

G7 Central Locker System

GT7 Terminal with G7 Central Locker App for Controlling
GANTNER Electronic Locker Systems



© Copyright 2024 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

The contact information for questions regarding the GT7 terminals, G7 Central Locker app, and the GAT SMART.Lock 7000 system or for 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.

The GT7 terminal was developed and fabricated under the quality management standard ISO 9001 and GANTNER Electronic GmbH is also certified according to standard ISO 14001.



This product is in conformity with the following EC directives, including all applicable amendments:

- 2014/53/EU (Radio Equipment Directive)

The complete text of the CE Declaration of Conformity is available on the following internet link:

https://www.gantner.com/en/downloads-gt7-x500_1k3rpf49s2



GANTNER is committed to meeting or exceeding the requirements of the RoHS directive (2011/65/EU). The RoHS directive requires that manufacturers eliminate or minimize the use of lead, mercury, hexavalent chromium, cadmium, polybrominated biphenyls and polybrominated diphenyl ethers in electrical and electronic equipment sold in the EU after July 1, 2006.



The WEEE symbol on GANTNER products and their packaging indicates that the corresponding material must not be disposed of with normal household waste. Instead such marked waste equipment must be disposed of by handing it over to a designated electronic waste recycling facility. Separating and recycling this waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. Please contact your local authority for further details of your nearest electronic waste recycling facility.

WARNING!

This is a Class A device. This device can cause radio interference in the home. In this case, the operator may be required to take appropriate measures.



Only valid for the GT7.x500 FCC INFORMATION (U.S.A.)

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that of which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Warning Statement:

[Any] changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Compliance Information Statement:

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions: (1)
This device must not cause harmful interference, and (2)
this device must accept any interference received,
including interference that may cause undesired operation.

Only valid for the GT7.x500 IC (Canada)

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

- (1) This device may not cause interference; and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- 1) l'appareil ne doit pas produire de brouillage;
- 2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CONTENTS

1	INTRODUCTION	9
1.1	About this manual	9
1.2	Chapter overview	9
1.3	Target groups	10
1.4	Formatting	10
1.4.1	Safety-critical information	10
1.4.2	General information	10
1.4.3	Instructions and results	10
1.5	Terminology	11
1.6	Contact & inquiries	12
2	GENERAL INFORMATION	13
2.1	Intended use	13
2.2	Functional description	13
2.3	System overview	14
2.4	System components	15
2.5	GT7 terminal	18
3	TERMINAL AND APP INSTALLATION	19
4	CONFIGURATION	21
4.1	Target group	21
4.2	Requirements for use	21
4.3	Configuration options of the GT7 Central Locker	21
4.4	Configuration menu of the GT7 Central Locker	22
4.5	Configuration via G7 Connect (GANter Cloud)	23
4.6	Configuration via web interface (direct device configuration)	25
4.7	Device configuration settings	27
4.7.1	System overview	27
4.7.2	Network	29
4.7.3	G7 Connect	32
4.7.4	External web server	33
4.7.5	Web proxy	34
4.7.6	WLAN	35
4.7.7	Security and user	36
4.7.8	SCEP (Simple Certificate Enrollment Protocol)	37
4.7.9	Time	39
4.7.10	Display	40
4.7.11	Data carrier	41
4.7.12	Device	42
4.7.13	Fingerprint	44
4.7.14	Barcode interface	45
4.7.15	Sub controller	46
4.7.16	Sub controller RFID	50
4.8	App configuration settings	53
4.8.1	General settings	53
4.8.2	Free Locker	54
4.8.3	Personal Locker	57
4.8.4	Dynamic Locker	58
4.8.5	PIN code	60
4.8.6	Display texts	62

4.8.7	Hardware	64
4.8.8	Emergency mode	65
4.8.9	Design (LED color)	66
4.9	Installed apps	68
4.10	Cloud pairing	69
4.11	Licensing and coding points	72
4.12	Certificate management	74
4.13	Maintenance	76
4.13.1	Device	76
4.13.2	Update firmware	78
4.13.3	Addon bus (external devices)	79
4.13.4	Log viewer	80
4.13.5	Device state	81
4.13.6	Legal information	82
4.14	Integration in Relaxx	83
4.14.1	Step 1 - Add GT7 Central Locker to Relaxx	83
4.14.2	Step 2 – Select locker mode	85
4.14.3	Step 3 - Assign locker numbers	85
4.14.4	Step 4 – Authorize the users	88
4.14.5	Step 5 – Settings for PIN verification	89
5	OPERATION	91
5.1	Target group	91
5.2	Operation of the lockers	91
5.3	Operation of the GT7 Central Locker	92
5.4	Free locker	93
5.4.1	Door behavior of unoccupied lockers	93
5.4.2	Selecting a locker	94
5.4.3	Locking a locker	95
5.4.4	Unlocking a locker	97
5.5	Free locker with PIN code	99
5.5.1	Selecting a locker with PIN	99
5.5.2	Unlocking and opening a locker with PIN	101
5.6	Dynamic locker	103
5.6.1	Selecting and locking a locker	103
5.6.2	Unlocking and opening a locker	105
5.6.3	Releasing a locker	106
5.7	Personal locker	108
5.7.1	Selecting and locking a locker	108
5.7.2	Unlocking and opening a locker	109
5.8	PIN verification for data carriers	111
5.8.1	Selecting or opening the locker	111
5.8.2	Changing the PIN code	112
5.9	Master Dashboard	113
5.10	Language	117
5.11	Operation with Relaxx Management Software	118
5.12	Maintenance cards	119
6	TECHNICAL DATA	121
6.1	GT7 with G7 Central Locker App	121
6.2	GT7 dimensions	123

1 INTRODUCTION

1.1 About this manual

This manual contains a detailed description of how to install and configure the GT7 terminal with G7 Central Locker app. Furthermore, the operation for the end user is described. The installation and electrical connection of the GT7 terminal is also provided in this manual.

i Information on the installation and commissioning as well as the general settings for the GT7 devices is provided in the GT7 terminal manual. This manual only provides information on the configuration settings and operation of the GT7 Central Locker.

i The following terms for the device and app are used in this manual:

- GT7 terminal: The GT7 device (hardware), regardless of the installed app.
- G7 Central Locker app: The app that runs on the GT7 terminal.
- GT7 Central Locker: The combination of GT7 terminal with activated G7 Central Locker app.
- G7 Central Locker system: Sum of all components of the Central Locker System (GT7 terminal with G7 Central Locker app and the connected controllers and locks).

For the GT7 Central Locker to be able to control the connected GAT SMART.Lock 7001 or GAT NET.Lock 7020 locker locks, the GAT SMART.Controller S 7020 or GAT NET.Controller S 7020 controllers and PC software (Relaxx) are also required for the configuration and control of the system. The information needed to configure and operate the GT7 Central Locker for these system components is described in this manual. For a more detailed description of the GAT SMART.Lock 7000 or GAT NET.Lock 7020 systems, please refer to the manual of the respective system.

1.2 Chapter overview

In chapter "2 GENERAL INFORMATION", a functional description and a summary of system components of the GT7 Central Locker and GAT SMART.Lock 7000 systems and an explanation of the key terms used in this manual can be found.

Provided in chapter "4 CONFIGURATION" are the different configuration possibilities and parameters for the GT7 Central Locker. How the GT7 Central Locker is integrated into the Relaxx configuration software can also be found here.

Chapter "5 OPERATION" describes the process for opening and closing a locker via the GT7 Central Locker in the different operating modes. The Master Dashboard, which displays information about the locker system, is described as well.

Chapter "6. TECHNICAL DATA" lists the technical specifications and shows the measurement diagrams of the GT7 terminal.

1.3 Target groups

This manual contains information relevant for the different stages in the operating life of the GT7 Central Locker. Information regarding the installation, commissioning, and configuration of the GT7 Central Locker is separated into corresponding chapters. When a chapter is intended for a specific audience, this is clarified at the beginning of the chapter:

- Installation technicians (installation and configuration).
- Service technicians (service and operation).
- End users of the GT7 Central Locker (user manual).

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.

1.4 Formatting

1.4.1 Safety-critical information

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

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

1.4.2 General information

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



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

1.4.3 Instructions and results

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

- This symbol represents an action or instruction that must be followed.
 - This symbol represents the result after completing the previous instruction.

1.5 Terminology

Some terms are used frequently in this manual and these are defined below.

GT7 terminal

The device on which the G7 Central Locker app is running. Other apps can also be installed and activated (provided sufficient license points are available). This term refers to the hardware, i.e., the GT7 device, regardless of which app is currently active.

GT7 Central Locker

Denotes the combination of GT7 terminal with active G7 Central Locker app. The end user identifies themselves at the GT7 Central Locker using their RFID data carrier to unlock and lock their locker. Following valid authorization, the GT7 Central Locker sends a signal to the sub controller for the corresponding locker to be unlocked or locked.

G7 Central Locker App

The name of the software (app) that is enabled on the GT7 terminal to provide the Central Locker functionality for controlling the GAT SMART.Lock 7001 or GAT NET.Lock 7020 locks.

Locker

As used herein, the term "locker" refers generally to a locker, depot box, cabinet, or similar, which is locked by a GAT SMART.Lock 7001 or GAT NET.Lock 7020.

Lock

General term for the GAT SMART.Lock 7001 and the GAT NET.Lock 7020.

Sub controller

The GAT SMART.Lock 7001 is connected to a GAT SMART.Controller S 7020 sub controller (up to 24 locks per sub controller) and the GAT NET.Controller S 7020 sub controller is used for the GAT NET.Lock 7020 (also up to 24 locks per controller). The sub controllers receive control signals from the GT7 Central Locker via the connected serial network (RS-485) thereby controlling the corresponding locks.

PC software

Designates a software (e.g., Relaxx software), which is installed on a PC or server and via which the lockers (locks) can be managed, configured, and controlled.

User

In this manual, the term "user" refers to the person who wants to open or close lockers that are controlled by the GAT SMART.Lock 7001 or GAT NET.Lock 7020.

Data carrier

Data carriers are used by the end users to identify themselves at a GT7 Central Locker and unlock their assigned lockers. Data carriers with contactless RFID chips (Radio Frequency Identification) are available in various forms such as cards, key tags, or wristbands, and for different identification systems (LEGIC, MIFARE® or ISO 15693). The data carriers are read at the GT7 Central Locker's integrated RFID reader (LED ring below the display). If a barcode reader is connected to the GT7 Central Locker terminal, barcode media can also be used for identification.

TLS

The term "TLS" (previously "SSL") is an encryption protocol for secure data transmission. TLS can be enabled for a GT7 Central Locker in order to encrypt the data transmission between Relaxx and GT7 Central Locker using TLS.

1.6 Contact & inquiries

If you have any questions concerning the products contained herein, please contact your local sales partner or one of the GANTNER branch offices directly. The contact details are available via the following link:

www.gantner.com/locations

2 GENERAL INFORMATION

2.1 Intended use

The GT7 Central Locker is used to operate the GAT SMART.Lock 7001 and GAT NET.Lock 7020 locker locks. These GANTNER locks are the ideal solution for the convenient electronic locking of different lockers in a diverse range of industries, logistics, organizations, and educational institutions.

2.2 Functional description

The GT7 terminal can operate with different apps thereby providing flexible use for a variety of applications. This manual describes the operation with the G7 Central Locker app, which allows the terminal to control the GAT SMART.Lock 7001 and GAT NET.Lock 7020 electronic locker locks. In this manual, the combination of GT7 terminal with G7 Central Locker app is referred to as "GT7 Central Locker".

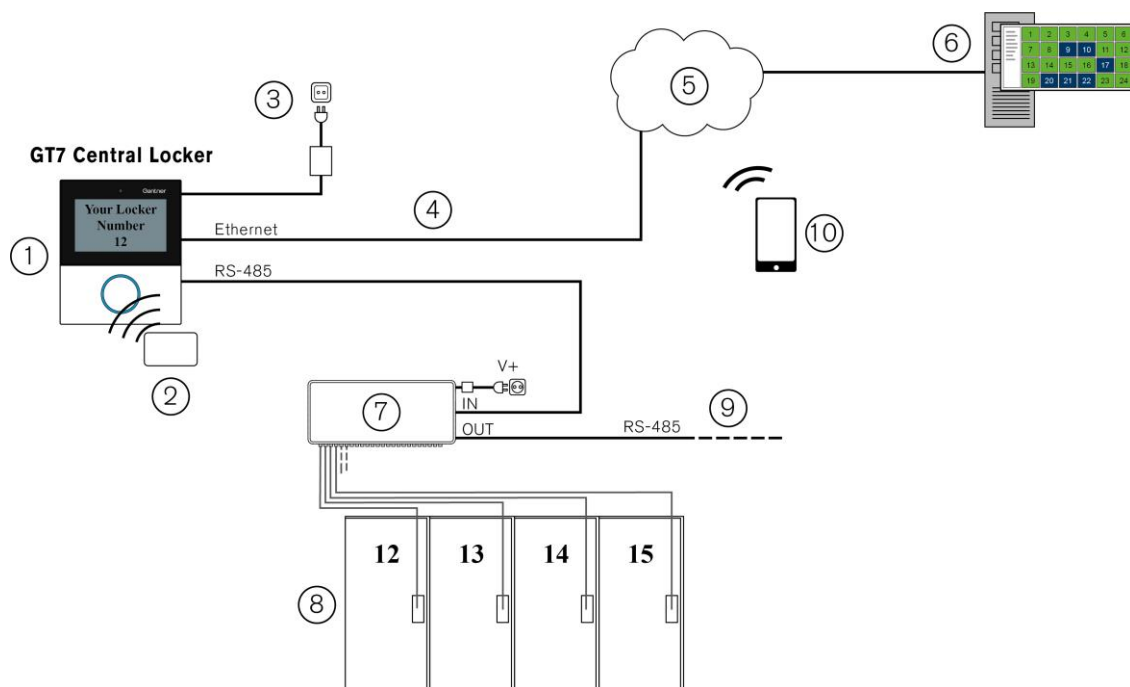
The control of the GAT SMART.Lock 7001 and GAT NET.Lock 7020, i.e., the locking and unlocking, is completed via the GAT SMART.Controller S 7020 or GAT NET.Controller S 7020 sub controller connected to the GT7 Central Locker. For the configuration and authorization control of the users, the GT7 Central Locker is connected to a LAN network via a network interface. The configuration can be completed via a web browser (web interface) or conveniently via the GANTNER Cloud (G7 Connect). Through the configuration, the functionality of the GT7 Central Locker can be customized to the respective requirements.

The PC software Relaxx is used for authorizing users. The GT7 Central Locker is integrated into this software. Relaxx then provides a graphical overview of all lockers that are controlled by the GT7 Central Locker. Here, the status of each locker is displayed in real time in addition to the direct control of the lockers (e.g., unlocking) being possible. To use this software, the authorized persons must log in with their username and password.

The "LockPal" app, which operates on mobile devices such as smartphones, can also be used to control the lockers. This app connects to Relaxx (min. version 7.0) and displays the lockers with their occupancy status. A locker can be selected and locked or unlocked directly via the app. Authorizations are assigned in Relaxx. For more information, see the LockPal manual.

2.3 System overview

The following figure shows schematically how the GT7 Central Locker operates within a GAT SMART.Lock 7000 system.



- 1 GT7 Central Locker
- 2 User identification via RFID data carrier
- 3 Power supply
- 4 Network connection
- 5 Connection to G7 Connect and/or a local network
- 6 Connection to PC/server via Relaxx management software
- 7 GANTNER sub controller
- 8 Lockers with GANTNER electronic locks
- 9 Connection possibility to additional GANTNER sub controllers
- 10 Locker operation using the LockPal app on a mobile device

Figure 2.1 - System overview + LockPal

2.4 System components

To operate the GT7 Central Locker with the GAT SMART.Lock 7000 system, the following components are available:

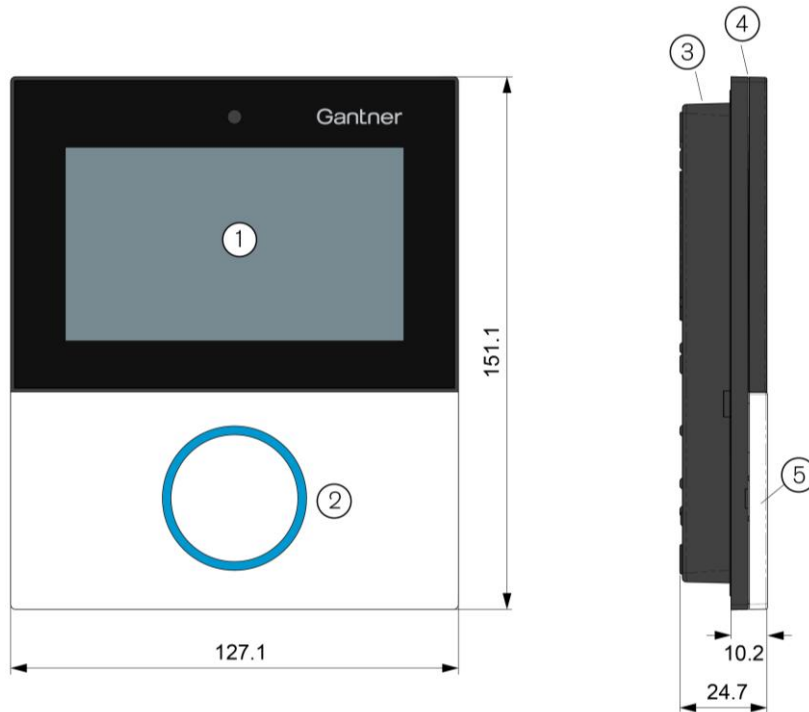


Figure 2.2 - Components of the GT7 Central Locker with GAT SMART.Lock 7001 and GAT NET.Lock 7020 locker systems

1. GT7.3300 (Part No. 1106119) LEGIC advant RFID reader and Proxy reader (125 kHz)
GT7.3500 (Part No. 919229) ISO 14443 (MIFARE®) and ISO 15693 RFID reader
GT7.3700 (Part No. 919229) LEGIC advant RFID reader, Proxy reader (125 kHz) and HID iCLASS®
GT7 terminal with installed G7 Central Locker app. Other variants are available (e.g., flush-mounted and built-in variants, etc.). Contact GANTNER for assistance with selecting the best GT7 terminal for you. In addition, an ordering guide for the GT7 terminals is available via the GANTNER homepage.
(Link: <https://www.gantner.com/download/46716/?v=46722>).
By ordering the article "G7 Device Initialisation" (Part No. 1102713), the G7 Central Locker app can be pre-installed by GANTNER when ordering the GT7 terminal.
2. GAT SMART.Controller S 7020 (Part No. 1101689)
Sub controller, i.e., the control unit for interconnecting the GAT SMART.Lock 7001 locks (max. 24 locks).
3. Power Cord 2m xxx – IEC 60320 C7
2 m power cord with a country-specific connector for the GAT NET.Power Supply 7020-1 100-240V / VI.
 - Power Cord 2m EU CH – IEC 60320 C7 (Part No. 494181). For European (incl. Swiss) power outlets.
 - Power Cord 2m UK – IEC 60320 C7 (Part No. 494282). For United Kingdom power outlets.
 - Power Cord 2m AUS – IEC 60320 C7 (Part No. 511474). For Australian power outlets.
 - Power Cord 2m USA – IEC 60320 C7 (Part No. 636835). For United States power outlets.
 - Power Cord 2m IND – IEC 60320 C7 (Part No. 636734). For Indian power outlets.
Power Cord Xm xxx – IEC 60320 C13
2 m or 2.5 m power cord with a country-specific connector for the GAT NET.Power Supply 7020 USB 100-240V / VI.
 - Power Cord 2.5m EU – IEC 60320 C13 (Part No. 495624). For European (excl. Swiss) power outlets.
 - Power Cord 2m CH – IEC 60320 C13 (Part No. 499123). For Swiss power outlets.
 - Power Cord 2.5m UK – IEC 60320 C13 (Part No. 499022). For United Kingdom power outlets.
 - Power Cord 2.5m AUS – IEC 60320 C13 (Part No. 402877). For Australian power outlets.
 - Power Cord 2m USA – IEC 60320 C13 (Part No. 270615). For United States power outlets.
 - Power Cord 2.5m IND – IEC 60320 C13 (Part No. 696892). For Indian power outlets.
4. GAT NET.Power Supply
 - GAT NET.Power Supply 7020-1 100-240V / VI (Part No. 1104784). Power supply for the sub controller without USB function.
 - GAT NET.Power Supply 7020 USB 100-240V / VI (Part No. 1100052). Power supply for the sub controller with the GAT NET.Lock 7020 USB (P) locks.
5. GAT SMART.Lock 7001 (Part No. 369737)
Electronic locker lock without connection cable and without bolt set.
6. GAT SMART.Lock 7001 Bolt Set (Part No. 1100400)
Bolt set with door shackle, door, and spacer plate. The bolt set is mounted onto the inside of the locker door.
7. GAT NET.Lock 7020
Electronic locker lock without connection cable and without bolt set.
 - GAT NET.Lock 7020 (Part No. 1100394).
 - GAT NET.Lock 7020 P (Part No. 1100391). Additional 125 kHz proxy reader.
 - GAT NET.Lock 7020 USB (Part No. 1100393). 2 x USB ports and LED locker light.
 - GAT NET.Lock 7020 USB P (Part No. 1100392). 2 x USB ports and LED locker light and additional 125 kHz proxy reader.

8. GAT NET.Lock BoltSet 7120 (Part No. 1100395)
Bolt set, consisting of door bracket and booster. Used for non-metallic doors. The bolt set is mounted on the inside of the locker door.
GAT NET.Lock BoltSet 7220 (Part No. 1100396)
Bolt set, consisting of door bracket and booster. Used for metallic doors. The bolt set is mounted on the inside of the locker door. The label carrier is also included in this bolt set.
GAT NET.Lock BoltSet 7320 (Part No. 1100397)
Bolt set, consisting of door bracket, booster, and metal carrier. Used for glass doors where the bolt set with the metal carrier is adhered to the glass door. Adhesive is not included. The bolt set is mounted on the inside of the locker door.
9. Patch Cable Open End 1.5 m (Part No. 618027)
1.5 m cable for the RS-485 connection, RJ45 plug on one end, open end on the other end.
10. GT7 Ethernet PoE Cable 25 cm (Part No. 1103383)
Ethernet cable, 1 x RJ45 plug as well as 2 x screw terminals for the GT7.
11. GAT NET.Lock Cable 5m (Part No. 734430)
5 m cable to connect a GAT SMART.Lock 7001 to a GAT SMART.Controller S 7020 sub controller. 4-pin MOLEX plug on both ends.
12. GAT NET.Lock Cable Extension 3m (Part No. 810021)
3 m extension cable for the GAT NET.Lock Cable 5m.
13. GAT Patch Cable 5805 - 5m (Part No. 909321)
Standard network cable (min. CAT.5) to connect the GAT SMART.Controller S 7020 sub controller to the GT7 Central Locker.

2.5 GT7 terminal



- 1 Display (touchscreen)
- 2 RFID reader with status LED
- 3 Rear part
- 4 Front part
- 5 RFID reader cover

Figure 2.3 – GT7 Central Locker

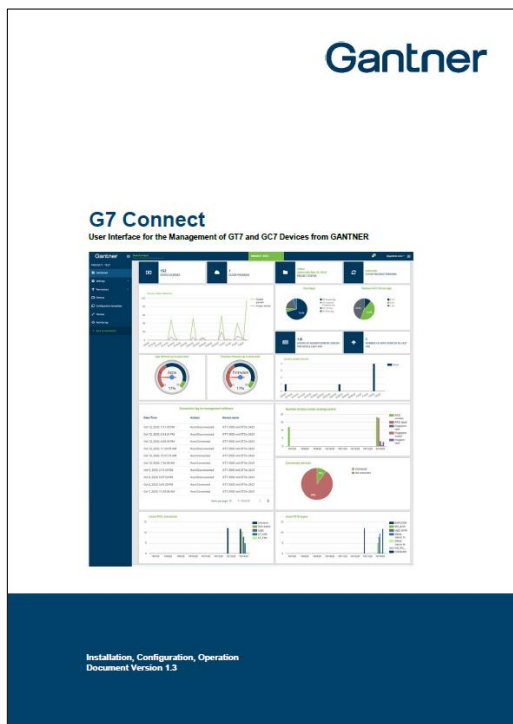
The GT7 Central Locker has a reader for RFID data carriers (Radio Frequency Identification) thereby enabling persons to be identified at the RFID reader of the GT7 via their personal data carriers. Further operation, such as the selection and confirmation of functions, is carried out directly on the device by touching the display (touchscreen).

3 TERMINAL AND APP INSTALLATION



The installation, electrical connection, and commissioning of the GT7 terminals are described in a separate device manual. For installation and commissioning, please read and carefully follow the information provided in the GT7 manual.

Figure 3.1 – GT7 terminal manual



G7 Connect (GANTNER Cloud) can be used for the convenient configuration and monitoring of the GT7 terminals. This is particularly recommended for larger systems with several GT7 terminals. A separate manual is available for G7 Connect with a description of all functions.

Figure 3.2 – G7 Connect manual

4 CONFIGURATION

4.1 Target group

This chapter provides information for technicians responsible for commissioning and configuring the GT7 Central Locker. Basic electro-technical knowledge is required. GANTNER recommends that the configuration of the system be completed by trained personnel only; GANTNER regularly offers training for its partners. This chapter provides an overview of the GT7 Central Locker's most important configuration settings. The PC software Relaxx can be used to configure the controller of a locker system with a GT7 Central Locker. The Relaxx manual describes the system configuration in greater detail.

4.2 Requirements for use

The following requirements must be met to use the G7 Central Locker app version 6.0 as described in this manual:

- Min. firmware version 3.0 must be installed in the GT7 Central Locker.
NOTE! The firmware can be installed via the web interface or via the GANTNER Cloud (see "4.13.2 Update firmware").
- At least one sub controller (GAT SMART.Controller S 7020 or GAT NET.Controller S 7020) must be connected (see the GT7 manual).
- Min. firmware version 2.5 must be installed in the sub controller and min. firmware version 3.1 in the GAT NET.Lock (can be imported via the web interface).
- To ensure there is sufficient power for the locks, the first sub controller must be connected to its own power supply. Supplying power from the GT7 Central Locker via the RS-485 cable does not provide sufficient power to lock the locks.
- When the Relaxx software is being used, min. software version 7.3 is required.

4.3 Configuration options of the GT7 Central Locker

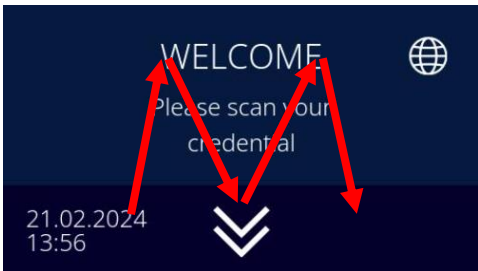
The functionality of the GT7 Central Locker can be configured in different ways:

- Basic settings can be directly set in the configuration menu of the GT7 Central Locker.
- Via G7 Connect (GANTNER Cloud): The GT7 devices in a system integrate conveniently into the GANTNER Cloud. There, all GT7 terminals are listed in an overview for the user and if the devices are online, they can be configured directly via this platform.
- Direct network connection via web interface: An HTTP connection to the GT7 Central Locker is established in a web browser and the web server integrated in the GT7 Central Locker then displays the configuration page with all settings.

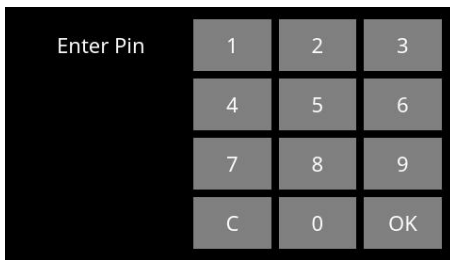
4.4 Configuration menu of the GT7 Central Locker

On the GT7 Central Locker, basic settings such as the IP address, DHCP address, etc., can be viewed and configured by opening the configuration menu. In the web interface you can select whether the configuration menu is able to be opened and whether the configuration of settings is possible. See chapter "4.7.12 Device" for more information.

- Write an "M" on the display with your finger (continuously without removing).



- A keypad for PIN-code entry is displayed.



- Enter the PIN code to access the configuration menu.

CAUTION! The default code is 0815, which should be changed in the configuration for security reasons after commissioning the GT7 terminal (see the GT7 terminal manual).

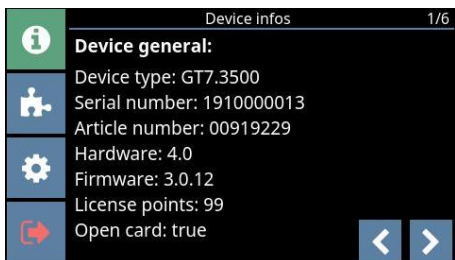


Figure 4.1 – Configuration menu

- In this menu, you can select the desired configuration page via the four icons to the left.



... Display of the device settings



... Display and start installed apps



... Configure device settings (DHCP, network, cloud connection, date & time)



... Exit configuration menu

- To exit the configuration menu, press the icon at the bottom left and then select "start active App" to start the last active app or press "reboot" to restart the GT7 Central Locker.

4.5 Configuration via G7 Connect (GANTER Cloud)

G7 Connect is GANTNER's web service to easily and conveniently manage and control all of a user's GANTNER devices. With their personal account, the user logs in and can then conveniently configure all their devices. In addition, it is possible to manage subordinate users (e.g., different gyms in a fitness chain). For this purpose, different hierarchy levels are used. All devices can be distributed among the subordinate users.

- Open a web browser and enter the following link: <https://gantner.cloud>
 - The login window for G7 Connect opens.

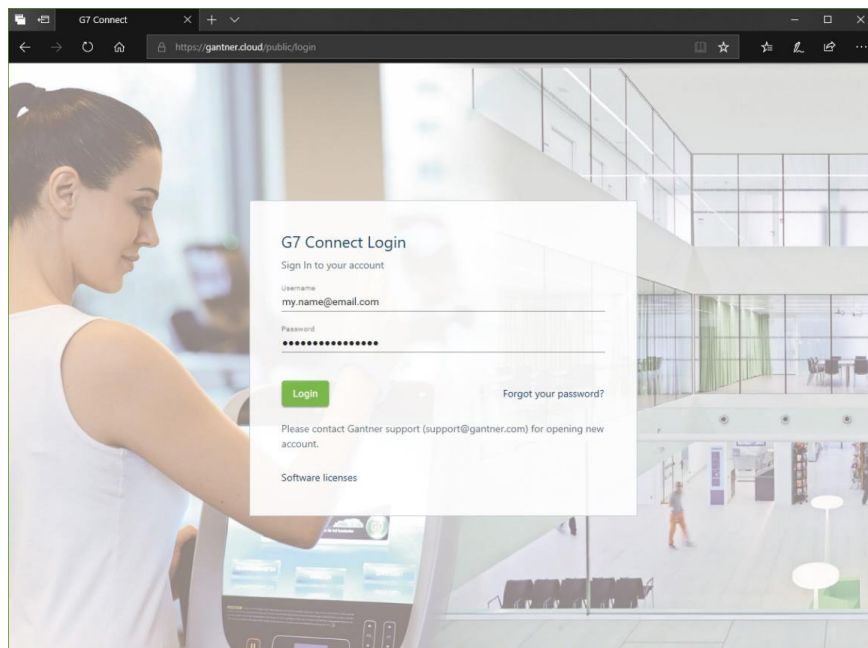


Figure 4.2 – Login window for G7 Connect

- Enter your username and password and click on "Login".
 - Your personal dashboard is displayed.

