gantner

INSPIRED ACCESS

MANUAL

GT7.2x00 / GT7.3x00 / GT7.3x01

Document Version 1.6

SALTO WECOSYSTEM

Copyright © 2024 Gantner

© Copyright 2025 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

For all inquiries concerning this product, please contact your local sales partner or one of the Gantner branch offices directly. The contact details are available via the following link: https://www.gantner.com/locations

Contact address of manufacturer

Gantner Electronic GmbH

Bundesstraße 12

6714 Nüziders, Austria

Dear Customer,
Our aim is to ensure that our product operates with safety and to your complete satisfaction. To achieve this aim, please take this opportunity to familiarize yourself with the following guidelines.

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

Notation of safety information and safety symbols

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

1. Safety messages for personal injury

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

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

Format of safety messages that apply to an entire section:

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

⚠CAUTION

Electrical shock

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

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

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

2. Property damage messages

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

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

NOTICE

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

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

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

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

3. Definition of the signal words

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

4. Definition of the safety symbols

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

⚠ Important Safety Information ⚠

- The installation, commissioning, and servicing of our products must be performed only by suitably trained personnel. Electrical connections may 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 especially applies 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 due to 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 manufactured 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 via the following link:
https://www.gantner.com/en/qr_CVSiwMPv40

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.

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.

FCC INFORMATION (U.S.A.)

Note:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 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.

INDUSTRY CANADA INFORMATION

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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.

ICES Statement (Canada)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Software License Information

Free software remark

This product contains free software and open-source software. Information about the software used and the corresponding licenses can be found on the integrated web interface of the device.

WARRANTY DISCLAIMER

The open-source software contained in this product is distributed in the hope that it will be useful to you, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the corresponding License texts for more details.

WRITTEN OFFER

The software contained in this device contains copyrighted software whose license requires source code disclosure. A copy of this license is included in the integrated web interface of the device. You can receive the appropriate source code from us for a period of three years after the last delivery of the device at a cost of 25 euros (our internal handling and shipping costs).

Please send the device article number, serial number, firmware revision, and your contact details (name, address, city, state, and email address) to the following address:

Software License Compliance
c/o OSS Service Department
Gantner Electronic GmbH
Bundesstraße 12
6714 Nüziders
Austria
This offer is valid to anyone in receipt of this information.

CONTENTS

1 INTRODUCTION 13
1.1 About this manual 13
1.2 Target groups 13
1.3 Contact & inquiries 13
1.4 Formatting 14
1.4.1 Safety-critical information 14
1.4.1 General information 14
1.4.2 Instructions and results 14
1.5 Terminology 14
2 GENERAL INFORMATION 17
2.1 Intended use 17
2.2 Functional description 17
2.3 System overview 18
2.4 GT7 variants 18
2.5 Device features and dimensions 19
2.6 Communication ports 19
2.7 Ordering guide 20
3 INSTALLATION 21
3.1 Target group 21
3.2 Installation guidelines 21
3.3 Installing the rear part 22
3.4 Attaching the front part 24
3.5 Opening the housing 26
4 ELECTRICAL CONNECTIONS 27
4.1 Target group 27
4.2 Network connection (LAN / Ethernet) 27
4.3 Power supply connection 28
4.4 Digital inputs and outputs 30
4.5 Sub controller connection GAT SMART.Controller S 7020 / GAT NET.Controller S 7020 31
4.6 USB barcode interface connection 33
5 CONFIGURATION 35

5.1 Target group 35
5.2 Requirements for use 35
5.3 Configuration options of the GT7 terminal 35
5.4 Configuration via the GT7 terminal 36
5.4.1 Device info 37
5.4.2 Installed apps 40
5.4.3 Device configuration 40
5.4.4 Start active app / Reboot device 43
5.5 Configuration via G7 Connect (GANTER Cloud) 44
5.6 Configuration via Web Interface 45
5.6.1 Overview 47
5.6.2 Network 48
5.6.3 G7 Connect 51
5.6.4 External webserver 52
5.6.5 Web proxy 53
5.6.6 WLAN 54
5.6.7 Security and user 55
5.6.8 SCEP (Simple Certificate Enrollment Protocol) 56
5.6.9 Time 58
5.6.10 Display 59
5.6.11 Data carrier 60
5.6.12 Device 61
5.6.13 Fingerprint 63
5.6.14 Barcode interface 64
5.6.15 Sub controller 65
5.6.16 Sub controller RFID 68
5.6.17 Camera 71
5.6.18 App configuration 72
5.6.19 Installed apps 73
5.6.20 Cloud pairing 75
5.6.21 Licensing and coding points 78
5.6.22 Certificate management 80
5.6.23 Device maintenance 83
5.6.24 Update firmware 85
5.6.25 Addon bus (external devices) 86
5.6.26 Log viewer 87
5.6.27 Device state 88
5.6.28 Legal information 89
5.7 Authorizing the GT7 terminal 90
5.8 Integration in eLoxx Relaxx 91
6 MAINTENANCE 93
6.1 Target group 93
6.2 Cleaning 93

7 TECHNICAL DATA 95
7.1 Power supply 95
7.2 Reading field 95
7.3 Inputs & outputs 96
7.4 Memory and time management 96
7.5 User guidance 96
7.6 Interfaces 96
7.7 Housing 97
7.8 Environmental conditions 97

1 INTRODUCTION

1.1 About this manual

This manual contains a detailed description of how to install and complete the electrical connections of the GT7.2x00 and GT7.3x00 terminals. The different options for configuring the terminals as well as the technical data are also provided herein.

As the configuration of the GT7.3x01 (installation variant with different housing) is identical, this manual is also valid in large parts for this variant. However, the assembly and ordering instructions for this variant are available in a separate document (VB_GT7-3x01-EN+EN).

Henceforth, the term "GT7 terminal" is used to refer to the GT7.2x00, GT7.3x00, and GT7.3x01 terminals collectively. If information is applicable to a particular terminal type, this will be noted.

The configuration and operation of the various apps available for the GT7 terminal, which determine the functionality, are described in separate manuals. In these manuals, you will find further information on the respective app.
The installation and operation of other GT7 terminal variants and the various installation accessories (e.g., mounting brackets) are also described in separate documentation.

1.2 Target groups

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

Information for the following target groups is available in this manual:
> Installation technicians / locker manufacturers (installation, commissioning)
> Service technicians (service and maintenance)

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.

1.3 Contact & inquiries

For all inquiries concerning the GT7 terminal, 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/EN/locations

1.4 Formatting

1.4.1 Safety-critical information

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

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

1.4.1 General information

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

The text accompanying this symbol contains interesting information relevant to the current chapter. It will help you better understand the information in this section or provide tips for the described device or the operation of the software.

1.4.2 Instructions and results

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

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

1.5 Terminology

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

Computer / PC
These terms refer to all desktop and laptop computers used to configure and maintain the GT7 terminal.

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

GT7 Terminal
This term refers to all variants of the GT7.2xx0, GT7.3xx0, and GT7.3xx1 model ranges, regardless of which app is currently active. Since the configuration of the GT7.3x01 (built-in variant) is identical to the GT7.2x00 and GT7.3x00, this manual is also valid in large parts for this variant. However, the installation and order information for this variant are available in a separate document (VB_GT7-3x01-EN+EN).

G7 App
The name of the software (app) that is activated on the GT7 terminal to provide the desired functionality.

G7 Connect
G7 Connect is Gantner's Cloud service for the configuration and management of projects that contain multiple Gantner devices. G7 Connect is accessible via a web browser following registration and login.

Web interface
The GT7 terminals are equipped with a web-browser accessible interface that allows the device and app settings to be easily viewed and configured.

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

User / Person
In this manual, these terms refer to the end user who is operating the GT7 terminal to complete a function, e.g., accessing a door (G7 Access App) or obtaining information (G7 Info App).

2 GENERAL INFORMATION

2.1 Intended use

The GT7 terminal is a multipurpose device that allows different functions to be implemented through the installation of various apps. Some of the intended uses include:

- The control of turnstiles and doors (G7 Access App and G7 Advanced Access App).
- The display of locker information or visitor information (G7 Info App).
- The timed control of devices such as solariums and spas (G7 Time App).
- The display of a countdown for using time-limited services such as showers and power plates (G7 Countdown App).
- The central reader in a networked locker system (G7 Central Locker App).
- The acquisition and display of personnel time and attendance information (G7 Time & Attendance App).
- An interface for gathering customer feedback (G7 Customer Feedback App).
- The enrollment and writing of fingerprint data onto users' data carriers (G7 Enrollment App).
- The registration of ECO LockPal users (G7 ECO LockPal Registration App).

2.2 Functional description

To activate a function on the GT7 terminal, e.g., to open locked doors, to view information, or to use a time-controlled device, the user must first identify themselves. Identification can be performed in a variety of ways: using data carriers with the RFID reader (Radio Frequency Identification) of the GT7 terminal, via NFC (Near Field Communication), or with a barcode scanner (e.g., GBS7.1x00 barcode scanner).

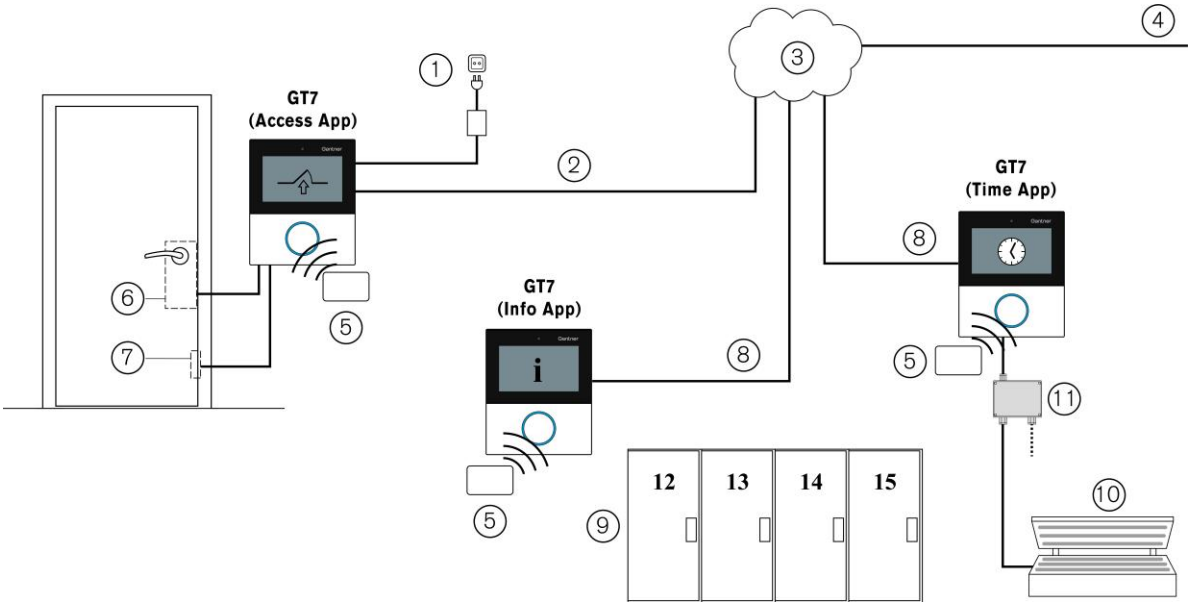
Following identification, further operation, such as the selection and confirmation of functions, is completed directly on the device by touching the display. The ultra-clear touchscreen intuitively guides the user through the clearly structured levels of the app. The wide range of executable apps (see "2.1 Intended use) allow the flexible use of the terminal. Depending on the application, the GT7 terminal can operate as a standalone device or direct authorization decisions on via the network to a locker management software, e.g., eLoxx Relaxx. The communication can occur via Ethernet or Wi-Fi.

The GT7 terminals are suitable for both indoor and protected outdoor use. Every installation requirement is covered with the various terminal models and holders provided to surface mount, flush mount, pole mount, or table mount the GT7 terminal.

The configuration of the terminal can be completed on the device itself with limited settings or the full range of settings are available via a web browser (web interface) or via the Gantner Cloud (G7 Connect). Through the configuration, the functionality of the GT7 terminal can be customized to the respective requirements.

2.3 System overview

The following figure shows the typical application of a GT7 terminal system.



1. Power supply
2. Network cable (Ethernet)
3. Network
4. To server
5. RFID data carrier
6. Electronic lock
7. Door contact
8. Network and supply (PoE)
9. Electronic locker locks (info display of locker no.)
10. Sunbed (time control)
11. Relay box

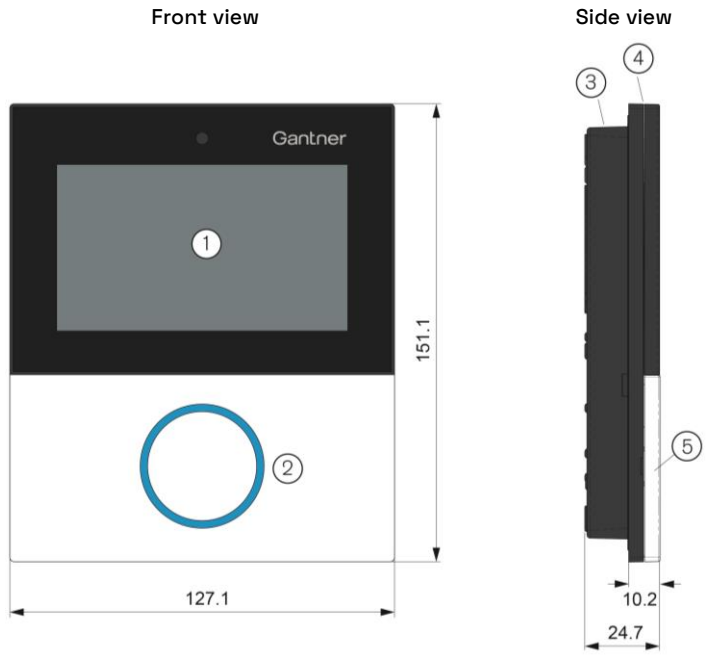
Fig. 2.1 – Typical application of the GT7 terminal

2.4 GT7 variants

The number designation of the GT7 terminals indicates the type of terminal and its functionality. The four numbers in the device name GT7.xxxx indicate the following information.

GT7.Axxx Number of inputs/outputs	**2** = one relay output and one optocoupler input	**3** = two relay outputs, one optocoupler input, WLAN, Wiegand interface (can be used as a status input), RS-232 barcode interface, Gantner extension bus	
GT7.xBxx RFID reader technology	**3** = LEGIC advant and Proxy reader	**5** = MIFARE (ISO 14443) and ISO 15693 reader	**7** = LEGIC advant, Proxy, and HID iCLASS reader
GT7.xxCx Reader type	**0** = RFID reader (no additional reader)	**2** = RFID reader and additional barcode reader	**3** = RFID reader and additional fingerprint reader
GT7.xxxD Housing	**0** = Standard surface-mounted housing	**1** = Flush-mounted variant	

2.5 Device features and dimensions



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

Fig. 2.2 – GT7 terminal (GT7.2x00 / GT7.3x00 shown)

2.6 Communication ports

The following ports are used for communication with the GT7 terminal. The response ports are chosen randomly.

Port type	Port number	Incoming / Outgoing	Function
TCP	80 (http) or 443 (https) (secure connection)	outgoing	For G7 Connect
	80 (http) or 443 (https)	incoming	For the web interface
	80 (ws) or 443 (wss)	incoming	For communication with the host software (if used)
	80 (ws) or 443 (wss)	outgoing	For communication with cloud services from software partners, if used (disabled by default)
	8000	incoming	For communication with the host software if the G6 adapter is enabled (disabled by default)
UDP	123	outgoing	Required for the time (NTP server)
	8216	incoming	For GAT DeviceFinder, so that Gantner devices can be searched for in the network (optional)

2.7 Ordering guide

To plan and order your GT7 terminal system, the document “GT7 Terminal System Ordering Guide” is available to help guide you through the process.

3 INSTALLATION

⚠CAUTION

Electrical shock

Touching current-conducting parts may result in injury due to electrical shock.

- Always disconnect the power supply before working on the device or installation/deinstallation.
- The applicable safety and accident prevention regulations must be observed.
- Do not remove safety protection and covers.

NOTICE

Risk of damage or failure to the GT7 terminal

Incorrect work on the device can damage the GT7 terminal.

- Read the information in this chapter carefully before installing the GT7 terminal.
- Installation and service tasks may only be performed by appropriately trained and certified personnel.
- Carefully observe the measurement diagrams and technical specifications.
- Use the correct tools to install the GT7 terminal.

RF exposure statement

The users must keep at least 20 cm separation distance from the device, except during the identification and operation process at the device (e.g., touchscreen input), which must be performed as described in this manual.

The GT7.2x00 and GT7.3x00 terminals are designed for mounting onto a flat, smooth surface. They can be surface mounted or semi-flush mounted in a wall cutout or, alternatively, the terminals can be semi-flush mounted in a desktop.

The GT7.3x01 is the built-in variant with a different housing. This variant can be installed directly into a cutout or with different mounting frames (GT7m.xxxx). The installation instructions for this variant are provided in a separate document (VB_GT7-3x01--DE+EN).

3.1 Target group

This chapter provides information for technicians responsible for installing the GT7 terminal. Experience in mechanical work and basic electrical knowledge is required. Previous knowledge of the GT7 terminal is not required.

3.2 Installation guidelines

Pay attention to the following points during installation:

> Recommended mounting height: 1.3 m to middle of device display.

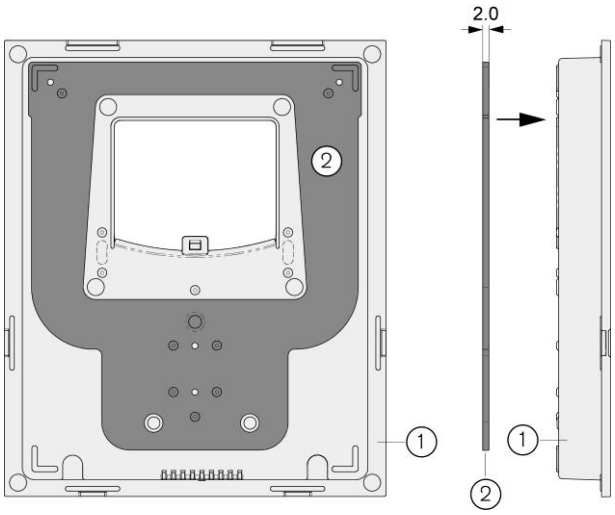
> The GT7 terminal should not be exposed to direct sunlight. Otherwise, limitations in the readability of the display can occur.

