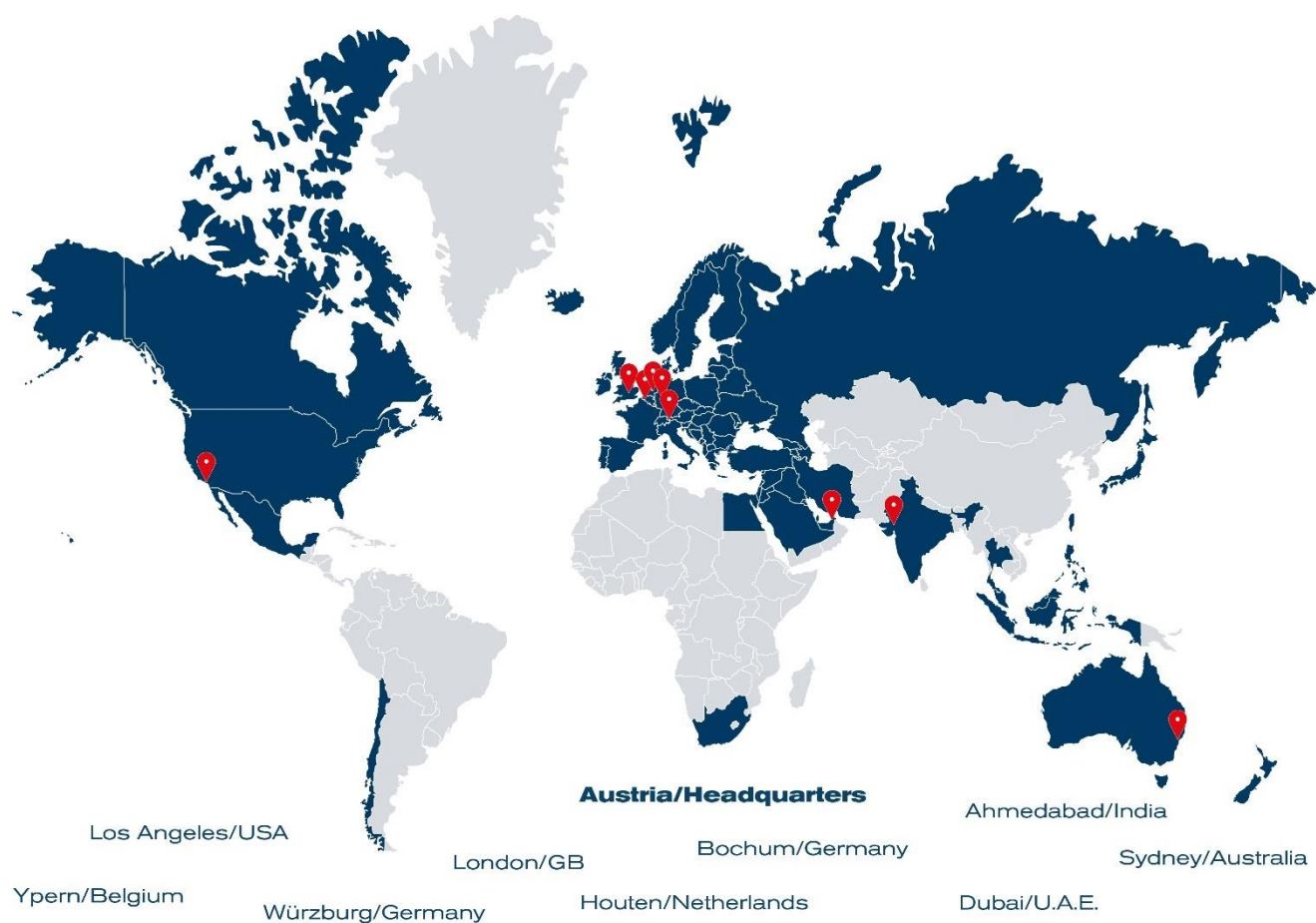
 To configure the GAT NET.Lock or GAT NET.Controller S using GAT Config Manager, the APP KEY data carrier is not required.

4.5.7 BATTERY data carrier

This data carrier has no function in standalone mode.

Note:

This manual is valid as of November 21, 2023. It is subject to change.
Amendments and changes 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