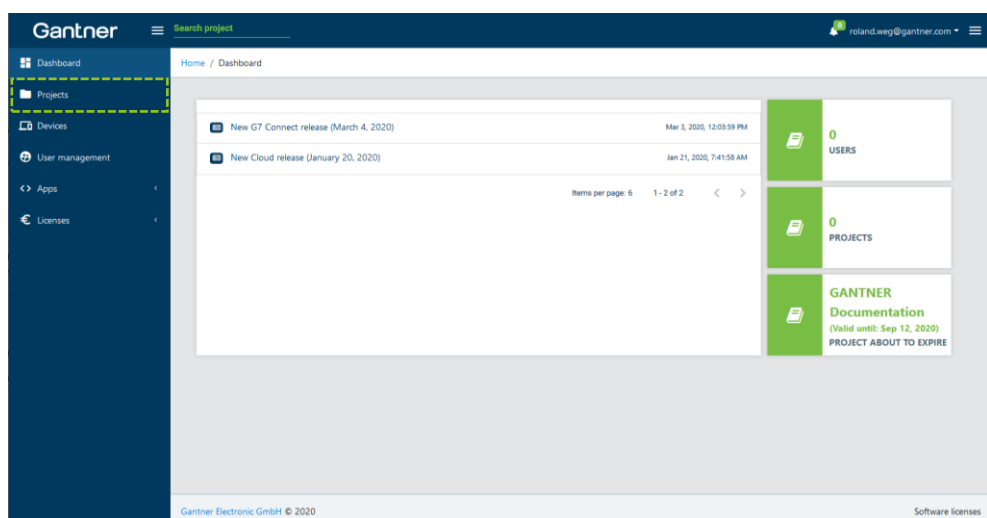


Figure 4.3 – Dashboard in G7 Connect

- Select the device to be configured here. To do this, you can, e.g., open the relevant project under "Projects" in the sidebar to the left.
 - The devices assigned to the project are listed.

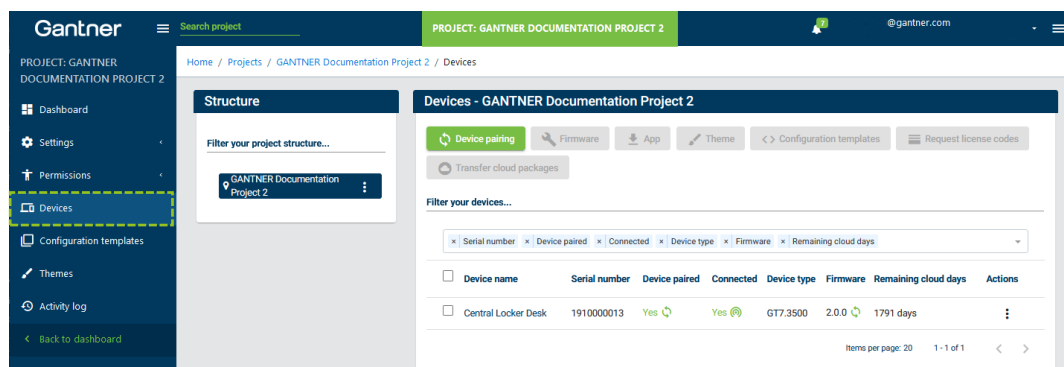


Figure 4.4 – Devices in the project

- Click on the device to be configured.
 - The device information opens with the configuration settings of the GT7 Central Locker.

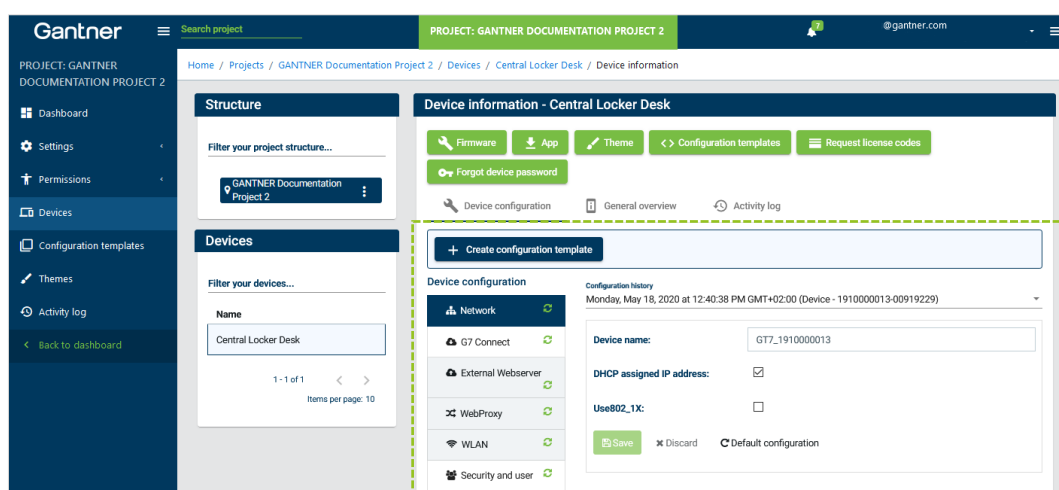


Figure 4.5 – Device configuration settings

- The configuration settings are displayed in the outlined area and can be edited there.
- After editing the settings, click on "Save" to save them in the GT7 Central Locker.
- Another possibility is the use of configuration templates. When a template is selected and confirmed, the configuration settings of that template are transferred to the GT7 Central Locker. To upload a configuration template, click on the green "<> Configuration" button.
 - The "Configuration" pop-up window opens.
- Select a configuration template and confirm with "Apply configuration".



See the G7 Connect manual for instructions on how to create an account and use the G7 Connect Cloud Service. There you will also find a description of how to create configuration templates.

4.6 Configuration via web interface (direct device configuration)

The configuration of a GT7 Central Locker via web interface is analogous to the configuration process in G7 Connect. Provided that the terminal is reachable via the network, a GT7 Central Locker can be directly accessed via a web browser.

- Open a web browser.
- Enter the IP address of the GT7 Central Locker into the address bar.

i The IP address of the GT7 Central Locker is displayed on the screen in the first row (eth0) during startup, i.e., when the supply voltage is applied. The IP address can also be accessed in the configuration menu of the GT7 Central Locker (see “4.4 Configuration menu of the GT7 Central Locker”).

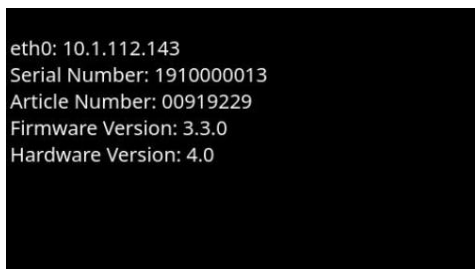


Figure 4.6 – Home screen of the GT7 Central Locker

- The login page of the web server opens on the GT7 Central Locker.

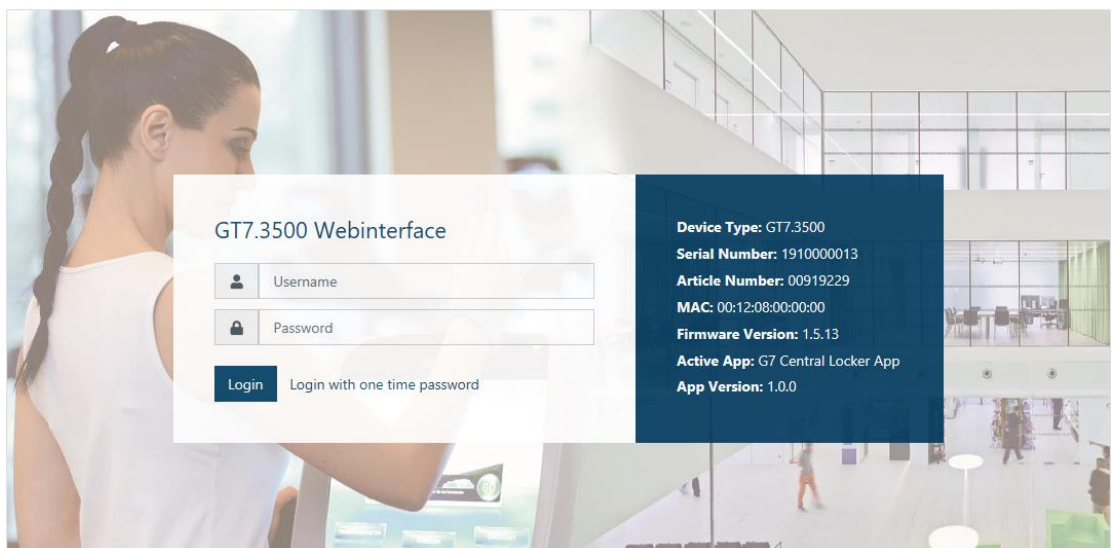


Figure 4.7 – Login screen of the GT7 Central Locker web interface

- In the login window, enter your username and password and click on “Login”.

NOTE! By default, the username is “admin” and the password is “GAT”. After the first login, please change the default details to maintain security (see “4.7.7 Security and user”).

- The configuration page of the GT7 Central Locker opens with the overview of the system settings.

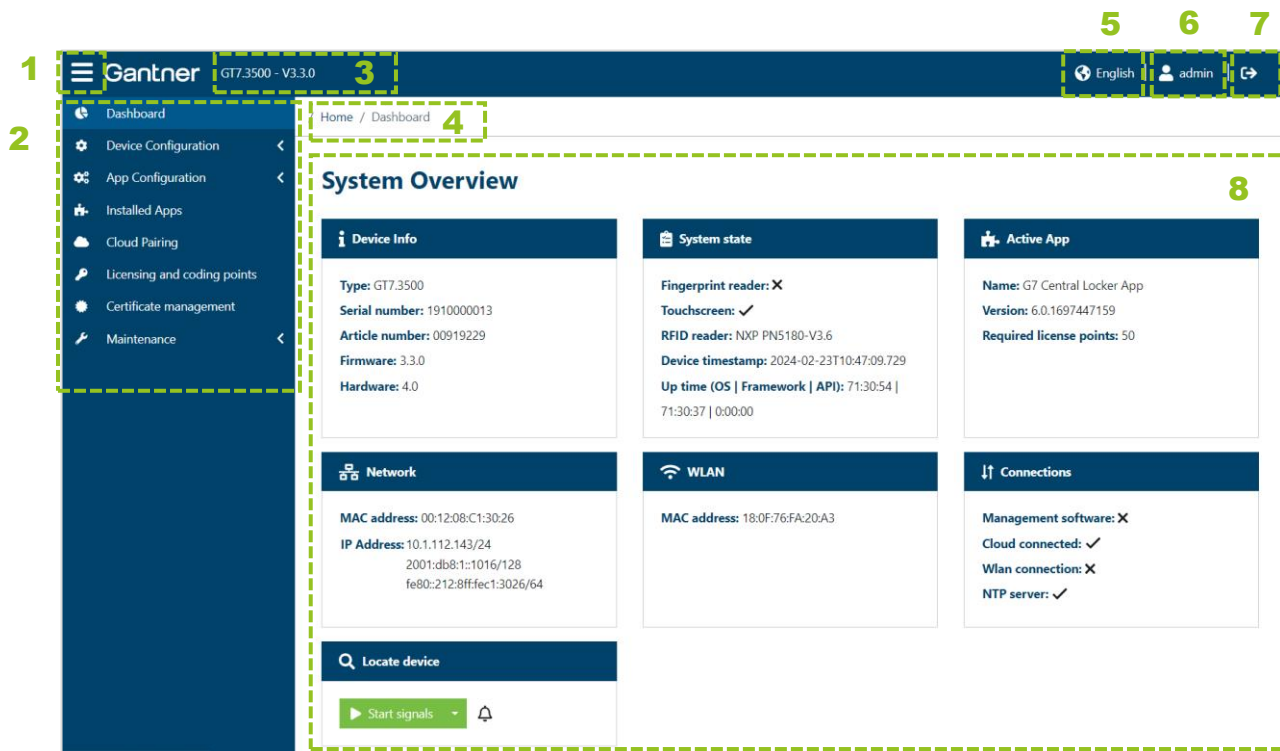


Figure 4.8 – GT7 Central Locker web interface - System overview

The following areas and functions can be selected in this window.

- | | |
|--------------------------------|---|
| 1 – Show / Hide menu: | This button allows you to show or hide the configuration menu to the left. |
| 2 – Configuration menu: | Available here is the menu list that you can use to access the respective settings pages of the GT7 Central Locker. |
| 3 – Firmware version: | Version of the firmware installed in the GT7 Central Locker. |
| 4 – Current path: | Displays a navigation aid with the name of the menu you are currently in. |
| 5 – Language: | The display language can be selected here. |
| 6 – User: | The logged in user is displayed here. |
| 7 – Log out: | By clicking here, the current user is logged out. |
| 8 – Display area: | This area displays all information and settings of the selected menu item. |

Below, all menu items are described with the possible settings.

4.7 Device configuration settings

4.7.1 System overview

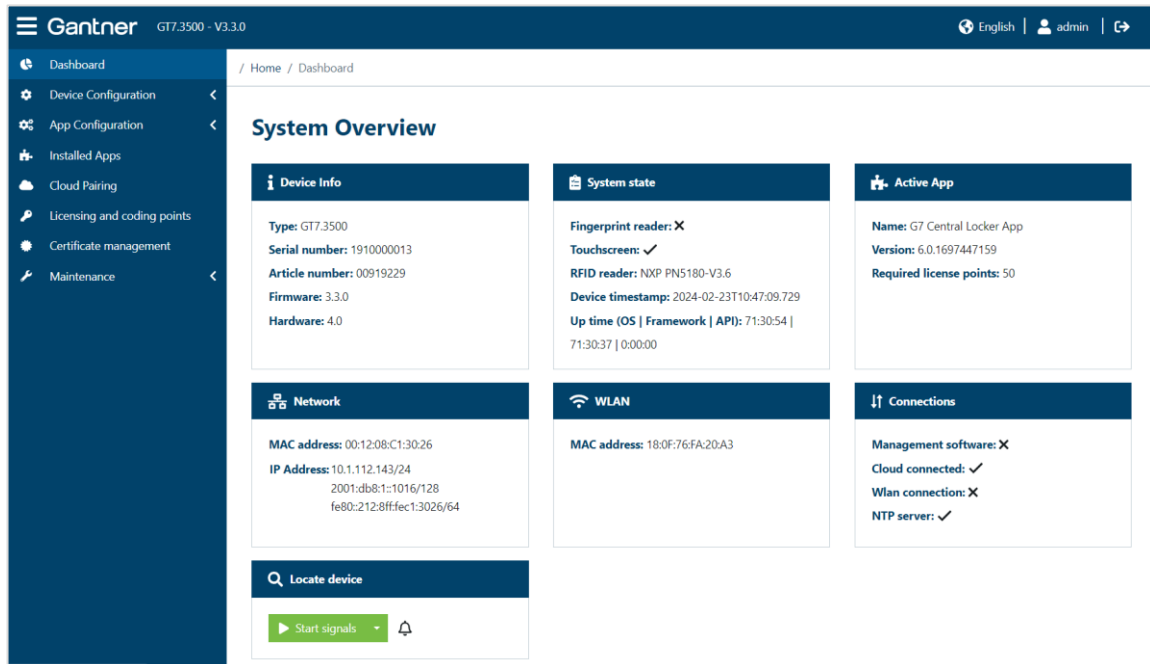


Figure 4.9 – GT7 Central Locker web interface - System overview

Provided here is an overview of the most important settings and status information of the GT7 terminal.

- Device Info: The device type as well as the serial/article numbers and versions of the hardware/firmware of the GT7 terminal are displayed here.
- System state: Here you see if a fingerprint reader is connected and if a touchscreen is connected and in use (which is usually true for the GT7 terminal). Also shown here is the firmware version of the RFID reader, the current time of the GT7 terminal, and for how long the GT7 terminal has been in continuous operation.
- Active App: Different apps can be installed on a GT7 terminal with only one app being active at a time. The active app, the app version, and the required license points are displayed here. License points are required for certain apps, which can be added via the "Licensing and coding points" page. There you can also add coding points in order to encode data carriers using the corresponding GT7 coding app.
- Network: The network addresses of the GT7 terminal are displayed here.
- WLAN: Shown here is the MAC address for the WLAN network (if used).

- Connections: The connections to the management software (e.g., eLoxx Relaxx), the G7 Cloud, a WLAN device or an NTP server (time synchronization) are displayed in this field.
- Locate device: If the “Start signals” button is clicked, the status LED of the RFID reader on the GT7 terminal flashes green briefly. Provided that the tone symbol (bell) next to it is not deactivated, a tone is also emitted from the device. This makes it easy to identify the device if you are unsure which configuration is currently open on which device.

4.7.2 Network

Figure 4.10 – GT7 Central Locker web interface - Network

Here, the settings for the connection to the GT7 Central Locker are displayed and can be changed via the network.

- Device name: An arbitrary name can be entered for the GT7 Central Locker here. When the network is scanned for devices, e.g., to add the GT7 Central Locker to Relaxx, the device is shown with this name.
- DHCP assigned IP address: When this option is enabled, the IP address of the GT7 Central Locker is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, disable this option and enter the network settings into the "Static IPv4 configuration" section. The Static IPv4 Configuration pane only appears if the option is disabled.
- IPv6 mode: If the network supports the IPv6 protocol for device addresses, here you can select whether to use this protocol and how the address assignment should take place.
 - Disabled: IPv6 mode is not used.
 - DHCP assigned IP address: IPv6 is used and addresses are assigned automatically using a DHCP server.
 - Static configuration: The IPv6 addresses can be set manually. The following settings are then displayed:

The screenshot shows the 'IPv6 mode' dropdown set to 'Static configuration'. Below it, the 'Static IPv6' section is expanded, showing fields for 'Static IPv6' (2001:db8:1234:5678), 'Subnet prefix length' (32), 'Static router' (2001:db8:1234:1001), 'Static primary DNS' (2001:4860:4860:8888), and 'Static secondary DNS' (2001:4860:4860:8844).

Enter the IPv6 address of the GT7 terminal and the information about the subnet mask, gateway and DNS server here. If you do not know this information, please speak to your network administrator.

- Stateless address autoconfiguration: With stateless address autoconfiguration, the GT7 terminal can automatically obtain an IP address by communicating with a router responsible for its network segment and thus determining the address.
- Use 802.1X authentication:

Select this option to enable 802.1X authentication. 802.1x authentication is a security protocol that works with 802.11 wireless networks such as 802.11g and 802.11b, as well as with wired devices. From the "Select authentication" menu, select the type of authentication method and define the relevant settings.

The screenshot shows the 'Use 802.1X authentication' checkbox checked. Below it, the 'Select authentication' dropdown menu is open, showing options: 'Protected EAP (PEAP)', 'Tunneled TLS (TTLS)', and 'TLS'. A 'Default' button is also visible.

NOTE! For further assistance with configuring these settings, please speak to your system administrator.

Protected EAP (PEAP)

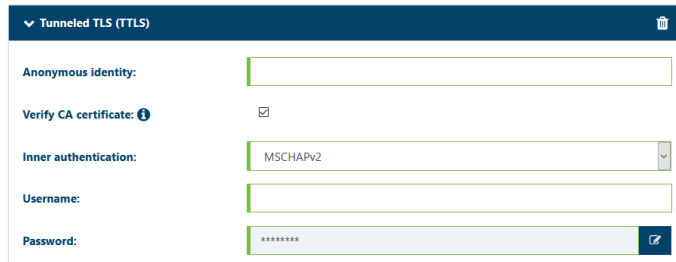
The screenshot shows the 'Protected EAP (PEAP)' section expanded. It includes fields for 'Anonymous identity', 'Verify CA certificate' (checked), 'Inner authentication' (set to MSCHAPv2), 'Username', and 'Password' (masked with asterisks).

Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Define the following settings:

- Anonymous identity: An anonymous identity can be entered here for systems that support a separate authentication outside of a secure tunnel. If no anonymous identity is provided, the default is to use the "Username" for outer and inner authentication.
- Verify CA certificate: It is recommended to enable this option. Certificates are managed via the "Certificate management" page (see chapter "4.12 Certificate management").

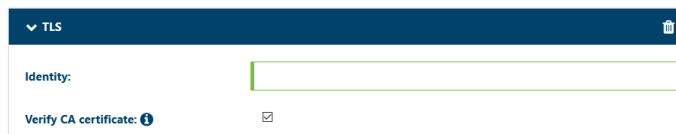
- Inner authentication: Select the type of protocol to use for inner authentication from the menu.
- Username: Enter the username to be used for authentication.
- Password: Enter the password to be used for authentication.

Tunneled TLS (TTLS)



Tunneled Transport Layer Security (TTLS) is a variant of TLS. In contrast to this, TTLS allows authentication not only via certificates but also via all other EAP mechanisms such as MD5 and one-time password. Unlike TLS, TTLS requires only server-side certificates. The settings for TTLS are analogous to those of PEAP described above.

TLS



Transport Layer Security (TLS) relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure communications between the WLAN client and the access point.

- Identity: Enter the value of the server identity field here.
- Verify CA certificate: It is recommended to enable this option. Certificates are managed via the “Certificate management” page (see chapter “4.12 Certificate management”).

4.7.3 G7 Connect

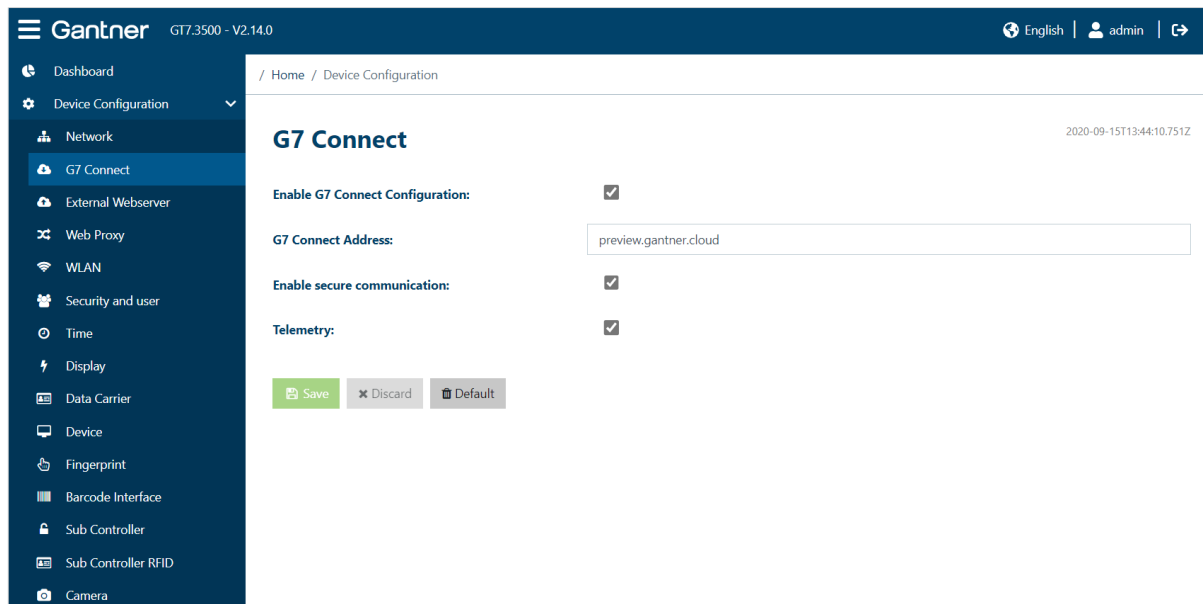


Figure 4.11 – GT7 Central Locker web interface - G7 Connect settings

The settings regarding the connection to the GANTNER Cloud G7 Connect are configured here.

- **Enable G7 Connect Configuration:** Select this option if you want to use the configuration set via G7 Connect for the GT7 Central Locker.
- **G7 Connect Address:** Enter the address of G7 Connect here.
- **Enable secure communication:** Select this option to encrypt the communication using TLS.
- **Telemetry:** Select this option if you want to send telemetry data to G7 Connect. This data does not contain any personal data (see the terms and conditions of G7 Connect for more information).

4.7.4 External web server

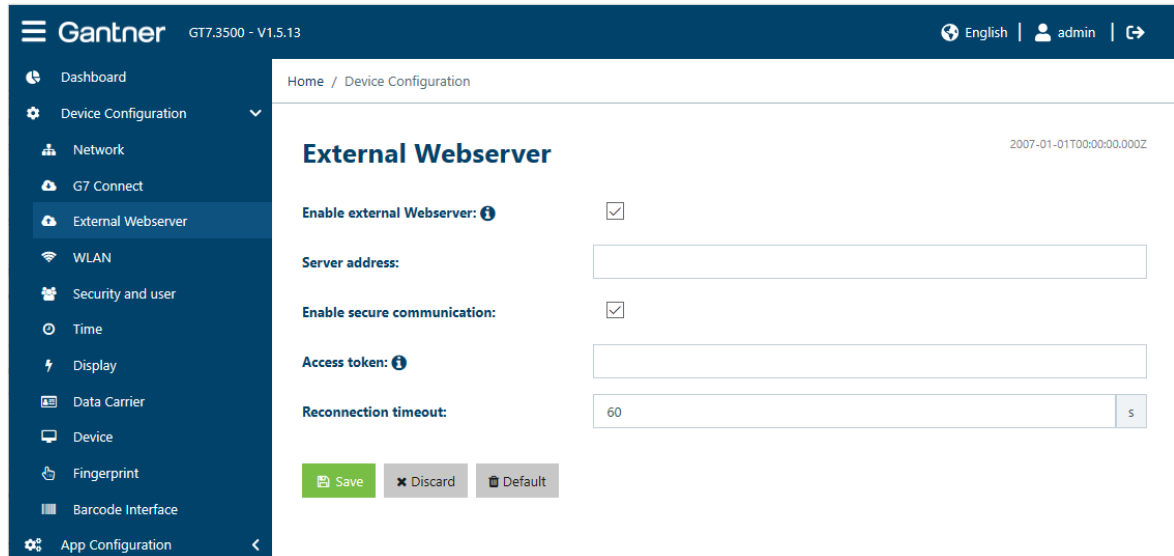


Figure 4.12 – GT7 Central Locker web interface - External web server settings

The GT7 Central Locker can function as a client or server. For the configuration as described here, the GT7 Central Locker is operating as a server, i.e., the PC connects to the GT7 Central Locker. If the GT7 Central Locker is operating as a client, an external web server can be used. In this case, communication is completed via this web server.

- Enable external Webserver: Select this option if a web server is to be used for communication. After selection, the following settings are visible.
- Server address: IP address of the web server (IPv4 format).
- Enable secure communication: When this option is selected, TLS is used for the web socket connection.
- Access token: In this field, an additional value for authentication can be specified, which is entered in the authorization field of the HTML header. What must be entered here depends on the implementation by the third-party software.
- Reconnection timeout: In this field, enter the waiting time in seconds until reconnection is attempted after the connection between the GT7 Central Locker and the management software has been interrupted.

4.7.5 Web proxy

The screenshot displays the Gantner web interface for configuring the Web Proxy. The sidebar on the left lists various system settings, with 'Web Proxy' currently selected. The main panel shows the 'Web Proxy' configuration page, which includes a header with the Gantner logo, version (GT7.3500 - V1.7.16), and user information (English, admin). The page title is 'Web Proxy', and the breadcrumb is 'Home / Device Configuration'. The 'Enable web proxy' checkbox is checked. Below this, the 'Http proxy' section is expanded, showing fields for 'Server address', 'Server port' (set to 8080), 'User name', and 'Password' (masked with asterisks). At the bottom of the form, there are three buttons: 'Save', 'Discard', and 'Default'.

Figure 4.13 – GT7 Central Locker web interface – Web proxy settings

A web proxy server can be configured in order to rout all outgoing connections over this web proxy server.

- Enable web proxy: Select this option if a web proxy is to be used for communication. After selection, the following settings are visible.
- Server address: IP address of the web proxy server (IPv4 format).
- Server port: Port number of the web proxy server.
- Username: Username used to access the web proxy server.
- Password: Password used to access the web proxy server.

4.7.6 WLAN

Figure 4.14 – GT7 Central Locker web interface - WLAN settings

A GT7 Central Locker can communicate via Wi-Fi instead of over the LAN network. If Wi-Fi is enabled, more options become available.

- Enable WLAN: With this option, WLAN can be activated or deactivated.
- DHCP assigned IP address: How the IP address is set is defined here. Select the option to obtain the address automatically from a DHCP server. If disabled, the static IP addresses can be entered into the “Static IPv4” configuration area.
- SSID: Enter the name of the WLAN network here.
- Authentication: Select “WPA PSK” here for the WLAN encryption method. You can then enter the PSK Key (password for the wireless network).
- IPv6 mode: Here you can select whether to disable the WLAN connection or, if not disabled, how the address should be assigned (“DHCP assigned IP address”, “Static configuration” or “Stateless address autoconfiguration”). Refer to chapter “4.7.2 Network” for information about the IPv6 network configuration settings.
- Standard gateway selection: Select from the menu the connection type (LAN Ethernet or Wi-Fi) to use for communication. When “Ethernet” or “WLAN” is selected, only the chosen connection type will be used with preference.

4.7.7 Security and user

Figure 4.15 – GT7 Central Locker web interface - Security and user settings

Here, you can define the users who are allowed to access the GT7 Central Locker via the web interface (Administrator user “Web interface”) and via the G7 WebSocket API (“Management software access”).

The user “Management Software Access (G7 WebSocket API)” is used, for example, by the management software Relaxx.

- Disable plain http and plain WebSockets:
Enable this option to prevent the GT7 from communicating using an unencrypted connection (e.g., HTTP instead of HTTPS).
- Activate account:
With this option, you can activate the respective user. If the option is disabled, the user has no access rights.
- Username:
The name of the user is displayed here. The name cannot be changed.
- Password:
Click on the blue edit button to the right and enter a password for the user. The password must be min. 8 characters long and contain at least one uppercase letter, one lowercase letter, and one number.
NOTE! If the default password is not changed for the “Management Software Access (G7 WebSocket API)” user, the Relaxx software creates a new, secure password for communication. If the password is changed here, it must also be entered into the Relaxx software.
- Enable FTP access:
Enable or disable the FTP server in the GT7 terminal via this setting.

4.7.8 SCEP (Simple Certificate Enrollment Protocol)

The screenshot shows the Gantner configuration interface for the GT7-3500 - V3.3.0 device. The left sidebar contains a menu with options like Dashboard, Device Configuration, Network, G7 Connect, External Webserver, Web Proxy, WLAN, Security and user, SCEP (selected), Time, Display, Data Carrier, Device, Fingerprint, Barcode Interface, Sub Controller, Sub Controller RFID, Camera, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'SCEP' and includes the following settings:

- Enable Simple Certificate Enrollment Protocol (SCEP):** ☒
- SCEP server URL:**
- Challenge password:**
- Encryption:**
- Use RA certificates from SCEP server:** ☒
- Renew server certificate:** ☒
- Renew 802.1X user certificate:** ☒
- Renew before expiration:** days

Below these settings is a section titled 'Certificate parameters' with the following fields:

- Country name (2 letter code):**
- State or province name (full name):**
- Locality name (eg, city):**
- Organization name (eg, company):**
- Organizational unit name (eg, section):**
- Common name (domain name or IP):**

At the bottom of the form are buttons for 'Save', 'Discard', and 'Default'.

Figure 4.16 – Configuration page of the GT7 Central Locker - SCEP

SCEP is a protocol for requesting and issuing digital certificates quickly and easily. These certificates are used to establish secure communication between the GT7 terminal and a host computer or server.

- Enable Simple Certificate Enrollment Protocol (SCEP):
Enable this option to use the SCEP function. The following additional settings and input fields are then displayed.
- SCEP server URL:
Enter the address (URL) of the server where the certificates are located here.
- Challenge Password:
Password that is used to access the SCEP server.
- Encryption:
Select the type of encryption to be used (AES or 3DES).
- Use RA certificates from SCEP server:
With this option, the certificates of the RA (registration authority) can be used. The RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.

- Renew server certificate: If this option is enabled, the certificate for the GT7 web interface and the certificate for the management software connection are renewed. The device restarts after the certificates have been installed.
- Renew 802.1X user certificate: If this option is enabled, the certificate for 802.1x authentication is renewed. The GT7 terminal is restarted after the certificate has been installed.
- Renew before expiration: The number of days entered here determines when the certificates will be renewed (xx days before the validity expires).
- Certificate parameters: Enter the data for the certificate in this area. The parameters must match those that were used to create the certificate.