> For GT7 terminals installed outdoors, the electrical installation and any empty conduits must be sealed airtight (e.g., with silicone) to prevent condensation in the terminal.

3.3 Installing the rear part

If the GT7 terminal is being installed in an outdoor area or another location that is not protected against dripping water, the wall gasket (2) must be used (see Fig. 3.1). Proceed with the following steps:

- ► Remove the protective foil from the back of the wall gasket.
- ► Attach the wall gasket onto the back of the rear part as shown in Fig. 3.1. Ensure that the gasket sits flat between the domes of the housing.



1 GT7 rear part
2 Wall gasket

Fig. 3.1 – Attaching the wall gasket (measurements in mm)

- ► To mount the rear part, drill the appropriate mounting holes in the wall or desktop. The following three installation options are available:

1. <u>Surface mounting without flush-mounted box (3 holes)</u>

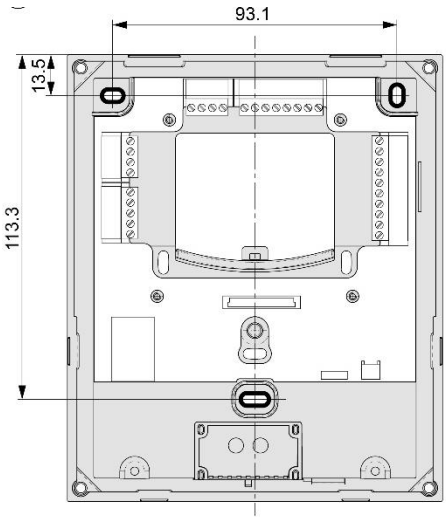


Fig. 3.2 - Surface mounting without flush-mounted box (measurements in mm)

2. Mounting on a standard 60 mm flush-mounted box (3 holes)

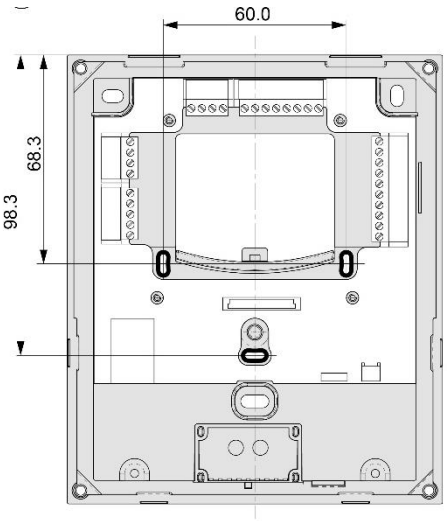


Fig. 3.3 - Installation on standard flush-mounted box (measurements in mm)

3. Semi-flush mounting (approx. 110 x 136 mm cutout and 4 holes)

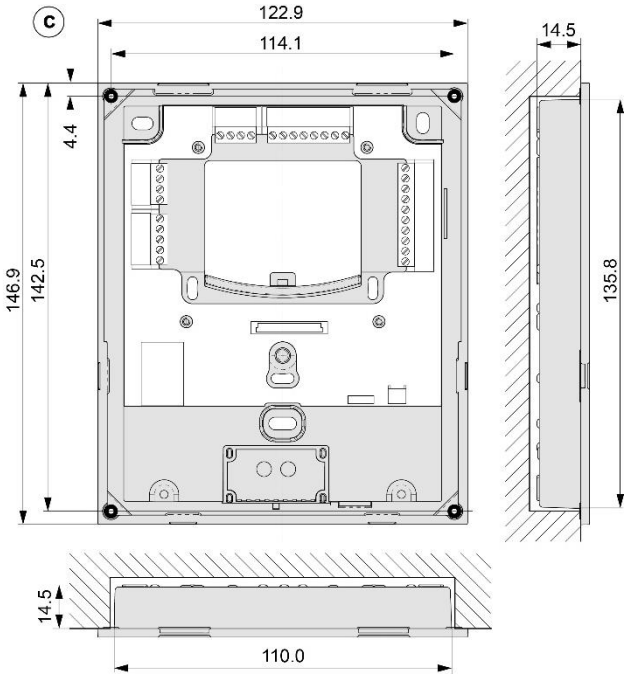


Fig. 3.4 - Semi-flush mounting (measurements in mm)

- Align the rear part with the mounting holes while guiding the connection cables (see "4 ELECTRICAL CONNECTIONS") through the central opening in the rear part.
- Using screws, attach the rear part onto the wall or into the desktop.

3.4 Attaching the front part

This section describes how to complete the installation by attaching the front part and RFID reader cover. Before completing these steps, first connect the connection cables. For more information, see chapter "4 ELECTRICAL CONNECTIONS".

CAUTION! Electrical shock. The electrical connections must be made in a de-energized state.

NOTE! Ensure that the electronics and printed circuit board of the GT7 terminal are not damaged or scratched during assembly.

► Check that the gasket (3), which is inserted in the inner edge of the front part, and the central connector (4) are clean and undamaged.

CAUTION! Do not use liquids for cleaning.

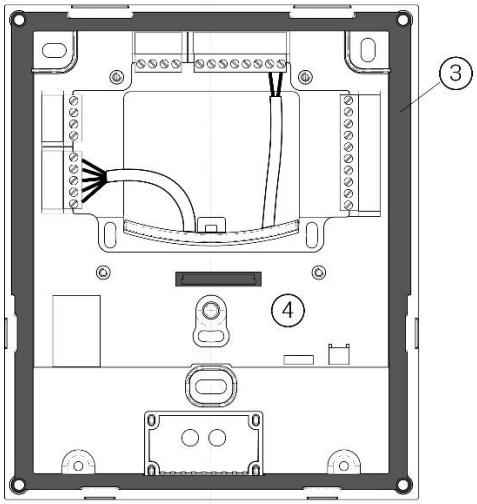


Fig. 3.5 - Gasket and connector

► Hook the two tabs of the front part over the top of the rear part (5).

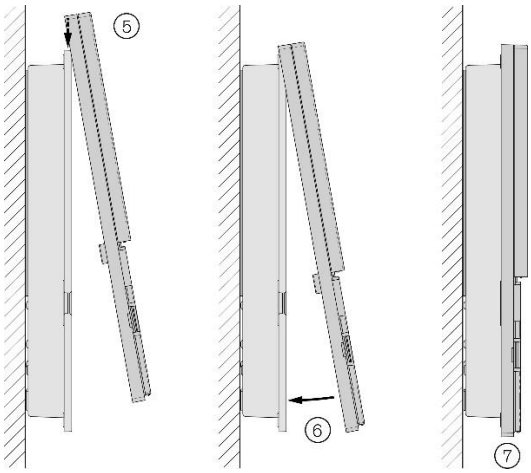


Fig. 3.6 – Attaching the front part to rear part

► Swing the front part forward to meet the rear part (6).

- Gently press the front part onto the rear part until it clicks into the tabs around the edge of the rear part (7). Do not exert excessive pressure. If the front part cannot be attached without great effort, check the tabs and the central connector, and repeat the process.
  NOTE! Through this process, the front part is electrically connected to the rear part via the central connector (4). The front part must sit flush with the rear part and be securely attached.
- Screw the fixing screw (8) into the front part in the location shown below to firmly attach it to the rear part.

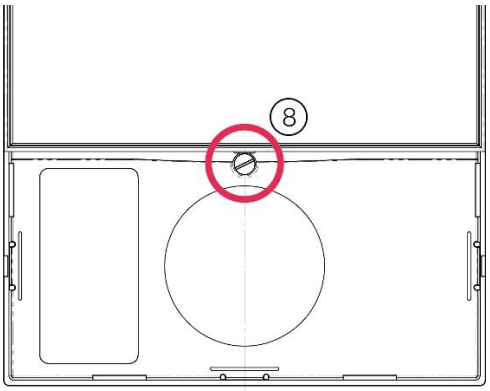


Fig. 3.7 - Fixing screw for top part

- Attach the RFID reader cover (9) to the front part. It locks into place via 3 tabs.
  NOTE! The reader cover must sit flush with the front part and be securely attached.

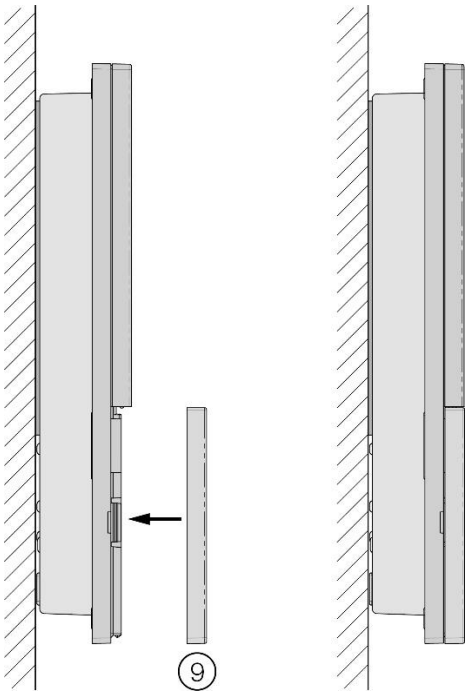


Fig. 3.8 – Attaching the RFID reader cover

- Remove the protective film from the reader cover.

3.5 Opening the housing

Should the housing need to be opened, e.g., for cabling modifications or servicing, proceed as follows:

- Release the RFID reader cover using a flat-blade screwdriver on the 2 side tabs and remove the cover.

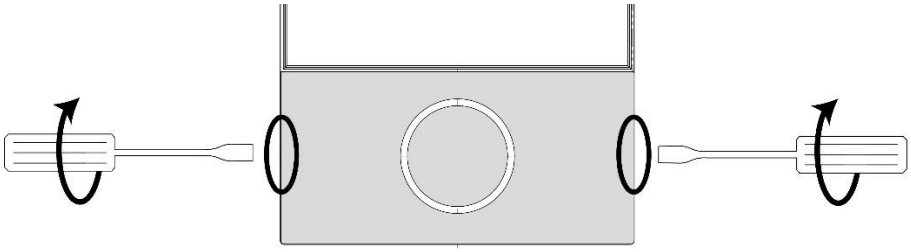


Fig. 3.9 - Opening the housing - Step 1

- Unscrew the fixing screw from the front part.

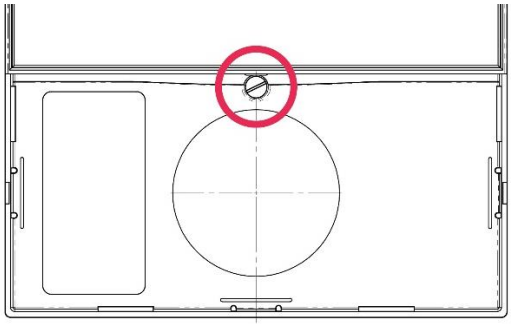


Fig. 3.10 - Opening the housing - Step 2

- On the four slots in the front part as indicated in Fig. 3.11**,** press the edges outwards so that the tabs underneath release, and remove the front part from the rear part.

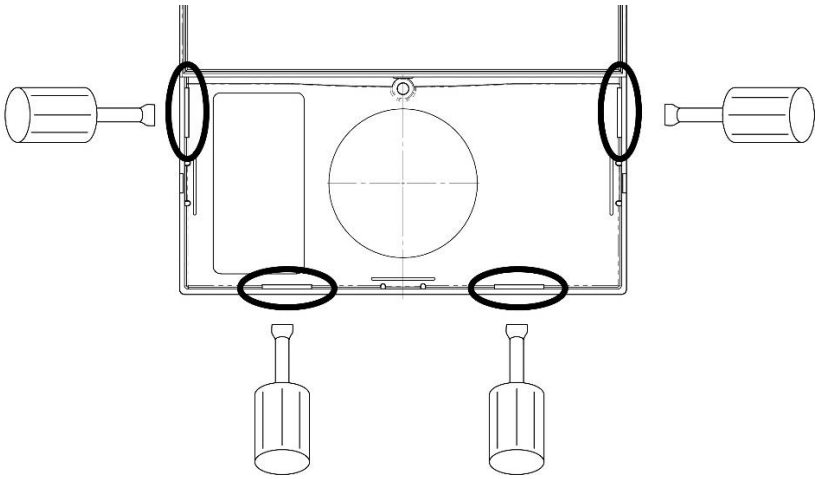


Fig. 3.11 - Opening the housing - Step 3

4 ELECTRICAL CONNECTIONS

⚠CAUTION

Electrical Shock

Touching current-conducting parts may result in injury due to electrical shock.

- Always disconnect the power supply before working on the device or installation/deinstallation.
- The applicable safety and accident prevention regulations must be observed.
- Carefully observe the measurement diagrams and technical specifications.
- Do not remove safety protection and covers.

The GT7 terminal is connected to a network via a LAN interface. This interface is used for configuration and communication during operation. Power can be supplied via a separate power supply or via Power over Ethernet (PoE). The electrical connection described in this chapter is valid for the GT7.2x00, GT7.3x00, and GT7.3x01.

4.1 Target group

This chapter describes the electrical connections required for the GT7 terminal. The information is intended for trained personnel responsible for completing the electrical connections. Previous knowledge of the GT7 terminal or other Gantner devices is not required.

4.2 Network connection (LAN / Ethernet)

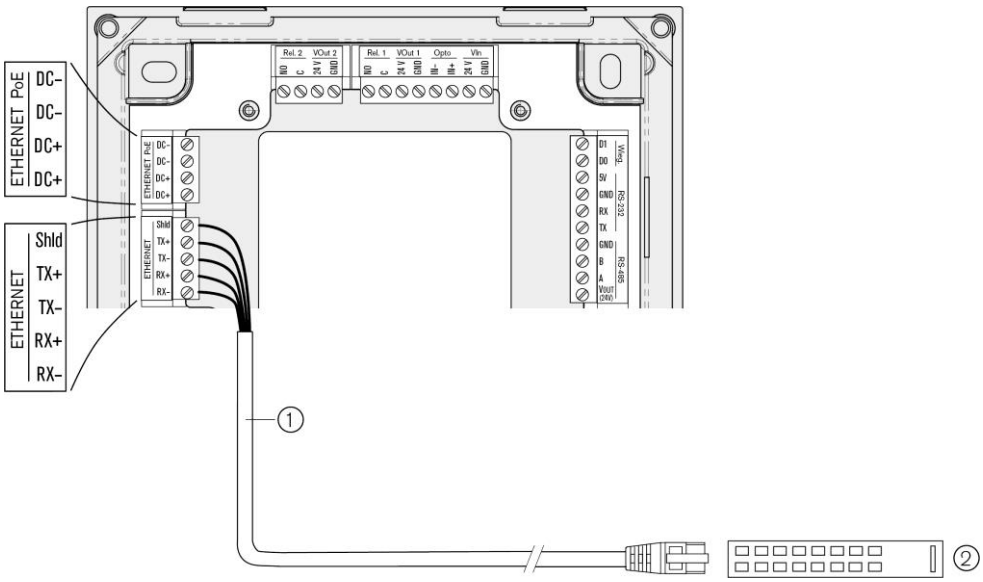


Fig. 4.1 – Connecting the network cable

Recommended cabling / cable lengths for LAN Ethernet

> Shielded and twisted data cable (recommended min. CAT 5 for 100 MBit)
> Supply voltage via 2 wire pairs (PoE)
> Max. cable length = 100 m

- ► Connect the Ethernet cable (1) to a separate port on the network switch (2).
- ► Connect the other end of the Ethernet cable to the ETHERNET RX/TX screw terminals of the GT7 terminal. Depending on the Ethernet standard being used, terminate the wire colors as follows:

Terminal	Signal	Wire Color TIA-568A	Wire Color TIA-568B
TX +	Send signal TX +	green/white	orange/white
TX -	Send signal TX -	green	orange
RX +	Receive signal RX +	orange/white	green/white
RX -	Receive signal RX -	orange	green
Shld	Shield	-	-

Table 4.1 – Wire colors for Ethernet connection

4.3 Power supply connection

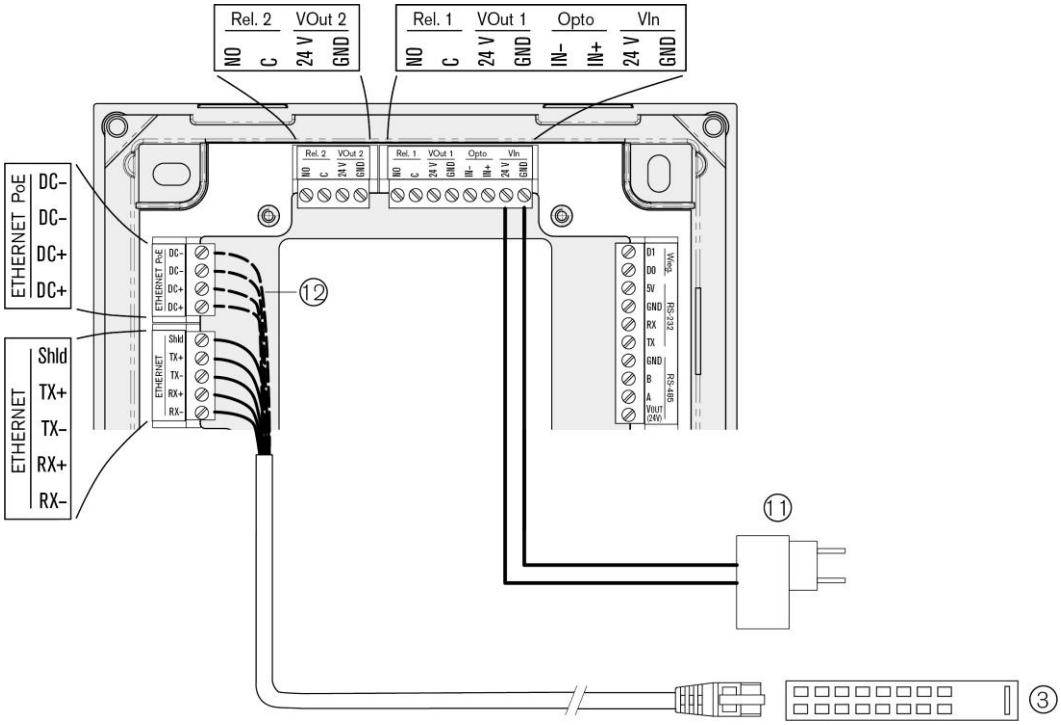


Fig. 4.2 – Connection of the power supply

There are two options for supplying power to the GT7 terminal:

1. See (11) - Via a separate power supply (LPS and SELV - Limited Power Source and Safety Extra-Low Voltage)

- ► Connect the wires of the power supply connection cable to the "Vin" screw terminals as shown in Fig. *4.2*.
- ► Plug the power supply (11) into the power outlet.