4.7.9 Time

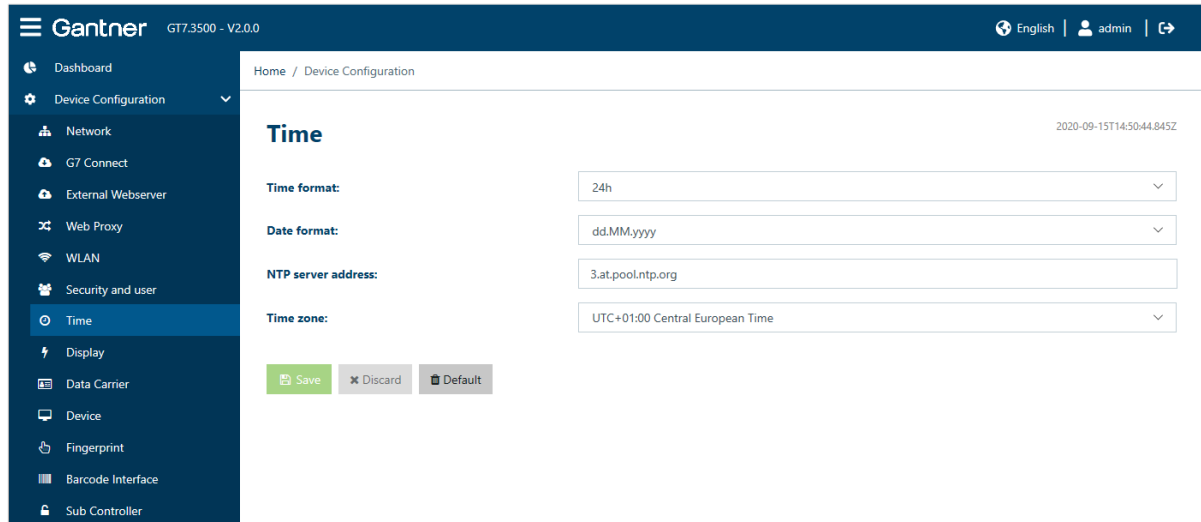


Figure 4.17 – GT7 Central Locker web interface – Time settings

With these settings, you can define how the time is displayed on the screen of the GT7 Central Locker.

- Time format:
 - 24h: The time is displayed in 24-hour format (example: 15:48)
 - 12h: The time is displayed in 12-hour format (example: 3:48 pm)
 - Hide clock: The time is not displayed on the screen of the GT7 Central Locker.
- Date format:
 - dd.MM.yyyy: The time is displayed in the international standard format, i.e., day.month.year (example for 15th September: 15.09.2020).
 - MM/dd/yyyy: The time is displayed in American format, i.e., month.day.year (example for 15th September: 09/15/2020).
 - Hide date: The date and time are not shown on the GT7 Central Locker's display.
- NTP server address:

An NTP server can be used to deliver the time to the users/devices in a network. Enter the address of the NTP server here. If no address is entered here (blank field), the NTP server will not be used.
- Time zone:

Select the time zone where the GT7 Central Locker is operating.

4.7.10 Display

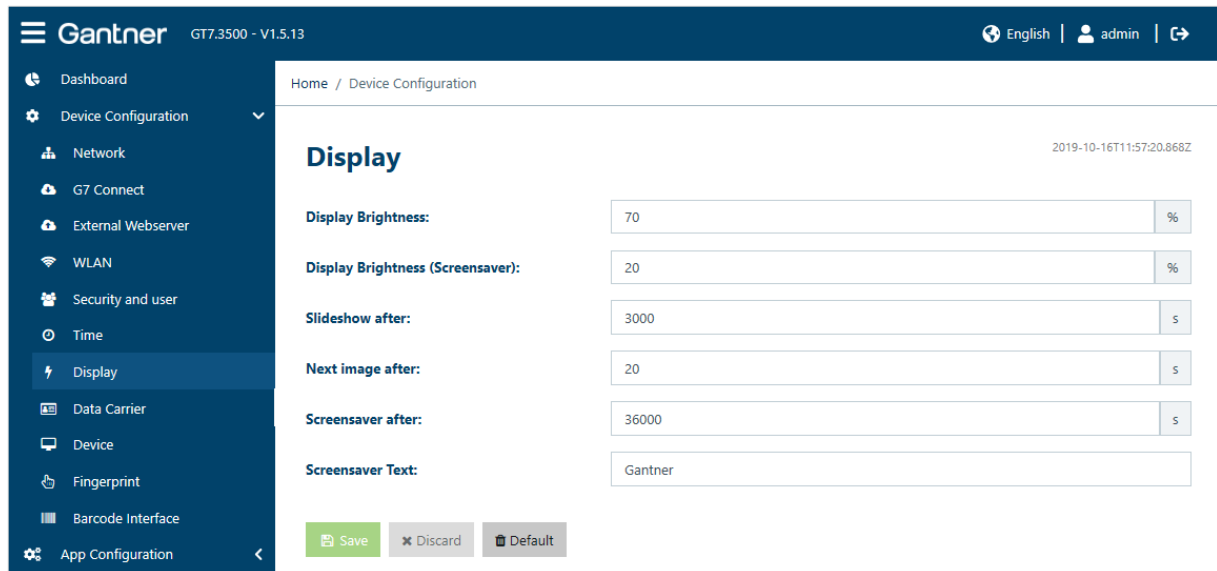


Figure 4.18 – GT7 Central Locker web interface – Display settings

These settings determine the brightness of the GT7 Central Locker display and when the display should switch to the screensaver or to the image slideshow.

- Display Brightness: Intensity of the display backlight between 0 and 100%. At 0%, the display is switched off.
- Display Brightness (Screensaver): Intensity of the display backlight when the screensaver (see below) is enabled.
- Slideshow after: Time in seconds for terminal inactivity after which an image slideshow (i.e., different pictures from the theme) is displayed. For more information on themes, see “4.9. Installed apps”.
- Next image after: Time in seconds after which the images in the slideshow are changed.
- Screensaver after: Time after which the screensaver is displayed. This time starts to run as soon as the slideshow is activated.
- Screensaver text: Text that is displayed when the screensaver is active. If no images are selected for the slideshow, this text will also be displayed when the slideshow is activated.

4.7.11 Data carrier

Figure 4.19 – GT7 Central Locker web interface – Data carrier settings

Here, the settings for the data carrier types to be used with the GT7 Central Locker are configured. These settings must be set correctly so that the data carriers can be used. Multiple data carrier types can be configured.

i The data carrier settings for the sub controller are defined in the menu “Sub Controller RFID” (see “4.7.16 Sub controller RFID”).

- Add Data Carrier: To configure a new data carrier type, click here and select the desired type from the list.
- Delete Data Carrier: You can delete an existing data carrier type or a segment in the data carrier via the trash icons   to the right.

The settings for the data carrier types vary depending on the type of data carrier you are using. For questions regarding the exact settings, please speak to your sales partner.

4.7.12 Device

Figure 4.20 – GT7 Central Locker web interface – Device settings

The general settings of the GT7 Central Locker are available here. These include:

- Location: You can enter a location here. This name is displayed for the user to help differentiate between many GT7 terminals. Special characters are not allowed. A notification is shown if you enter a special character.
- Serial/Article number: Display of the serial number and article number of the GT7 Central Locker.
- Sound volume: Loudspeaker volume; adjustable from 0 to 100%. Entering 0% mutes the sound.
- Pin code configuration menu: This code opens the configuration menu on the display of the GT7 Central Locker. To enter the code, write an “M” on the display. For more information see “4.4 Configuration menu of the GT7 Central Locker”.
- Configuration menu mode: Here you can select whether the configuration menu can be opened on the display of the GT7 terminal on-site and whether configuration changes are allowed. The configuration menu is described in chapter “4.4 Configuration menu of the GT7 Central Locker”.
 - Modify configuration: The menu can be opened and changes are possible, e.g., to the network settings, which can also be saved.
 - Show configuration: The configuration can be shown on the display of the GT7 Central Locker. However, changes to the settings are not possible.
 - Configuration menu disabled: The configuration menu cannot be opened on the local display.

- Log level:

Here you can define which types of events should be recorded by the GT7 terminal. This log can be downloaded and read in the "Log Viewer" menu (see "5.6.22 Log Viewer"). Different messages are logged depending on the setting configured here:

- ERROR: All errors are displayed. This includes connection errors to G7 Connect or locker operation errors, e.g., when a locker that is already locked must be locked again.
- WARNING: Warning messages are displayed. These include, e.g., log-in messages in the web interface.
- INFO: Information messages are displayed, e.g., when a data carrier is in the reading field and when it has been read.
- DEBUG: Detailed debug messages are displayed for service purposes.

4.7.13 Fingerprint

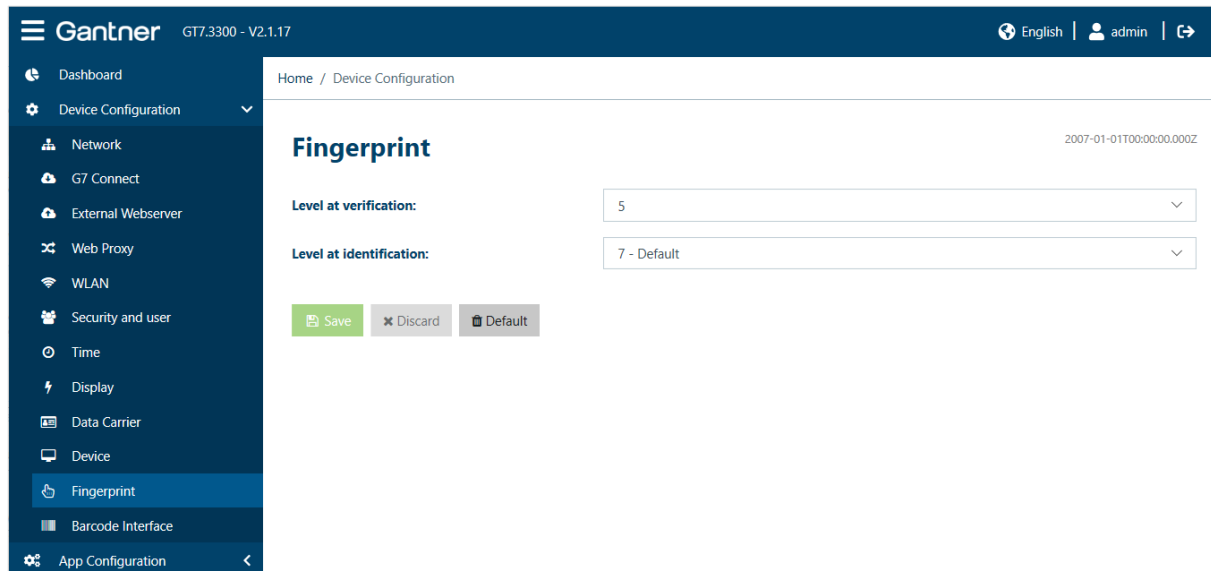


Figure 4.21 – GT7 Central Locker web interface – Fingerprint settings

These settings are only applicable when a fingerprint reader is used with the GT7 terminal. The settings here determine the level of accuracy of the fingerprint reader; 1 = lowest level, 10 = highest level. Certain people (e.g., tradespersons who work with their hands) may have weaker fingerprints than others. If many users are having difficulty reading their fingerprint, it may help to lower this value.

- Level at verification: This value determines the accuracy of the fingerprint reader for verification, i.e., when the fingerprint is used as additional confirmation of identification after identification via data carrier or similar.
- Level at identification: Similar to the previous “Level at verification” setting, this value determines the accuracy of the fingerprint reader for identification, i.e., when the fingerprint is used as the primary means of identification for the user.

4.7.14 Barcode interface

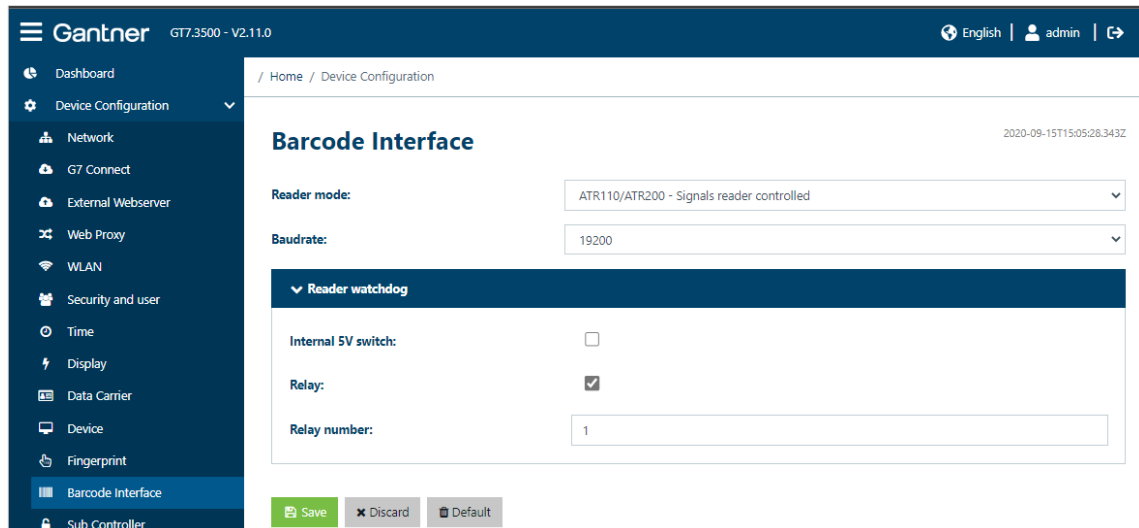


Figure 4.22 – GT7 Central Locker web interface – Barcode interface settings

These settings are only effective when a barcode reader is used with the GT7 Central Locker.

- Reader mode: When a barcode reader is connected to the GT7 Central Locker, select the type of reader or interface here.
 - Default: General/undefined barcode reader.
 - ATR110/ATR200 – Signals reader controlled: Setting for the ATR 110 and ATR 200 barcode readers from GANTNER. With this setting, the signaling on the barcode reader is automatically set as soon as a barcode is read.
 - ATR110/ATR200 – Signals host controlled: Setting for the ATR 110 and ATR 200 barcode readers from GANTNER. With this setting, the signaling on the barcode reader is not set until the approval or rejection is made by the management software.
 - GBS7.1xxx – Signals reader controlled: Setting for the GBS7.1xxx barcode reader from GANTNER. With this setting, the signaling on the barcode reader is automatically set as soon as a barcode is read.
 - GBS7.1xxx – Signals host controlled: Setting for the GBS7.1xxx barcode reader from GANTNER. With this setting, the signaling on the barcode reader is not set until the approval or rejection is made by the management software.
- Baud rate: The transmission rate of the barcode reader.
- Reader watchdog: This section is displayed if one of the “ATR110/ATR220” settings is selected for the “Reader mode” option.
The settings for “Internal 5V switch” and “Relay” with the relay number relate to the barcode reader monitoring. If the communication connection from the GT7 terminal to the barcode reader is interrupted, the barcode reader will be restarted using the internal 5 V switch or the relay (if the barcode reader is connected to the corresponding relay).

4.7.15 Sub controller

Gantner

GT7.3500 - V3.3.0

English

admin

Dashboard

Device Configuration

Network

G7 Connect

External Webserver

Web Proxy

WLAN

Security and user

SCEP

Time

Display

Data Carrier

Device

Fingerprint

Barcode Interface

Sub Controller

Sub Controller RFID

Camera

App Configuration

Installed Apps

Cloud Pairing

Licensing and coding points

Certificate management

Maintenance

Home / Device Configuration

Sub Controller

2024-02-21T09:55:27.411Z

Emergency mode:

Full

Only locking SMART.Locks by command:

☐

Locking timeout:

300

s

Auto close free locker:

☒

Auto lock personal/dynamic locker:

☒

Push to Open - Personal Locker:

☐

Push to Open - Dynamic Locker:

☐

Push to Open - Free Locker:

☒

Push to Open timeout:

30

s

Enable locker light:

☐

Enable USB charging:

☐

Lock manipulation detection:

☒

Alarm mode:

☒

Locker signalling

Beeper:

☐

Acoustic alarm:

☐

Advanced Acoustic Signaling Mode:

☐

Beeper volume:

100

%

GAT Lock 5xxx compatibility:

☐

Show rented:

☐

Color unlocked / not reserved:

Deep green

Intensity unlocked / not reserved:

70

%

Color locked / reserved:

Light red

Intensity locked / reserved:

70

%

One time signalling (Eco.Lock compatibility):

☐

Master card

Card number:

BD8A151E

HEX

Save

Discard

Default

Figure 4.23 – GT7 Central Locker web interface – Sub controller settings

These settings apply to the sub controller connected to the GT7 Central Locker.

- Emergency mode: If communication between the sub controller/GT7 and the host is interrupted, these settings determine how the sub controller and connected locks behave until communication is restored.
 - Disabled: All lockers can only be locked or unlocked by a master card.
 - Full: All free lockers and personal lockers can continue to be used as they were configured before the interruption.
 - Unlock only: Each user can unlock their locker, but they cannot lock another locker after that.
 - Last user: The last user who used a locker can lock/unlock their locker.

NOTE! If the “PIN verification for data carrier” option is enabled (see “4.8.5 PIN code”), the emergency mode of the sub controller should not be used, i.e., this option should be disabled. Otherwise, PIN verification would be bypassed if the connection between the GT7 Central Locker and the sub controller is interrupted.
- Only locking SMART.Locks by command: For the GAT SMART.Lock system only. This option is set by the app and cannot be changed here. When enabled, the locker can only be locked when a previous locking command is sent.
- Locking timeout: This option is set by the app and cannot be changed here. The displayed value (in seconds) shows the time for locking via command.
- Auto close free locker: If the option is enabled in the GAT NET.Lock system, a user can close an unused locker in free locker mode by simply pressing it shut (door is not locked, only held shut) and reopen it by pressing again. The lock LED remains green to indicate its status.

NOTE! The door is not locked. It can be opened by anyone without a data carrier.

NOTE! In the SMART.Lock system, this setting operates in the same way as the following “Auto lock” setting.
- Auto lock personal/dynamic locker: If the option is enabled, a personal locker (= locker in personal locker mode) or a dynamic locker (= locker in dynamic locker mode) can be locked by simply pressing it shut without needing to read a data carrier.
- Push to Open – Personal Locker / Dynamic Locker / Free Locker: Only valid for the GAT NET.Lock system. The Push to Open function is available for the Free Locker, Personal Locker, and Dynamic Locker modes. If this option is enabled, the user must first complete a valid identification using a data carrier, e.g., at the GT7 Central Locker, and then briefly press the locker door in to open their locker. If the Push to Open function is not enabled, the locker door will automatically open immediately after valid identification. The timeout time (see next option) determines how long the user has to open the door after identification.

- Push to Open timeout: This setting is only applicable for the Push to Open function. Enter the time (in seconds) that a user has after identification to go to their locker and open it by pressing the locker door. If the time expires without the door being opened, the door is locked again. If "0" is entered here, the time is unlimited. The maximum time is 255 seconds (approx. 4.5 minutes).
- Enable locker light: Enable this setting to allow lockers with an integrated LED light in the lock (GAT NET.Lock 7020 USB) to turn on automatically when the door is opened.
- Light on duration time: This time (in seconds) determines how long the locker light is switched on for.
- Enable USB charging: Enable this setting to allow lockers with USB charging functionality (GAT NET.Lock 7020 USB) to be used.
- Lock manipulation detection: For the GAT NET.Lock system only. This setting prevents the locker from being locked when manipulation of lock is detected, e.g., manipulation of the door closed sensor.
- Alarm mode: For the GAT NET.Lock system only. This setting turns the alarm function on/off. When an alarm is triggered, the GAT NET.Lock 7xxx locks emits a loud alarm tone (see setting "Acoustic alarm" to turn off), the status LED flashes red, and the locker management software is notified.

Locker signaling (for the GAT NET.Lock system only)

- Beeper: When this setting is enabled, the lock beeps to signal each locking and unlocking action.
- Acoustic alarm: Switches on/off the acoustic signal in the GAT NET.Lock in the event of an alarm.
- Advanced Acoustic Signaling Mode: This setting can be used to influence the type of audio signal. When enhanced signaling is enabled, tones are generated with ascending/descending pitches.
- Beeper volume: The volume of the integrated acoustic signal generator can be defined here. Input is in percent (1 = minimum volume, 100 = maximum volume).
- GAT Lock 5xxx compatibility: When this setting is enabled, the LED of the GAT NET.Lock functions in the same way as with the predecessor GAT Lock 5000 system, i.e., the LED color is limited to red. The LED is off when the door is open, on when the door is locked, and the LED flashes red to indicate when a data carrier should be read.
- Show rented: Enable this setting to indicate whether a personal locker has been rented or not. When a locker has been rented, the lock LED is then red even if it is not locked.
NOTE! To ensure the correct LED signaling, disable this setting for dynamic lockers.
- Color unlocked / not reserved: From the menu, select the color that you want the lock LED on the locker door to indicate when the locker is available (unlocked and not reserved).
- Intensity unlocked / not reserved: Here you can set the brightness of the lock's LED indicator on the locker door, which is used when the locker is available (unlocked and not reserved). Values from 1 (minimum brightness) to 100 (maximum brightness) can be entered.

- Color locked / reserved: From the menu, select the color that you want the lock LED on the locker door to indicate when the locker is unavailable (locked or reserved).
- Intensity locked / reserved: Here you can set the brightness of the lock's LED indicator on the locker door, which is used when the locker is unavailable (locked or reserved). Values from 1 (minimum brightness) to 100 (maximum brightness) can be entered.
- One time signaling (Eco.Lock compatibility):
When activated, the LED display on the lock behaves like the LED at the GAT ECO.Lock.

Master card

MASTER cards (data carriers) can be defined for the system and can be used, e.g., to open a locker for which the user data carrier has been lost. The numbers of the MASTER data carriers are only displayed here; the configuration is completed in the management software (Relaxx/eLoxx).

4.7.16 Sub controller RFID

Gantner

GT7.3500 - V2.14.0

English

admin

Dashboard

Device Configuration

Network

G7 Connect

External Webserver

Web Proxy

WLAN

Security and user

Time

Display

Data Carrier

Device

Fingerprint

Barcode Interface

Sub Controller

Sub Controller RFID

Camera

App Configuration

Installed Apps

Cloud Pairing

Licensing and coding points

Certificate management

Maintenance

Home / Device Configuration

Sub Controller RFID

2022-05-13T06:42:46.903Z

Card reading sequence:

1. RFID setting and 2. RFID setting

RFIDSettings

1. RFID setting

Site key:

73E0818B8DFB835DEB9797076C922DDA534D

Keyset:

Data to read:

Locker Segment

Flip unique number:

☐

Send card data to host:

☐

Locker segment data

Free locker universal mode:

☐

Legic Prime locker segment number:

1

ISO 15693 block number base info:

13

ISO 15693 block number certificate:

15

ISO 15693 block number lockerinfo:

19

Mifare DESFire file data offset:

0

Add Data Carrier

System data carrier

Read from:

1. RFID setting

Extended reader parameter

ECP frame:

Legacy parameter (FW < 2.0)

Number format:

HEX LSB first data format

Card id source:

UID

Free locker universal mode:

☐

HID iClass reader:

PACS data

Save

Discard

Default

Figure 4.24 – GT7 Central Locker web interface – Sub controller RFID settings

These settings relate to the sub controllers connected to the GT7 terminal when used with the G7 Central Locker app. The settings for the RFID data carriers that will be read by the GAT NET.Lock 7020 locks can be defined.

- Card reading sequence: Two separate RFID configurations can be defined (see below) thus allowing two different data carrier types to be used. Via the "Card reading sequence" setting, you can define how the two RFID configurations should be used.
 - "1. RFID setting and 2. RFID setting": Both RFID configurations are considered in parallel and when a data carrier is read, it must match one of the RFID settings.
 - "1. RFID setting, if not readable then 2. RFID setting": The first RFID configuration is always used first to read data carriers. If this is unsuccessful, the second setting is used.

RFID settings

By clicking on the "RFID setting" menu, you can insert the blocks of configuration settings for the 1st RFID setting and the 2nd RFID setting.



By clicking on the arrow on the left , the settings blocks can be collapsed and expanded. The order of the two RFID settings blocks can be changed by clicking on the arrow on the right . The settings block can be deleted again by clicking on the trash can symbol .

The following settings are available:

- Site key: This number (hexadecimal) is the specific site key (site number) for the facility. The data carriers, GT7 terminals, and controllers must use the same site key.
- Keyset: This value is necessary when using MIFARE DESFire data carriers and contains the system-specific access keys.
- Data to read: Here you can define which data shall be read from the data carriers.
 - UID: With this setting, the unique ID numbers are read from the data carriers. These are used to identify the user data carriers.
 - Locker Segment: The data from the locker segment will be read. This segment is used to operate the GANTNER locker locks. When this setting is selected, the "Locker segment data" section is displayed in which the settings for the locker segment can be defined:

Locker segment data	
Free locker universal mode:	☐
Legic Prime locker segment number:	1
ISO 15693 block number base info:	13
ISO 15693 block number certificate:	15
ISO 15693 block number lockerinfo:	19
Mifare DESFire file data offset:	0

- Custom Segment: With this setting, customer-specific areas of the data carrier can be read. The necessary settings such as segment ID and length can be entered in the "Custom segment data" block that is

displayed when this menu item is selected.

Custom segment data

Custom segment id:

1

Data offset:

0

Data length:

0

Checksum mode:

NONE

Number format:

HEX LSB first data format

Use number as unique number:

☐

- Flip unique number: Enable this setting to reverse the unique number read from the data carriers, i.e., MSB-LSB becomes LSB-MSB.
- Send card data to host: If this setting is enabled, the configured card data is sent to the connected locker management software.

System data carrier

- Read from: This setting determines which RFID settings defined above should be used by the system data carriers. The system data carriers are system-specific and are required by the system administrator for various tasks (e.g., SYSTEM, MASTER, or SERVICE data carriers).

Extended reader parameter

ECP frame: Enhanced Contactless Polling (ECP) for an NFC reader (from GANTNER).

Legacy parameter (FW <2.0)

These settings are valid for older devices with firmware versions prior to V2.0.

- Number format: Here you can define how the card number is encoded on the data carrier or how it should be handled.
- Card id source: Select where the card ID number is stored on the data carrier (use unique number UID as ID or read from customer-specific segment 1 or 2).
- Free locker universal mode: The data carriers must be encoded accordingly for this mode. Enable this setting if this mode is used.
- HID iClass reader: This setting is only required if HID iClass data carriers are being used.

4.8 App configuration settings

4.8.1 General settings

The GT7 Central Locker or the connected controllers respectively can operate in different operating modes. The settings on the general settings page are applicable for all operating modes. For each operating mode there are also specific settings that affect the operation for that mode, and these settings are found on separate pages. The following operating modes are available:

- Free Locker: Each user is assigned to a pool or group of lockers. From these lockers, the user can choose any unoccupied locker to use. See chapter “4.8.2 Free Locker” for more information.
- Free Locker PIN Code: This function allows the user to lock and unlock their chosen free locker using a PIN code. See chapter “4.8.5 PIN code” for more information.
- Personal Locker: Each user is assigned to a specific locker or several specific lockers. The user can only use the locker(s) they are assigned to. See chapter “4.8.3 Personal Locker” for more information.
- Dynamic Locker: Dynamic locker mode is a combination between a free locker and a personal locker. See chapter “4.8.4 Dynamic Locker” for more information.

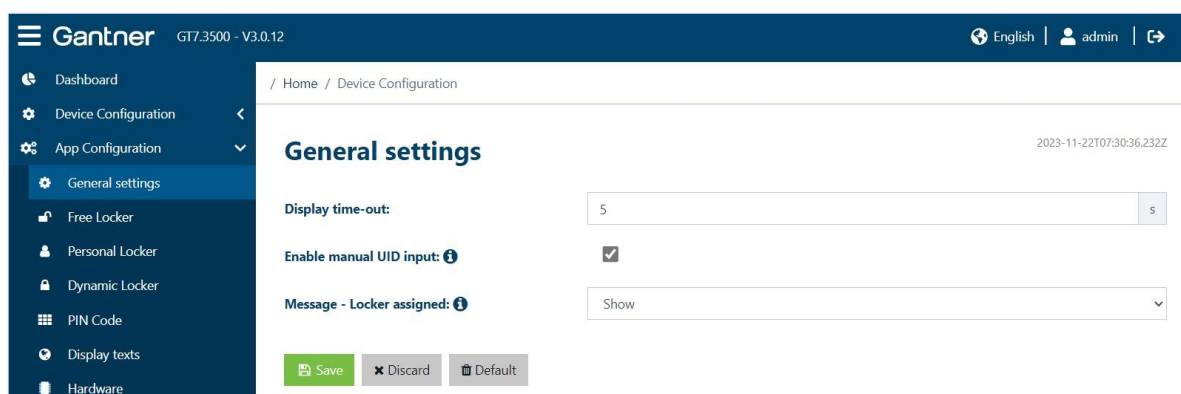


Figure 4.25 – GT7 Central Locker web interface – General settings

- Display time-out: If the user does not carry out any more commands on the GT7 Central Locker before the time (in seconds) entered here expires, the idle screen is displayed.
- Enable manual UID input: If this setting is enabled, a keypad symbol is displayed in the bottom right of the idle screen. This allows the user to enter their UID number manually via a keypad screen that is displayed after pressing the button.
Note: This function can only be used if the “Allow PIN usage in Free Locker mode” setting is not enabled (see “4.8.5. PIN code”).
- Message – Locker assigned: This setting determines whether the “locker assigned” message should be displayed on the screen. Select an option from the menu:
Show: The message is displayed each time a locker is assigned.
Don’t show: The message is never displayed.
Locking at terminal: The message is only displayed when the user locks the locker at the terminal rather than at the locker.

4.8.2 Free Locker

In free locker mode, each user is assigned to a group of lockers. From these lockers, the user can choose any unoccupied locker to use. The settings on this page are organized into subgroups, which can be expanded and collapsed.

Figure 4.26 – GT7 Central Locker web interface – Free locker mode

The following settings can be configured in free locker mode.

Allow authentication at the door

Only for GAT NET.Lock systems. These locks can be identified using an RFID data carrier at the lock or locker.

- Nothing: The identification option at the locker cannot be used. Identification is only possible at the GT7 Central Locker.
- Only Open: A locker must be selected at the GT7 Central Locker. To unlock and open the locker door, the data carrier can be read directly at the locker.
- Selection & Open: A locker can be opened and locked directly at the locker using a data carrier.

NOTE! If the “PIN verification for data carrier” option is enabled (see “4.8.5 PIN code”), select “Nothing” here. If not, it will be possible to bypass the PIN verification. If another option is selected, a corresponding message is displayed:

Allow authentication at the door: Only Open

PIN Code: PIN verification for data carrier is enabled. Please set Allow authentication at the door to Nothing, otherwise it will be possible to bypass PIN verification.

Locker selection and release process

- Opening confirmation: When this option is enabled, opening a locker at the terminal requires a confirmation on the touchscreen. When disabled, the locker opening process starts immediately.
- Number of locker suggestions: This number determines how many free lockers are displayed to a user for selection. The user can scroll through these lockers and select one of them.
 *The G7 Central Locker app decides which available lockers are displayed to the user autonomously according to the requirements, which result from the authorization groups in Relaxx when these are being used.*
- Enable selection by number: When this option is enabled, the user can enter a specific locker number for selection via a keypad on the display. This saves the user from having to scroll through each available free locker when they have a specific locker that they want to use.
- Confirmation of selection: When this option is enabled, the user must confirm the action on the screen after identification and selecting the function on the GT7 Central Locker. When this option is not enabled, the action is automatically carried out immediately after valid identification and function selection (after the lead time before opening has expired).
Depending on the further configuration, the confirmation function has different effects on the behavior of the lockers/locks. A distinction must be made between the following behavior and the "Door behavior of available lockers" option:
 - "Open": Confirmation is required before closing the locker. After confirmation on the screen, the locking closing time starts.
 - "Locked": Confirmation on the screen is required to open a locker door. If the "Door opening mode" is also set to "Spring open", the door will spring open after confirmation and the "Locking closing time" starts. If this option is set to "Push to open", the door must be opened by pushing it in briefly. After opening, the "Locking closing time" starts.
 - "Closed": The "Locking closing time" starts immediately after confirmation. If the door is already closed, it is locked directly.
- Allow locker changes: This option allows the user to change their locker selection from the closing confirmation screen. The previous "Confirmation of selection" option must therefore be enabled to use this function.
- Release process:
 - "Always release": With this option, a locker is automatically shared with other users after it has been opened.
 - "Keep / release question":
When this option is selected, the user is asked when opening their locker whether they want to release this locker for other users or to keep the locker, e.g., when only opening the locker briefly to add or remove an object. If the user chooses to keep the locker, the locker can be closed again after opening without re-identification (unless the "Locker closing time" has expired, in which case, re-identification is required).
- Release time: Only displayed when the previous "Keep / release locker" option is set to "Always release". This time determines how long the locker remains assigned to the current user after opening. After this time has expired, the locker becomes available to every other user.

- Locking suggestion mode: This option defines the order in which the available lockers are displayed to the user for selection. Select one of the following options from the menu:
 - First available: The next available locker is displayed for selection.
 - Random: The GT7 Central Locker selects a random locker.
 - Last closed first: The locker that was closed last is displayed.

Lead times for opening and locking

- Lead time before opening: If a value greater than 0 is entered here, a countdown for this time in seconds is displayed after selecting a locker at the GT7 Central Locker to indicate when the locker will open. If the value is 0, the locker opens immediately after selection at the GT7 Central Locker.
- Lead time before locking: If a value greater than 0 is entered here, a countdown for this time in seconds is displayed after selecting a locker at the GT7 Central Locker to indicate when the locker can be locked. A value of 0 means that the locker can be locked immediately after selection on the GT7 Central Locker.

NOTE: If identification is carried out at the door (reading of the data carrier), no lead time is used, i.e., the door opens or locks immediately after the data carrier is read.

4.8.3 Personal Locker

In personal locker mode, each user is assigned to a specific locker or several specific lockers. The user can only use the locker(s) they are assigned to. The following settings can be defined for personal locker mode:

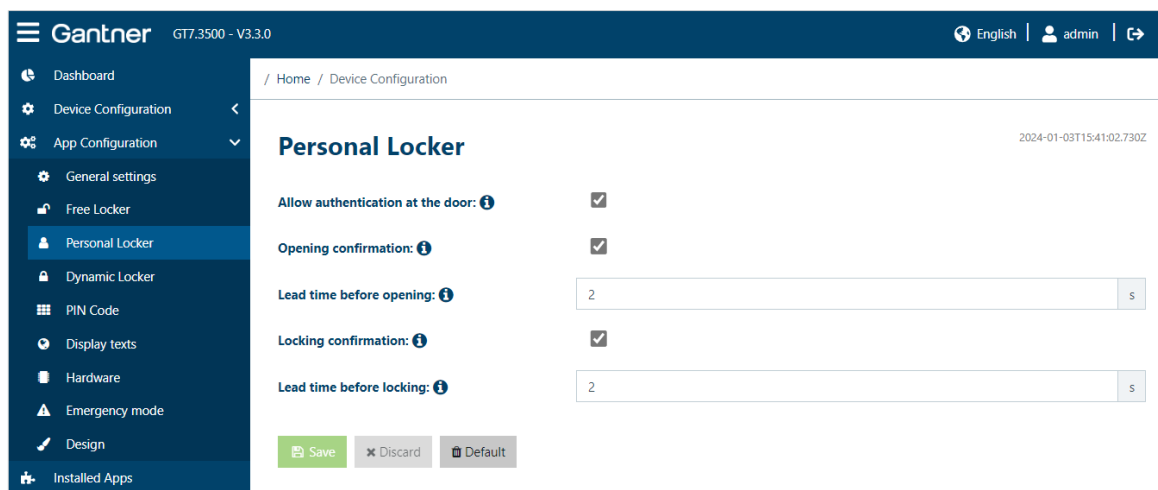


Figure 4.27 – GT7 Central Locker web interface - Personal locker mode

- Allow authentication at the door: Only for GAT NET.Lock systems. For these locks, an RFID data carrier can be used for identification at the locker. When this option is activated, a user can open or close their locker by holding their personal data carrier near the lock or locker door. Operation at the GT7 Central Locker is not necessary.

NOTE! If the "PIN verification for data carrier" option is enabled (see "4.8.5 PIN code"), select the "Nothing" option here. If not, it will be possible to bypass the PIN verification. If another option is selected, a corresponding message is displayed:

PIN Code: PIN verification for data carrier is enabled. Please disable Allow authentication at the door, otherwise it will be possible to bypass PIN verification.

- Opening confirmation: When this option is enabled, opening a locker at the terminal requires a confirmation on the touchscreen. When disabled, the locker opening process starts immediately.
- Lead time before opening: This time determines the countdown time after valid identification (and confirmation) until the locker is opened. The user has this time to go to their locker before it opens.
- Locking confirmation: When this option is enabled, the user must confirm the action on the screen after identification and selecting the function on the GT7 Central Locker. When this option is not enabled, the action is automatically carried out immediately after valid identification and function selection (after the lead time before opening has expired).
- Lead time before locking: If a value greater than 0 is entered here, a countdown for this time in seconds is displayed after selecting a locker at the GT7 Central Locker to indicate when the locker can be locked. A value of 0 means that the locker can be locked immediately after selection on the GT7 Central Locker.

4.8.4 Dynamic Locker

A locker in dynamic locker mode is a combination between a free locker and a personal locker. When the locker has no authorization assigned to it, it acts as a free locker and can be locked by any valid data carrier. When the locker is locked by a data carrier, this data carrier is automatically added to the authorization list of Relaxx, and the dynamic locker is assigned to this data carrier. The locker then acts as a personal locker.

An example of use for this mode is a group of lockers that are used to store service material (e.g., towels). Only users belonging to a certain group can use these lockers, but they can freely choose between any of the lockers. The lockers can be dynamically assigned.

NOTE!

- Dynamic locker mode is currently only possible for lockers with a GAT NET.Lock 7020 lock.
- To ensure the correct LED signaling, disable the "Show rented" option in the "Sub Controller" settings (see "4.7.15 Sub controller"). If not disabled, the dynamic locker's LED will signal like a personal locker.

The screenshot displays the Gantner web interface for configuring a Dynamic Locker. The interface is in English and shows the user 'admin'. The left sidebar contains a menu with various configuration options. The main content area is titled 'Dynamic Locker' and includes a breadcrumb trail 'Home / Device Configuration'. The settings are organized into sections: 'Allow authentication at the door' (set to 'Selection, Open & Lock'), 'Locker selection and release process' (with options for opening confirmation, number of suggestions, selection by number, confirmation of selection, suggestion mode, and release of dynamic lockers), and 'Lead times for opening and locking' (with input fields for lead times before opening and locking). At the bottom, there are buttons for 'Save', 'Discard', and 'Default'.

Figure 4.28 – GT7 Central Locker web interface – Dynamic locker mode

The following settings can be configured for dynamic locker mode.

Allow authentication at the door

Only for GAT NET.Lock systems where the locks can be identified using an RFID data carrier at the lock.

- Nothing: The identification option at the locker cannot be used. Identification is only possible at the GT7 Central Locker.

- Open & Lock: A locker must be selected at the GT7 Central Locker. To unlock and open the locker door, the data carrier can be read directly at the locker.
- Selection, Open & Lock: A locker can be opened and locked directly at the locker using a data carrier.

NOTE! If the "PIN verification for data carrier" option is enabled (see "4.8.5 PIN code"), select the "Nothing" option here. If not, it will be possible to bypass the PIN verification. If another option is selected, a corresponding message is displayed:

Allow authentication at the door: ⓘ

Only Open

PIN Code: PIN verification for data carrier is enabled. Please set Allow authentication at the door to Nothing, otherwise it will be possible to bypass PIN verification.

Locker selection and release process

- Opening confirmation: When this option is enabled, opening a locker at the terminal requires a confirmation on the touchscreen. When disabled, the locker opening process starts immediately.
- Number of locker suggestions: This number determines how many lockers are displayed to a user for selection. The user can scroll through these lockers and select one of them.

i

The G7 Central Locker app decides which available lockers are displayed to the user autonomously according to the requirements, which result from the authorization groups in Relaxx when these are being used.
- Enable selection by number: When this option is enabled, the user can enter a specific locker number for selection via a keypad on the display. This saves the user from having to scroll through each available free locker when they have a specific locker that they want to use.
- Confirmation of selection: When this option is enabled, the selection of a locker at the terminal requires a confirmation on the touchscreen. When disabled, the locker is assigned immediately after selecting a locker number and the locker unlocks.
- Locking suggestion mode: This setting defines the order in which the available lockers are displayed to the user for selection. Select one of the following options from the menu:
 - "First available": The next available locker is displayed for selection.
 - "Random": The GT7 Central Locker selects a random locker.
- Release dynamic lockers: Select this option to show the "Release" button on the start screen of the GT7 Central Locker. This button allows the user to remove the assignment of their data carrier to the locker thereby releasing the locker for other users to use.

Lead times for opening and locking

- Lead time before opening: If a value greater than 0 is entered here, a countdown for this time in seconds is displayed after selecting a locker at the GT7 Central Locker to indicate when the locker will open. If the value is 0, the locker opens immediately after selection at the GT7 Central Locker.
- Lead time before locking: If a value greater than 0 is entered here, a countdown for this time in seconds is displayed after selecting a locker at the GT7 Central Locker to indicate when the locker can be locked. A value of 0 means that the locker can be locked immediately after selection on the GT7 Central Locker.

4.8.5 PIN code

These settings are used to configure the use of PIN codes for locker operation. If this function is enabled, it is possible to lock or unlock lockers operating in free locker mode by entering the locker number and a PIN code. In this case, a data carrier is not required for identification.

In addition, the settings can also be configured for the "PIN verification for data carrier" function.

NOTE! These two functions cannot be used simultaneously, i.e., if PIN verification is being used, then a data carrier must be used for identification. The locker operation with PIN code identification and subsequent PIN code verification is therefore not possible.

Figure 4.29 – GT7 Central Locker web interface – PIN code settings for free lockers

- Allow PIN usage in free locker mode:

Selecting this option allows the user to lock any unoccupied free locker using a PIN code instead of a data carrier. The user enters their PIN after locker selection and does not need to read a data carrier for identification. See chapter "5.5 Free locker with PIN code" for more information.

- PIN verification for data carrier:

This option is used to enable PIN verification (2-factor authentication) for the locker service. If enabled, each user must also enter their personal PIN code after identification with a data carrier at the GT7 Central Locker (see chapter "5.9 Master Dashboard"). This function must also be enabled in Relaxx (see "4.14 Integration in Relaxx").

NOTE! If this function is used, identification at a free locker is only possible using a data carrier, and not with PIN alone (i.e., the previous option must be disabled).

NOTE! If you enable this option and click on "Save", the "Authentication at the door" option must be set to "Nothing" for all modes (see previous pages), as identification must be verified at the GT7 Central Locker terminal by entering a PIN code. A corresponding message is also displayed.

NOTE! It is also recommended to disable emergency mode in the sub controller (see "4.7.15 Sub controller") if the PIN verification option is enabled. Otherwise, PIN verification will be bypassed if the connection between the GT7 Central Locker and the sub controller is interrupted.

NOTE! If the emergency mode of the GT7 Central Locker is used, the restrictions as described in "4.8.8 Emergency mode" must be observed.

- Minimum/maximum PIN length: In these two fields, define the minimum and maximum length of the PIN (1–8 digits).
- Number of attempts until blocking time | PIN base blocking time | Free locker mode: Number of blocking times | Free locker mode: Action when maximum exceeded:

These four settings for the locking times are used to define the behavior in the event of incorrect PIN code entry. The settings are applicable to the "Allow PIN usage in Free Locker mode" and "PIN verification for data carrier" functions, i.e., one of these functions must be enabled. The interaction of these settings is as follows:

If the PIN code is entered incorrectly several times ("Number of attempts until blocking time"), the PIN code entry is blocked for the specified time, i.e., the first blocking time is activated (duration = "PIN base blocking time"). The user can then enter their PIN code for the locker. If the PIN code is entered incorrectly again as often as defined, the second blocking time is activated (duration = double the base time). How often this process can be repeated is defined in the "Number of blocking times" field. If the defined number of blocking times is reached, the action selected in the "Action when maximum exceeded" field is executed. This action then determines how the locker behaves -> The locker can either be deactivated or set to maintenance mode. It can then no longer be opened with a PIN code or user data carrier and must be opened and activated via the Relaxx software or a master data carrier. If you select "Nothing", the verification process restarts the blocking times, i.e., the PIN code can be re-entered, and if an incorrect PIN is entered again, the first blocking period with the base blocking time is activated.

NOTE! These settings apply to each individual locker, i.e., if a locker is locked after incorrect PIN entry, the PIN code for another locker can be entered without hindrance.

- Free locker mode: Duplicate PIN-entry:

When this option is enabled, the locker user must enter their PIN twice for confirmation in order to lock a locker. Otherwise, only one PIN entry is required.

NOTE! This option is displayed only if the PIN code verification option is enabled for free lockers (see setting 2).

4.8.6 Display texts

The display of the GT7 Central Locker can be shown in different languages. When several languages are available, the user can switch between languages on the GT7 Central Locker via the language icon (see following picture).

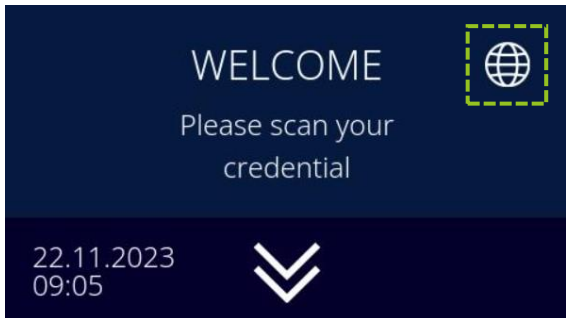


Figure 4.30 – Display language selection

The display texts for German and English are predefined by default and more languages can be added.

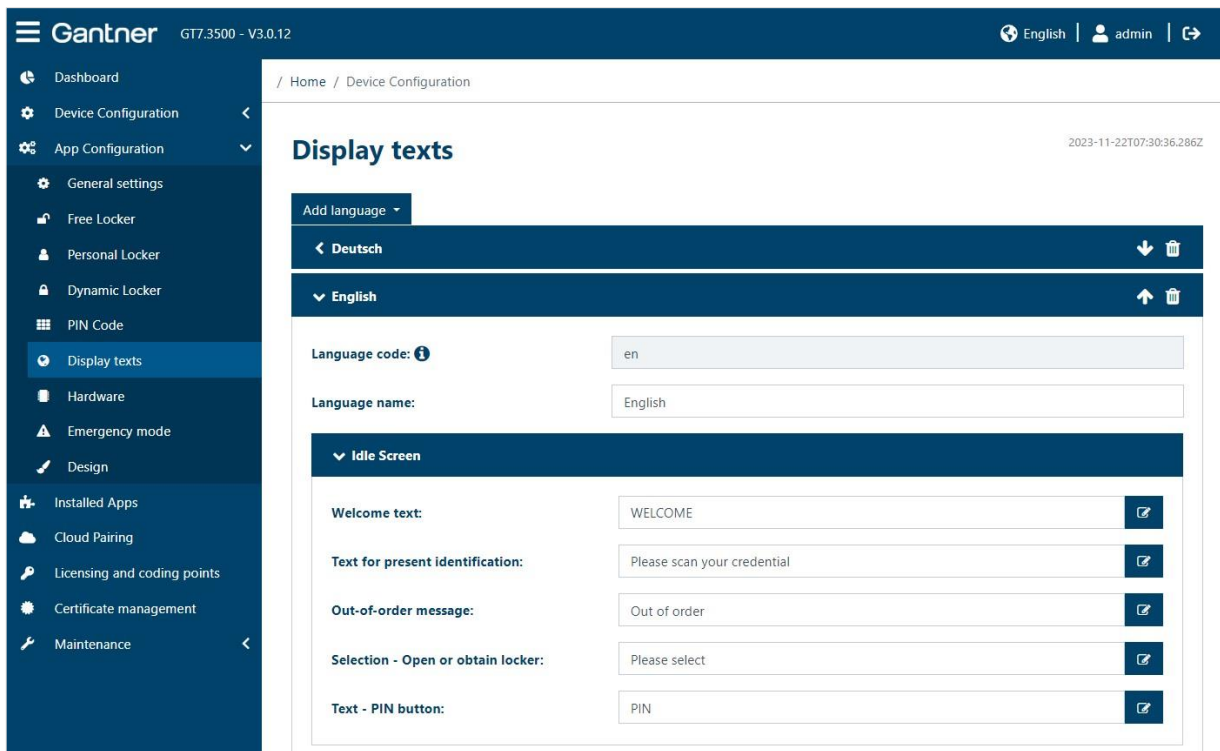


Figure 4.31 – GT7 Central Locker web interface – Display texts

The predefined text modules, which are automatically displayed by the GT7 Central Locker depending on the function, are listed for each language. The texts are divided into groups which can be opened and closed by clicking on the group name (e.g., “Idle Screen” or “General Messages” in the example above). You can also expand and collapse the languages by clicking on the name.

- The display texts are already predefined in German and English. If one of these languages is deleted, you can insert it again by clicking on “Add language”.

- ▶ To add a new language, click on "Add language" and select "Custom".
 - A new block with the text modules behind the last currently available language is inserted.
- ▶ For a new language, enter the language code according to ISO 693-1 (en, de, it, fr, etc.).
- ▶ Enter a "language name". This text is shown on the GT7 Central Locker display when selecting the language.
- ▶ The order of the language blocks can be changed using the arrows in the language headers.



- ▶ To edit a text, write directly into the text field.
 - The field turns green. This indicates that this text has been changed but has not been saved yet.
- ▶ Via the edit icon  next to a text field, formatting options (font sizes, bold, italics, fonts, etc.) can be defined for the texts.
 - An editor is displayed where you can mark text and then set certain options for this text.

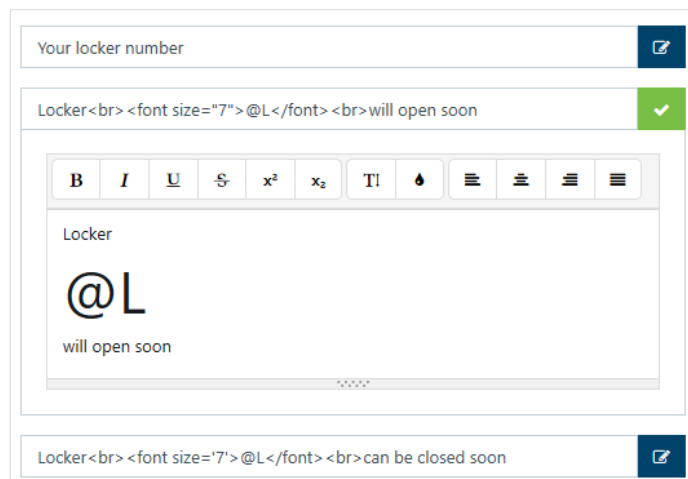


Figure 4.32 – Editing display texts

- ▶ Confirm the formatting by clicking on .
 - The formatting is displayed graphically in the editor (bold font, color, etc.). In the text line, the formatting is displayed as HTML tags in the text line (e.g.,).

NOTE! Formatting must always be done within the editor; text cannot be edited directly.
- ▶ Via the trash can icon  , a language block including all text modules can be deleted.
- ▶ Variable data can also be displayed. For this purpose, the following codes are entered in the texts, which are then replaced by the GT7 Central Locker when displaying the current information.
 - @L ... Current locker number.
 - @LA... List of all lockers in the current locker group.

4.8.7 Hardware

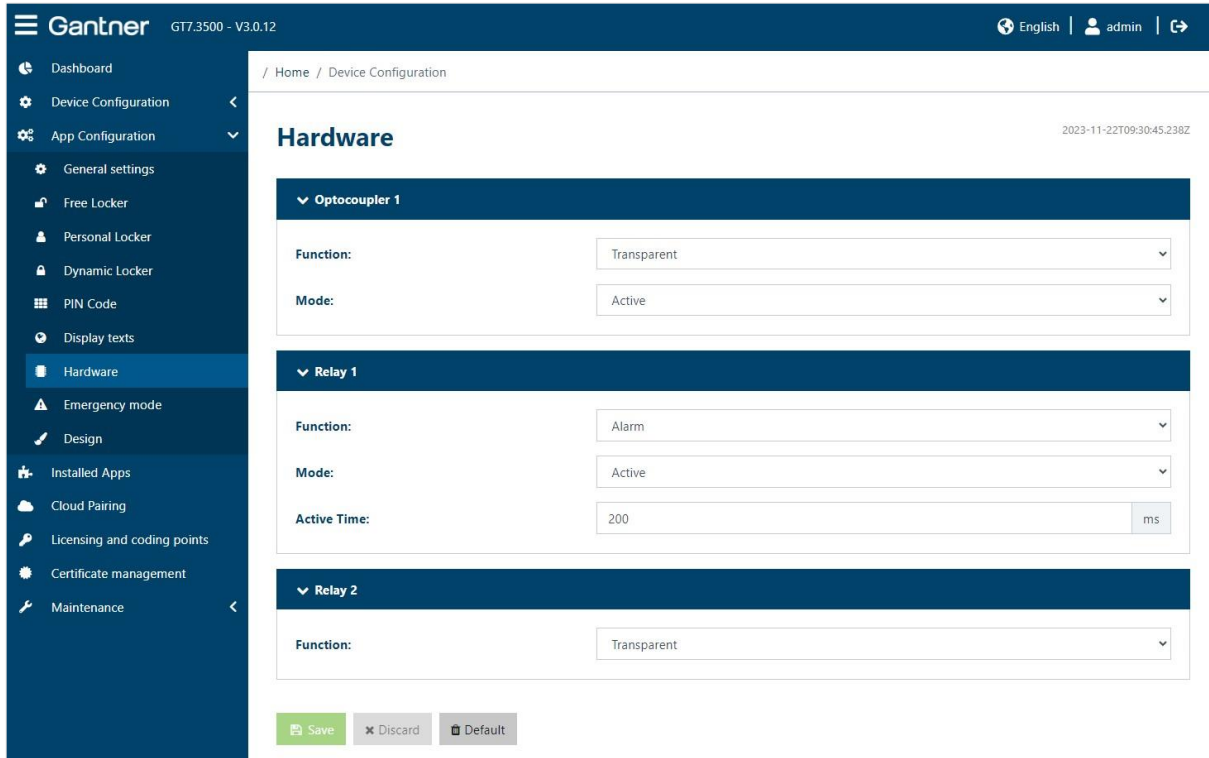


Figure 4.33 – GT7 Central Locker web interface – Hardware

The optocoupler inputs and relay outputs of the GT7 Central Locker terminal can be configured for the desired functionality on this page.

- Optocoupler 1:
 - Function:
 - Transparent: The input is not used.
 - Unlock all: With this setting, all lockers can be unlocked by an input signal (e.g., via a push button).
 - Quit alarms: With this setting, an active alarm that was activated by a relay input can be deactivated again using a signal from the input.
 - Mode:
 - Active: The function assigned to the input is executed / activated when the input is energized.
 - Passive: The function assigned to the input is executed / activated when the input is de-energized.
- Relay 1 / 2:
 - Alarm messages can be signaled via the two relay inputs.
 - Function:
 - Transparent: The output is not used.
 - Alarm: The output is used to signal an alarm for which the following two options are displayed.
 - Mode:
 - Active: If the alarm is active, the relay is energized.
 - Passive: If the alarm is active, the relay is set from energized to de-energized status.
- Active time:
 - This time defines how long the relay is energized or de-energized when the alarm is triggered (depending on the previous setting).

4.8.8 Emergency mode



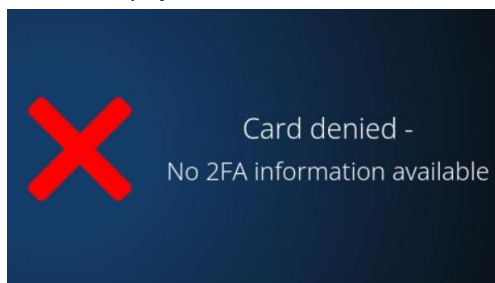
Figure 4.34 – GT7 Central Locker web interface – Emergency mode

If communication between the GT7 Central Locker and the Relaxx software is interrupted, operation of the GT7 Central Locker is not possible when emergency mode is deactivated. The default text “Out of order” is then displayed.

You can enable emergency mode here. In this case, operation of the GT7 Central Locker with the current configuration is still possible but there is no communication with Relaxx, i.e., the following restrictions must be observed:

- In personal locker mode, all previously authorized data carriers can continue to open and lock the assigned lockers. The assignments cannot be changed.
- In free locker mode (with or without PIN), all valid data carriers can select and lock a locker. However, be aware that if the authorization list is active in Relaxx, data carriers that are not on the authorization list but can still occupy lockers during emergency operation cannot reopen them.

If PIN verification is enabled (see “4.8.5 PIN code”), a new locker cannot be selected using a data carrier that is not yet known to the GT7 Central Locker terminal, because no PIN code verification data is available. In this case, the following screen is displayed:



- In dynamic locker mode, all previously authorized data carriers can continue to open and lock the assigned lockers. The assignments cannot be changed, and it is not possible to select a new locker.
- The “PIN renewal” function (setting in the Relaxx software) is not possible because a connection to Relaxx is required.

4.8.9 Design (LED color)

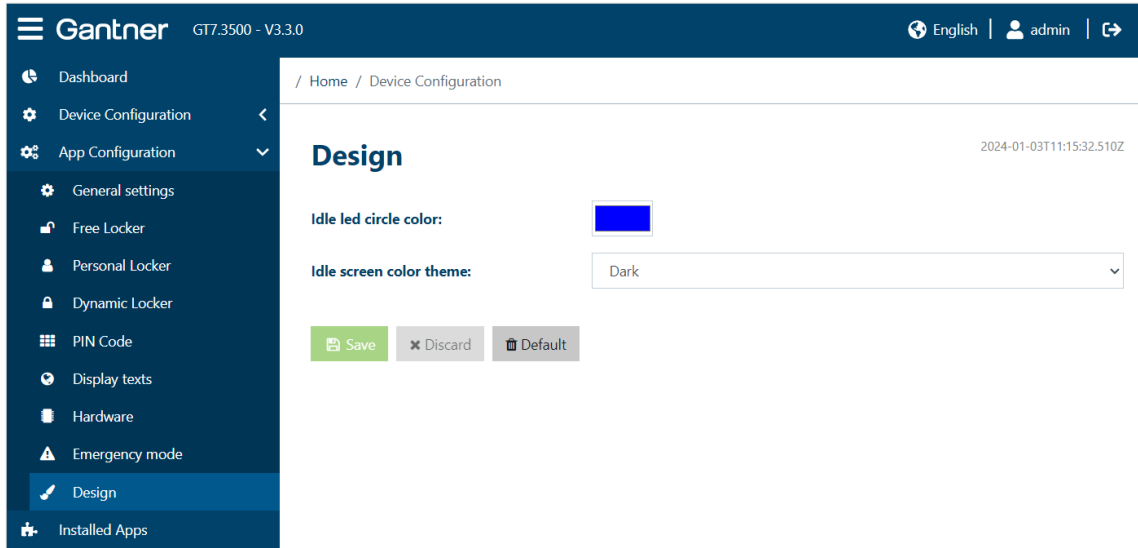


Figure 4.35 – GT7 Central Locker web interface - Design

Here, you can define the color of the GT7 Central Locker's LED ring that will be displayed in the basic state. The colors in the other modes or states (e.g., green or red for valid or invalid identification) are controlled by the GT7 Central Locker. The display can also be switched between light and dark mode.

- Click on the color field next to "Idle LED circle color".
 - A color selection window opens, which can look different depending on the internet browser used.

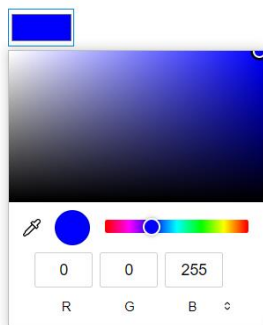


Figure 4.36 – Color selection window (e.g., in Microsoft Edge)

- Select the desired color here and click on "Save".
 - The LED ring on the GT7 Central Locker displays the new color.
- If you would like to return to the default color (blue), click on "Default" and then "Save".

- Select the style of the display in the idle state via the “Idle screen color scheme” setting. Here you can choose between a dark or a light design:

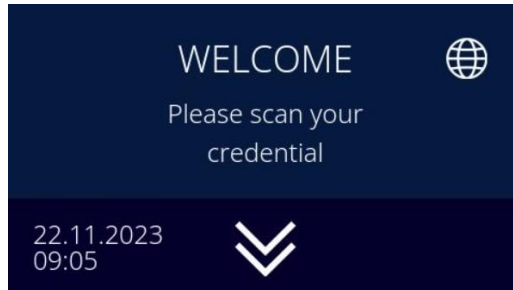


Figure 4.37 – Idle theme “Dark”

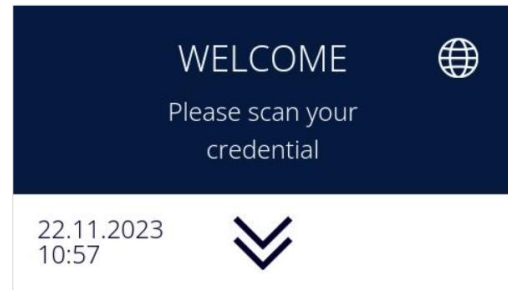


Figure 4.38 – Idle theme “Light”

4.9 Installed apps

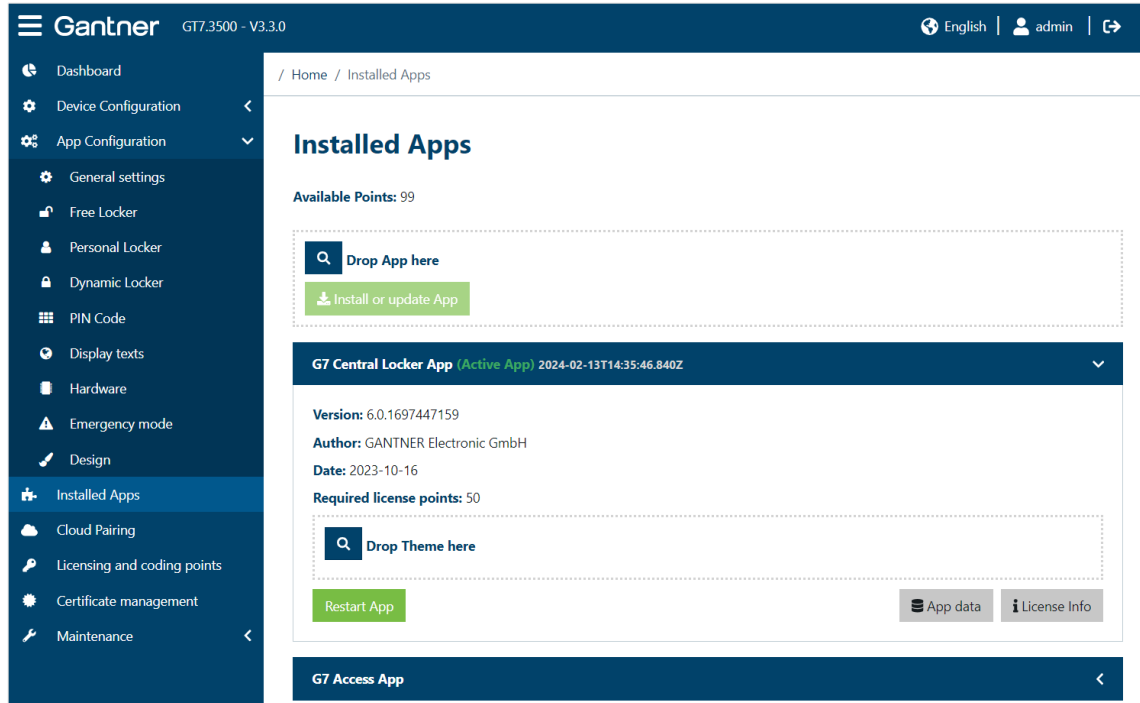


Figure 4.39 – GT7 Central Locker web interface - Installed Apps

Different apps can run on a GT7 terminal. In addition to the G7 Central Locker app described in this manual, other apps can also be activated. Activation requires license points, which you can purchase from GANTNER. On this page, all installed apps are listed, and the currently active app is marked with the green “Active App” text.

- ▶ To start another app, click on the “Activate” button for the desired app.
 - The app starts, which can take up to a minute, and the GT7 terminal operates according to the activated app.
 - Only one app can be active at a time, i.e., before activating an app, the previously active app is automatically stopped.
- ▶ In the upper “Drop App here” field, another app can be loaded into the GT7 terminal. To do this, the app package is needed.
- ▶ An app can also be assigned a theme. To do this, drag a theme file (ZIP file) from Windows Explorer directly into the “Drop Theme here” box.

i A theme is a template file (ZIP file) that defines the format of the display advertisement (e.g., text types, colors, positions, etc.). The formatting in a theme is done using CSS, which offers a lot of freedom in the design of the themes. In addition, a theme archive may contain images that can be viewed using the GT7 Central Locker's screensaver function (see “4.7.10. Display”). The images are located in the screensaver subfolder in the archive file.