2. See (12) - Via Power over Ethernet (PoE)

Consider the following requirements for PoE switches when operating a GT7 terminal with PoE:

- > Must comply with IEEE 802.3af
- > Power class: 0
- > Min. 15.4 W per PoE port
- > Total power budget: min. 15.4 W x number of ports

NOTE! When connecting via PoE, please note that some PoE switches do not transmit the supply voltage on separate wires (DC+ and DC-) but superimpose it on the transmit and receive lines (RX+/- and TX+/-). In this second case, the GT7 terminal is supplied with voltage even if only RX and TX are connected.

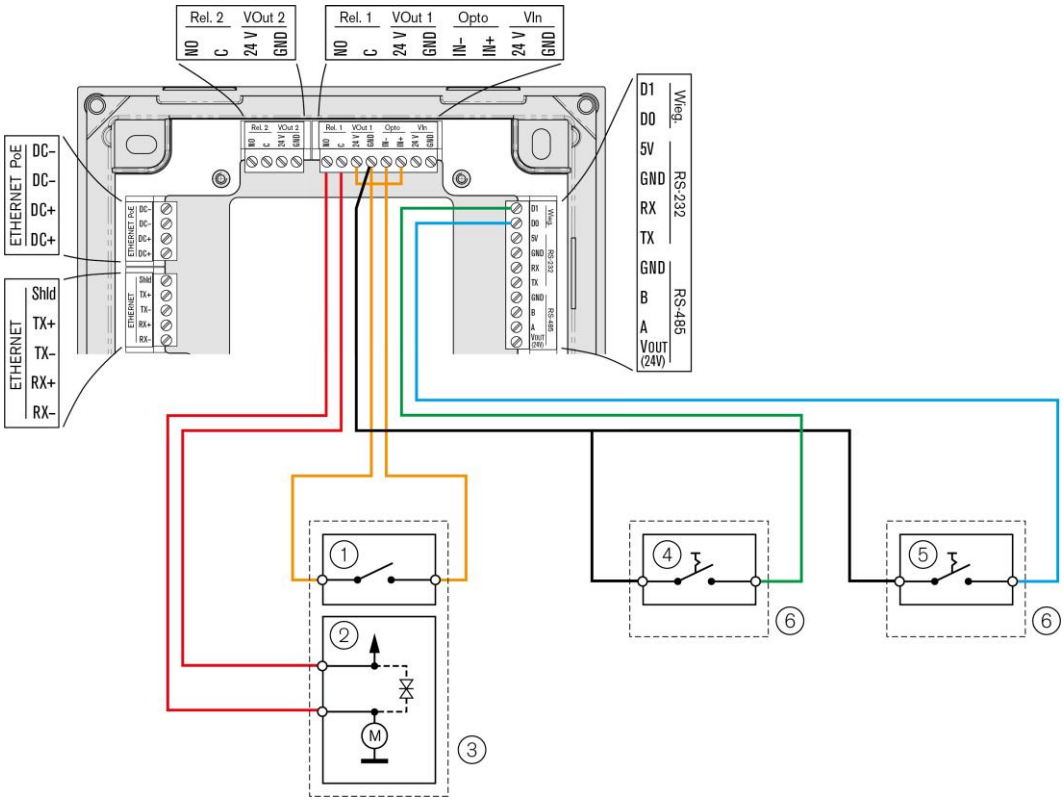
► Depending on the Ethernet standard being used, terminate the wire colors of the Ethernet cable to the "ETHERNET PoE" screw terminals (12) as follows.

Terminal	Signal	Wire Color TIA-568A	Wire Color TIA-568B
DC +	PoE supply +	blue/white	blue/white
DC +	PoE supply +	blue	blue
DC –	PoE supply –	brown/white	brown/white
DC –	PoE supply –	brown	brown

Table 4.2 – Wire colors for PoE

► Plug the other end of the cable into an RJ45 socket on the PoE switch (3).

4.4 Digital inputs and outputs



1 Door feedback contact
2 Door opener
3 Door
4 Exit button
5 Normally open contact
6 Devices for external signals

Fig. 4.3 – Connection of the digital inputs and outputs (example)

External components can be controlled, and status information can be acquired via the digital relay outputs and optocoupler inputs.

In order to use the inputs and outputs, the respective function of these inputs and outputs must be set in the app configuration of the active app on the GT7 terminal (see below). Not all apps allow these settings, which is why the inputs and outputs cannot be used with every app.

NOTE! Observe the permitted voltage and power values of the inputs and outputs in the technical data (see “7. TECHNICAL DATA”).

Relay outputs

The two relay outputs “Rel. 1” and “Rel. 2” can be used to output digital signals to control external components such as door openers. Both relay outputs are normally open contacts (NO).

The terminals GT7.2x00 have only one relay input. The GT7.3x00 terminals have two.

The desired function such as unlock door, deny access, or block external device must be selected in the configuration of the GT7 terminal in the “App configuration” section (see “5.6.19 Installed apps”). The activation time of the relay can also be set here. The app (e.g., Access App) must provide this option to use the relays.

Optocoupler inputs

Digital signals can be received via the three inputs.

The “Opto” input (see 1 - ”Door feedback contact” in Fig. 4.3) is a potential-free input, i.e., a voltage and ground (GND) must be applied. The voltage or GND can be used from the terminals “VOut” of the GT7 terminal (see example). The voltage must not exceed max. DC +30 V.

The inputs “D1” and ”D0” (Clock) of the Wiegand interface can be used as inputs 2 and 3. These inputs have potential and must be connected to GND to set the input active.

The function of the inputs is set in the same way as for the relays in the “App Configuration” of the active app on the GT7 terminal. The app (e.g., Access App) must provide this option to use the inputs.

4.5 Sub controller connection GAT SMART.Controller S 7020 / GAT NET.Controller S 7020

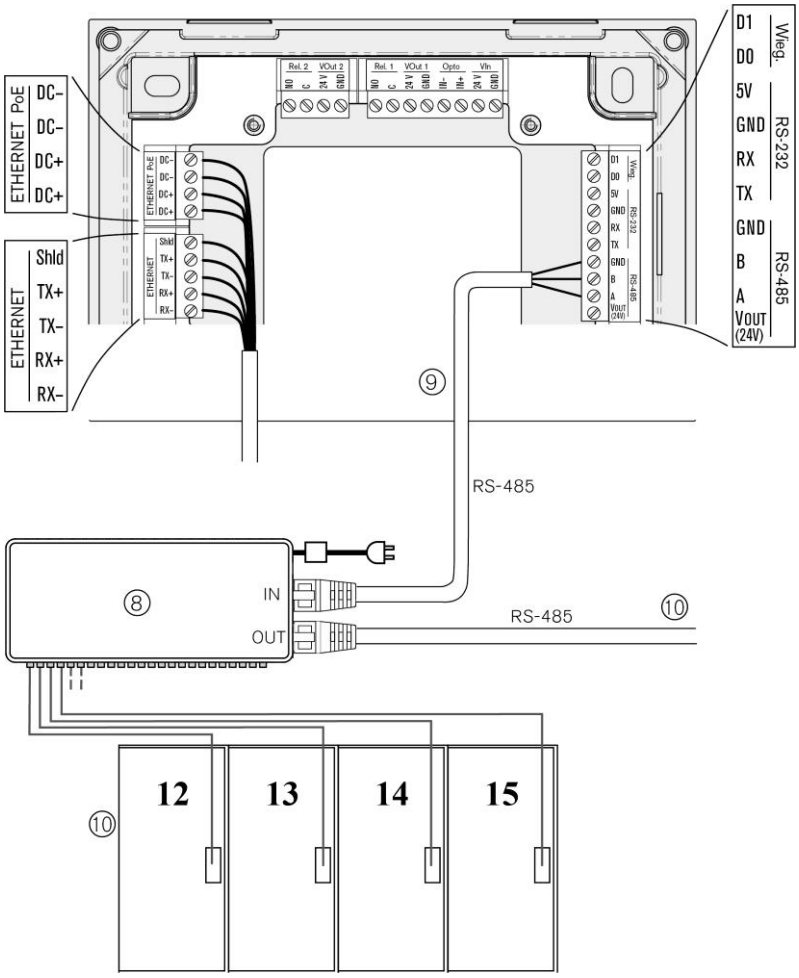


Fig. 4.4 – Connection of the sub controller GAT SMART.Controller S 7020 and GAT NET.Controller S 7020

The GAT SMART.Controller S 7020 and GAT NET.Controller S 7020 sub controllers are connected to the GT7 terminal via an RS-485 interface. Additional sub controllers can be connected directly to the previous sub controller via the RJ45 socket labelled "OUT".

The NET and SMART controllers can be used together. However, ensure that only the GAT NET.Lock locks are connected to the NET controller and only the GAT SMART.Lock locks are connected to the SMART controller (see documentation).

- Connect the RS-485 cable (min. CAT. 5) (9) to the RJ45 socket on the sub controller (8) labelled "RS 485 IN".
- Connect the other end of the RS-485 cable to the "RS-485" screw terminals on the GT7 terminal (see Fig. *4.4*). The recommended wire colors are:

Terminal	Signal	Wire Color
VOut (24V)	Supply voltage for sub controller*	brown + brown/white
A	Data line A	blue
B	Data line B	blue/white
GND	Ground	green + green/white

Table 4.3 – Wire colors for RS-485 connection

* Power supply for the sub controllers must always be via a separate power supply.

4.6 USB barcode interface connection

Gantner's GBS7.1100 and GBS7.1200 barcode scanners can be connected to the GT7.2xxx and GT7.3xxx terminals via the terminal's USB interface. This option allows a barcode scanner to connect to existing terminals and offers a cost-effective solution when combined with the GT7.2500 terminal.

The USB barcode interface uses the same connection as the fingerprint reader. Therefore, both functions cannot be used at the same time.

The following components are required:

> GT7 USB Interface cable (Part No. 1112806).
> USB Adapter A socket-socket (Part No. 1113516).
> Barcode scanner connection cable (supplied with the GBS7.1100 and GBS7.1200 barcode scanners).
> In addition, the GT7 terminal must have min. firmware V3.6.0.

Connect the components to the GT7 terminal as follows:

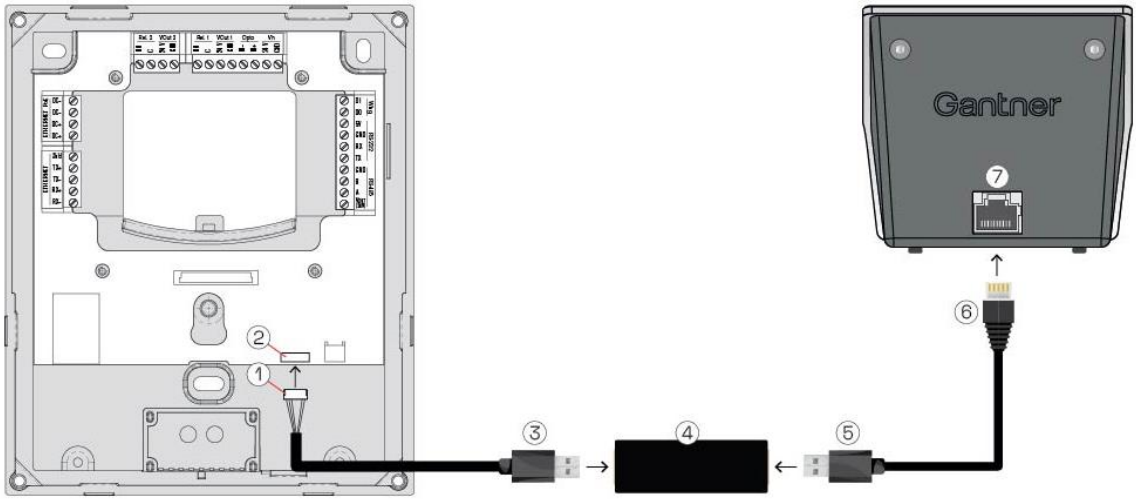


Fig. 4.5 – Connection between the GT7 and GBS7 via USB interface

- If necessary, open the GT7 housing as described in "3.5 Opening the housing".
- Connect the terminal connector (1) of the GT7 USB Interface cable to the USB interface socket (2) on the GT7.
- Connect the USB connector (3) of the USB interface cable to the USB Adapter A socket-socket (4).
- Connect the USB connector (5) of the barcode scanner cable to the USB Adapter A socket-socket (4).
- Connect the RJ50 connector (6) of the barcode scanner cable to the RJ50 port (7) on of the barcode scanner.

The configuration settings required for the USB barcode function are available in "5.6.14 Barcode interface".

5 CONFIGURATION

RF exposure statement

The users must keep at least 20 cm separation distance from the device, except during the identification and operation process at the device (e.g., touchscreen input), which must be performed as described in this manual.

5.1 Target group

This chapter provides information for technicians responsible for commissioning and configuring the GT7 terminal. Basic knowledge of electronics and web applications 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 contains information on all configuration settings of the GT7 terminal that are independent of the apps. In addition to the direct web interface, configuration can also be performed via the G7 Connect web platform. The web browser software G7 Connect can also be used to configure the GT7 terminal. A G7 Connect manual is available that describes the operation of this software in detail.

5.2 Requirements for use

To use all the information described in this manual, min. firmware version 3.0 must be installed in the GT7 terminal.
NOTE! The firmware can be installed via the web interface or via the G7 Connect (see "5.6.24 Update firmware ").
The configuration is valid for the GT7.2x00, GT7.3x00, and GT7.3x01.

5.3 Configuration options of the GT7 terminal

The configuration and functionality of the GT7 terminal can be defined in different ways:
Via the configuration menu: "5.4 Configuration via the GT7 terminal"
Basic information and settings are accessible and configurable via the configuration menu of the GT7 terminal.

Via G7 Connect: "5.5 Configuration via G7 Connect (GANTER Cloud)"
The GT7 terminals in a system integrate conveniently into the G7 Connect or Gantner Cloud resp. There, all terminals are listed in an overview for the user and if the devices are online, they can be configured directly via this platform.

Via the web interface: "5.6 Configuration via Web Interface"
In a web browser, an HTTP or HTTPS connection to the GT7 terminal is established and the GT7 terminal's integrated web server with all the configuration settings is displayed after login.

5.4 Configuration via the GT7 terminal

Basic settings such as the IP address and DHCP address, etc., can be viewed and configured directly on the GT7 terminal via the configuration menu. To open the configuration menu, proceed as follows:

- Write a large "M" on the touchscreen with your finger without removing it.

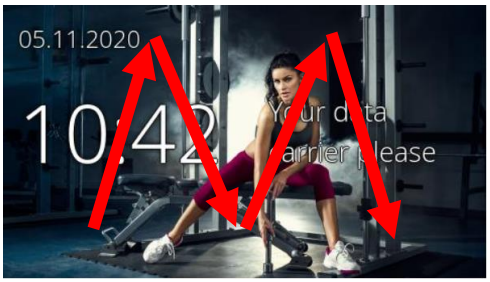


Fig. 5.1 – Configuration menu

  - A keypad for PIN entry is displayed.

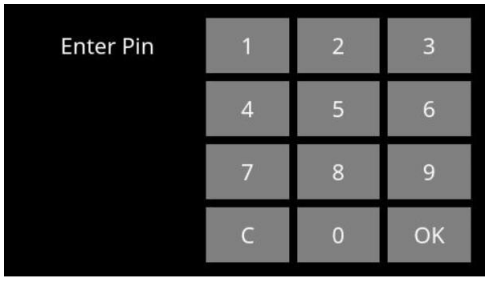


Fig. 5.2 – PIN code entry

- Enter the PIN code "0815", and then press "OK".
  ATTENTION! For security reasons, change the default PIN code to a secret code. This can be done via the "Device Settings" (see "5.6.12 Device") of the web interface.
  - After entering the PIN code, the configuration menu is displayed.
- Via the icons to the left, you can select the desired information or configuration page.

Display of device settings →
Display and start installed apps →
Configure device settings →
Start active app or restart GT7 →

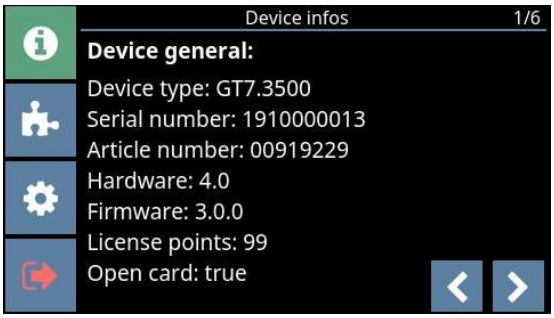


Fig. 5.3 – Configuration menu

- Each configuration page has subpages (see display at top right). Use the arrow buttons in the lower-right corner of the screen to scroll through the different subpages.

5.4.1 Device info

Device information is displayed on the five sub-pages of this menu. Most of the settings shown here can be configured via the device configuration page (see “5.4.3 Device configuration”).

General device info

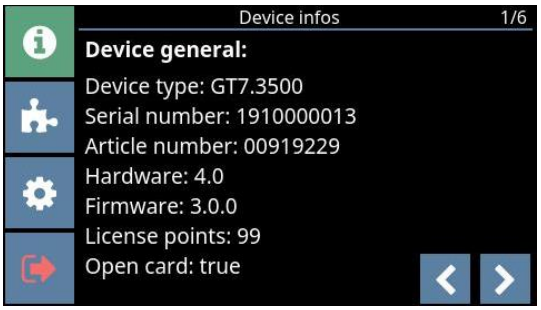


Fig. 5.4 – Device Info 1 - General

- Device type: The type/model of GT7 terminal (e.g., GT7.3500).
- Serial number: The serial number the device.
- Article number: The article number the device.
- Hardware: The hardware version running on the device.
- Firmware: The firmware version running on the device.
- License points: The number of device licenses (points) that have loaded to the device. Each app requires a certain number of points to operate (see chapter “5.6.21 Licensing”).
- Open card: When “true” is shown here, the GT7 terminal can read the UID number of third-party data carriers, i.e., those not sold by Gantner. To activate this function, the “G7 Device License Points Open Card” license code must be purchased and entered into the web interface (see chapter “5.6.21 Licensing” for more information).

Network settings

Fig. 5.5 – Device Info 2 - Network

- MAC: The MAC address of the device.
- IP: The IP address of the device. The first line shows the IPv4 address. If IPv6 is activated (possible via the configuration menu or web interface), the IPv6 address is also displayed in the second line.

WLAN settings

Fig. 5.6 – Device Info 3 - WLAN

Displayed here is whether the Wi-Fi connection is enabled or disabled. If enabled, the quality of the Wi-Fi signal and the address (depending on the hardware) are also displayed.

Network routing settings

Fig. 5.7 - Device Info 4 - Network routing

The routing settings for the network connection are displayed here. The top two lines display the information for the IPv4 settings. Displayed below are the IPv6 settings if this protocol has been enabled. These settings are assigned automatically and cannot be changed.

Status

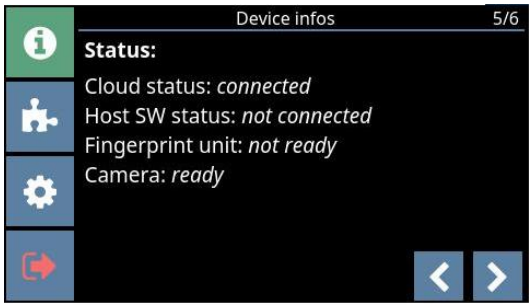


Fig. 5.8 – Device Info 5 - Status information

- Cloud status: When “connected” is shown here, the connection to G7 Connect is functioning.
- Host SW status: When “connected” is shown here, the connection to the host software (e.g., eloxx Relaxx locker management software) is functioning. The text “not connected” means that there is no connection to any host software.
- Fingerprint unit / Camera: When “ready” is shown in these fields, the fingerprint reader (GT7b.2000) / integrated camera of the GT7.3xxx terminal is ready for operation.

RFID reader test

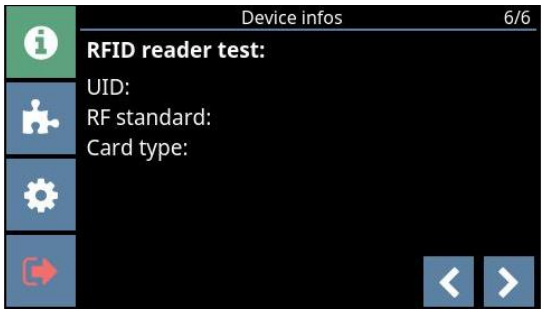


Fig. 5.9 – Device Info 6 - RFID reader test

On this page you can use the GT7 terminal's RFID reader to display the UID number, the used RFID technology, and the type of a data carrier.

► Hold a data carrier next to the reading field (LED ring) of the GT7 terminal.

- The data carrier is read, and the following data displayed.

Fig. 5.10 – Display of read data carrier information

5.4.2 Installed apps

On the "Installed Apps" page, all apps that have been installed in the GT7 terminal are displayed. Information, such as which app version is installed and the required license points, is provided here.

New apps can be uploaded to the GT7 terminal via G7 Connect or the web interface.

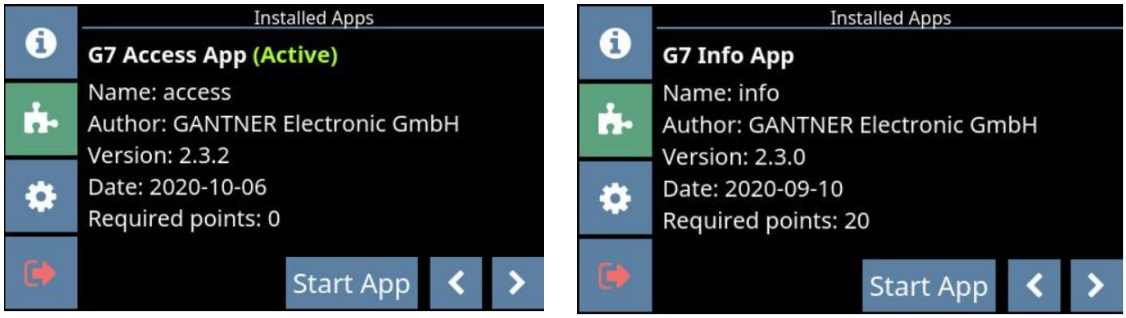


Fig. 5.11 – Installed apps – G7 Access

- To scroll through each installed app, press the arrow buttons in the bottom right of the display.
- To begin using an app, press the "Start App" button.
  - The app is loaded (which takes a few seconds), and the default page of the app is displayed after restarting.

5.4.3 Device configuration

The following settings can be configured for the GT7 terminal via the configuration menu. Depending on the model, some of the settings shown here may not be available for your GT7 terminal.

- To enable a setting, press the box so that a tick is displayed.
- To define a setting that has numbers (e.g., the IP address), press the "Spanner" icon.
  - A keypad is displayed where you can enter the number.
    NOTE! Settings that require the input of characters must be defined via the web interface or G7 Connect.
- Once you have defined the settings on a page, press the "Disc" icon to save the settings.

LAN settings

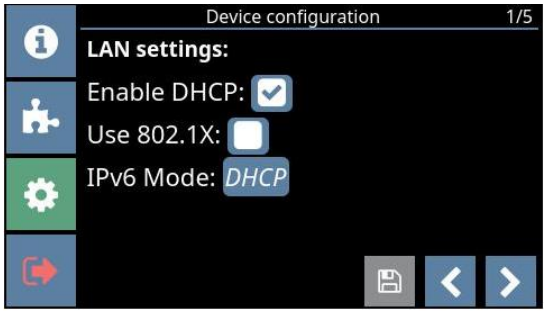


Fig. 5.12 – Device configuration – Page 1

- Enable DHCP: When this option is enabled, the network router will assign a dynamic IP address to the GT7 terminal. When not enabled, the "LAN static IP settings" (page 2) are used to determine LAN communication.
- Use 802.1X: When this option is enabled, the GT7 terminal will use the 802.1x protocol for identification.
- IPv6 Mode: Displayed in this field is the method for assigning the IP address when using IPv6. DHCP uses a DHCP server to automatically assign the address. Static means that the address can be defined manually. With stateless address autoconfiguration, the GT7 terminal automatically obtains an IP address by communicating with the router responsible for its network segment and thus determining the address.

LAN static IP settings

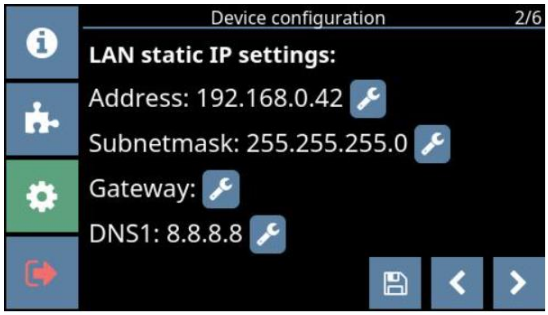


Fig. 5.13 – Device configuration – Page 2

- Address: The static IP address of the GT7 terminal for LAN communication.
- Subnet mask: The static subnet mask of the GT7 terminal for LAN communication.
- Gateway: The static gateway address of the GT7 terminal for LAN communication.
- DNS1: The address of the primary DNS server for LAN communication.

GT7 terminal time settings

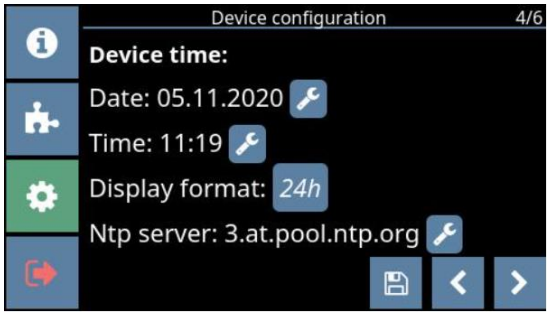


Fig. 5.14 – Device configuration – Page 4

- Date: The date can be manually set here.
- Time: The time can be manually set here.
- Display format: Select between 12h or 24h time format or select “None” to not display the time.
- NTP server: The location of the NTP server from which the time is taken automatically. The default server is displayed. To change this address, use the web interface, as only numbers can be entered in the configuration menu on the GT7 terminal.

WLAN settings

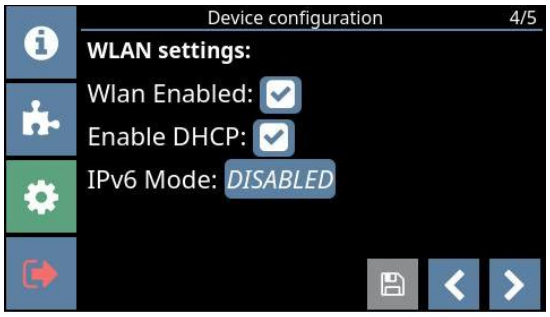


Fig. 5.15 – Device configuration – Page 5

- WLAN enabled: Enable or disable the GT7 terminal’s ability to communicate via Wi-Fi.
- Enable DHCP: When this option is enabled, a dynamic IP address will be assigned for wireless communication. When not enabled, a static IP address must be defined for wireless communication.
- IPv6 Mode: Here you can enable or disable the use of IPv6. For more information, see chapter ”5.6.2 Network”.

WLAN static IP settings

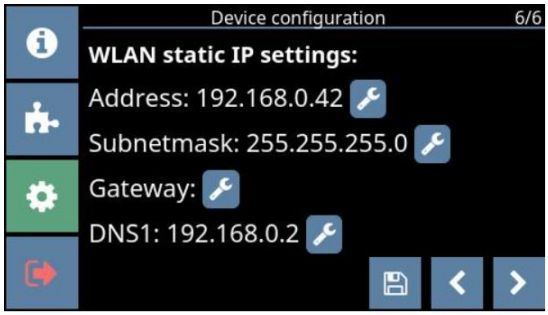


Fig. 5.16 – Device configuration – Page 6

- Address: The static IP address of the GT7 terminal for WLAN communication.
- Subnet mask: The static subnet mask of the GT7 terminal for WLAN communication.
- Gateway: The static gateway address of the GT7 terminal for WLAN communication.
- DNS1: The address of the primary DNS server for WLAN communication.

5.4.4 Start active app / Reboot device

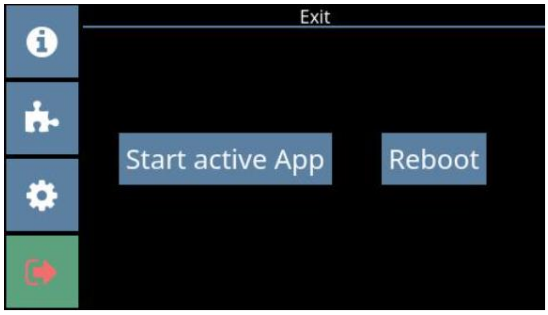


Fig. 5.17 – Exit device configuration

► To exit the configuration menu, press the exit icon .

► Select “Start active App” to start the last active app.

  - The active app is loaded and after a few seconds the app’s home screen is displayed.

► Alternatively, press the “Reboot” button if you would like to restart the GT7 terminal.

  - The terminal restarts, and the last active app is displayed.

5.5 Configuration via G7 Connect (GANTER Cloud)

G7 Connect is Gantner 's web platform that provides a clear, user-friendly interface for managing projects that include GT7 and GC7 devices. Users can access G7 Connect via an Internet browser such as Chrome or Firefox. The user is required to log in with a username and password to begin using G7 Connect and after doing so, the various users and projects defined in G7 Connect can be viewed and configured. A detailed view is provided on the "Dashboard" page of each project that shows information on the device licenses, cloud packages, used apps, app versions, and statistics from the current app.

The configuration of a GT7 terminal using G7 Connect is analogous to the direct configuration via web interface, which is described in chapter "5.6 Configuration via Web Interface". To begin using G7 Connect, you must register with Gantner (if you are the first user within your organization) or be invited from a registered user from your organization.

For detailed information on how to start using the G7 Connect Cloud Service, see the G7 Connect manual.

After activating your account, you can log in to G7 Connect as follows:

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

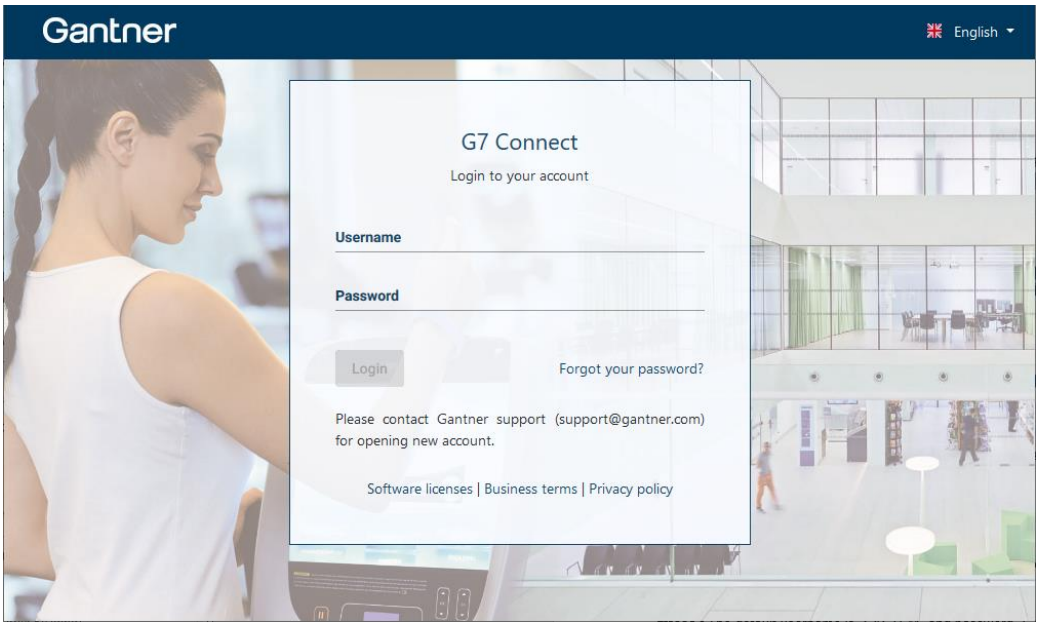


Fig. 5.18 – Login window for G7 Connect

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

NOTE! See the G7 Connect user manual for detailed instructions on using the application. It is available to download from the Gantner website (login required).

5.6 Configuration via Web Interface

Provided that the terminal is reachable via the network, a GT7 terminal can be directly accessed via a web browser. All settings for the device and the installed GT7 apps are available for configuration in the web interface.

- ► Open a web browser.
- ► Enter the IP address (IPv4 or IPv6) of the GT7 terminal into the address bar.
  NOTE! If an IPv6 address is entered into the browser, the IP address must be written in square brackets.
  Example: [2001:db8:1:0:212:8ff:fec1:29e2]/app/webinterface

The IP address of the GT7 terminal 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 terminal (see "5.4 Configuration via the GT7 terminal").

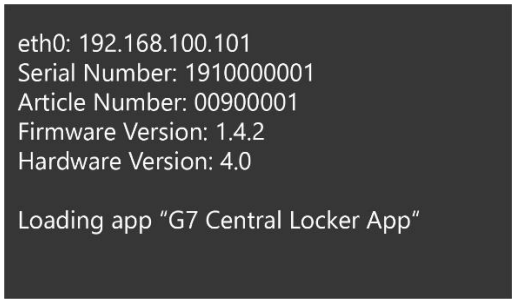


Fig. 5.19 – Start-up screen of the GT7 terminal

- o The login page of the GT7 web interface opens in the web browser.

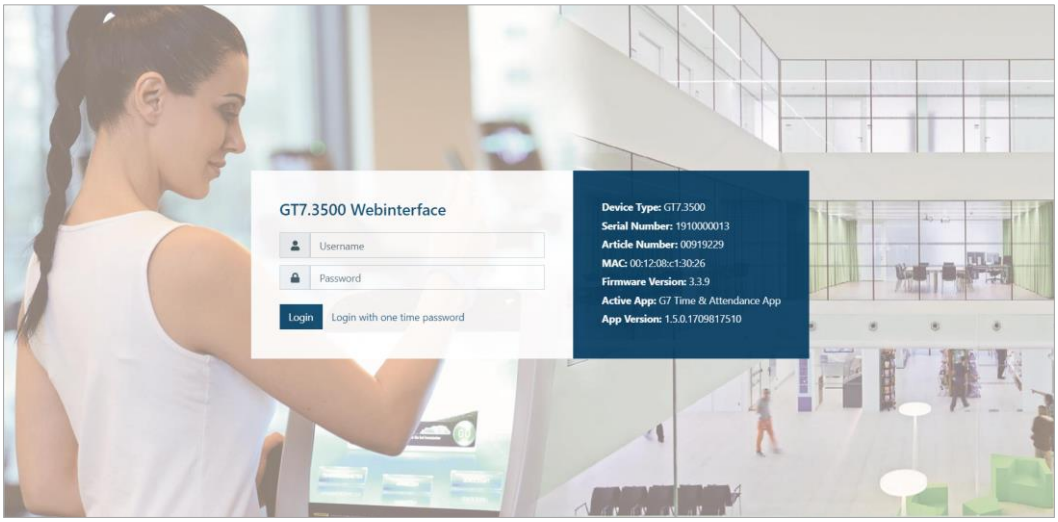


Fig. 5.20 – Login screen of the GT7 terminal

► In the login window, enter your username and password and click on "Login".

NOTE! By default, the username "admin" and the password "GAT" are preset. After the first login, please change this data to a secure login details (see "5.6.7 Security and user").

- The configuration page of the GT7 terminal opens with an overview of the system settings.