4.10 Cloud pairing

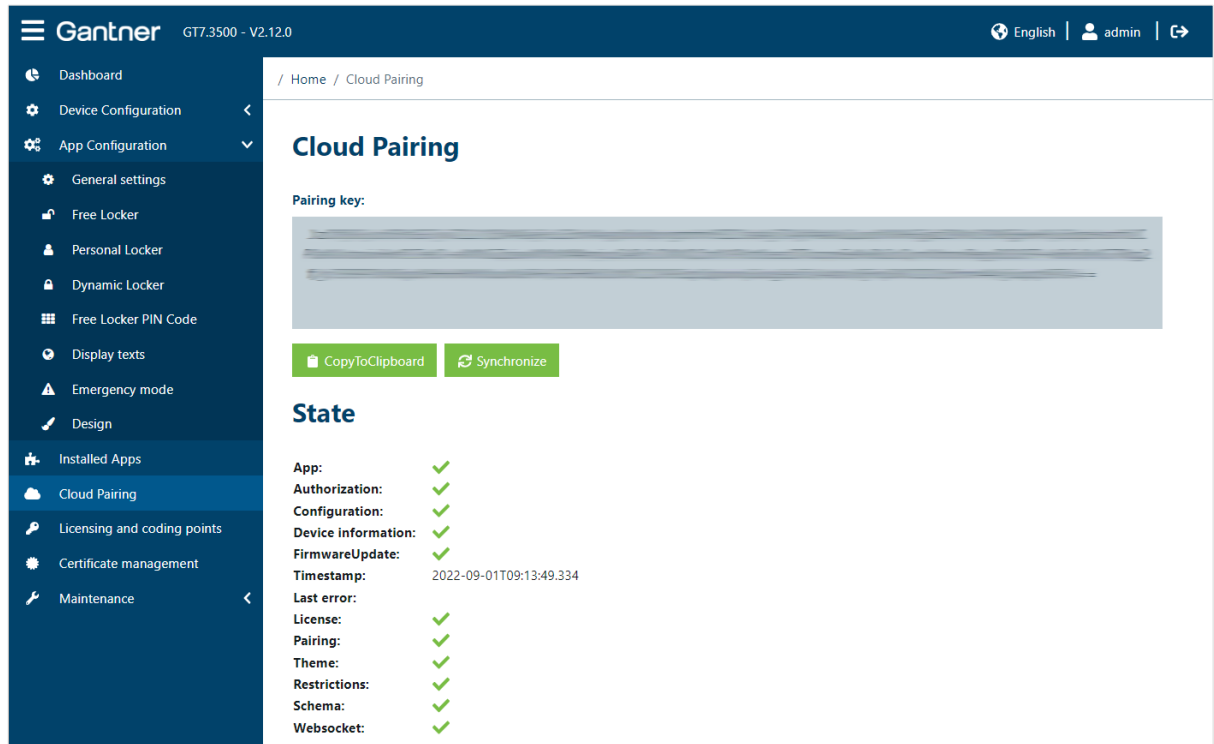


Figure 4.40 – GT7 Central Locker web interface - Cloud Pairing

G7 Connect is GANTNER's cloud service for the convenient management of clients' projects and systems that contain G7 Generation devices. To add a GT7 terminal to a project in G7 Connect, the GT7 terminal must first be paired with G7 Connect once. This requires a pairing key, which is displayed on this page.

- ▶ Log in to G7 Connect (<https://gantner.cloud>) with your username and password.
 - The home page ("Dashboard") is displayed.
- ▶ Click on "Projects".

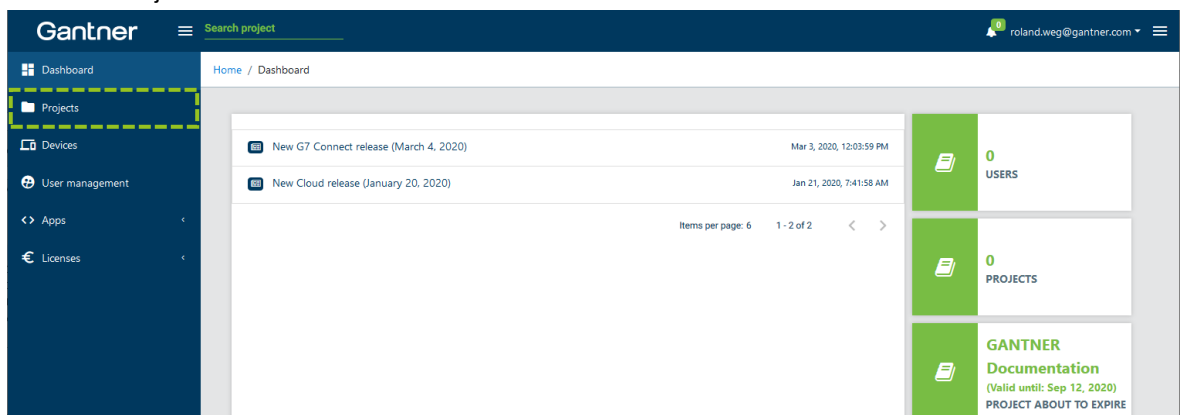


Figure 4.41 – G7 Connect – Dashboard

- Your available projects are displayed.

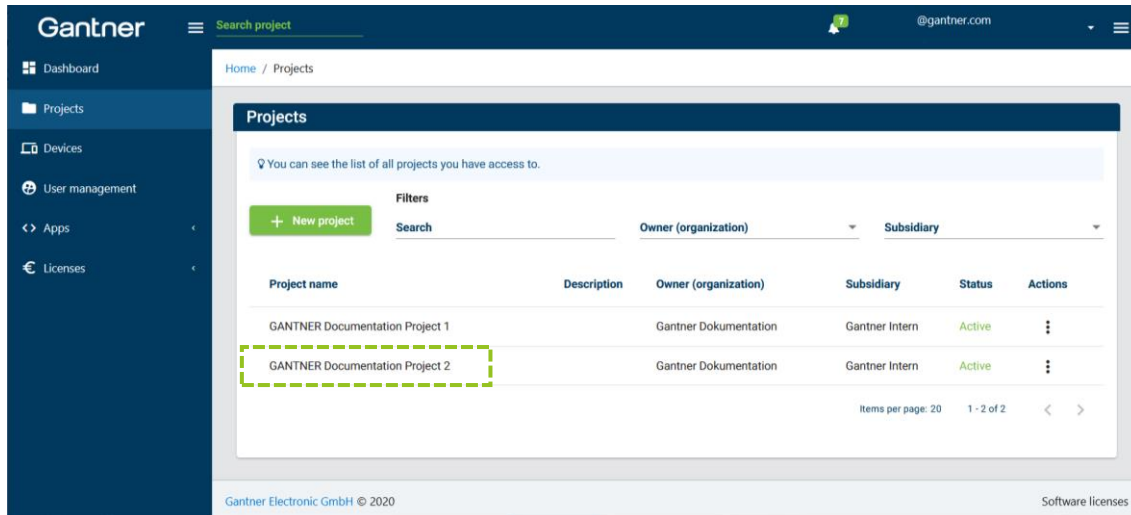


Figure 4.42 – G7 Connect – List of available projects

- ▶ Click on the project where the GT7 Central Locker is to be added.
- ▶ Click on "Device pairing".

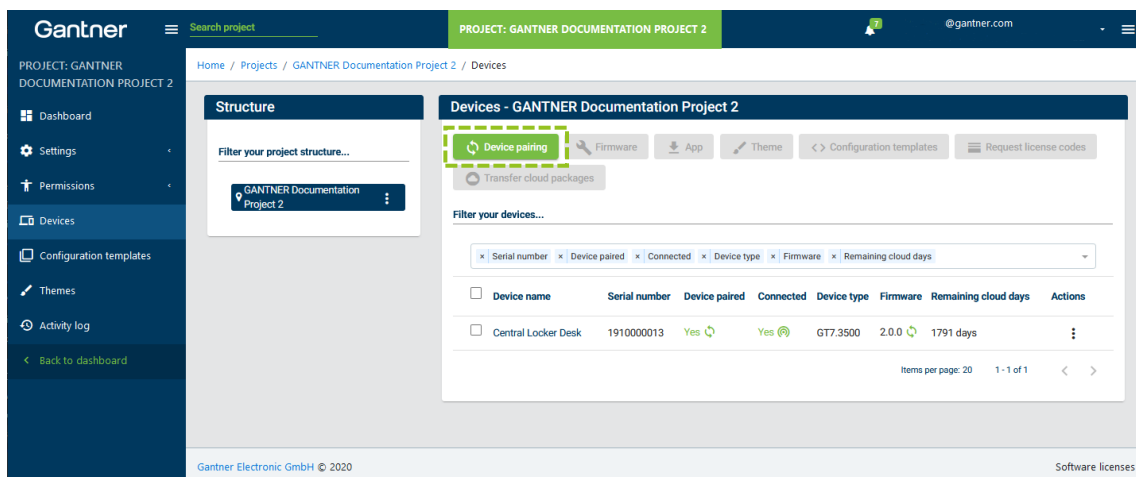


Figure 4.43 – G7 Connect – Device pairing

- A new window is displayed.

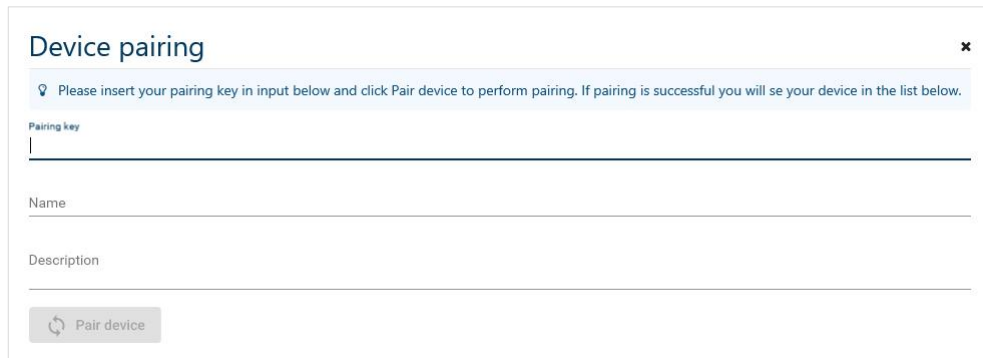
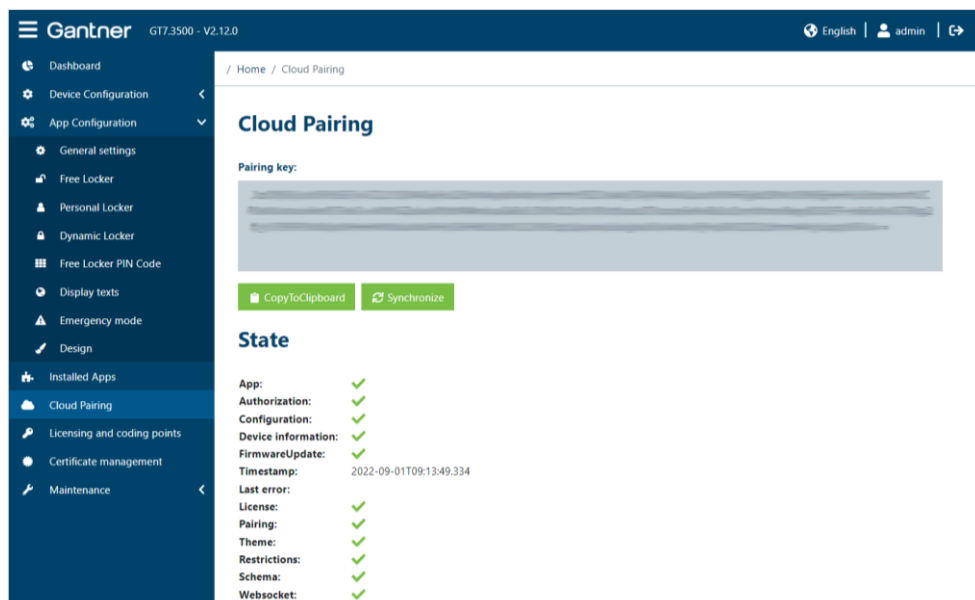


Figure 4.44 – Device pairing – Enter pairing key

- ▶ Enter the pairing key, as displayed on the “Cloud Pairing” page, into the configuration of the GT7 Central Locker.
 - ▶ Enter a name for the device. This can be selected freely.
 - ▶ You can also enter an optional descriptive text in the “Description” field.
 - ▶ Click on “Pair device”.
 - The GT7 Central Locker is displayed in the list of devices in the project.
- NOTE!** To use G7 Connect for configuring/updating or maintaining the G7 device, an outgoing internet connection from the G7 Central Locker Terminal to the cloud is required.
- In the web interface, the state of the pairing process is displayed via the processing of the individual steps. After pairing is completed, the different states are shown to indicate whether an update is required. For example, a red “X” after “FirmwareUpdate” indicates that the device firmware is not up to date and a red “X” after “License” indicates that there are no license points in the device.



State	
App:	✓
Authorization:	✓
Configuration:	✓
Device information:	✓
FirmwareUpdate:	✓
Timestamp:	2022-09-01T09:13:49.334
Last error:	
License:	✓
Pairing:	✓
Theme:	✓
Restrictions:	✓
Schema:	✓
Websocket:	✓

Figure 4.45 – Cloud pairing – State of the pairing process

4.11 Licensing and coding points

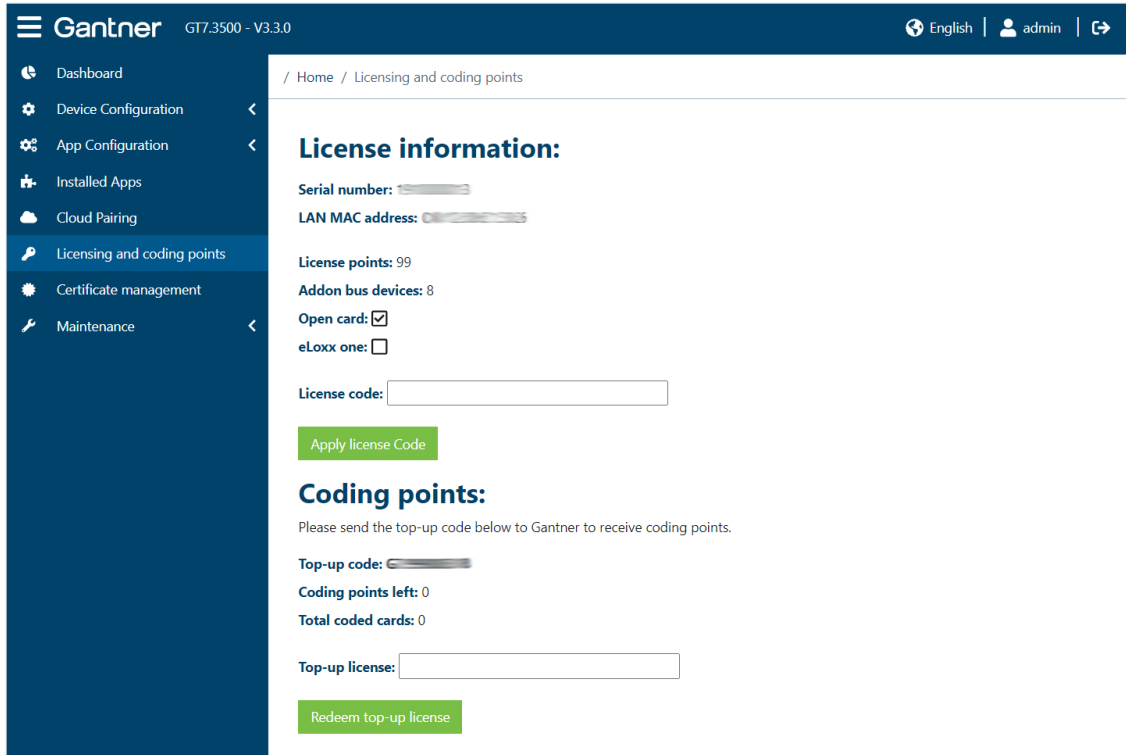


Figure 4.46 – GT7 Central Locker web interface – Licensing and coding points

On this page, the network and license information for the GT7 Central Locker are displayed and you can also add new license points here.



License codes can also be conveniently managed via projects in the G7 Connect and allocated to the individual devices.

License information

- Serial number: The serial number of the GT7 Central Locker.
- LAN MAC address: Unique, internal network address of the GT7 Central Locker.
- License points: To start apps (e.g., G7 Central Locker, G7 Access, or G7 Info) and enable other features, license points are required. These can be purchased from GANTNER. The available license points are displayed here.
- Addon bus devices: Maximum number of devices (controller, reader, etc.) that can be connected to the expansion bus of the GT7 Central Locker.
- Open card: This field indicates whether the “Open Card” license is active. If the license is active, the certificate check is switched off, i.e., data carriers that were not supplied and released by GANTNER can also be used.

- eLoxx One: If the license for the eLoxx One software has been activated, this option is marked with a tick. eLoxx One can then be started on the “System Overview” page.
- License code: A license code to activate additional functions can be entered here.

Coding points can also be added at the bottom of the page, which can then be used to encode data carriers using the corresponding GT7 app.

NOTE! The G7 Central Locker app does not support the coding function!

4.12 Certificate management

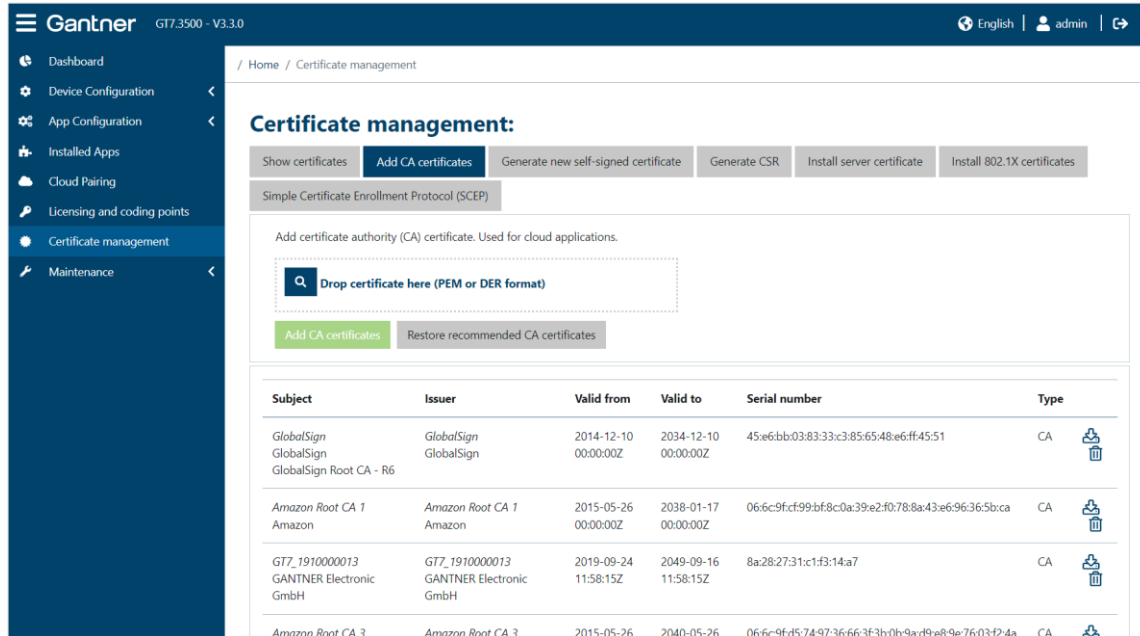


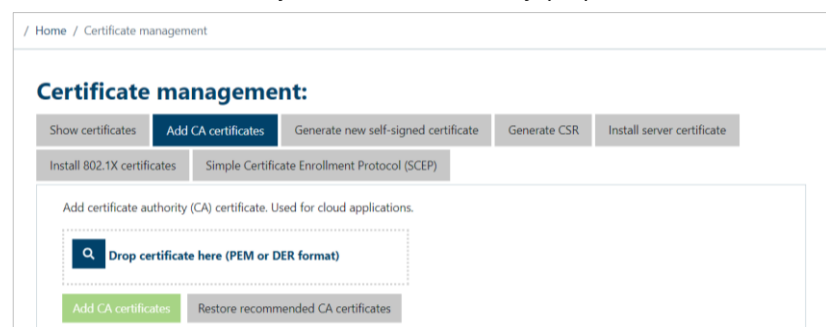
Figure 4.47 – GT7 Central Locker web interface - Certificate management

Here, the certificates stored in the GT7 Central Locker are displayed. The certificates are used to verify the authenticity and integrity of persons and/or objects, especially when communicating over the Internet or network, which can prevent unauthorized access and manipulation.

- ▶ With the button “Show certificates”, the installed certificates are listed as previously described.
- ▶ The following functions can be performed with the other buttons.

- Add CA certificates:

Add a certificate issued by a certification authority (CA).



To do this, drag the file with the certificate (in PEM format) to the location in this window and click on “Add CA certificates”. This way you can also install a certificate that was previously deleted.

- Generate new self-signed certificate: If the encrypted communication between the GT7 Central Locker and the server is to be used (using TLS over HTTPS or WSS), the GT7 Central Locker requires a certificate. It is recommended that you use a certificate issued by a certification authority. You can also have a certificate created yourself. To do this, click on "Create new self-signed certificate". The GT7 Central Locker must then be restarted.
NOTE! If a self-signed certificate already exists on the device, it will be replaced by the new certificate.
- Generate CSR: To have a server certificate or a user 802.1X user certificate created by a certification authority, you can create a Certificate Signing Request (CSR). Enter your data such as company name, country, and IP here.
- Install server certificate: If the GT7 Central Locker is acting as a web server (e.g., when using Relaxx software, which acts as a "client", to establish the connection to the "server" GT7 Central Locker, see "4.14 Integration in Relaxx"), a certificate on the server, i.e., on the GT7 Central Locker is required for a secure connection via TLS. You can create this using CSR and then install it here. To do this, drag the file with the certificate to the field provided and click "Install server certificate".
- Install 802.1X certificates: Here, you can install an official certificate from a certification authority for authentication using 802.1X. To do this, drag the file with the certificate to the field provided and click "Install 802.1X CA Certificate".
- Install 802.1X user certificate: Here, you can install a certificate previously created using CSR for authentication using 802.1X. To do this, drag the file with the certificate to the field provided and click on "Install 802.1X user certificate".
- Simple Certificate Enrollment Protocol: Certificates can be issued, renewed and installed here using the Simple Certificate Enrollment Protocol (SCEP). The following window is displayed:

Subject	Issuer	Valid from	Valid to	Serial number	Type
Factory Default IP: 10.1.1.12.41 GANTNER Electronic GmbH	Factory Default GANTNER Electronic GmbH	2020-11-09 12:54:12Z	2050-11-02 12:54:12Z	30b9fbf5d219e9372bd101ad5c8f00e9a636d7c1	Server

Certificates and authorization authorities can be installed here.

Displayed in the "Configure SCEP" field is the status for SCEP. "Disabled" means that the SCEP function is not activated. Otherwise, the status of the SCEP connection is displayed here. Clicking on "Configure SCEP" takes you directly to the configuration page for SCEP in the device configuration menu (see "4.7.8 SCEP (Simple Certificate Enrollment Protocol)").

- If it is necessary to add a new certificate, simply drag the certificate file to the "Drop certificate here" field.

4.13 Maintenance

4.13.1 Device

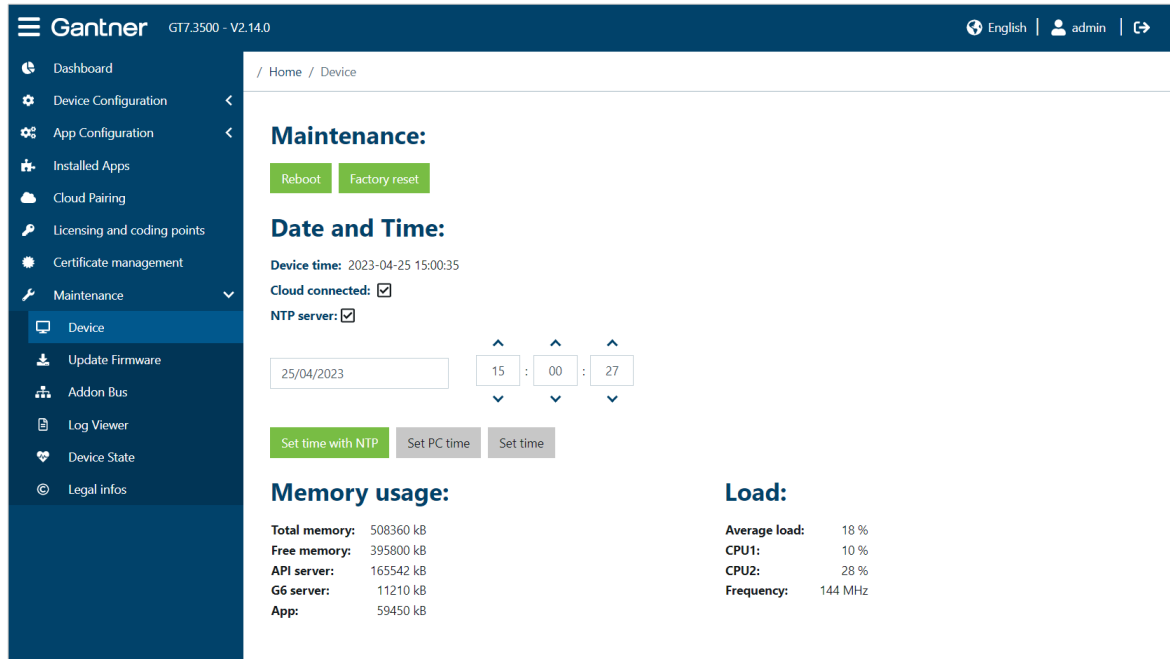


Figure 4.48 – GT7 Central Locker web interface - Maintenance

On this page, the following actions and the following information are available.

Maintenance

- Click on the “Reboot” button to restart the GT7 Central Locker device.
 - The web interface remains connected to the device and further work can be completed in the web interface after the restart is completed.
- To reset the GT7 Central Locker to its factory settings, click on the “Factory reset” button.

ATTENTION! All settings in the device are deleted during the reset process.

- After resetting to factory settings, the device is in same functional state it was upon delivery.

Date and Time

- Device time: The current time in the GT7 Central Locker is displayed here. This time is updated every second. The time can be changed in the device configuration (see “4.7.9 Time”).
- Cloud connected: When this option is selected, the device is paired with the G7 Connect. This setting can be set in the device configuration (see “4.7.3. G7 Connect”).
- NTP server: This setting defines whether an NTP server is used for automatic time synchronization in the GT7 Central Locker (tick = enabled). The setting for using an NTP server is provided in the configuration menu of the GT7 Central Locker (see “4.7.9 Time”).

► To reset the time in the GT7 Central Locker, select one of the following 3 options:

- Set time with NTP: The time is automatically obtained from an NTP server in the network.
- Set PC time: The current time of the PC is set in the GT7 Central Locker.
- Set time: You can manually enter a time and date into the input fields. After clicking on the “Set time” button, the entered values for the time and date are set in the GT7 Central Locker.

Memory usage

Information about the memory in the GT7 Central Locker, i.e., the total memory, free space, and memory used by each component, is shown here.

4.13.2 Update firmware

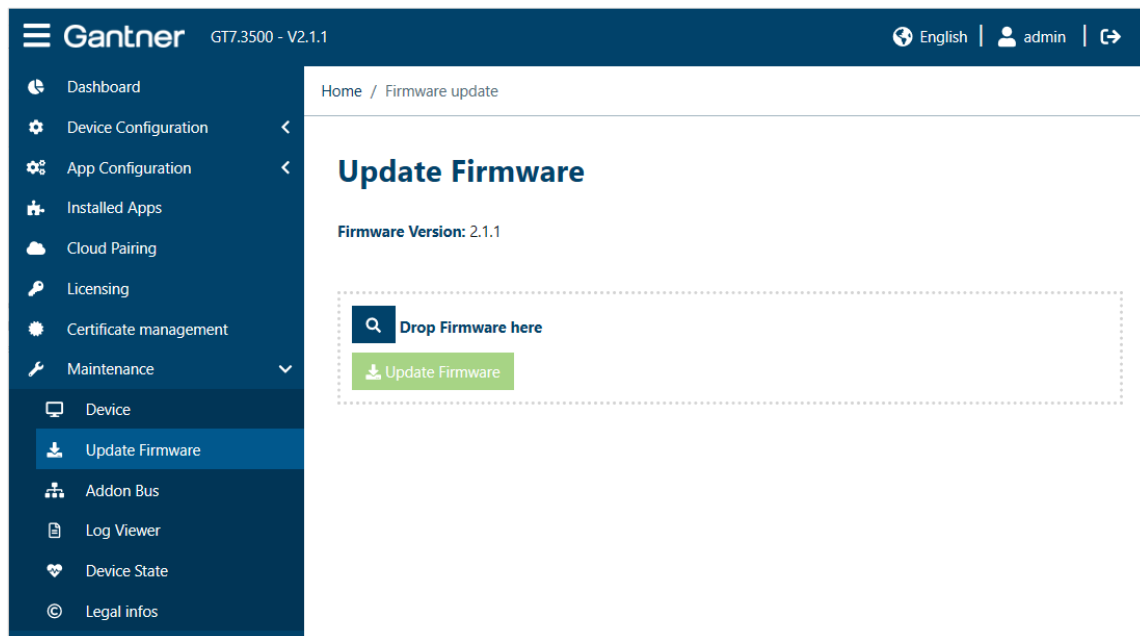


Figure 4.49 – GT7 Central Locker web interface – Update Firmware

Here, the firmware currently installed in the GT7 Central Locker is displayed.

- ▶ To install new firmware, drag the firmware file to the “Drop Firmware here” field.
 - ▶ Click on “Update Firmware”.
 - The new firmware is loaded into the GT7 Central Locker and the device restarts.
- NOTE!** During the firmware update, ensure that the power supply to the GT7 Central Locker is not disconnected.

4.13.3 Addon bus (external devices)

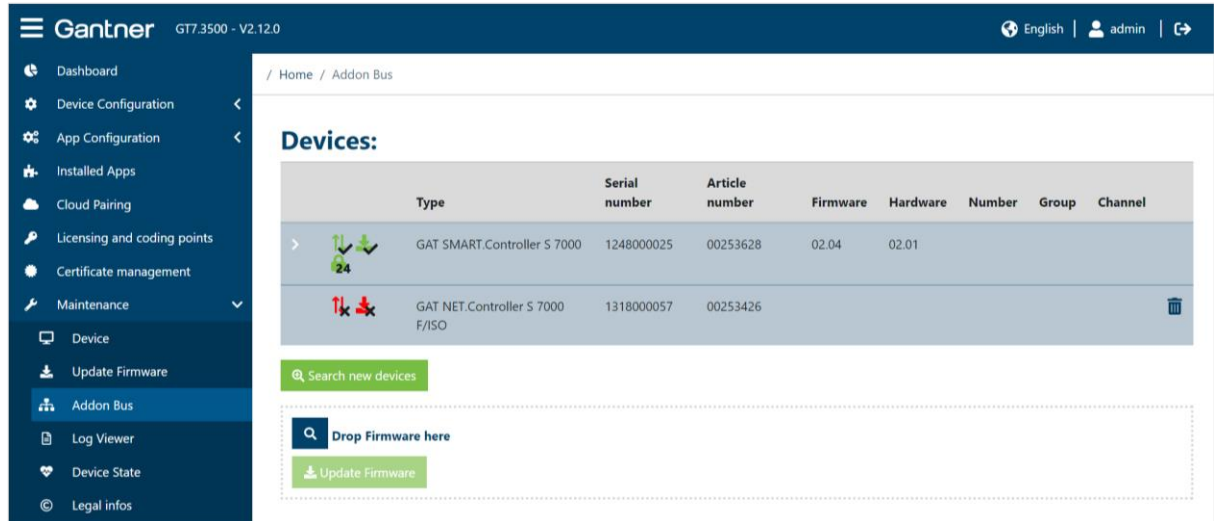


Figure 4.50 – GT7 Central Locker web interface – Addon Bus

Information about the devices (e.g., the GAT SMART.Controller S 7020 and GAT NET.Controller S 7020 sub controller) connected to the GT7 Central Locker via the Addon Bus are displayed here.

- ▶ A list of all locks connected to a sub controller can be displayed by clicking on the desired sub controller. Clicking again closes the list.
 - ▶ To search for new devices that have been connected to the GT7 Central Locker, click on “Search new devices”.
 - The GT7 Central Locker searches for new devices connected to the addon bus and display them in the list. This process can take up to one minute.
 - ▶ To install new firmware for the devices, drag the firmware file to the “Drop Firmware here” field.
 - ▶ Click on “Update Firmware”.
 - The new firmware is loaded to all devices of the appropriate type and the devices are restarted.
- NOTE!** During the firmware update, ensure that the power supply to the external device and the connected device are not disconnected.

4.13.4 Log viewer

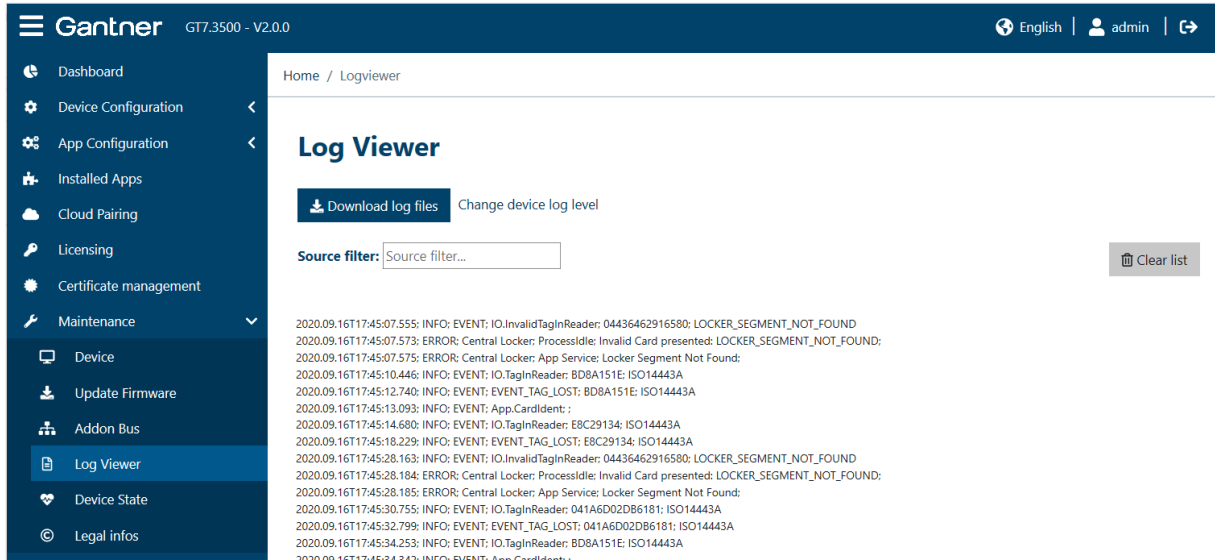


Figure 4.51 – GT7 Central Locker web interface – Log Viewer

In the GT7 Central Locker, all events such as locker openings, data carrier identifications, and even error messages are stored in log files. You can load these saved log files from the device to the PC (file format = .csv). In addition, it is possible to display the occurring events live.

- ▶ To load the log files from the GT7 Central Locker, click on “Download log files”.
 - A file window opens where you must specify the storage location.
 - The log files from the last 8 days are sent to an archive and saved in the selected storage location.

i The events that will be recorded are configured using the “Log Level” option (see chapter “5.6.10 Device”).

- ▶ Click on “Change device log level” to open the device settings (see “4.7.12 Device”). Here, you can change the log level to define which types of events will be displayed in the live view (e.g., all information + warnings or only errors, etc.).

4.13.5 Device state

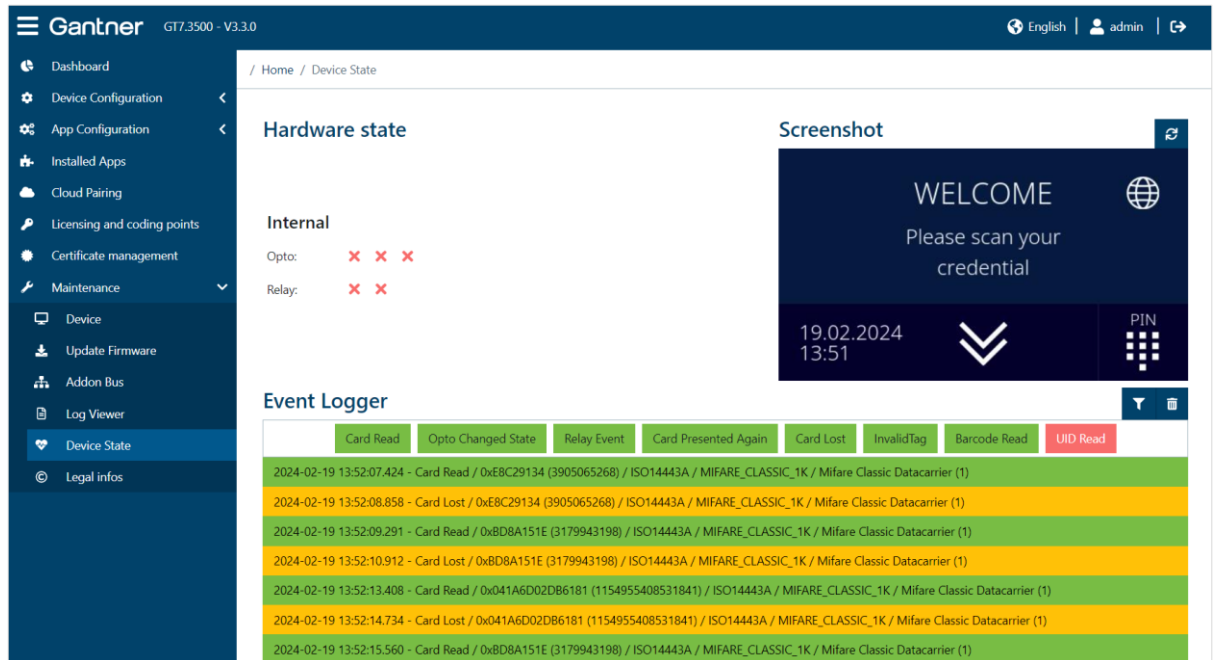


Figure 4.52 – GT7 Central Locker web interface – Device State

A GT7 Central Locker has two digital relay outputs and one digital optocoupler input. These can be used to receive status information and/or for control. The state of these inputs and outputs is displayed here under “Hardware state”. The inputs and outputs do not need to be used. In the example shown, the relay 1 is active, all other inputs and outputs are inactive.

To the right of the hardware state is the screenshot function for the GT7 Central Locker.

- ▶ To take a screenshot of the screen currently displayed on the terminal, press the refresh  button.

Below that is the Event Logger. Here, the live events occurring on the device are displayed.

- ▶ When an event occurs on the GT7 Central Locker (e.g., data carrier read) or when the optocoupler input state or one of the relay states changes, a corresponding entry is displayed.
- ▶ The filter icon  displays all event types. By clicking on these events, they can be switched between active (green) and inactive (red). Only the green events are shown in the list.
- ▶ To clear the list, click on the trash icon .

4.13.6 Legal information

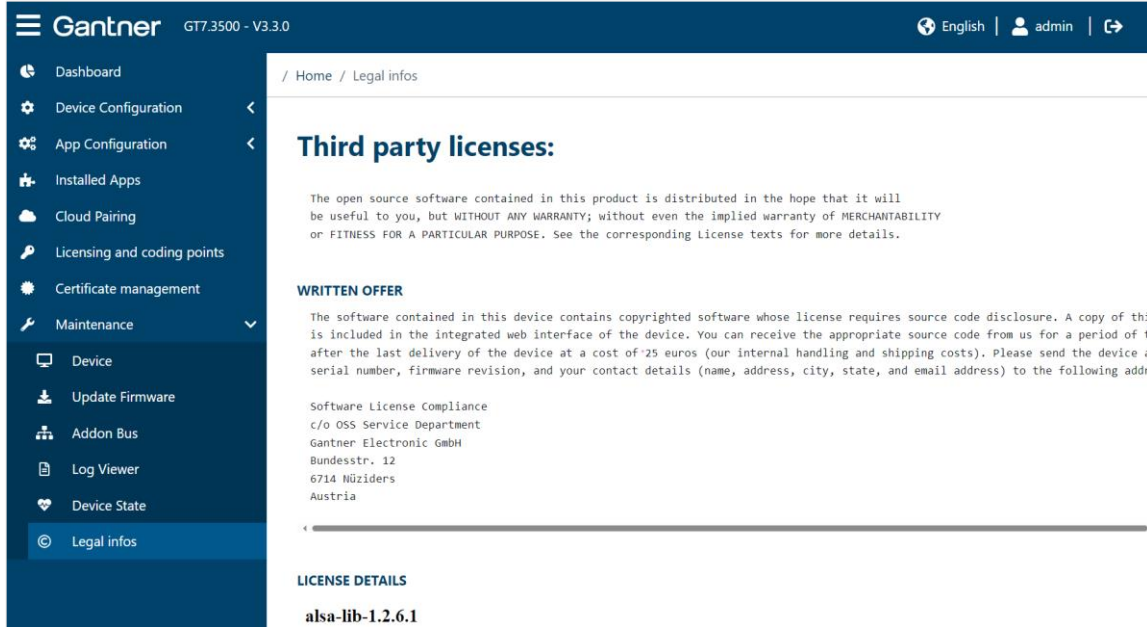


Figure 4.53 – GT7 Central Locker web interface – Legal info

Displayed here is the license information for the third-party software included with the GT7 Central Locker. For example, the GNU license information for the operating system in the GT7 Central Locker.

4.14 Integration in Relaxx

For the management of the user data carriers including authorization assignment as well as for setting the locker modes and all other locker settings, a GT7 Central Locker can be integrated into the Relaxx management software.

i A detailed description of the Relaxx software is provided in the software operating manual. The basic steps necessary to integrate a GT7 Central Locker into Relaxx and configure the associated locks are described below.

Basically, the following steps are necessary:

1. Add GT7 Central Locker to Relaxx
2. Select locker mode
3. Assign locker numbers
4. Authorize the users
5. Settings for PIN verification (data carrier + PIN), if this function is being used.

4.14.1 Step 1 - Add GT7 Central Locker to Relaxx

- In Relaxx, go to the "Lockers" tab (1) and then select "Hardware" (2).

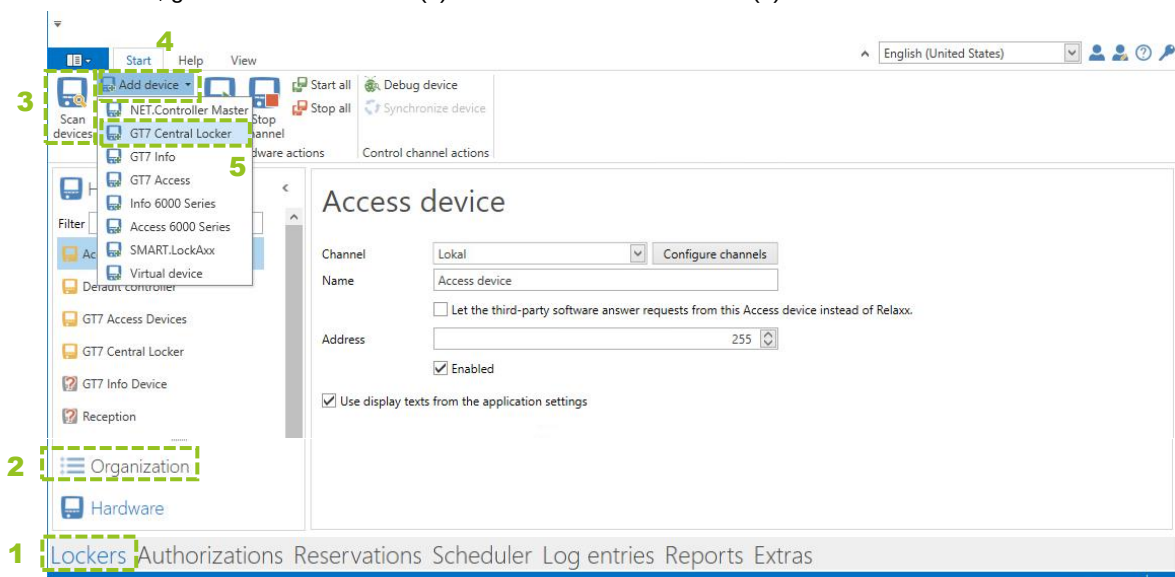


Figure 4.54 – Relaxx – Add a new GT7 Central Locker

NOTE! Before adding the GT7 terminal, it is important that the G7 Central Locker app is already enabled, and that this app is the active app.

- Add the GT7 Central Locker. You have two options:
- a) On the "Start" menu, click "Scan devices" (3). The network is scanned and the found devices are displayed. Highlight the GT7 Central Locker and then click "Add selected devices".
 - b) If you know the IP address of the GT7 Central Locker, you can also add it manually by clicking the "Add Device" button (4) and then selecting "GT7 Central Locker" (5) from the displayed menu.

- The “Device” window opens where you can enter the data and the communication channel for the new device.

Figure 4.55 – Relaxx - Enter data for the new GT7 Central Locker

- ▶ The “Save” button appears at the bottom of the window after the data has been entered. Click to add the new device to Relaxx.
 - The new GT7 Central Locker is displayed in the hardware list to the left.
- NOTE!** If communication encrypted via TLS is to be used, enable this option in Relaxx and also configure this in the device settings of the GT7 Central Locker. To do this, the GT7 must have a server certificate (“4.12 Certificate management”).
- ▶ Click on the GT7 Central Locker to see its settings.

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value
2	10	Personal locker	2010060041	11	
4	10	Personal locker	2010060041	13	
5	10	Free locker	2010060041	13	

HW 4.2, SW 3.3.0 App: 6.0.0 App Name: G7 Central Locker App

Dashboard Lockers Authorizations Reservations Scheduler Log entries Reports Extras

Figure 4.56 – Relaxx – Settings of the GT7 Central Locker

- The area to the right shows all lockers or channels that are connected to the sub controllers on the GT7 Central Locker.

4.14.2 Step 2 – Select locker mode

- In the “Locker mode” column, select the mode that each locker is to operate in. Please note the following:
 - There are four modes to choose from: Free locker, Personal locker, Reservable locker, and Dynamic locker.
 - The difference between “Reservable locker” and “Personal locker” in Relaxx is that for personal lockers, individual authorizations can be created and for reservable lockers, reservations are created in the calendar from which the authorizations are generated.
 - The locker mode set in the Relaxx software must always be the same as in the GT7 Central Locker, i.e., “Free locker” set in Relaxx -> “Free locker” also set in GT7 Central Locker, or when “Personal locker” or “Reservable locker” is set in Relaxx -> “Personal locker” must also be set in GT7 Central Locker. From version 3.0 of the G7 Central Locker app, both modes can also be used together, i.e., if some lockers are set to free locker and others to personal locker, both modes must be defined in the GT7 Central Locker.

GT7 Central Locker

✕ Advanced configuration

Channel: 10.1.112.239 Configure channels

Use custom ports ☐

TLS ☐

Name: GT7 Central Locker

Enabled ☒

Master card sets: Default Change password

Drag a column header here to group by that column

Address	Locker number	Locker mode	Max. number...	Sub controll...	Antenna value
2		Personal locker	10	2010060041	11
4		Personal locker	10	2010060041	13
5		Free locker	10	2010060041	13

HW 4.2, SW 3.3.0 App: 6.0.0 App Name: G7 Central Locker App

Figure 4.57 – Relaxx - Locker modes of the lockers connected to the GT7 Central Locker

- Firmware version min. 2.5 must be installed in the sub controllers to operate the GT7 Central Locker.

4.14.3 Step 3 - Assign locker numbers

- You can now assign locker numbers to the lockers. To do this, go to the “Organization” view (1), create, or select the locker group (2) to which you want to assign the lockers. Next, the “Assign lockers” button (3) is displayed where you can choose to assign the lockers manually or with data carriers (4).

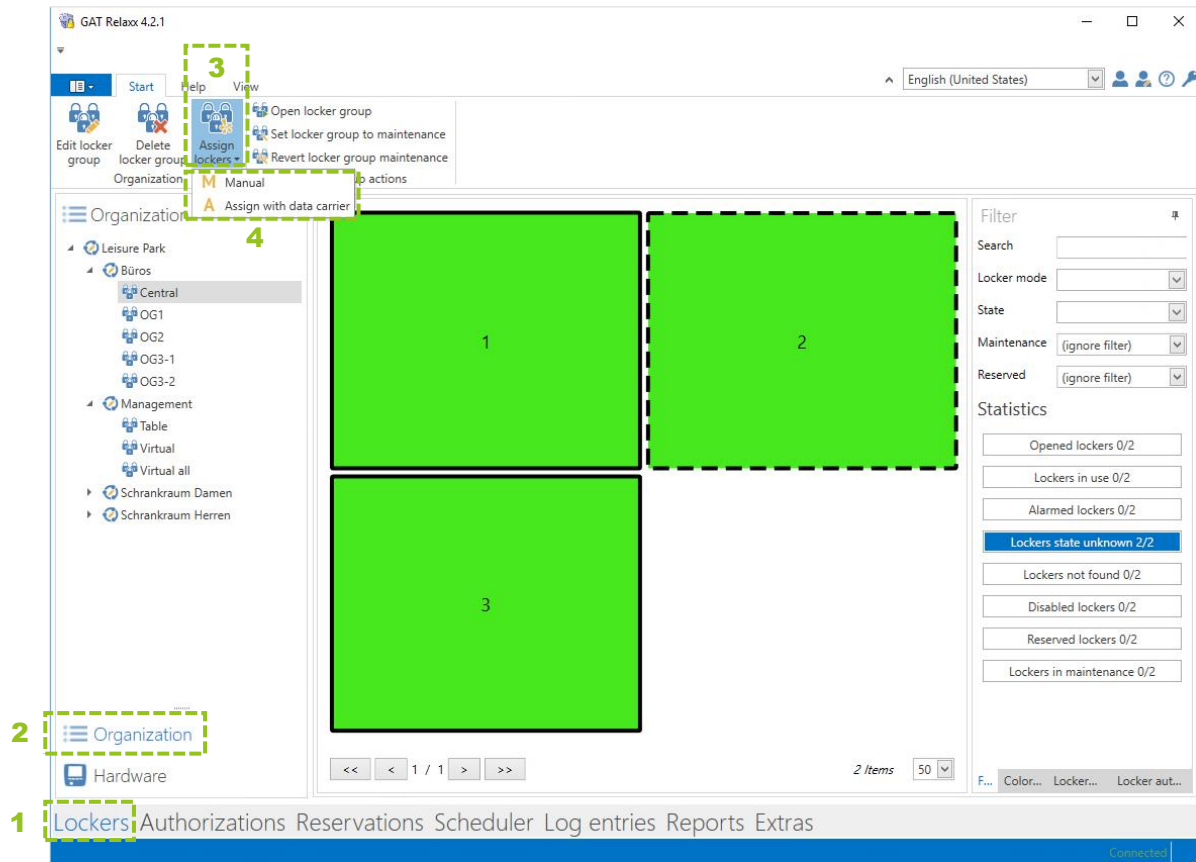


Figure 4.58 – Relaxx – Locker assignment

a) Manual locker number assignment

Assign lockers

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

Start with locker number:

Step:

Advanced options

Prefix: ☐

Postfix: ☐

Leading zeros and number of digits: ☐

Preview: 1

Locker Controller Name	Sub controller seri...	Address	Locker number	Selected
Locker Controller Name: Battery locks				
Sub controller serial number:				
	111			☐
	113			☐
Locker Controller Name: GT7 Central Locker Desk				
Sub controller serial number: 1248000025				
	1			☐
	2			☐
	3			☐

Figure 4.59 – Relaxx – Manual locker number assignment (M)

Manual locker assignment allows you to manually assign individual lockers to the locker group from all the available lockers connected to any controller.

- ▶ In the "Start with locker number" field, enter the number to assign to the first selected locker.
- ▶ In the "Step" field, you can enter a step size for numbering the lockers. Example: With "2" you can assign all even or odd numbers depending on the start value.
- ▶ Click on "Advanced options" to display additional settings (these options are only possible for online lockers):
 - In the "Prefix" and "Postfix" fields, you can enter alphanumeric values that are inserted before or after the locker numbers.
 - If you select the "Leading zeros and number of digits" option, you can enter a number that determines the length of the displayed locker number. Missing places are filled with leading zeros. Example: "4" -> 0001, 0002, 0012, 0123, 1234.
 - The text in the "Preview" field is a continuously updated display of how the number will be displayed with the settings.
- ▶ In the "Selected" column of the displayed list, mark all lockers to be assigned to the locker group.
 - The locker numbers are assigned automatically, beginning with the entered start number, and increasing by the entered increment.
- ▶ It is also possible to change individual locker numbers manually.
- ▶ After assigning all lockers, click on "Save".

b) Locker number assignment with data carrier

With this method, lockers can be locked on-site using a data carrier or simply by pushing the locker door shut, which automatically assigns the locker to the selected locker group with a number.

The screenshot shows a software window titled "Auto assign lockers". It contains the following elements:

- Data carrier to use:** A text input field followed by a "Read" button.
- Start with locker number:** A numeric input field with a spinner, currently set to 1.
- Step:** A numeric input field with a spinner, currently set to 1.
- Prefix:** A checkbox followed by a text input field.
- Postfix:** A checkbox followed by a text input field.
- Leading zeros and number of digits:** A checkbox followed by a numeric input field with a spinner, currently set to 1.
- Preview:** A label "Preview" followed by the number "1" and a large empty rectangular box.
- Start assign:** A button at the bottom of the window.

Figure 4.60 – Relaxx – Auto locker assignment

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

NOTE! It is not compulsory to enter a data carrier number here. However, not doing so entails the risk that locker numbers can be incorrectly assigned to other lockers if they are closed unintentionally after starting locker assignment mode (see below). This is prevented by entering a data carrier, as the data carrier can first be read at the GT7 Central Locker and then only the lockers at this GT7 Central Locker are considered for the locker assignment.

- ▶ In the "Start with locker number" field, enter the number to assign to the first selected locker.
- ▶ In the "Step" field, you can enter a step size for numbering the cabinets. Example: With "2" you can assign all even or odd numbers depending on the start value.
- ▶ In the "Prefix" and "Postfix" fields, you can enter alphanumeric values that are inserted before or after the locker numbers.
- ▶ If you select the "Leading zeros and number of digits" option, you can enter a number that determines the length of the displayed locker number. Missing places are filled with leading zeros. Example: "4" -> 0001, 0002, 0012, 0123, 1234.
- ▶ The text in the "Preview" field is a continuously updated display of how the number will be displayed with the settings.
- ▶ Click on "Start assign".
- ▶ If no data carrier has been entered, go directly to the lockers, and lock all lockers in the order that they should be assigned to the selected locker group.
- ▶ If a data carrier has been entered:
 - For GAT SMART.Lock 7001 lockers: Read the data carrier at the GT7 Central Locker to start the assignment. Lock all lockers in the order that they should be assigned to the selected locker group.
 - For GAT NET.Lock 7020 lockers: You can either read the data carrier at the GT7 Central Locker or go to the locker and read the data carrier there to start the assignment. Lock all lockers in the order that they should be assigned to the selected locker group.
 - The lockers are assigned numbers in increasing order, beginning with the entered start number, and assigned to the locker group.
- ▶ Once all lockers are assigned, close the window via the red "X" icon.
- ▶ The lockers locked during the assignment process can all be opened again via the "Open locker group" button.
 - The assigned lockers are displayed in the locker overview when the locker group is selected.
- ▶ Exit locker assignment mode by reading the data carrier on the GT7 Central Locker again (if a data carrier was used).
- ▶ After the assignment has been completed, close the window in Relaxx.
 - This ends the locker assignment mode.

4.14.4 Step 4 – Authorize the users

The authorization of the user data carriers is completed in Relaxx. The detailed instructions can be found in the Relaxx operation manual.

4.14.5 Step 5 – Settings for PIN verification

With the PIN verification function, a PIN code must be entered after reading a data carrier in order to use lockers (see "5.8 PIN verification for data carriers"). The function must be activated both in the GT7 Central Locker (see "4.8.5 PIN code") and in the Relaxx software as described briefly here. See the Relaxx operating manual for a detailed description.

- In the Relaxx software settings, go to the "Devices" page and click on the "GT7 Central Locker" tab.

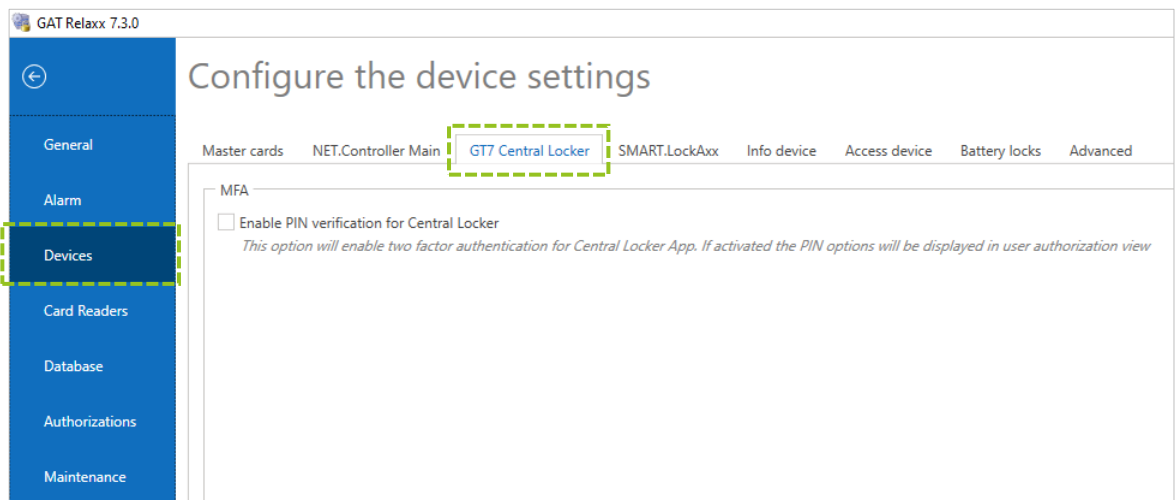


Figure 4.61 – Relaxx settings: GT7 Central Locker

- Select the "Enable PIN verification for Central Locker" option.
- Open the "Authorizations" page and select the "Authorization list enabled" option.

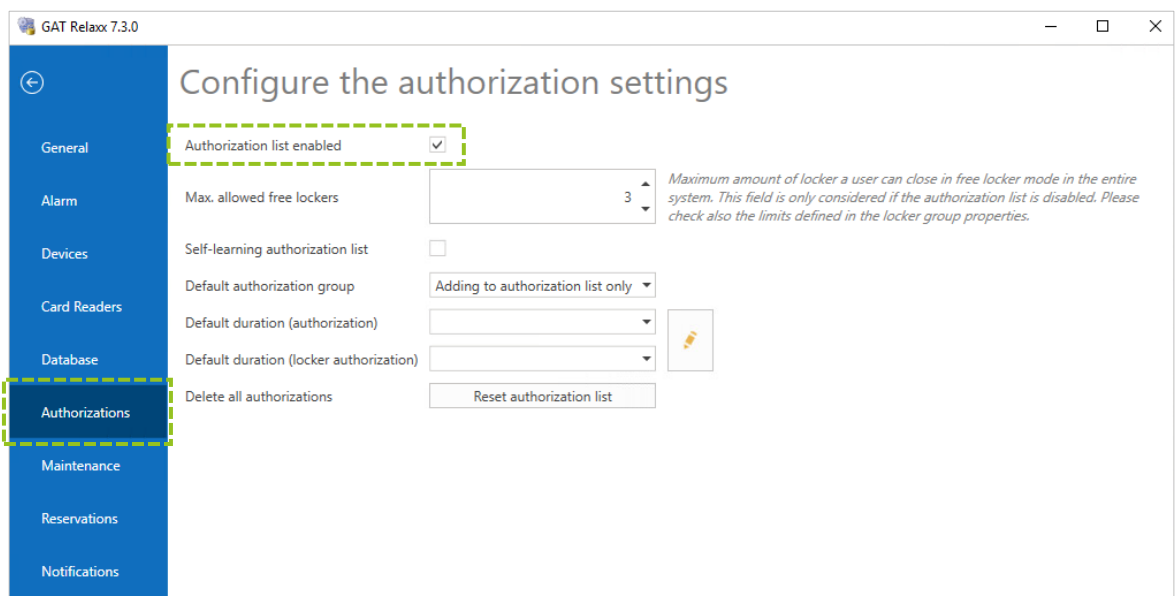


Figure 4.62 – Relaxx settings: Enable authorization list

- When a user is authorized, extended options for PIN entry are available.

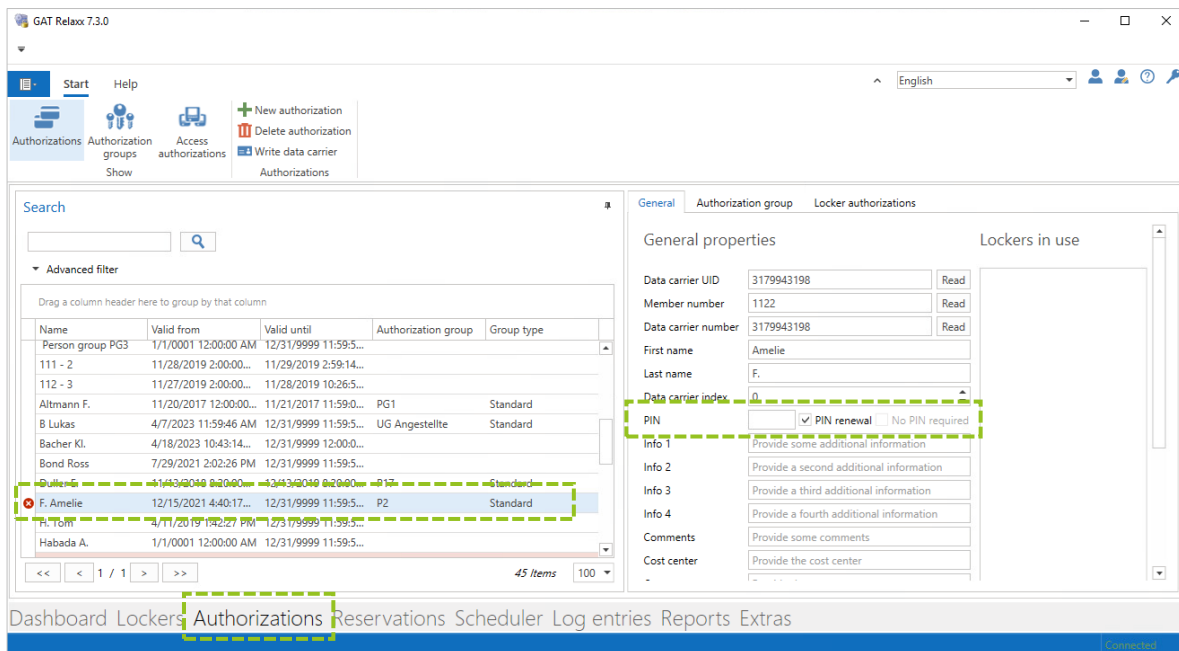


Figure 4.63 – Relaxx settings: User authorizations

- PIN: Enter the PIN code that the user will use for PIN verification.
- PIN renewal: If this option is enabled, the user must renew their PIN code or define a different one the next time they identify themselves. See also "5.8 PIN verification for data carriers".
- No PIN required: Enable this option for the user to exclude them from completing the PIN verification process at the GT7 Central Locker, even if this function is generally enabled in the GT7 Central Locker settings.

5 OPERATION

5.1 Target group

This chapter is intended for the system administrator and the operating personnel of the locker locking system. It contains information about the operation of the GT7 Central Locker and lockers. Operation using the LockPal app is also possible (from Relaxx version 5.3). For more information, see the LockPal app manual. No specific expertise is required for this chapter.

5.2 Operation of the lockers

If GAT NET.Lock 7xxx locks are used, a locker can be unlocked and locked directly at the locker. To use this function, the setting “Allow authentication at the door” must be enabled in the configuration settings.

i The authentication function at the door is not possible with the GAT SMART.Lock 7xxx locks.