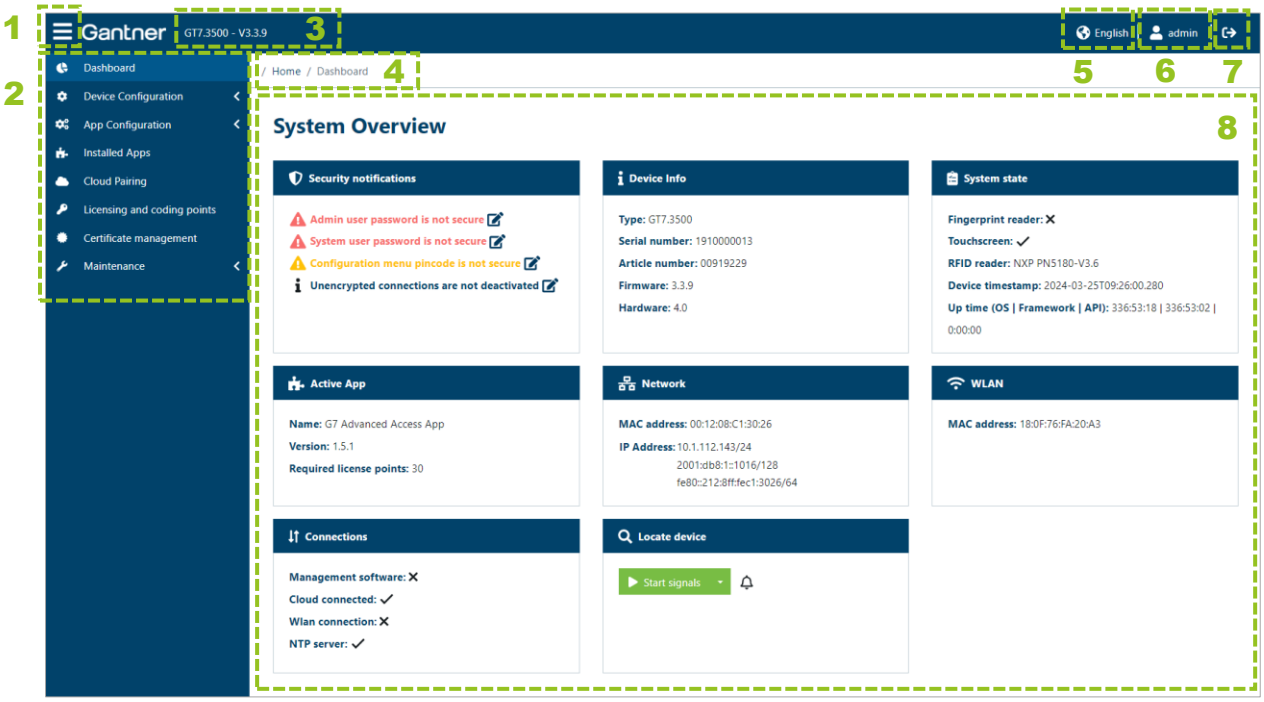


Fig. 5.21 – Configuration page of the GT7 terminal - System overview

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

1	Show / Hide menu:	This button allows you to show or hide the settings menu to the left.
2	Settings menu:	Available here is the menu that you can use to access the respective settings pages of the GT7 terminal.
3	Firmware version:	Version of the firmware currently operating in the GT7 terminal.
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.

All menu options and the available settings are described over the following pages.

5.6.1 Overview

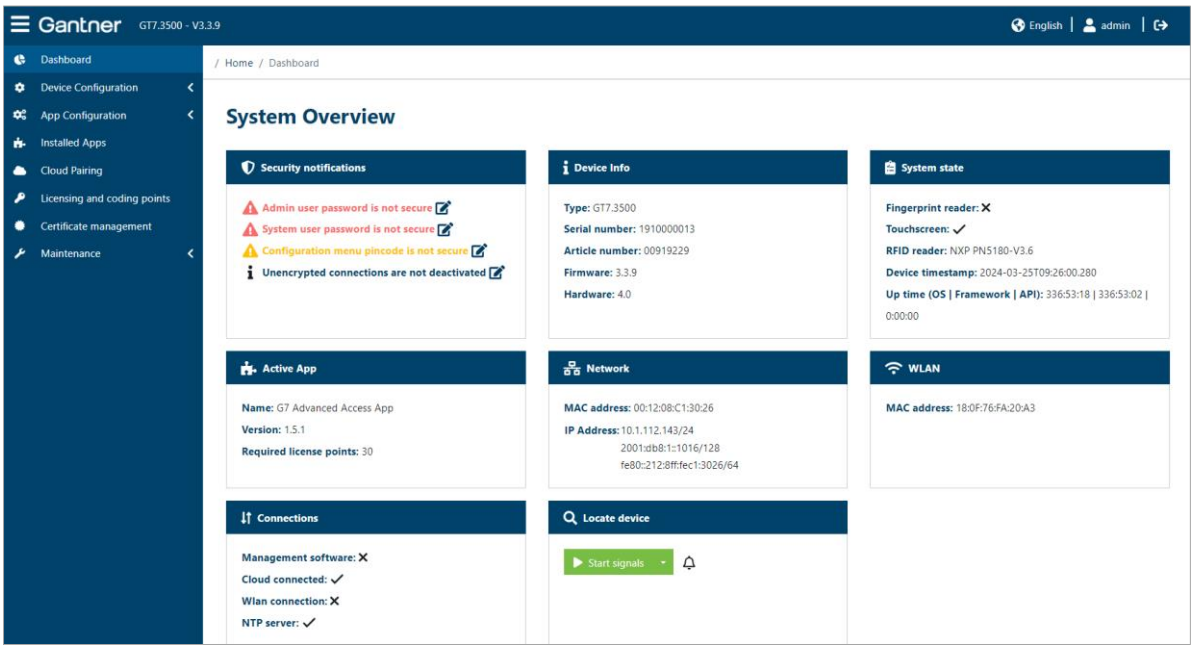


Fig. 5.22 – GT7 terminal web interface - System overview

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

- Security notifications: Useful information, e.g., login warnings, relating to the security of the GT7 terminal is displayed here.
- 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 touch screen is connected and in use (which is usually true for the GT7 terminal). After that you see the firmware version of the RFID reader, the time in the GT7 terminal and how long the GT7 terminal is 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. For certain apps license points are required, which can be added in the menu "Licensing and coding points". There you can also add coding points for coding data carriers with the corresponding GT7 coding app.
- Network: The network addresses of the GT7 terminal are displayed here. For the IP address, the IPv4 address is displayed first and, if enabled, the IPv6 address is displayed beneath.
- WLAN: If WLAN is enabled, the MAC address is displayed here.
- Connections: Here, the functions that are activated or in-use are displayed. The symbol after "Management software" shows if a connection to a PC software (e.g., eLoxx Relaxx), which controls the GT7 terminal, is established. A tick beside "Cloud connected" means that the GT7 terminal is currently connected to G7 Connect and can also be configured via the Gantner Cloud service.
- 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.

5.6.2 Network

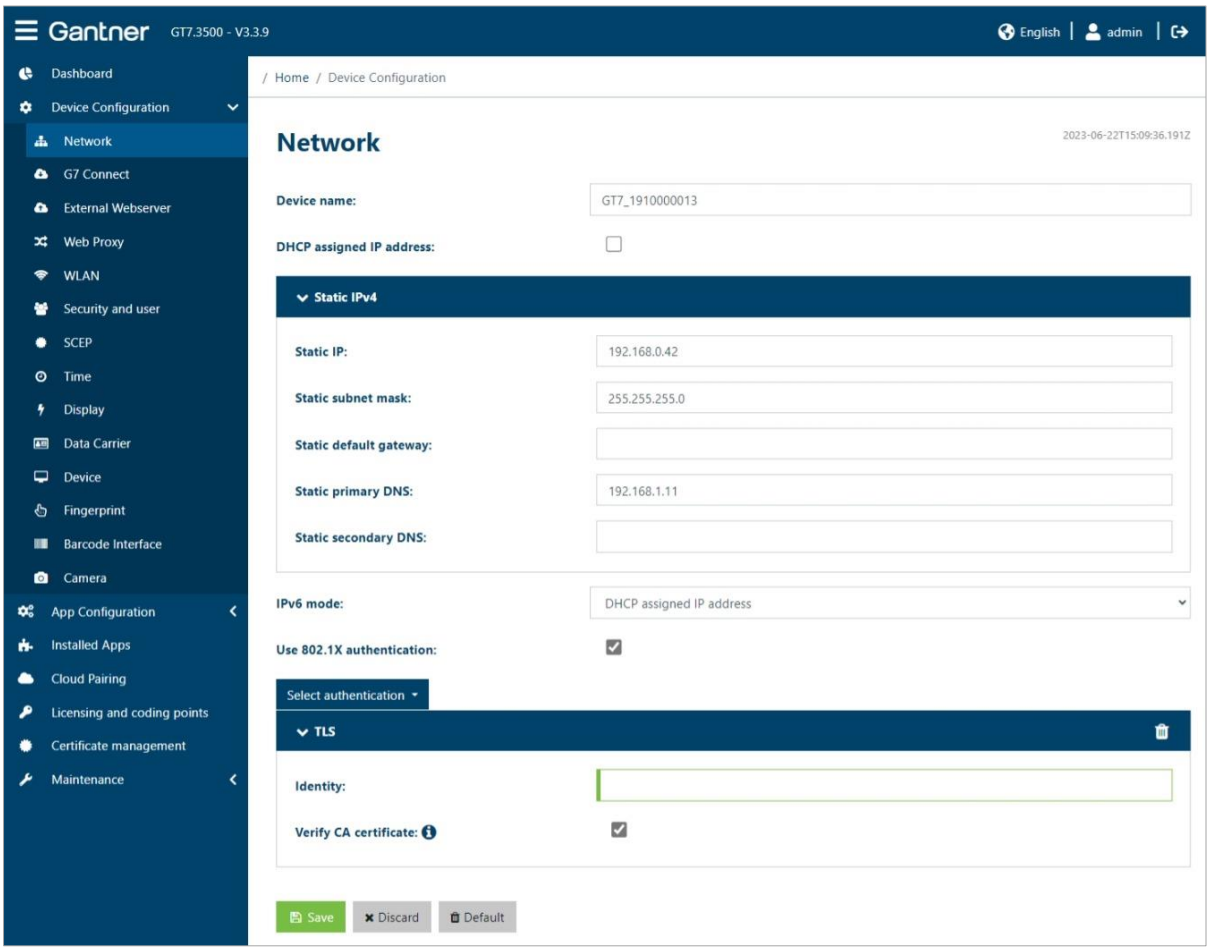
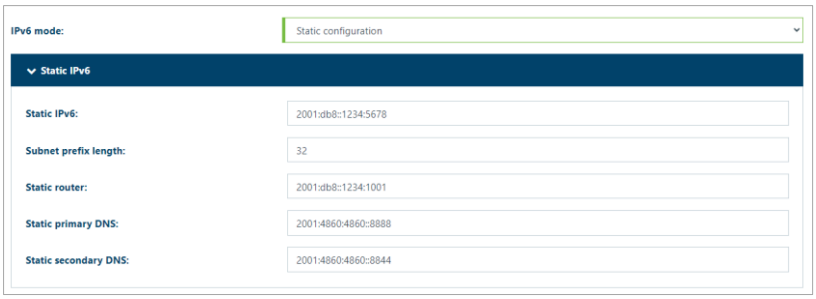


Figure 5.23 – GT7 terminal web interface - Network

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

- Device name: An arbitrary name can be entered for the GT7 terminal here. When the network is scanned for devices, e.g., to add the GT7 terminal to eLoxx Relaxx, the device is shown with this name.
- DHCP assigned IP address: When this option is selected, the IP address of the GT7 terminal is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, deactivate this option and enter the network settings into the "Static IPv4 configuration" section, which is displayed when this option is disabled.
- IPv6 mode: Here you can select whether to use IPv6 and how the address assignment should occur.
  - Disabled: IPv6 mode is not used.
  - DHCP assigned IP address: IPv6 is enabled, and addresses are assigned automatically using a DHCP server.

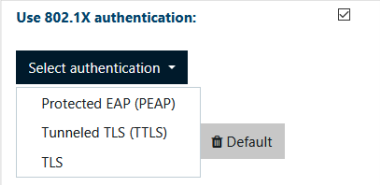
    Static configuration: The IPv6 addresses can be set manually. The following settings are then displayed:



Enter the IPv6 address of the GT7 terminal and the data required for 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.

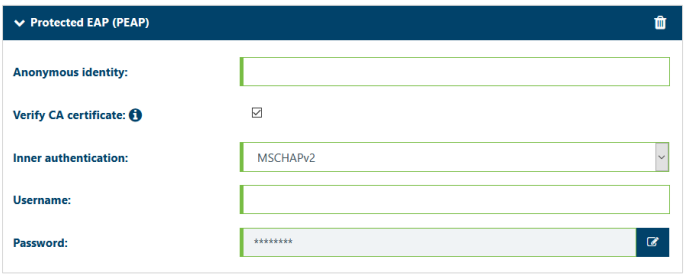
- Use 802.1X authentication: Select this option to enable 802.1X authentication. 802.1x authentication is a security protocol that works with 802.11 wireless networks such as 802.11g and 802.11b and also with wired devices. From the “Select authentication” menu, select the type of authentication method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



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

Protected EAP (PEAP)

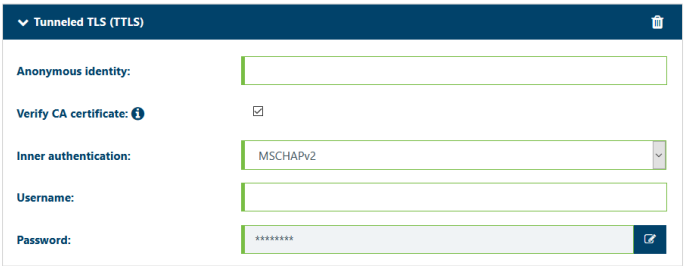
Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Define the following 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 "5.6.22 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.

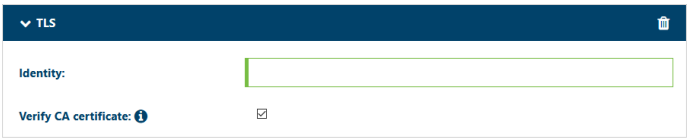
Tunneled TLS (TTLS)

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 "5.6.22 Certificate management").

5.6.3 G7 Connect

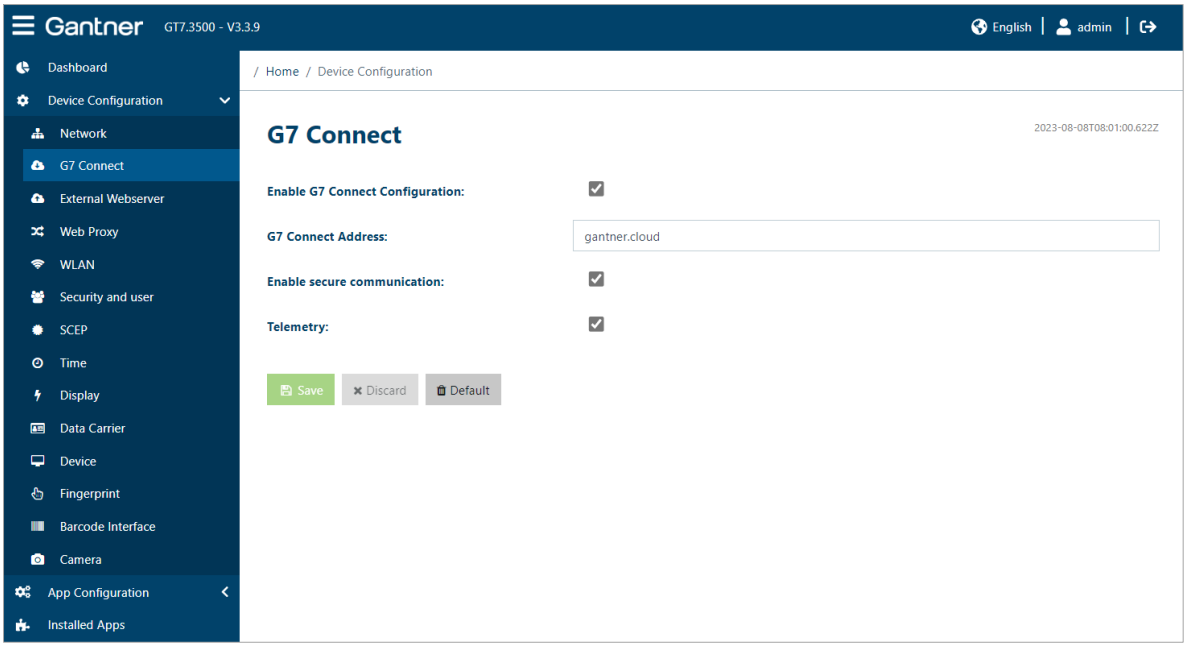


Fig. 5.24 – GT7 terminal web interface - G7 Connect

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 terminal.
- G7 Connect Address: Enter the address of G7 Connect here (default = “gantner.cloud”).
- 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 G7 Connect terms and conditions for more information).

5.6.4 External webserver

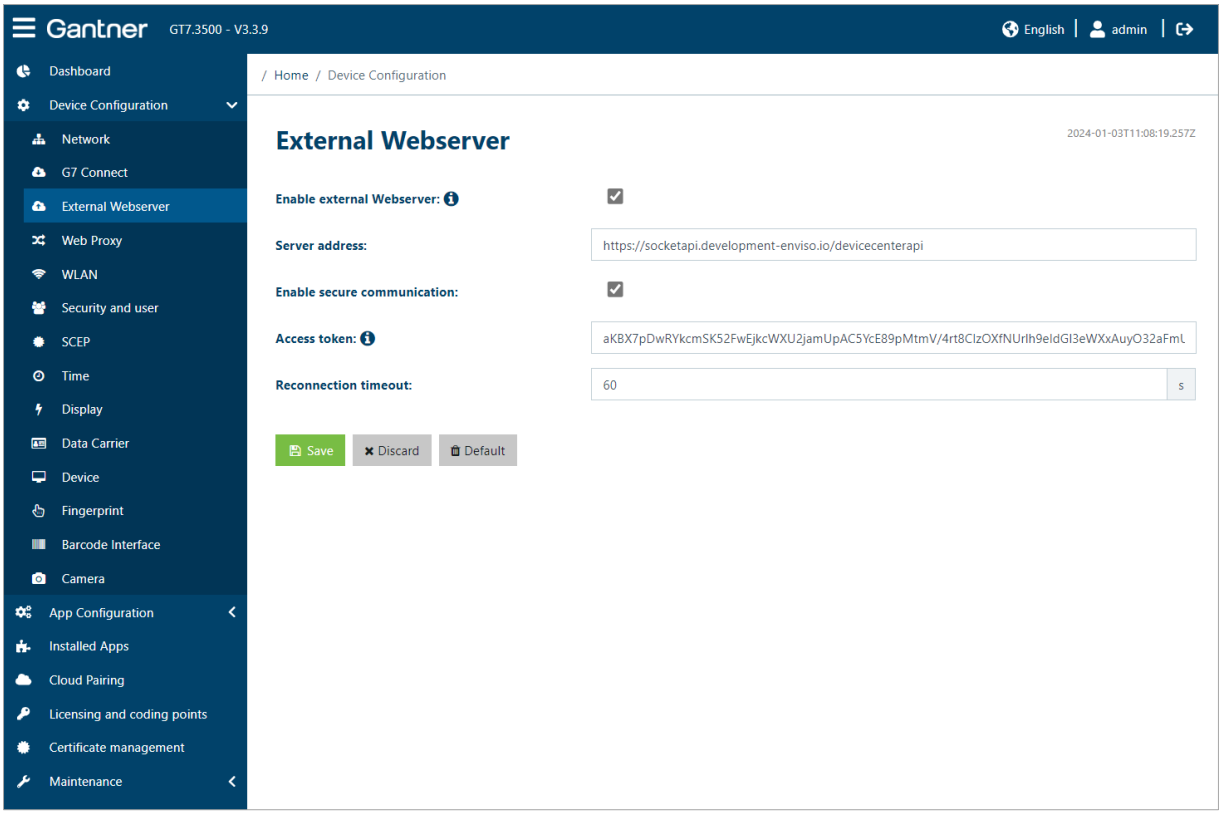


Fig. 5.25 – GT7 terminal web interface - External Webserver

The GT7 terminal can function as a client or server. For the configuration as described here, the GT7 terminal is operating as a server, i.e., the PC connects to the GT7 terminal. If the GT7 terminal 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/SSL 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 terminal and the management software has been interrupted.