NOTE! Identification at the locker is not available if the PIN verification function is enabled (= “PIN verification for data carrier”). See “4.8.5 PIN code” for more information.

a) Personal locker mode

Personal Locker

Allow authentication at the door: ☒

Opening confirmation: ☒

When the function is enabled, a data carrier can lock and open every personal locker for which it is approved. All you have to do is push the locker door shut and hold the data carrier in front of the LED on the locker door. The GAT NET.Lock 7xxx reads the data carrier and locks or unlocks the locker door accordingly.

b) Free locker mode

Free Locker 2007-01-01T00:00:00.000Z

Allow authentication at the door: ☒

Door behavior of available lockers: Nothing

Nothing

Only Open

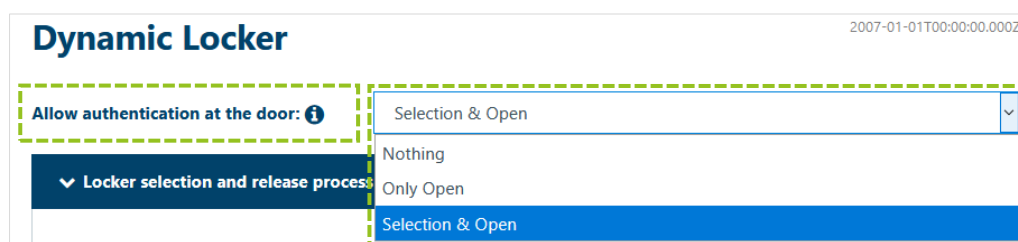
Selection & Open

▼ Locker selection and release process

- Nothing: Identification at the locker door is not possible. All locker actions must be processed at the terminal.

- Only Open: A locked locker door can be opened directly at the locker with an authorized data carrier. Simply hold the data carrier in front of the LED on the locker door. The door must be locked at the GT7 Central Locker.
- Selection & Open: The locker door of a free locker can be locked AND unlocked again directly at the locker using an authorized data carrier. To lock, press the locker door shut and hold your data carrier in front of the LED on the locker door. To open it, simply hold your data carrier in front of the LED. Operation via the GT7 Central Locker is still possible.

c) Dynamic locker mode



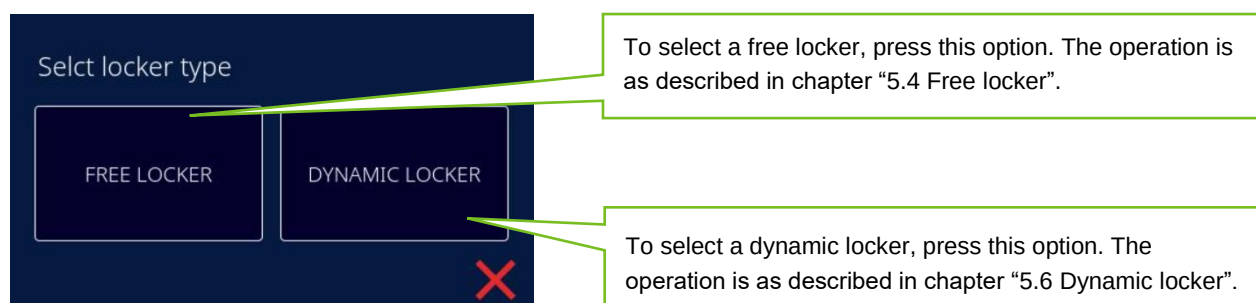
i The operation for dynamic lockers is analogous to that of the free lockers. See the previous section “b) Free locker mode” for the description.

5.3 Operation of the GT7 Central Locker

To operate the GT7 Central Locker, the user first identifies themselves by reading their data carrier at the reader of the GT7 terminal. Alternatively for lockers in free locker mode, the user can operate the locker with just a PIN code if this function is enabled in the PIN settings for free lockers. PIN verification can also be set for data carrier identification in which the user is required to enter a PIN code in addition to reading their data carrier (see “4.8.5 PIN code”). The GT7 Central Locker automatically recognizes whether a user has a locker in use or not, and the selection for opening or locking a locker is displayed accordingly.

The sequence of operation differs depending on the locker operating mode (free locker, personal locker, dynamic locker) and the settings configured for the mode.

If there are free lockers and dynamic lockers operating together in the system, the following screen is displayed on the GT7 Central Locker after user identification:



5.4 Free locker

The configuration settings for Free Locker define how the lockers in free locker mode operate as well as the type of locker selection and the opening and closing process of a locker controlled by the GT7 Central Locker. Also refer to chapter “4.8.2 Free Locker” for more information on the available settings.

5.4.1 Door behavior of unoccupied lockers

In order to adapt the behavior and appearance of the lockers to different operating requirements, several settings can be configured for the connected sub controllers. The settings are found in the web interface of the GT7 Central Locker on the “Device configuration” -> “Sub Controller” page. These settings determine how the locker doors of unoccupied lockers in free locker mode behave thus also determining the operation when the doors are closed.

- Auto close free locker: If this setting is enabled, the locker door of an unoccupied locker is held shut when it is pushed closed without reading a data carrier. This creates a uniform look with an even locker surface. The unoccupied lockers are indicated by a green LED. To avoid confusion when locking, the locker selection should take place at the lockers and then the respective locker number selected for locking at the Central Terminal.

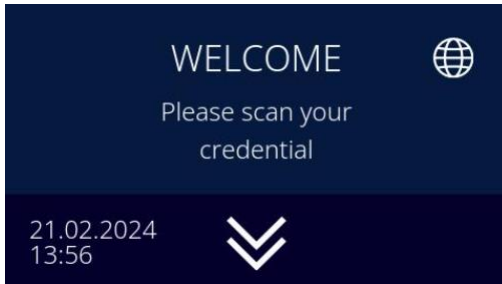
NOTE! The “Last closed first” setting is recommended for the “Locker suggestion mode” here. When “Last closed first” is enabled, the correct locker is suggested at the terminal directly after the user has selected a locker, put their belongings inside, and closed the door.

If this option is not enabled, the locker doors of available lockers are open and cannot be closed without identification. This allows potential users to see from a distance which lockers are still available and prevents misunderstandings when locking a locker.

- Push to Open - Free Locker: If this setting is enabled, a valid identification must first be completed in order to open a locked door in free locker mode. The door is then unlocked but is still held in the closed state. The LED is green. The user must then briefly press the door in to open it and has the set “Push to Open timeout” time to do this.

If the option is not selected, the door of a free locker is unlocked and opened immediately after a valid identification.

5.4.2 Selecting a locker

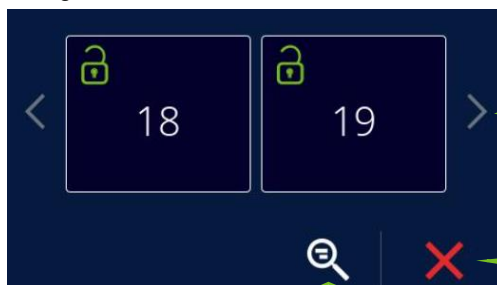


► Scan your credential. Three options are available:

1. No free lockers are available: A notification is shown and the display changes back to the default state.
2. If free locker mode and dynamic locker mode are both available in the system: A query is first displayed asking which locker type to use. In this case, select "FREE LOCKER".



3. If the "Number of locker suggestions" option is set to >1: You can select any displayed locker. The number of lockers displayed is determined by the value of this setting in the "Free Locker" configuration section.

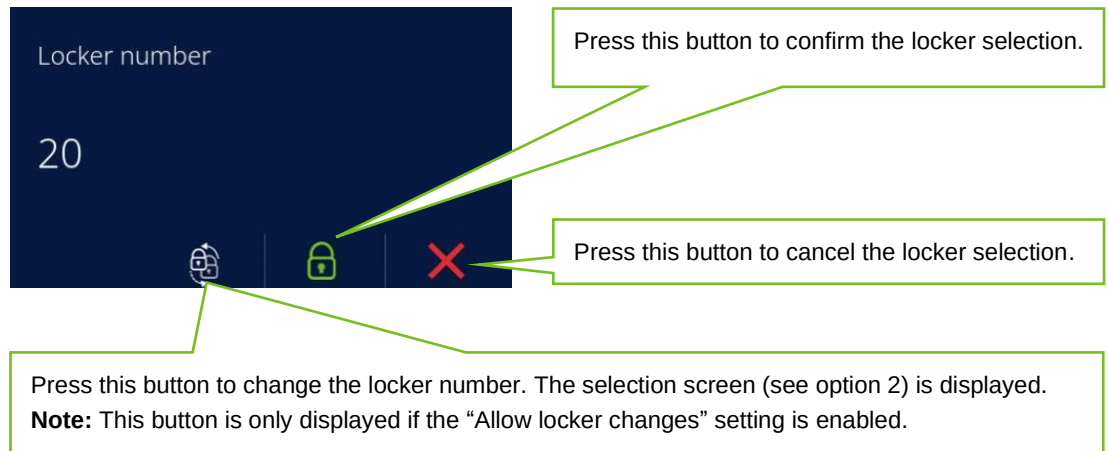


To select a locker number, use the arrow keys to scroll through the available lockers and then press the number to confirm.

Press this button to cancel the locker selection.

This symbol is only displayed when the "Enable selection by number" option is enabled in the settings. To search for a specific locker, press this button and enter the desired locker number using the keypad. If the locker does not exist or is unavailable, an error message is displayed.

4. If the "Number of locker suggestions" option is set to 1: The number of the next unoccupied locker is automatically displayed. The displayed number depends on the "Locker suggestion mode" setting. Furthermore, this screen is only displayed when the "Confirmation of selection" option is enabled. Otherwise, the locker closing process starts directly without this display.



5.4.3 Locking a locker

These instructions continue on from the locker selection process as described in "5.4.2 Selecting a locker" and "5.5.1 Selecting a locker with PIN".

a) Procedure when "Auto close free locker" is not enabled in the "Sub Controller" settings

In this mode, the doors of the unoccupied lockers in free locker mode are open. To lock a locker, you must first select it at the GT7 Central Locker Terminal as described on the previous page.

- If the "Lead time before locking" option on the "Free Locker" configuration page is set to 0, the selected locker can be locked immediately (see below).
- If the "Lead time before locking" option is set to >0: The following countdown screen is displayed. This time allows you to go to the locker and the locker can only be locked after this time has expired.



- The following display indicates that the locker can now be closed for locking.



- ▶ Push the locker door shut.
 - You have the configured “Locking timeout” time (see “4.7.15 Sub controller”) to close the locker. After this it will lock automatically and the locker is assigned to the user’s data carrier.
 - The display changes back to the default state after 5 seconds, but the time for closing the locker continues counting down. If the locker is closed after the “Locking timeout” time has expired, the locker door springs open again. To lock the locker, re-identification is required.

b) Procedure when “Auto close free locker” is enabled in the “Sub Controller” settings

This function is intended for the GAT NET.Lock system. Here you can choose a locker and put your belongings inside before locker selection at the GT7 Central Locker. Unoccupied lockers are indicated via a green LED. The locker door can be opened or closed because in this mode the locker door of an unoccupied locker is held shut (but not locked) by pressing it closed.

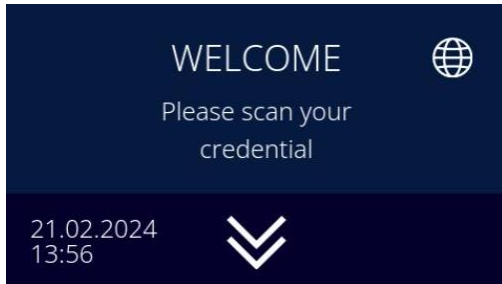
- ▶ Briefly push the closed door of an unoccupied locker (green LED) in.
 - The locker door springs open.
- ▶ Put your belongings into the locker and push the locker door shut.
 - The door is held shut.
- ▶ Go to the GT7 Central Locker and select your locker (see “5.4.2 Selecting a locker”).
 - If the “Lead time before locking” option on the “Free Locker” configuration page is set to 0, the locker can be locked immediately.
 - If the “Lead time before locking” option is set to >0, the following countdown screen is displayed:



- If the locker is opened again (see previous step), you have the configured “Locking timeout” time (see “4.7.15 Sub controller”) to close the locker door before it is then locked automatically.

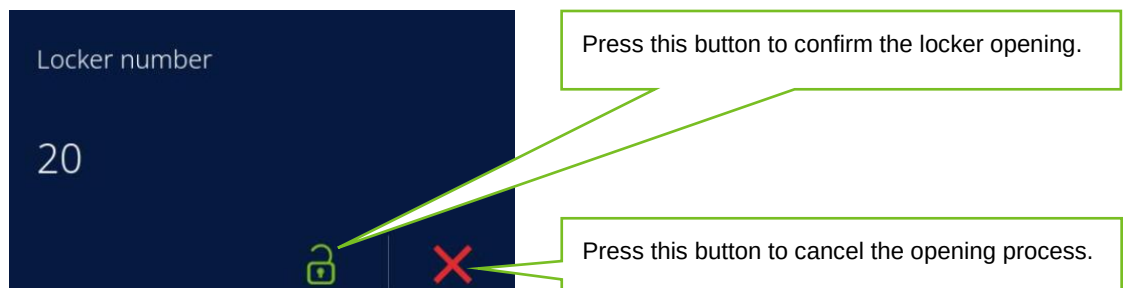
NOTE! If the locker is closed after the “Locking timeout” time has expired, the locker door is kept closed, but is not locked and can be opened by any other user by pushing the door in.

5.4.4 Unlocking a locker

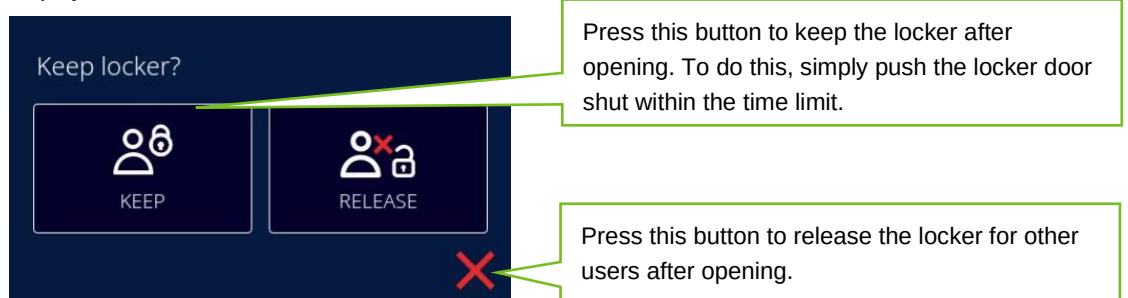


► Scan your credential.

- If the “Opening confirmation” option is not enabled: The confirmation screen is not displayed.
- If the “Opening confirmation” option is enabled: The following confirmation screen is displayed.



- If the “Release process” option is set to “Always release”: The release screen is not displayed.
- If the “Release process” option is set to “Keep-/release-question”: The following confirmation screen is displayed.



- If the “Lead time before opening” is set to 0: The locker opens immediately.
- If the “Lead time before opening” is set to >0: The countdown screen is displayed.



- ▶ The locker is unlocked.
 - If the “Push to Open - Free Locker” option is not enabled in the sub controller settings: The locker door opens.
 - If the “Push to Open - Free Locker” option is enabled in the sub controller settings: The locker door remains closed after unlocking and can be opened by pushing it in briefly.

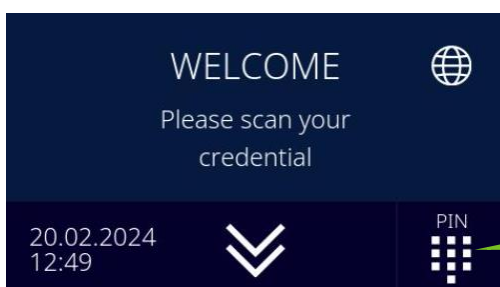


5.5 Free locker with PIN code

Lockers operating in free locker mode can also be locked and unlocked using a PIN code instead of identification via data carrier. The settings that are configured for the lockers determine how they operate as well as the locker selection/closing/opening process at the GT7 Central Locker. Please also refer to chapters “4.8.2 Free Locker” and “4.8.5 PIN code” for an understanding of the available settings.

i There is also a PIN code function for PIN verification of data carriers. This function is described in chapter “5.8 PIN verification for data carriers”.

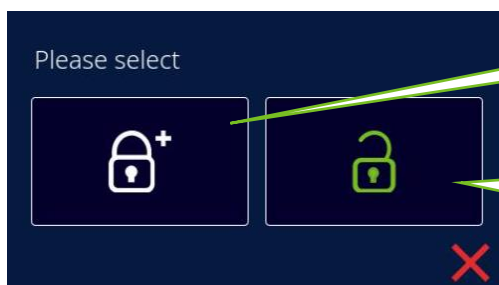
5.5.1 Selecting a locker with PIN



The keypad button allows you to select and close a locker via PIN. This function can be enabled by selecting the “Allow PIN usage in Free Locker mode” option on the “PIN Code” settings page.

► Press the keypad button.

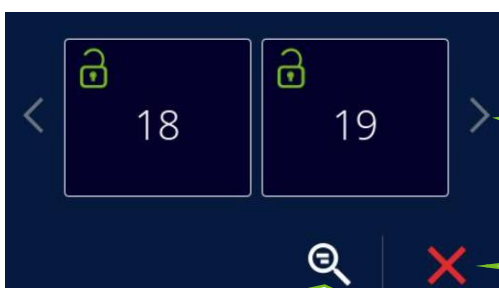
- The “new locker / open locker” screen is displayed.



Press this button to select a new locker.

Press this button to open a locker (see “5.5.2 Unlocking and opening a locker with PIN”).

- If no lockers are available: A notification is shown and the display changes back to the idle state.
- If the “Number of locker suggestions” option is set to >1: You can select any displayed locker. The number of lockers that are displayed for selection is defined in the settings.

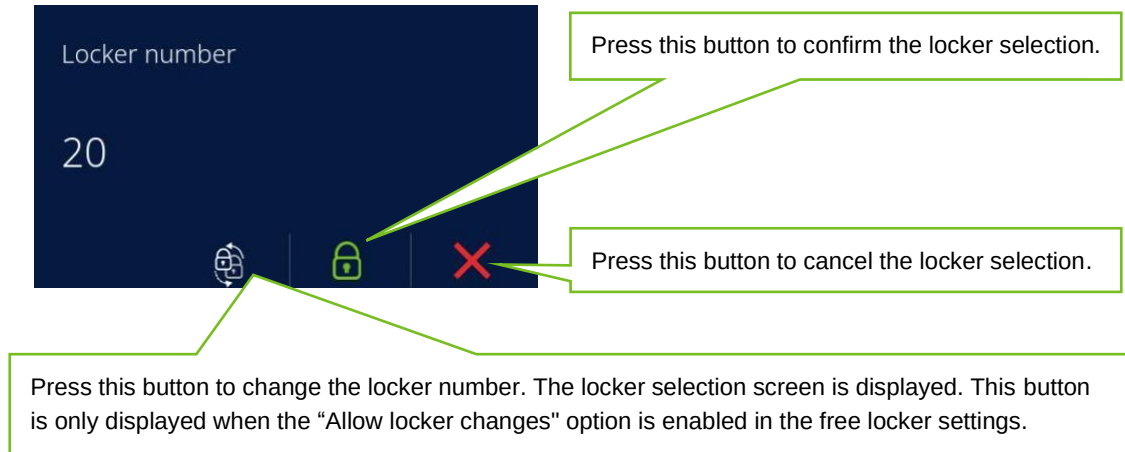


To select a locker number, use the arrow keys to scroll through the available lockers and then press the number to confirm.

Press this button to cancel the locker selection.

This button is only displayed when the “Enable selection by number” option is enabled in the free locker settings. To search for a specific locker, press this button and enter the desired locker number using the keypad. An error message is displayed if the locker does not exist or is unavailable.

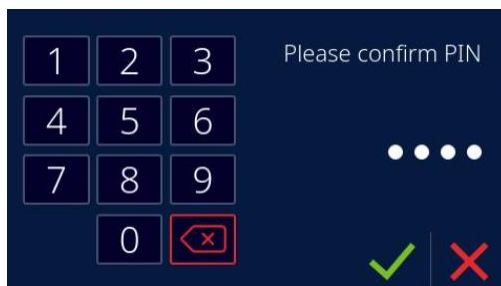
- If the “Number of locker suggestions” option is set to 1: The number of the next unoccupied locker is automatically displayed. In addition, this screen is only displayed when the “Confirmation of selection” option is enabled.



- ▶ The PIN entry screen is displayed. Enter your PIN.



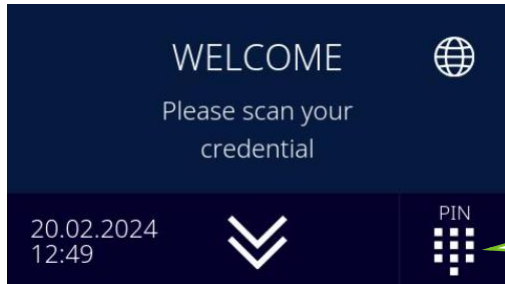
- If the “Duplicate PIN-entry” setting is enabled: The PIN confirmation screen is displayed.



- ▶ Re-enter your PIN and press the green tick button to confirm.

i After selecting a locker using a PIN code, the closing process begins. The process is analogous to that described in chapter “5.4.3 Locking a locker”.

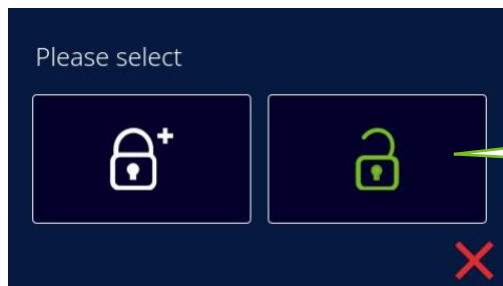
5.5.2 Unlocking and opening a locker with PIN



The keypad symbol allows you to select and open a locker by entering a PIN. This function is enabled by selecting the "Allow PIN usage in Free Locker mode" option in the "PIN code" settings.

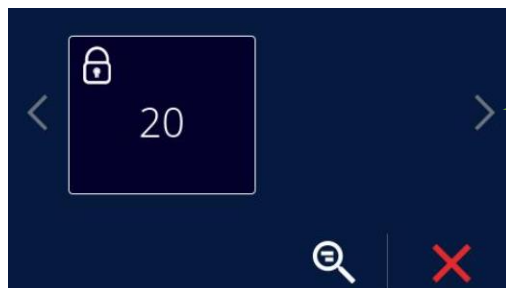
► Press the keypad button.

- The "new locker / open locker" screen is displayed.



Press this button to open a locker that was previously locked.

- The locker selection screen is displayed.



Use the arrow keys to scroll through the available lockers and then press the number to confirm.

- The PIN entry screen is displayed.



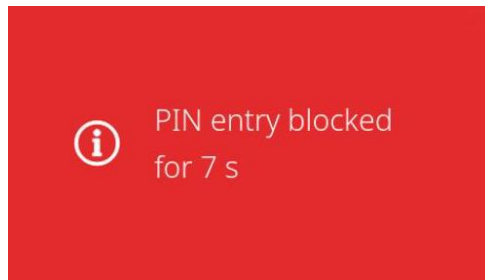
► Enter your PIN and press the green tick button to confirm.

- The following screens are only displayed if ...

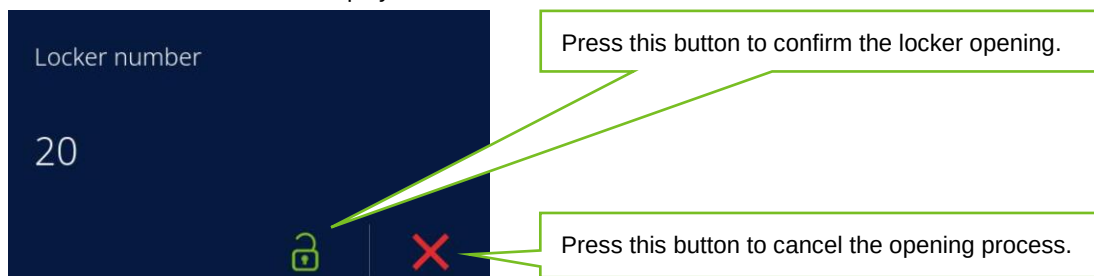
... the PIN is entered incorrectly:



... the max. number of incorrect PIN entries is reached:



- The following confirmation screen is only displayed if the “Opening confirmation” option is enabled. Otherwise, this screen is not displayed.

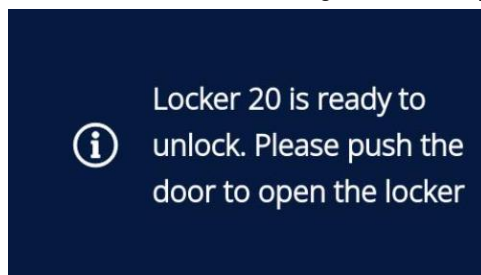


- If the “Lead time before opening” is set to 0: The locker opens immediately.
- If the “Lead time before opening” is set to >0: The countdown screen is displayed.



► The locker is unlocked.

- If the “Push to Open - Free Locker” option in the “Sub Controller” settings is not enabled: The locker door springs open.
- If the “Push to Open - Free Locker” option in the “Sub Controller” settings is enabled: The locker door remains closed after unlocking and can be opened by pushing it in briefly.



Lockers locked by PIN are released immediately after unlocking. For the user to keep using the same locker, they must select it and define the PIN again at the GT7 Central Locker.

5.6 Dynamic locker

The settings that are configured for the lockers determine how they operate as well as the locker selection/closing/opening process at the GT7 Central Locker. Please refer to chapter “4.8.4 Dynamic Locker” for an understanding of the available settings.

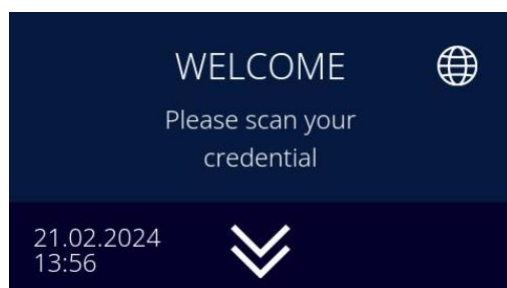
NOTE! Dynamic locker mode is currently only possible for lockers with a GAT NET.Lock 7020 lock.

Whether the user can select and lock a locker at the locker door depends on the “Allow authentication at the door” setting (see “5.2 Operation of the lockers”).

- If “Selection, Open & Lock” is enabled for this setting, all locker actions can be completed directly at the locker as well as at the terminal. The procedure for selecting and locking a locker is as follows:
 - ▶ Select any unoccupied dynamic locker as indicated by a green LED.
 - ▶ Read the user data carrier at the locker door.
 - The locker door opens.
 - ▶ Put your belongings inside and close the locker door.
 - The locker is locked and assigned to the user’s data carrier. The locker can only be locked and unlocked by this data carrier until the assignment is released (see “5.6.3 Releasing a locker”). After releasing the locker, it acts as a free locker again and can be selected by another user.
- If “Open & Lock” is enabled for the “Allow authentication at the door” setting, the user must first select a dynamic locker at the GT7 Central Locker. Once the dynamic locker has been locked and assigned to the data carrier, all subsequent locking and unlocking actions can be completed at the locker.
- If “Nothing” is enabled for the “Allow authentication at the door” setting, all locker actions (selection, locking, unlocking) must be carried out at the GT7 Central Locker.

i Operation at the locker is only possible if the PIN verification function for data carriers is disabled (see chapter “5.8 PIN verification for data carriers”).

5.6.1 Selecting and locking a locker

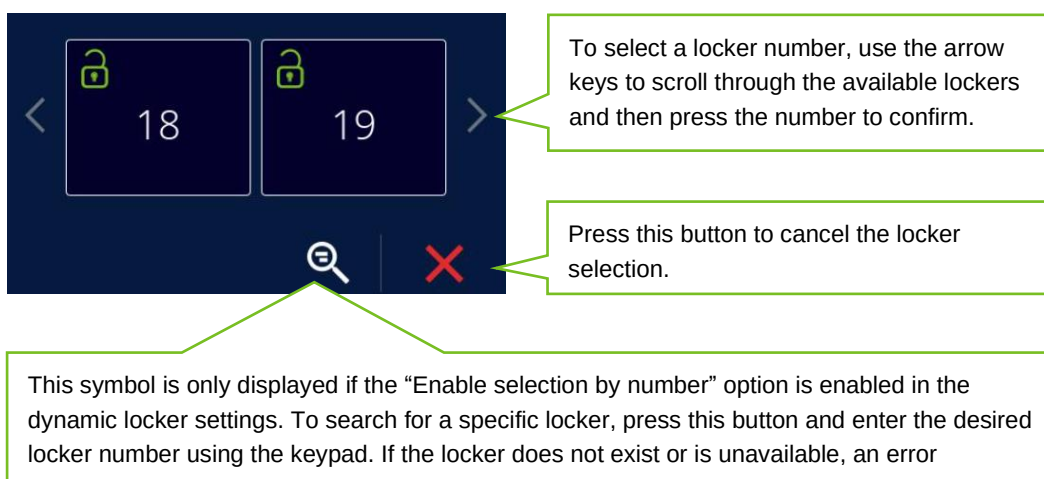


- ▶ Scan your credential. Three options are available:
 1. No lockers are available: A notification is shown and the display changes back to the idle state.

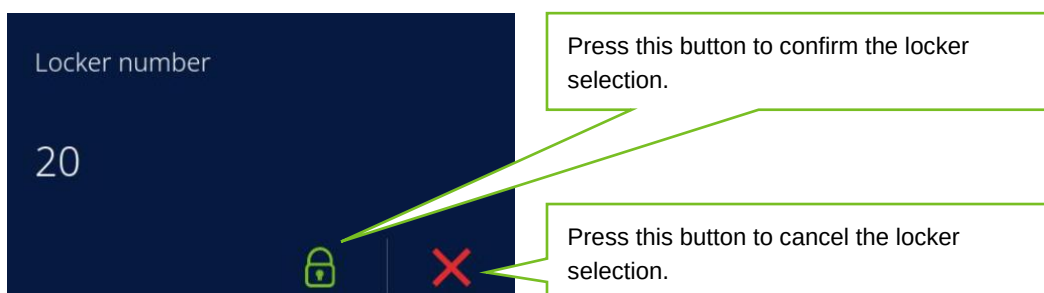
2. If there are free lockers in the system in addition to dynamic lockers: A query is first displayed asking which locker type to use. In this case, select "Dynamic locker".



3. If the "Number of locker suggestions" option is set to >1: You can select any displayed locker. The number of lockers that are displayed for selection is defined in the dynamic locker settings.



4. If the "Number of locker suggestions" option is set to 1: The number of the next locker is automatically displayed. In addition, this screen is only displayed if the "Confirmation of selection" option is enabled. Otherwise, the closing process starts directly without this display.



► After selecting a locker, the closing process starts.

- If the "Lead time before locking" option is set to 0: The locker door is locked immediately.
- If the "Lead time before locking" option is set to >0: The following countdown screen is displayed and the locker door is locked after this time has elapsed.

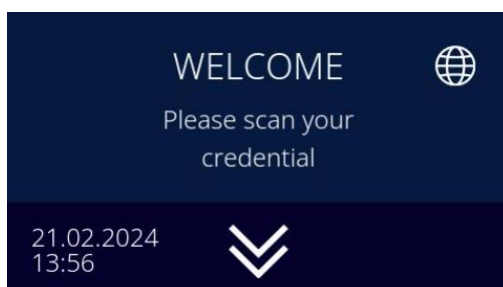


- The following screen indicates that the locker can now be closed to lock. Push the locker door shut.

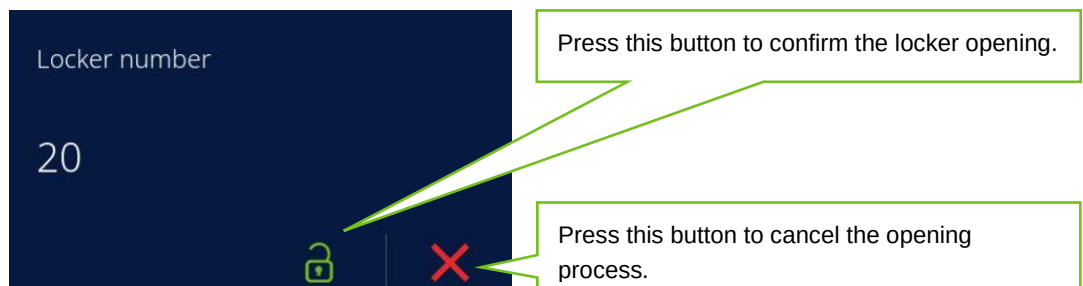


- The locker is assigned to your data carrier and can now only be unlocked and locked by this data carrier.

5.6.2 Unlocking and opening a locker



- Scan your credential.
 - If the "Opening confirmation" option is not enabled: The locker opening process starts immediately.
 - If the "Opening confirmation" option is enabled: The following confirmation screen is displayed.



- If the "Lead time before opening" is set to 0: The locker opens immediately.

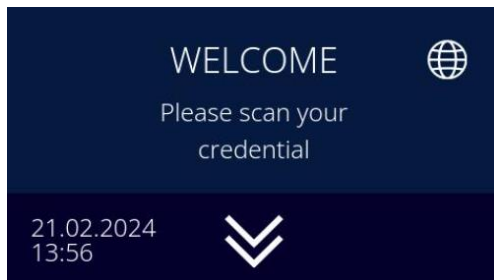
- If the “Lead time before opening” is set to >0: The countdown screen is displayed.



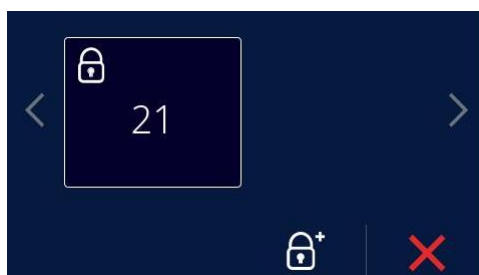
- ▶ Wait for the countdown time after which the locker will open.

5.6.3 Releasing a locker

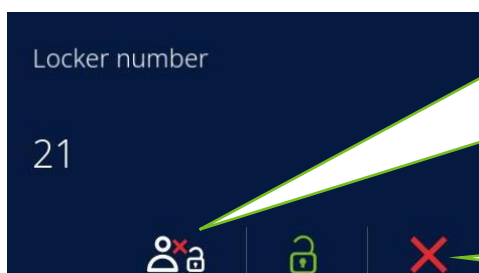
NOTE! Before releasing a locker, make sure that you have removed your personal belongings from the locker.



- ▶ Scan your credential at the terminal.
 - The locker currently in use is displayed. If several lockers are in use, select the desired one.



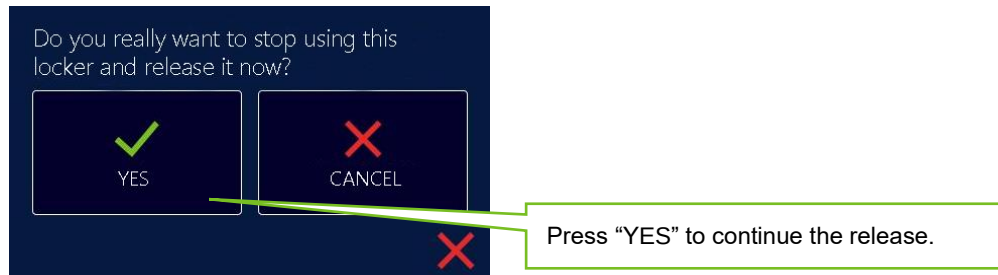
- ▶ Select the locker to be opened (here “21”).
 - The following window is displayed.



The release function allows you to delete the assignment of a locker to your data carrier. The locker then operates like a free locker again. This function is activated via the “Release dynamic lockers” option in the Dynamic Locker settings. If this option is disabled, a locker can only be released via the “Authorizations” in Relaxx.

Press this button to cancel the release process.

- The screen for confirming the release is displayed.



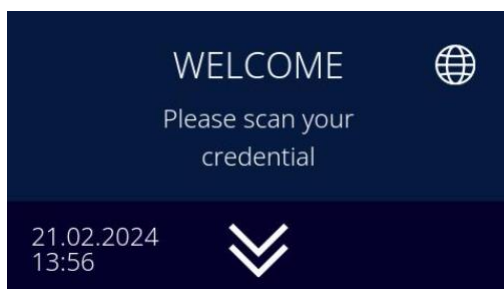
- The locker is released and can now be used by other users. The LED on the locker door turns green to indicate its unoccupied status.

5.7 Personal locker

The configuration settings for the personal lockers determine how the personal lockers operate as well as the type of locker selection and the process for locking / unlocking a locker at the GT7 Central Locker. Refer to chapter "4.8.3 Personal Locker" for more information on the available settings.

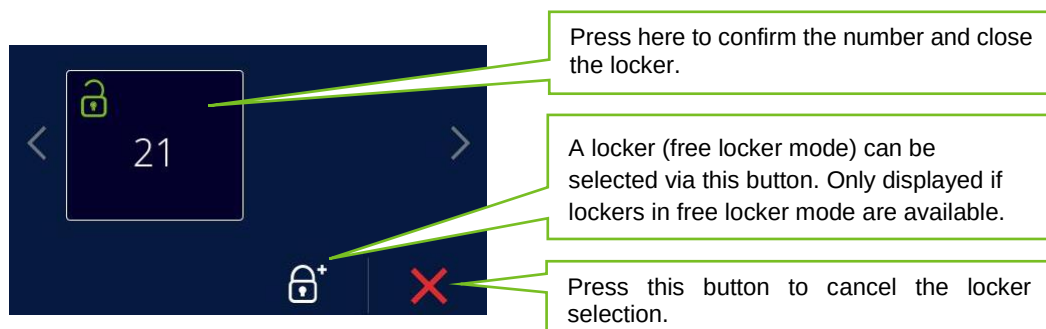
5.7.1 Selecting and locking a locker

a) Procedure when "Auto lock personal/dynamic locker" is not enabled in the "Sub Controller" settings



► Scan your credential. Two options are available:

1. No personal lockers are assigned to the data carrier: A "No authorization found" message is displayed and the display returns to the idle screen.
2. If the "Locking confirmation" option is enabled: The locker number assigned to you is displayed.



► If "Lead time before locking" is set to >0: A countdown displays the configured time that you have to go to the locker and put your belongings inside. The locker can only be locked after this time has expired.



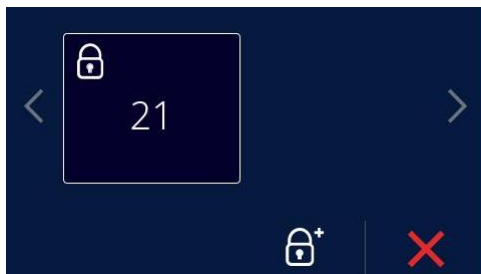
- The following display indicates that the locker can now be closed to lock:



- Push the locker door shut.
 - You have the time defined in the “Locking timeout” setting (see “4.7.15 Sub controller”) to close the locker. After this the locker locks automatically and is assigned to your data carrier.
 - The display changes back to the idle state after 5 seconds, but the time for closing the locker continues counting down. If the locker is closed after the time has expired, the locker door springs open again. To lock the locker, re-identification is required.

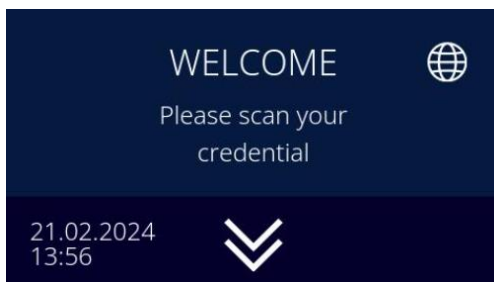
b) Procedure if “Personal Locker - close automatically” is enabled in the “Sub Controller” settings

In this case, the personal locker can be closed and locked simply by pushing the door shut. Identification via data carrier is not necessary. If you still read your data carrier at the GT7 Central Locker nevertheless, the following display is shown:



- Displayed here is which locker is locked (no. 21 in the example). It can be opened by pressing on the locker (see next section).

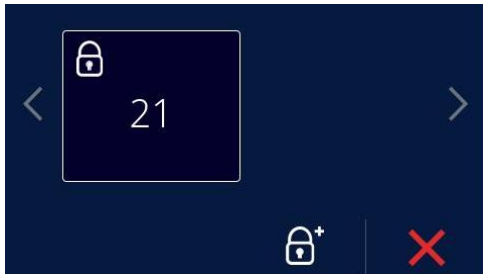
5.7.2 Unlocking and opening a locker



- Scan your credential.

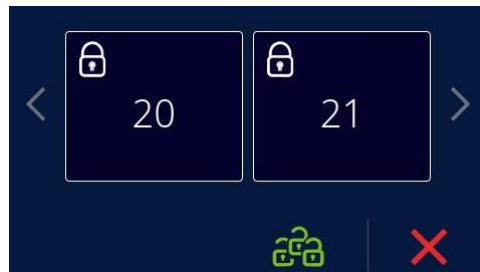
- Display only if “Opening confirmation” setting is enabled:

The data carrier has one locker assigned to it:



The currently occupied locker is displayed. You can select whether to open it now (press locker number) or not (X button). The lock button  at the bottom allows you to select another locker to lock.

The data carrier has multiple lockers assigned to it:



All lockers (and their locker groups) assigned to you are displayed. You can select whether to open one locker (press locker number), open all lockers (press lock button ) or to not open any lockers (X button).

- ▶ If “Lead time before opening” is set to >0: A countdown displays the configured time that you have to go to the locker before it is unlocked. After this time, the locker is unlocked and opens.



- ▶ Wait for the countdown time to expire.
 - Display indicating that the locker has now been unlocked and is open:



5.8 PIN verification for data carriers

The PIN verification function for data carriers can be activated in the configuration of the GT7 Central Locker (see “4.8.5 PIN code”).

i If PIN verification is enabled, identification is only possible at the GT7 Central Locker using a data carrier and PIN. Identification at the lockers directly, which can be configured for each locker mode, is therefore automatically deactivated for all locker modes.

If PIN verification is enabled, the user must enter a personal PIN code at the GT7 Central Locker in addition to identification via data carrier. However, this function can also be deactivated for individual users in the Relaxx software so that the respective user only needs to identify themselves using their data carrier and does not have to enter a PIN code.

NOTE! Min. Relaxx version 7.3 is required for PIN verification.

5.8.1 Selecting or opening the locker

- Scan your credential at the GT7 Central Locker.
 - The following screen is displayed asking you to enter your verification PIN code.



- Enter your PIN code and press the tick symbol.
 - If the PIN code was entered correctly:
The identification process is completed. You can now open your assigned locker or select another locker to use.
 - If the PIN code was not entered correctly:
The PIN code can be entered again. The number of attempts and the waiting time until re-entry is defined in the GT7 Central Locker configuration. These settings are described in chapter “4.8.5 PIN code”.

5.8.2 Changing the PIN code

Each user can renew or change their PIN code for the data carrier verification via PIN code function. This is useful, e.g., if a user's PIN code is no longer considered secure. There are two options for activating the PIN code renewal function.

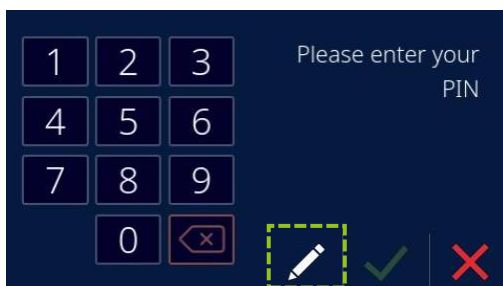
- a) The PIN renewal setting can be enabled for each user in the Relaxx software. The next time the user identifies themselves at the GT7 Central Locker, they are prompted to select a new PIN code after entering the current PIN code. This setting is found in Relaxx in the authorization list or the user authorization settings.

When this function is enabled, the procedure at the GT7 Central Locker is as follows:

- ▶ Scan your credential at the GT7 Central Locker.
 - A prompt to enter the PIN code for PIN verification is displayed.
- ▶ Enter your current PIN code.
 - The prompt to select and enter a new PIN code is displayed.
- ▶ Enter a new PIN code. This entry must be confirmed and both entries must match.

NOTE: The max. and min. length of the PIN code is defined in the device settings.

- If the entry is valid, a corresponding message is displayed and the new PIN code is saved in the GT7 Central Locker and Relaxx.
 - The idle screen on the GT7 Central Locker is displayed again and you must now identify yourself using your data carrier and the new PIN code.
- b) When entering the PIN code, you can press the edit icon to change the PIN code.



The rest of the procedure is as described in section a).

5.9 Master Dashboard

The Master Dashboard gives you a quick overview of the status of the lockers controlled by the GT7 Central Locker. A MASTER data carrier is required to display the Master Dashboard.

i The MASTER data carriers are defined in Relaxx under “Devices” in the software settings. To do this, master card sets are created and the MASTER data carriers are assigned to a set. The MASTER card sets must then be assigned to the GT7 Central Locker. For more information, see the Relaxx Operation Manual.

i As the MASTER data carriers are defined in Relaxx for the controller, but the data carriers are read by the GT7 terminal, care must be taken to ensure that the data carrier settings for the GT7 Central Locker (Device configuration -> Data carrier) match the sub controller settings (Device Configuration -> Sub Controller RFID). For example, if the “Flip unique number” option is enabled for the data carrier technology in the GT7 Central Locker settings and not in the Sub Controller RFID settings, the data carrier will not be correctly recognized as a MASTER data carrier.

- Read a defined MASTER data carrier at the GT7 Central Locker.
 - The Master Dashboard with the locker statistics is displayed.

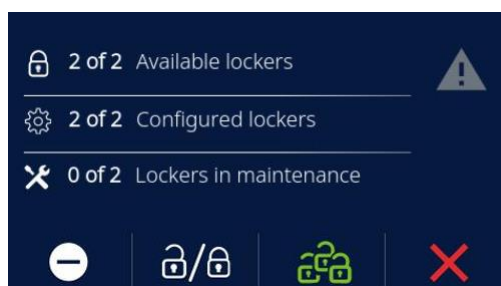


- If one or more alarms are currently active, the warning screen is displayed instead of the locker statistics (see next page) or you can also display this warning screen by pressing the symbol. Press the symbol in the top right-hand corner of the warning screen to switch back to the locker statistics.

At the bottom or on the right-hand side of the screen, icons are displayed that allow you to activate the following functions. These are described on the following pages.



... Locker statistics



The following information is displayed:

- Number of available lockers. In the example, 2 of a total of 2 lockers can be selected for locking.
- Number of configured lockers relative to all connected lockers. Unconfigured lockers cannot be used.
- Number of lockers in maintenance mode. These lockers are currently not usable.



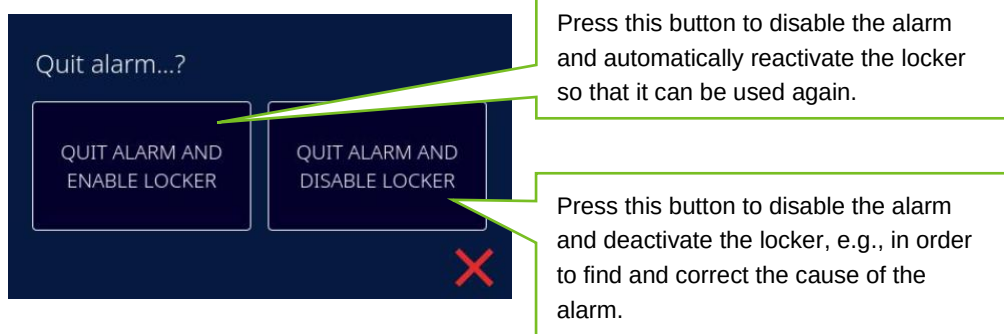
... Warning screen. If there are warnings, this symbol is displayed in yellow. When the symbol is gray, there are no warnings.



- ▶ Press the  symbol to display the warning screen. The following information is displayed:
 - How many lockers are in alarm mode ("Alarms")
 - How many lockers were last opened or locked by a MASTER data carrier ("Modified by master")
 - How many lockers are disabled ("Disabled lockers")
- ▶ Select one of the messages to display a list of affected lockers (see the following pages). The  symbol takes you back to the Master Dashboard.

a) Lockers in alarm mode

- ▶ Go to the locker and remove the cause of the alarm so that it will not be triggered again.
 - The following query is displayed.



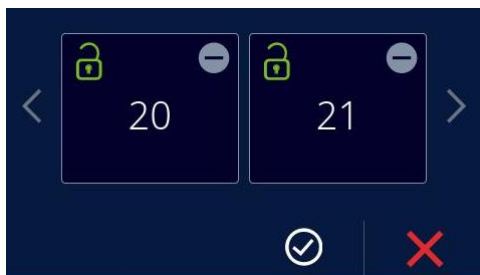
b) Lockers modified by MASTER data carriers

Here you can see how many lockers have been opened or closed with MASTER data carriers.

- ▶ To open/close a locker using MASTER data carriers, click on the lock symbol . See the next page for more information.
- ▶ Enter the number of the locker.

c) Disabled lockers

All disabled lockers are displayed here.



- ▶ Press a locker number to enable it.
- ▶ Alternatively, press the tick symbol  below to reactivate all affected locks.



- ▶ To enable all lockers, confirm by pressing "YES".

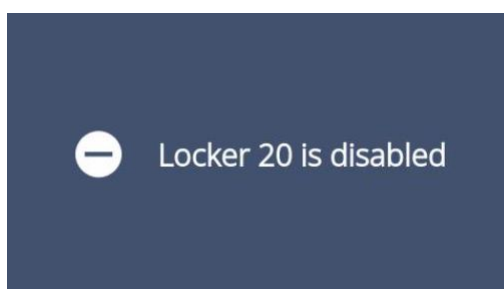


... Disable lockers.

- ▶ Press this symbol to disable a locker.
- ▶ Enter the desired locker number and confirm via the tick symbol.



- The following display indicates a successful deactivation.

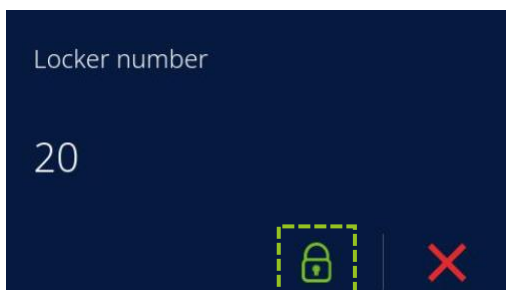


... Open/close lockers.

- ▶ Enter the desired locker number and confirm via the tick symbol.



- ▶ Now select either the close or open symbol.



- The selected locker is opened or released for closing.
- The lockers controlled in this way are displayed in the list of lockers that have been locked or unlocked using a MASTER data carrier (on the warning screen).

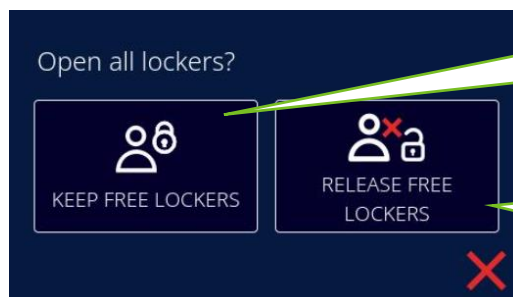
- If a free locker, which was assigned to a user's data carrier, is opened with a MASTER data carrier, it remains assigned to the data carrier for the set "Locker closing time" and can be closed again within this time by closing the locker door. If the locker is not closed within this time, the assignment to the user data carrier is removed and the locker is available for selection again for all users.
- Personal lockers do not lose their allocation if they are opened with MASTER data carrier.
- Lockers that have been explicitly closed with a MASTER data carrier are no longer available as a free locker.



... Open all lockers.

- ▶ Press this symbol to unlock and open all lockers.

- The following screen is displayed.



If you want to open all lockers and keep them assigned to the user(s) who closed them, select this option.

If you want to open all lockers and release them for new user(s) to use, select this option.

- All lockers are opened. Deactivated lockers remain closed.

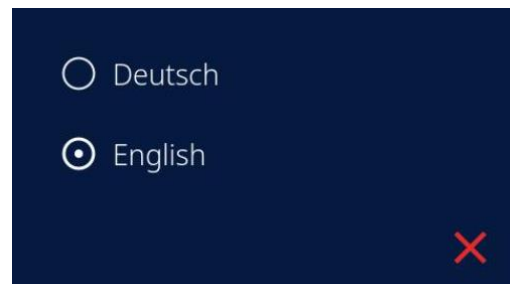
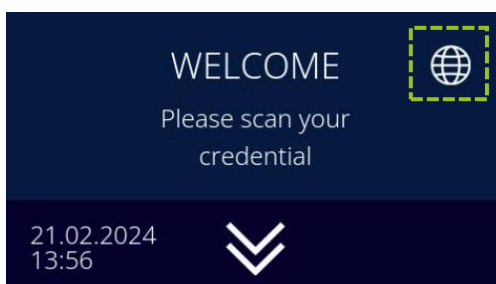


... Exit Master Dashboard.

- ▶ Press this button to return to the idle screen of the GT7 Central Locker.

5.10 Language

- ▶ To change the language on the GT7 Central Locker, press the language symbol in the top right corner.



- The language selection screen opens, and all the defined languages are displayed. Other languages can be defined in the configuration of the GT7 Central Locker (see "4.8.6 Display texts").
- ▶ Either select the desired language or close the screen via the "X" button.
 - The idle screen is displayed again.

5.11 Operation with Relaxx Management Software

To configure, operate, and monitor the locker system, GANTNER offers the PC software Relaxx. The GT7 Central Locker as well as the sub controllers connect to this software and the locks are displayed graphically. The communication between the GT7 Central Locker devices and the controllers in the system thereby operates over the Relaxx Windows service.

The lockers connected to the GT7 Central Locker via the sub controllers can be directly controlled from the graphical user interface of the software, e.g., to open or disable lockers. A free locker that is opened via Relaxx immediately loses the assignment to the data carrier with which it was locked. This also applies to the “Open locker group” function.

The users' data carriers are also configured in the Relaxx software and their validity set.

NOTE! A separate user manual is available for the software Relaxx in which the functions of the software are described in detail.

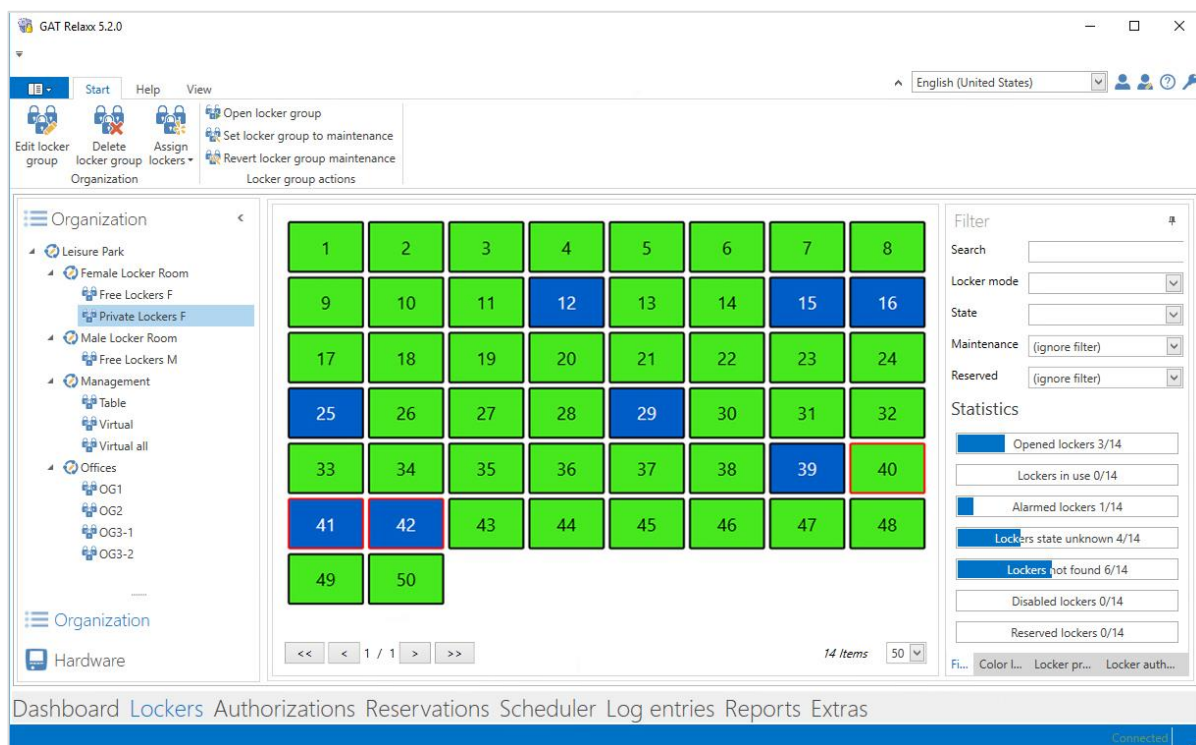


Figure 5.1 – Relaxx – Organization overview

5.12 Maintenance cards

Maintenance cards can be created in Relaxx that allow the lockers assigned to the maintenance group to be opened at the GT7 Central Locker. The following settings in Relaxx determine the operation of the maintenance cards.

GAT Relaxx 5.4.0

Start Help

Authorizations Authorization groups Access authorizations

+ New authorization group
Delete authorization gr.

Groups

Maintenance

Name Maintenance

Group type Maintenance

Allow open

- ☒ Allow the maintenance group to open lockers
- ☒ Allow the maintenance group to open only lockers in maintenance

Clear maintenance

☐ On open ☒ On close

Valid from 00:00:00

Valid until 23:59:59

Disabled ☐

Figure 5.2 – Creating a maintenance group in Relaxx

Allow the maintenance group to open lockers

Enable this setting to allow all maintenance data carriers in the group to open all lockers in addition to being able to lock them (regardless of operating mode). If the setting is not enabled, the maintenance data carriers can only lock open lockers in the group.

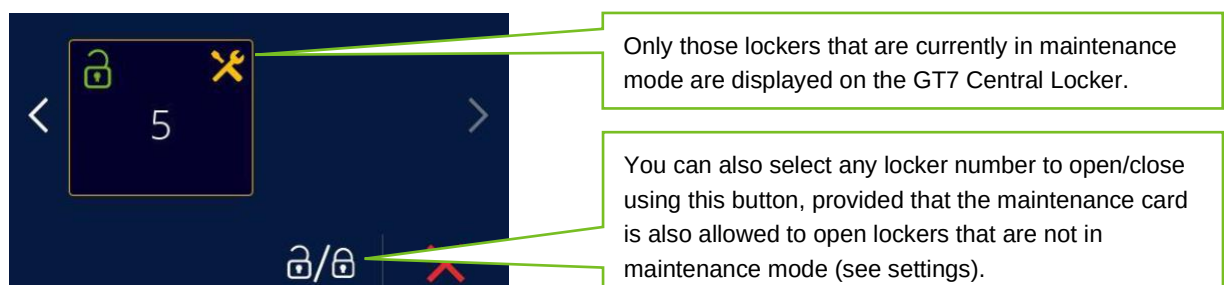
Allow the maintenance group to open only lockers in maintenance

Enable this setting to allow all maintenance data carriers in the group to open all lockers assigned to the group that are in maintenance mode. Lockers operating in other modes cannot be opened.

Clear maintenance

Define when to reset lockers in maintenance mode to their default operating mode using a maintenance data carrier. This can occur either when the locker is opened (On open) or closed (On close).

When the maintenance card is read by the GT7 Central Locker, Relaxx sends the GT7 Central Locker a list of all lockers that the maintenance card is allowed to open (depending on the configuration).



Further information on configuring authorization groups is provided in the Relaxx operation manual.

6 TECHNICAL DATA

6.1 GT7 with G7 Central Locker App

Nominal voltage

- Power supply: DC 24 V (LPS/SELV)
- PoE: PoE conf. to IEEE 802.3af, performance class 0

Permitted voltage range

- Power supply: DC 10 - 26 V (LPS/SELV)
- PoE: DC 36 - 57 V

Input current

- Power supply: 900 mA
- PoE: 300 mA

Nominal power consumption: 10 W

Output current

- Vout 24V: max. 300 mA
- Vout 5V: max. 300 mA

Data storage: Flash memory for configuration and booking data, screensaver, and advertisement pictures.

Internal clock: Time saved 1 hour

Reader type

- GT7.x300: LEGIC advant and Proxy (125 kHz) reader
- GT7.x500: MIFARE Classic (1k and 4k), Ultralight®, DESFire EV1® and EV2®
ISO 15693
GANTNER.Connect
- GT7.x700: LEGIC advant, Proxy (125 kHz), and HID iCLASS® reader

Reading field frequency

- RFID: 13.56 MHz
- Wireless interface: 2.4 GHz
- Proxy: 125 kHz (GT7.x300 and GT7.x700 only)

Max. transmission power

- RFID: 500 mW
- Wireless interface: 3.7 dBm (2.344 mW)
- Proxy: 200 mW

Reading range: 2 - 8 cm (depending on the data carrier)

Display elements/signaling

- Display: 4.3" color display with capacitive touchscreen, 16.7 million colors, resolution 480 x 272 px, visible area 95.04 x 53.86 mm
- RFID reader: LED ring, multi-color
- Acoustic signaling: Speaker

Signal input

- 1 x optocoupler input (potential-free, function configurable)
Input voltage: DC 0 to 30 V ($U_{Low} < 2 \text{ V}$, $U_{High} > 6 \text{ V}$)
- Wiegand (DATA, CLK): 2 x input, with potential, function configurable
Input voltage: open or GND (e.g., push button connected to GND)

Signal output

- 2 x relays
- Type: NO contact, function/timing configurable
- Switching voltage DC: max. 30 V (SELV)
- Switching voltage AC: max. 15 V (SELV)
- Continuous current: max. 1.8 A
- Switching capacity: max. 54 W, 27 VA

Host interface

- Ethernet: 10/100 Mbps, IPv4
- WLAN: IEEE 802.11b/g/n

Reader interfaces:

RS-232 (barcode)
RS-485 (GANTNER expansion bus)
Wiegand

Connection:

Screw terminals, 0.5 - 1.5 mm

Software integration:

JSON interface
Generation 6 compatibility adapter (limited functions)

Housing

- Front/rear part: Plastic PC black gray
- Reader cover: Plastic PC In-mold technology
- Display: Hardened glass

Weight:

370 g (13 oz)

Permitted ambient temperature:

-10 to +50 °C (+14 to +122 °F)

Storage temperature:

-25 to +70 °C (-13 to +158 °F)

Protection type:

IP 54 (installed state)

Protection class:

III (Safety Extra-Low Voltage)

Environment class (VdS 2110):

III (outdoor conditions, weather protected)

Compliances

- GT7.x300: CE
- GT7.x500: CE, CB, FCC, IC, ETL, EAC
- GT7.x700: CE, FCC, IC

6.2 GT7 dimensions

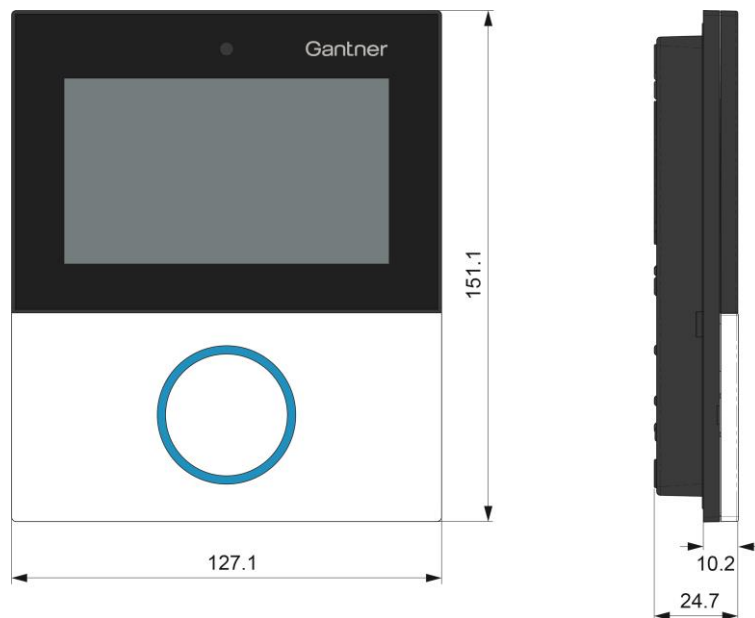


Figure 6.1 – Dimensions

NOTE:

This manual is valid as of March 15, 2024. It is subject to change.
Amendments can be made without prior notice at any time.
Information in this manual applies to version 6.0 of the G7 Central Locker app.



GLOBAL
PARTNER NETWORK



40+
OFFICES



40,000+
PROJECTS WORLDWIDE



40+ MILLION
USERS DAILY

Gantner

A SALTO GROUP COMPANY

www.gantner.com

© 2024 GANTNER ®

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

Photos: GANTNER, shutterstock, IMSinteriors, SALTO Systems

SCAN FOR CONTACT