5.6.5 Web proxy

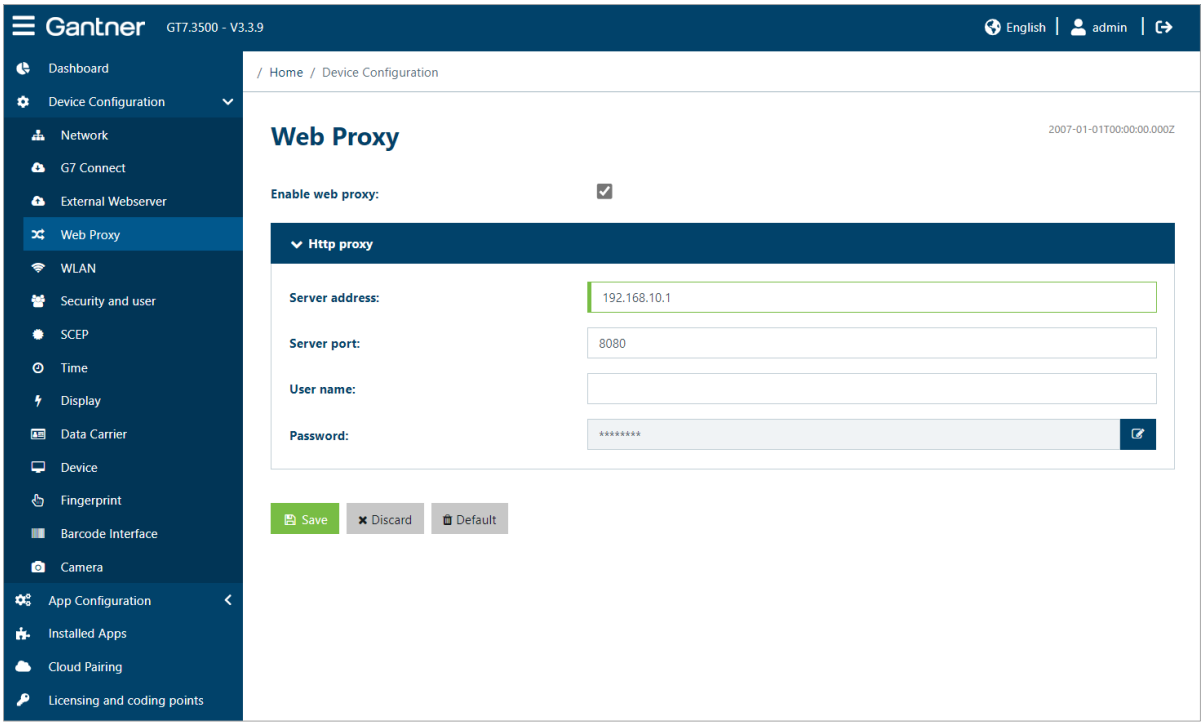


Fig. 5.26 – GT7 terminal web interface – Web Proxy

A web proxy server can be configured in order to route all outgoing connections via 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 displayed.
- Server address: IP address of the web proxy server (IPv4 format).
- Server port: Port of the web proxy server.
- Username: Username used to access the web proxy server.
- Password: Password used to access the web proxy server.

5.6.6 WLAN

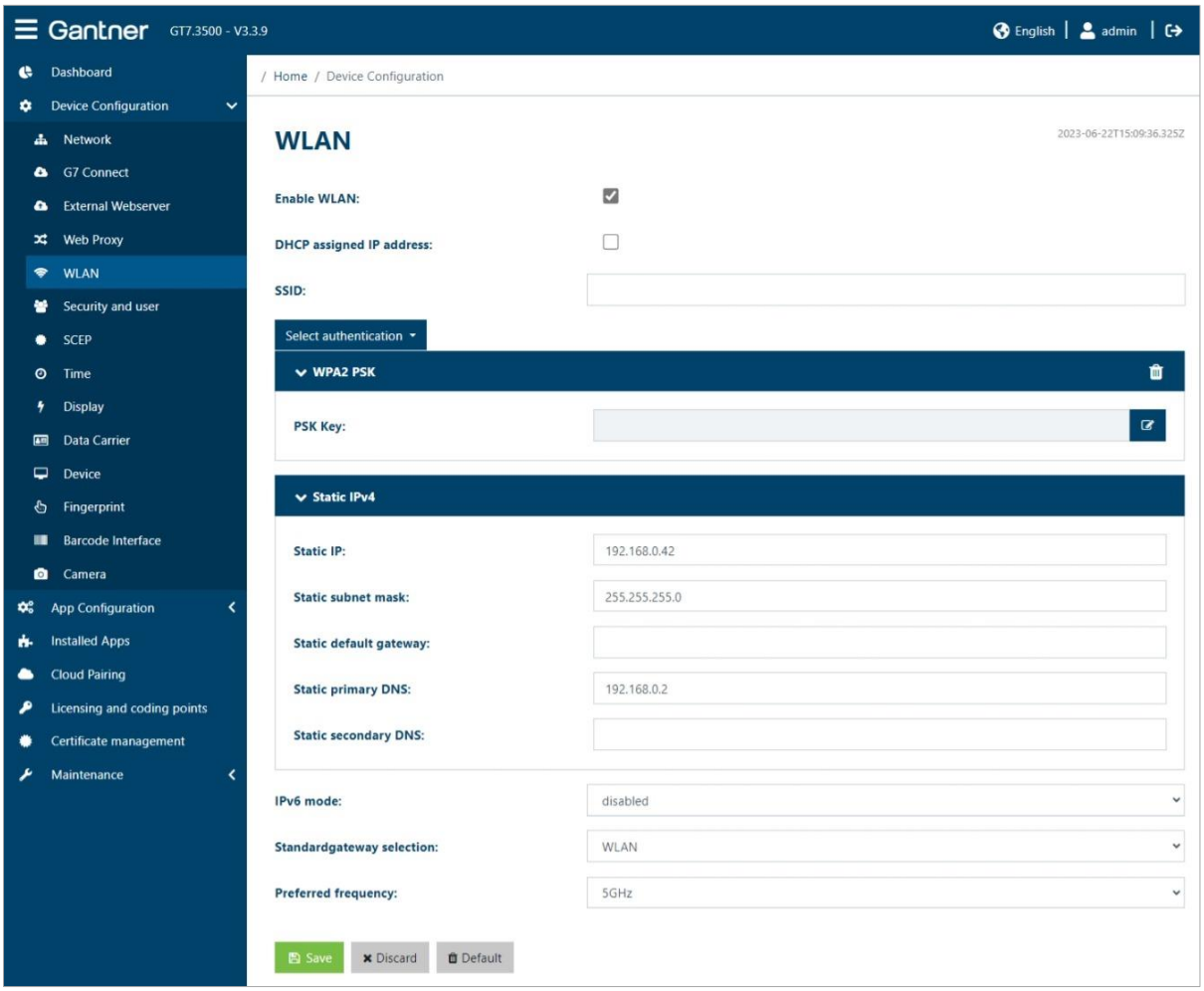


Fig. 5.27 – GT7 terminal web interface - WLAN settings

A GT7 terminal 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 use IPv6 mode for the WLAN connection or not (disabled). If enabled, select how the address assignment should occur (DHCP assigned IP address, Static configuration, Stateless address autoconfiguration). For more information on IPv6 in the network configuration, refer to chapter ”5.6.2 Network”.
- Standard gateway selection: Here you can select from the menu, which connection type (LAN Ethernet or WiFi) shall be used for communication. When selecting ”Ethernet” or ”WLAN” only the selected connection type will be used with preference.

5.6.7 Security and user

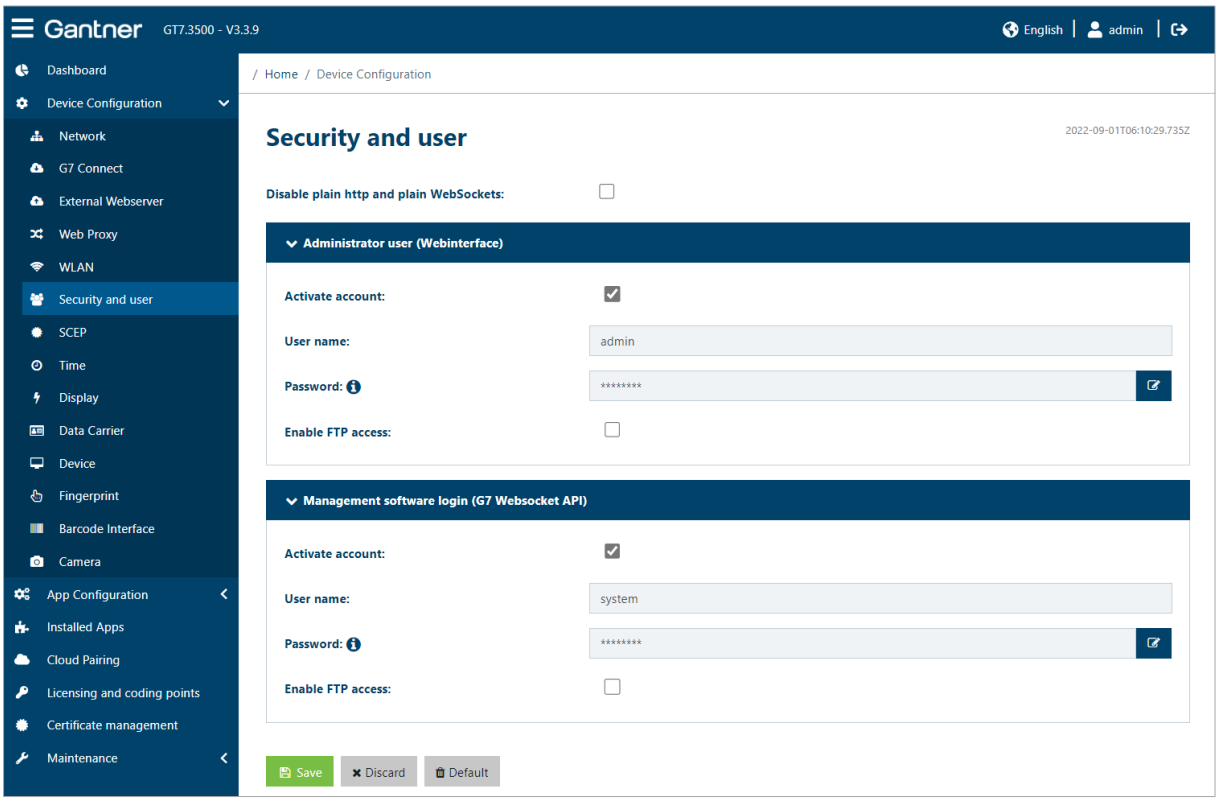


Fig. 5.28 – GT7 terminal web interface - Security and User

Here, you can define the users who are allowed to access the GT7 terminal via the web interface ("Administrator user (Web interface)") and via the G7 Websocket API ("Management software access" (G7 Websocket API)").
The user "Management Software Access (G7 Websocket API)" is used, e.g., by the management software eLoxx Relaxx.

- Disable plain http and plain WebSockets:
  To prevent the GT7 from communicating using an unencrypted connection (e.g. HTTP instead of HTTPS) you can disable these unencrypted connections here.
- 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: Enter a password for the user. Click on the blue edit button to the right.
  NOTE! If the default password is not changed for the "Management Software Access (G7 Websocket API)" user, eLoxx Relaxx creates a new, secure password for communication. If the password is changed here, it must also be entered into eLoxx Relaxx.
- Enable FTP access: Enable or disable the FTP server in the GT7 terminal via this setting.

5.6.8 SCEP (Simple Certificate Enrollment Protocol)

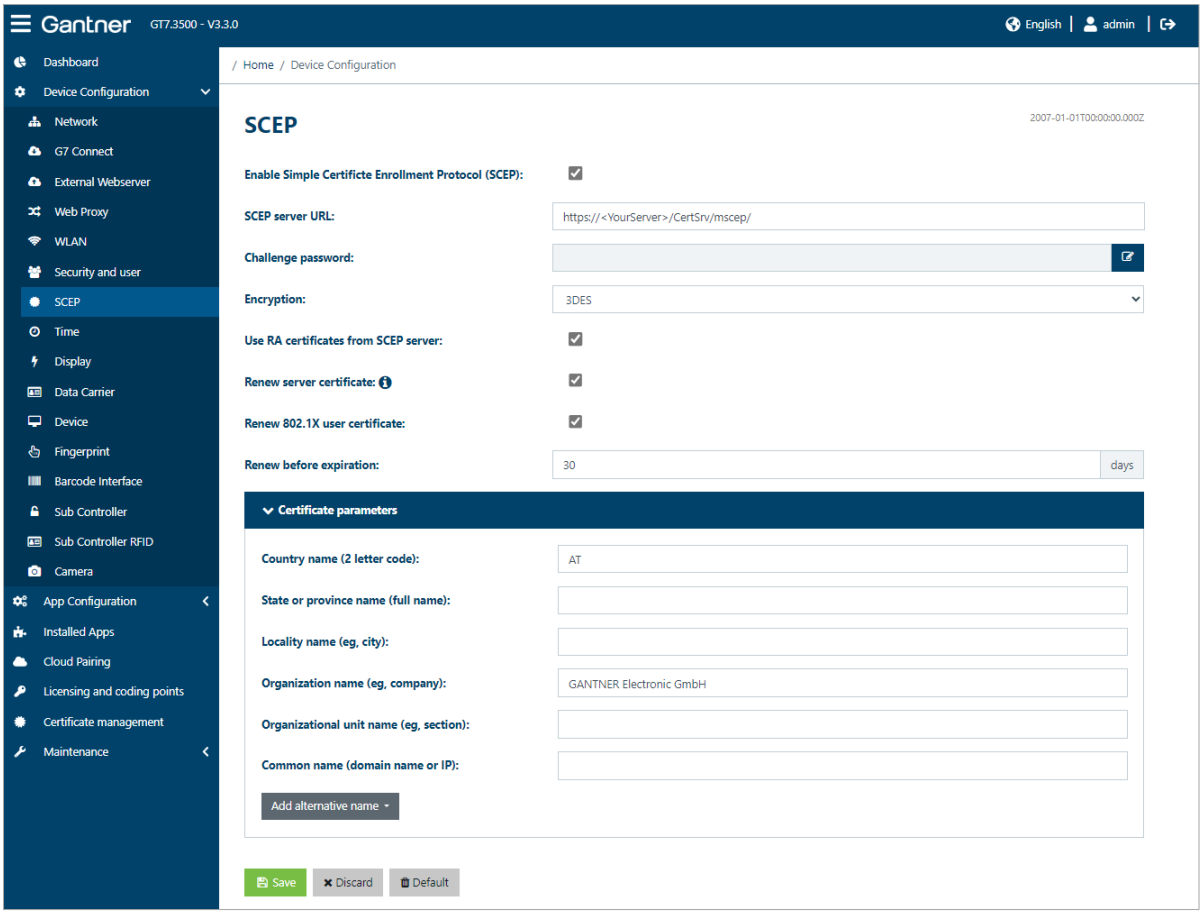


Fig. 5.29 – Configuration page of the GT7 Central Locker - SCEP

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.

5.6.9 Time

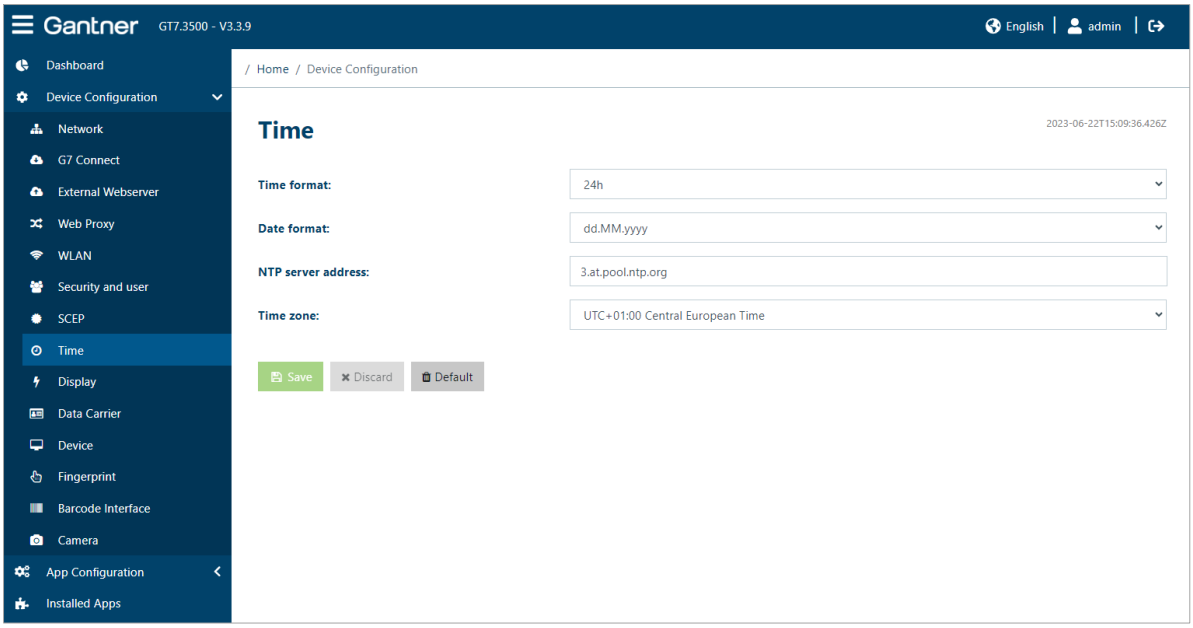


Fig. 5.30 – GT7 terminal web interface - Time

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

- 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 terminal.
- 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 US 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 terminal'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 terminal is operating.

5.6.10 Display

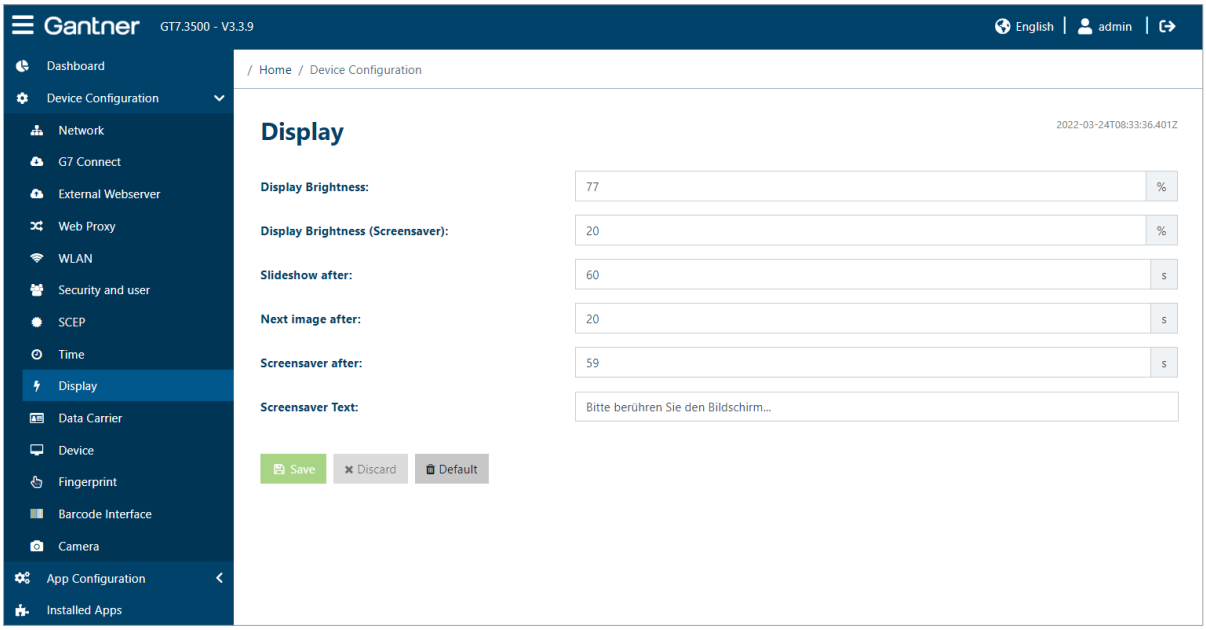


Fig. 5.31 – GT7 terminal web interface - Display

These settings determine the brightness of the GT7 terminal's 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 of terminal inactivity after which an image slideshow (i.e., different pictures from the theme) is displayed. For more information on themes, see "5.6.19. 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.

5.6.11 Data carrier

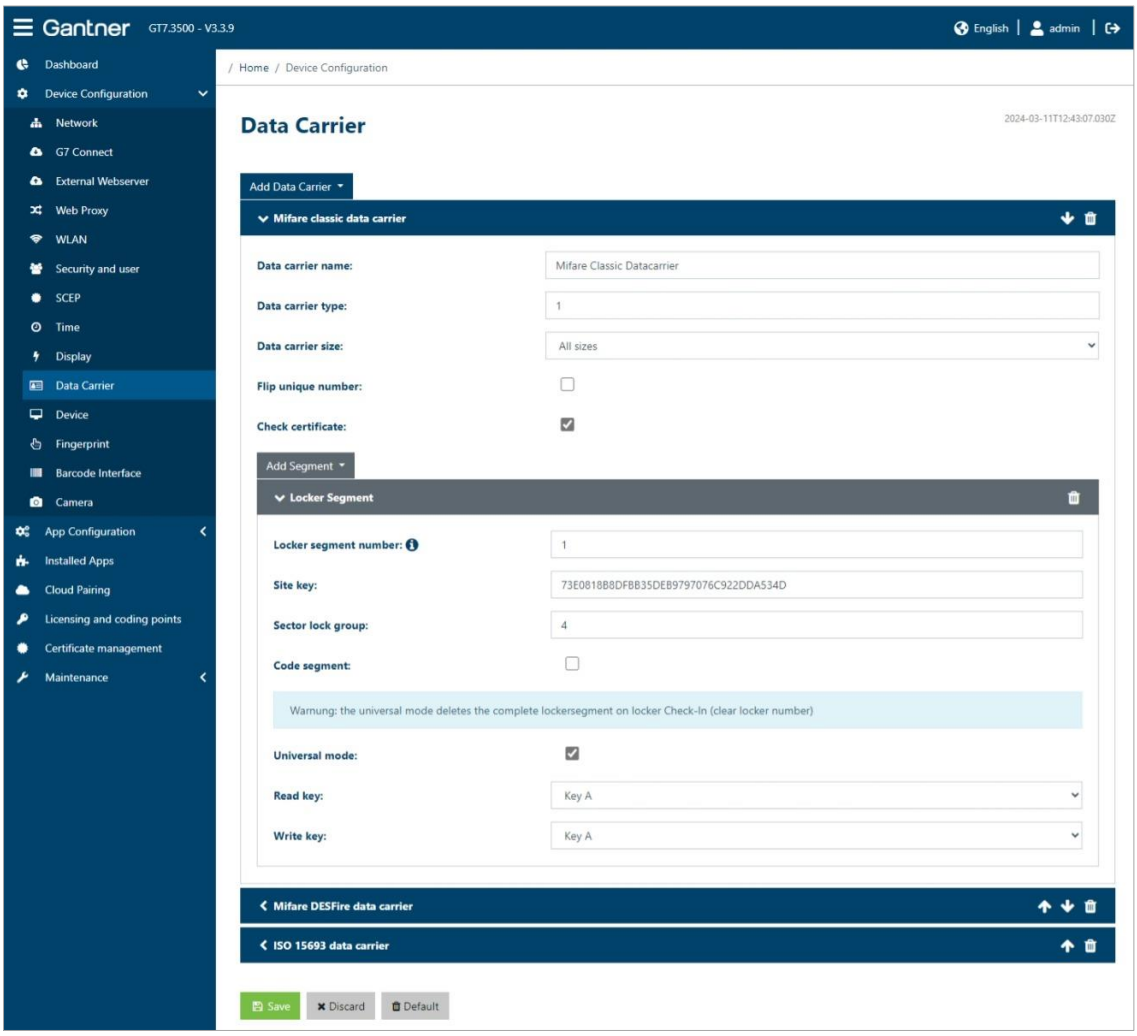


Fig. 5.32 – GT7 terminal web interface – Data carrier

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

The data carrier settings for the sub controller are defined in the menu "Sub Controller RFID" (see "5.6.16. 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.

5.6.12 Device

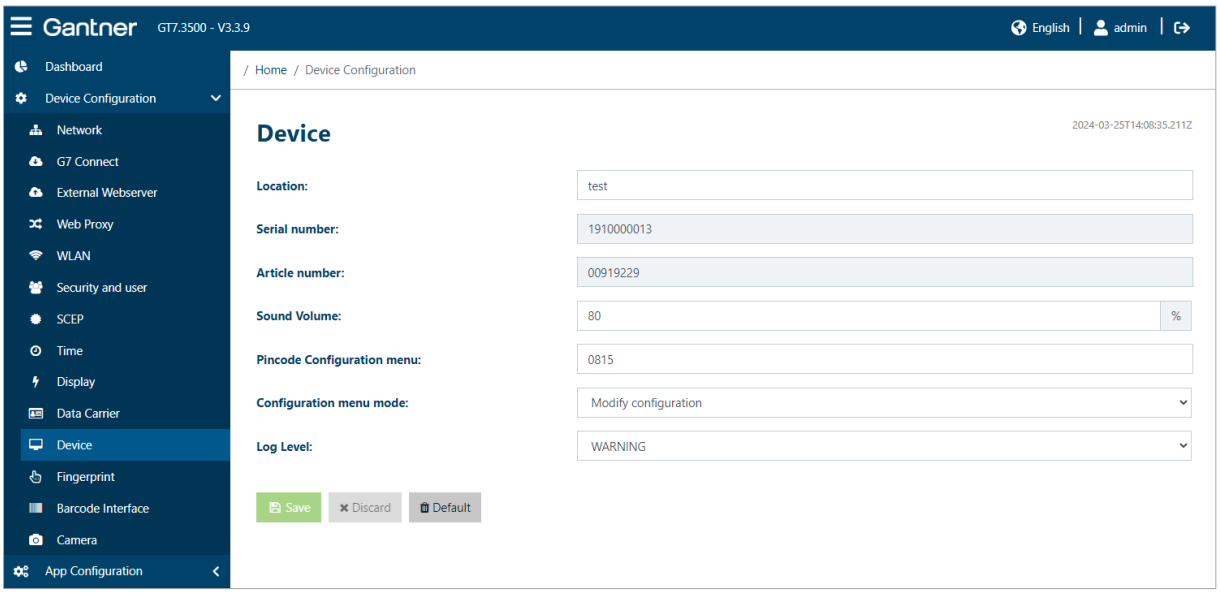


Fig. 5.33 – GT7 terminal web interface – Device

The general settings of the GT7 terminal 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 terminal.
- 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 terminal. To enter the code, write an "M" on the display. For more information see "5.4 Configuration via the GT7 terminal".
- Configuration menu mode: The configuration menu can be shown on the display of the GT7 device (see "5.4 Configuration via the GT7 terminal"). You can, e.g., for security reasons, select to only display the settings but not allow them to be edited or you can disable the display of the menu.
  - Modify configuration:

    The menu can be opened and changes to the settings can be made, e.g., to the network settings, which can also be saved.
  - Show configuration:

    This option only allows the configuration menu to be displayed, but the settings cannot be changed.
  - Configuration menu disabled:

    The configuration menu cannot be opened on the GT7 terminal.

- 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 ”5.6.26 Log viewer”). Different messages are logged depending on the setting configured here:
  - ERROR: All errors are displayed, e.g., connection errors to G7 Connect or locker operation errors.
  - 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.

5.6.13 Fingerprint

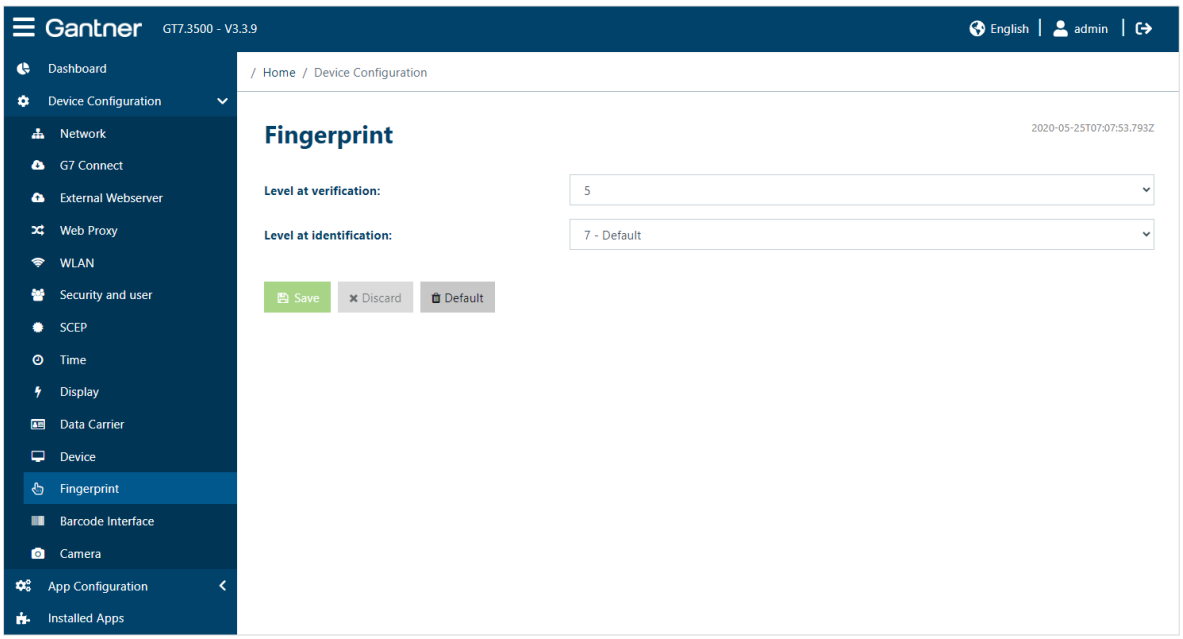


Fig. 5.34 – GT7 terminal web interface – Fingerprint

This setting is only effective 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.

5.6.14 Barcode interface

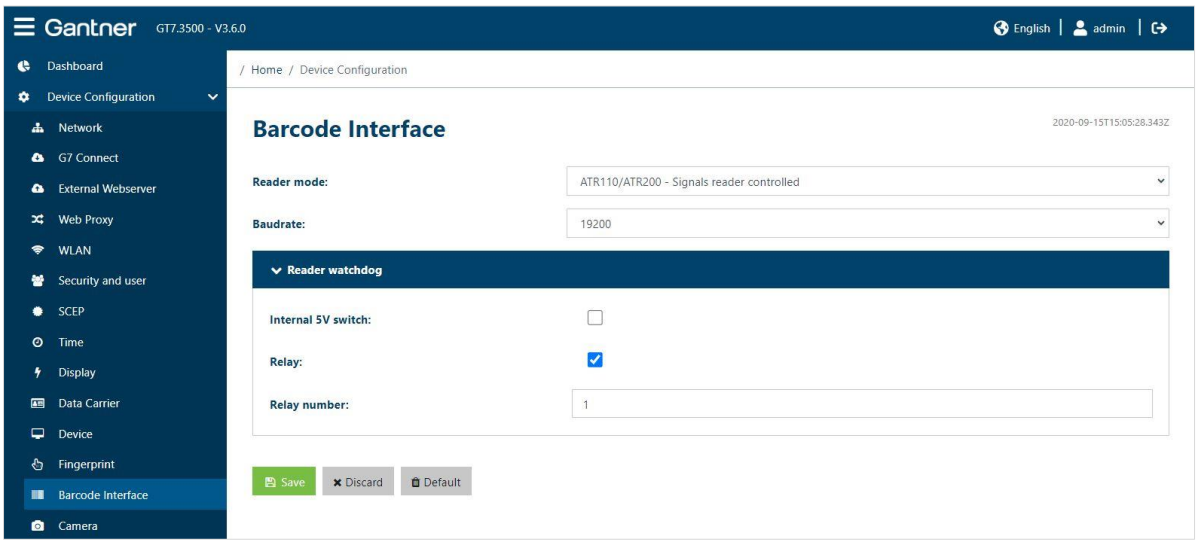


Fig. 5.35 – GT7 terminal web interface – Barcode Interface

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

- Reader mode: When a barcode reader is connected to the GT7 terminal, 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 confirmed by the management software.
  - GBS7.1xxx – Signals host controlled, USB: Setting for the GBS7.1xxx barcode reader from Gantner. Select this setting when the barcode reader is connected via the USB interface (see “4.6 USB barcode interface connection”). The signaling on the barcode reader is not set until the approval or rejection is confirmed by the management software.
- Baudrate: 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).

5.6.15 Sub controller

This menu is only displayed if an app that uses the sub controllers, such as the G7 Main Controller app or the G7 Central Locker app, is installed in the controller.

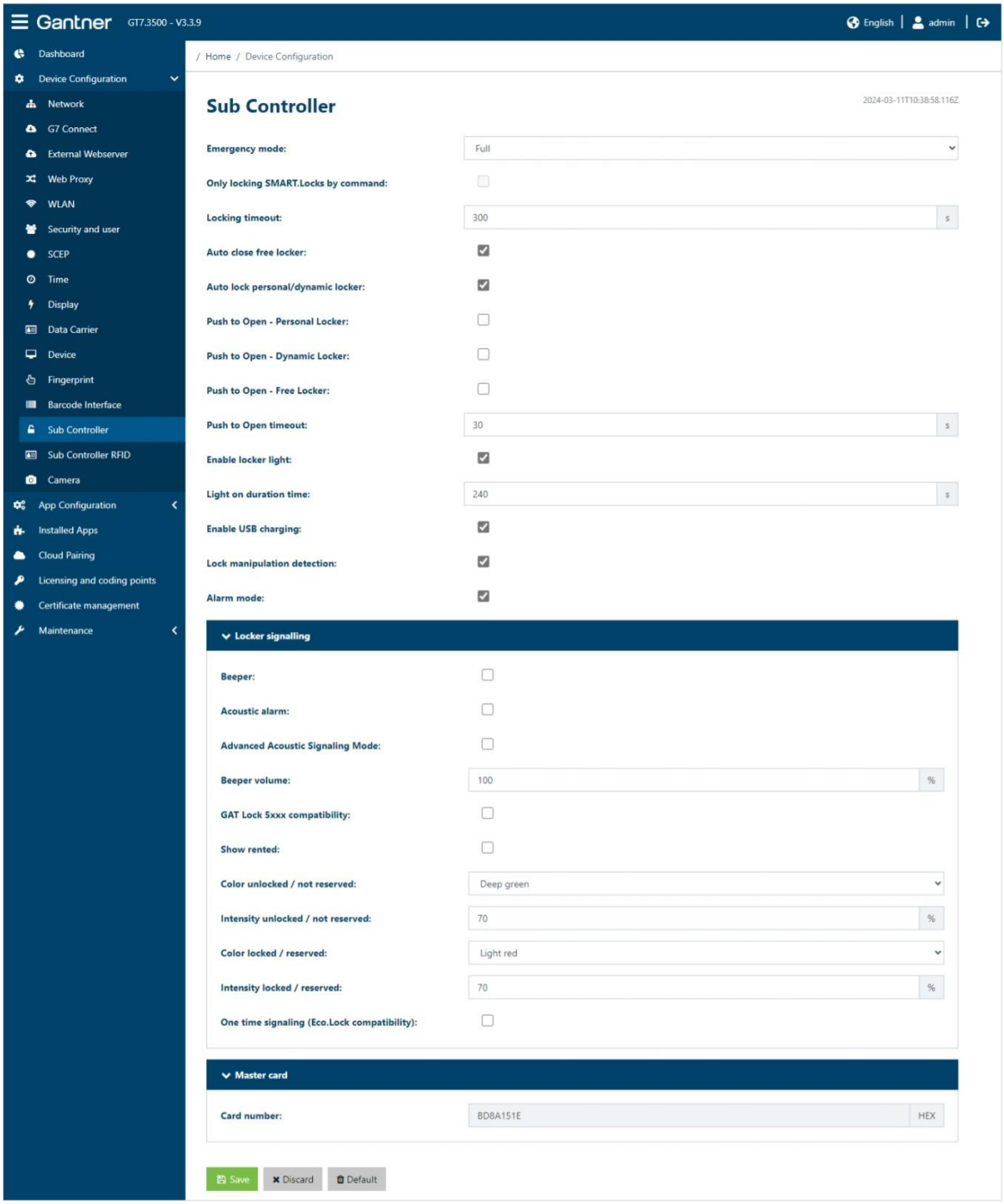


Fig. 5.36 – GT7 terminal web interface – Sub controller

These settings apply to the sub controller connected to the GT7 terminal.

- Emergency mode: These settings determine how the sub controllers behave with the lockers when the connection between the GT7 terminal and the host software (e.g., eLoxx Relaxx) is disconnected.
  - 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.
- 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: For the GAT NET.Lock system only. This option is set by the app and cannot be changed here. When enabled, a user can close an unoccupied free locker by pushing the locker door 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.
- Auto lock personal/dynamic locker: This option is set by the app and cannot be changed here. If enabled, personal lockers or dynamic lockers can be locked automatically when the locker door is pushed shut without needing to use 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 setting 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 used for the push to open function. Enter the time (in seconds) that a user has time after identification to go to their locker and open it by pressing the locker door. When the time has expired without opening, the door will be locked again. If you enter "0" the time is unlimited. The max. time is 255 seconds (about 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 will be switched on.
- 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 can be generated with ascending/descending pitches.
- Beeper volume: The volume of the integrated acoustic signal generator can be entered 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 option 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 option for dynamic lockers.
- Color unlocked / not reserved: From the menu, select a 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 cabinet door, which is used when the cabinet 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 a color that you want the lock LED on the locker door to indicate when the locker is not available (locked or reserved).
- Intensity locked / reserved: Here you can set the brightness of the lock's LED indicator on the cabinet door, which is used when the cabinet is not available (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

Four MASTER data carriers can be defined for the sub controllers. To do this, enter the card numbers in the "Card number" fields. MASTER data carriers can be used, e.g., to open a locker for which the user data carrier has been lost.

5.6.16 Sub controller RFID

This configuration page is only displayed if an app is running that also uses sub controllers (e.g., G7 Central Locker App or G7 Main Controller App).

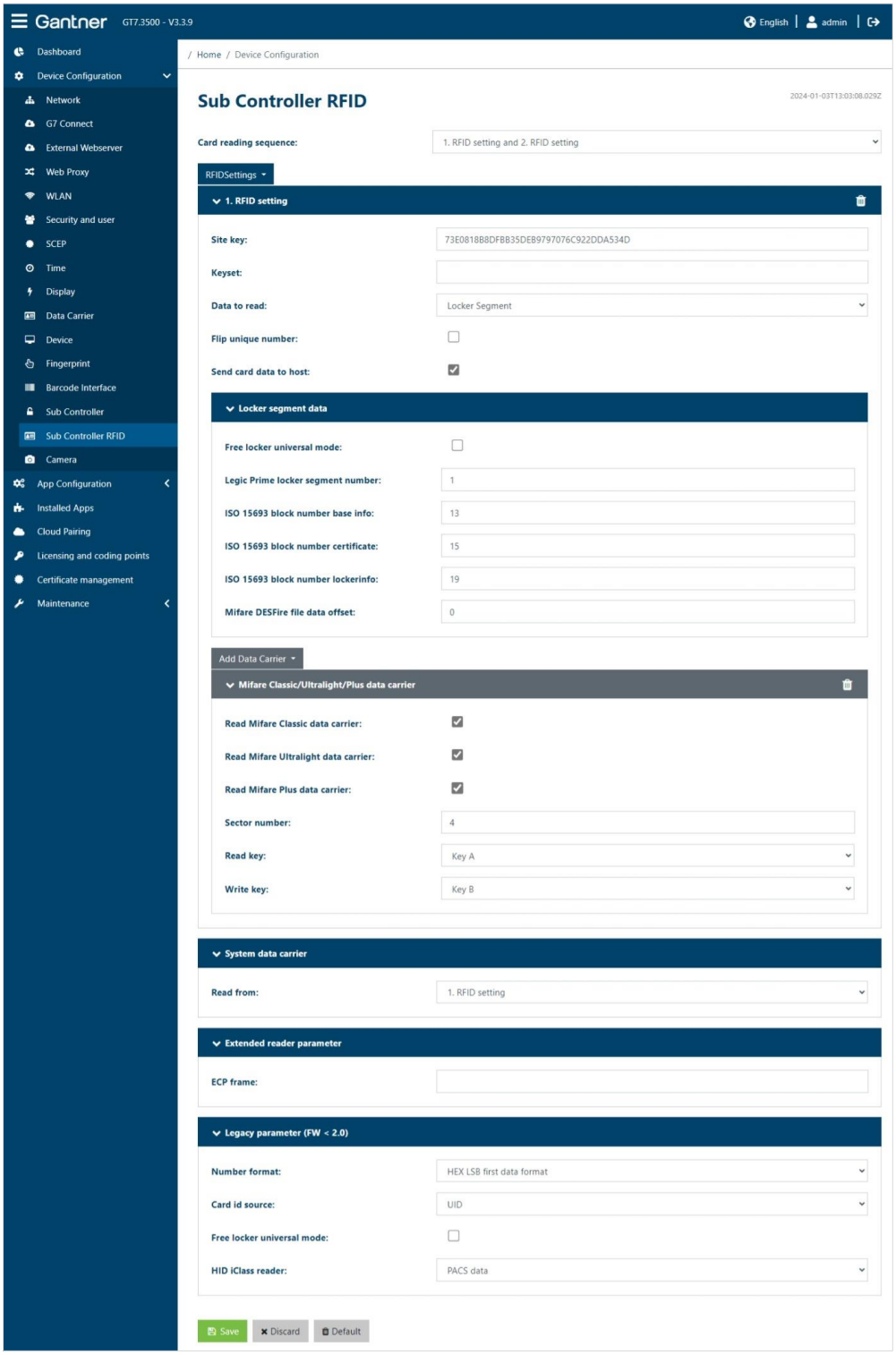


Fig. 5.37 – GT7 terminal web interface – RFID settings for sub controller

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 are to be read at the GAT NET.Lock 7020 locks can be defined.

- Card reading sequence: Two separate RFID configurations can be defined (see below) thereby allowing the use of two different data carrier types. With the setting "Card reading sequence", you can define how the two RFID configurations are to be used.
  - "1. RFID setting and 2. RFID setting":
    Both RFID configurations are treated 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 reading of data carriers is attempted first using the first RFID configuration. If this is unsuccessful, the second setting is used.

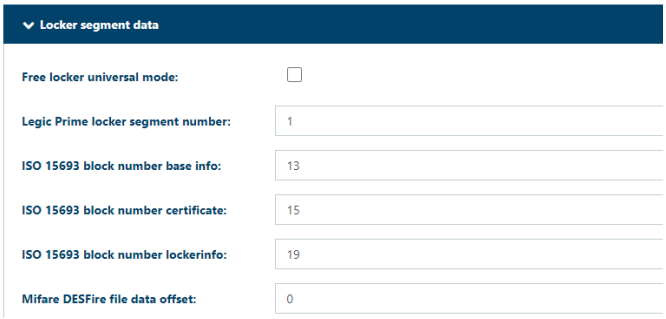
RFID settings

Click on the "RFID settings" menu to add the settings blocks for the 1st RFID setting and the 2nd RFID setting.

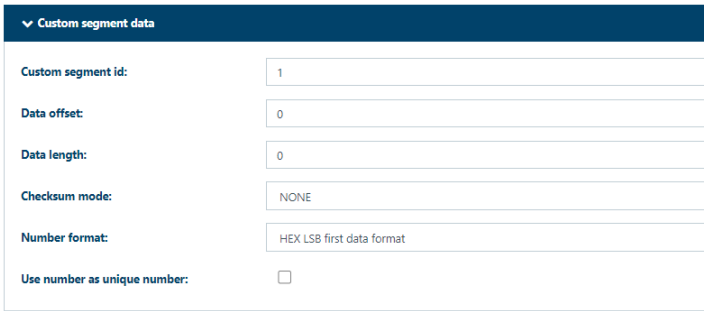
By clicking on the arrow on the left, the blocks with the settings can be collapsed and expanded. The order of the two RFID setting blocks can be changed by clicking on the arrow on the right. The setting block can be deleted again by clicking on the trash can symbol.

The following settings are possible:

- 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. With this setting, the "Locker segment data" section is displayed, in which you can specify the settings for the locker segment:



- 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.



- Flip unique number: With this setting, the unique number read from the data carriers is flipped, i.e. MSB-LSB becomes LSB-MSB.
- Send card data to host: You can use this button to insert different data carrier technologies (LEGIC, MIFARE, etc.) that are to be used with the respective RFID setting. Additional settings can then be defined for each technology. These are different for each technology and depend on the facility in which they are to be used. Ask your sales partner or service technician for the correct settings.

System data carriers

- Read from: With this setting you determine 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).

Legacy parameter (FW <2.0)

These settings are valid for older devices with firmware versions lower than 2.0.

- Number format: Here you can set how the card number is encoded on the data carrier or how it should be treated.
- 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: For this mode, the data carriers must be encoded accordingly. Mark this option if this mode is used.
- HID iClass reader: This setting is only required if you use HID iClass data carriers.

5.6.17 Camera

This configuration page is only displayed for the GT7.3xxx terminals when the optional camera is installed.

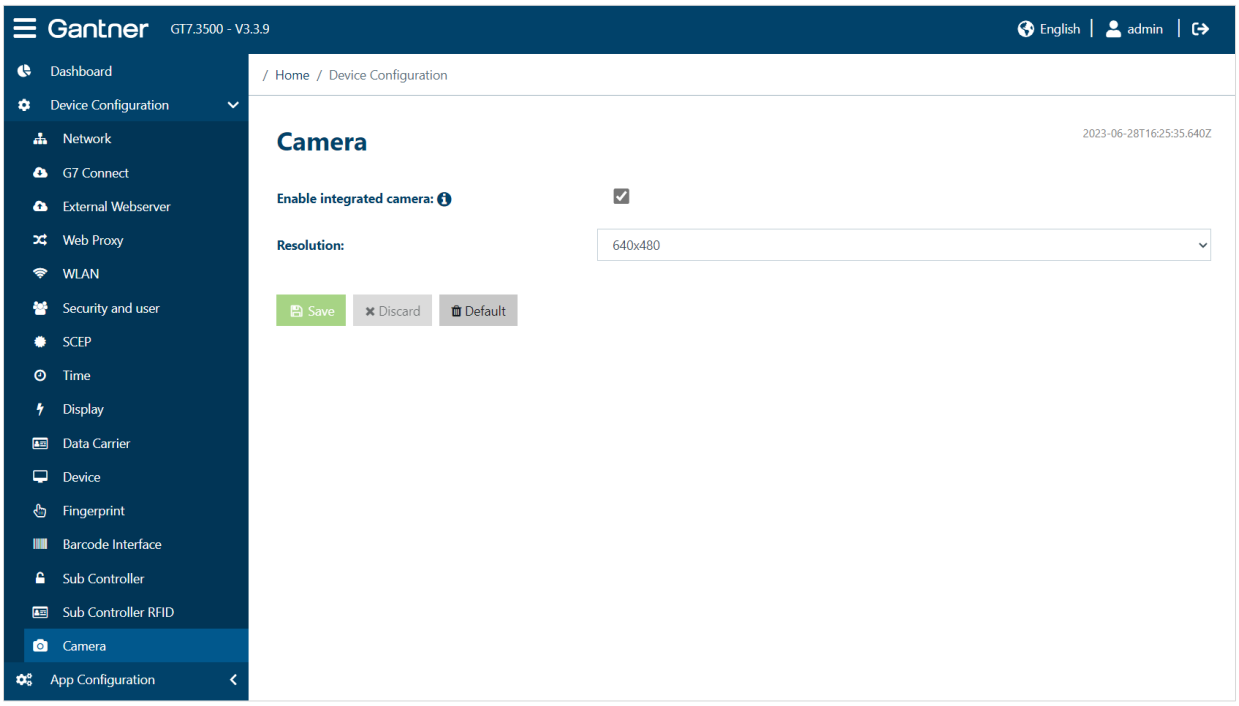


Fig. 5.38 – GT7 terminal web interface – Camera

- Enable integrated camera: Enable this option to turn the camera on (disabled by default).

  NOTE! Ensure that the relevant data protection regulations are adhered to when operating the camera.

- Resolution: Select the desired camera resolution from the menu.

5.6.18 App configuration

The settings pages displayed in the "App Configuration" section of the GT7 web interface apply to the app currently running on the GT7 terminal. Only one app can be active at a time. If another app is to be run, you can activate and start it in the "Installed app" menu item. See "5.6.19. Installed apps".

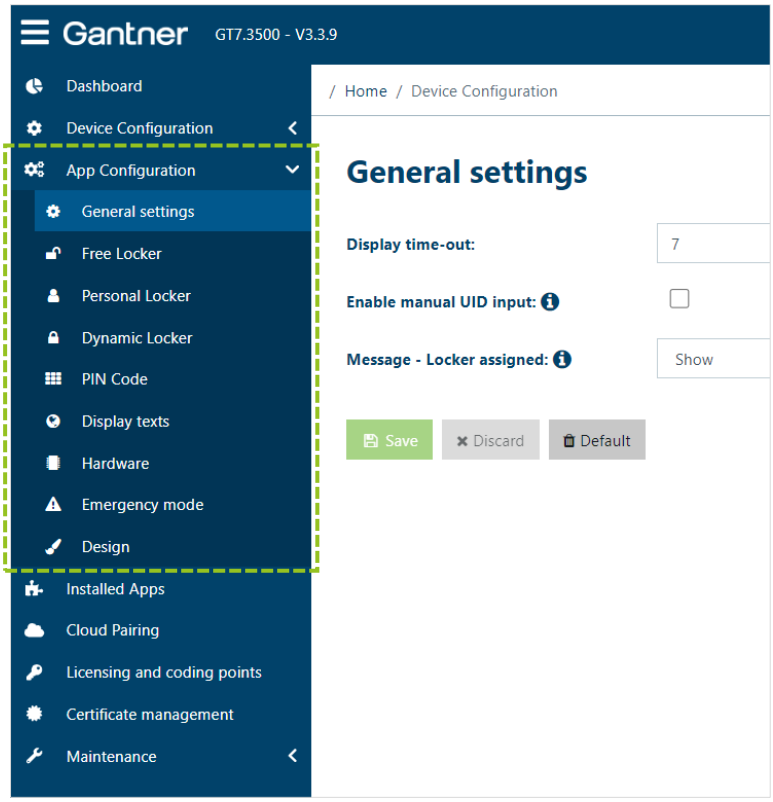


Fig. 5.39 – GT7 terminal web interface – App configuration

As the settings pages shown in the sidebar to the left are app specific and vary depending on which app is running, these settings are described in the manual of the respective app. Please read this documentation for more information.

5.6.19 Installed apps

Different apps can run on the GT7 terminal (only one at a time, i.e., not several at the same time). License points are required to activate some apps, and these are available to purchase from Gantner. When you order license points from Gantner, the desired number of points are transferred to your organization in G7 Connect. From then on, you can transfer the points to the projects and then on to individual devices as required.

For a detailed description of how to transfer license points in G7 Connect, see the G7 Connect manual.

The following table lists all apps currently available for the GT7 terminal, their function, and the required license points.

App	Function	License Points
G7 Access App (default app)	For access control to an area separated by a door or turnstile, etc. Access is granted or denied after identification with the user's data carrier, fingerprint, or barcode.	0
G7 Advanced Access App	Enables the standard access app functions as well as other additional functions such as an authorization list, support for multiple GR7 readers on a GT7/GC7 or coding of MIFARE Classic data carriers.	30
G7 Customer Feedback App	Allows customers to complete a survey or enter feedback via the touchscreen. Feedback can be entered anonymously or personalized with the customer's data carrier.	0
G7 Countdown App	Displays a configurable countdown timer (e.g., 5 mins) to show the user when the use of a time-limited device, such as a shower or power plate, will expire.	0
G7 Info App	For the display of customer information after their data carrier is read. The information displayed is configurable, e.g., the customer's locker number or the validation date.	20
G7 Time App	For the control of time-controlled devices, e.g., sunbeds. A timer is activated, and the device switches on for the set time after the customer's data carrier is read. The cost for use can also be displayed.	30
G7 Enrollment App	For the enrollment of fingerprint data to store a fingerprint template on the user's data carrier (used for fingerprint verification during identification processes).	40
G7 Time & Attendance App	Allows the flexible acquisition of personnel time and attendance information, and the display of employee time accounts after valid identification on the GT7.	40
G7 Central Locker App	Allows the device to operate as the central reader and control device in a networked locker system.	50
G7 ECO Lockpal Registration App	Allows you to authorize the ECO LockPal App for the smartphones of a specific system. This app allows users to use lockers that are controlled by Gantner battery locks. The app is authorized via a QR code shown on the display.	40
G7 Main Controller App	Allows you to control the Gantner electronic locker locks. The app is usually only installed on a GC7 controller.	0

Table 5.1 – App functionality and required license points

There are also some extensions for the apps. The extension "G7 Open Card" can be used to disable certificate checking on the GT7 terminal so that third-party data carriers can work with the device. G7 Open Card requires 10 license points and can be applied to apps with 0 license points.
On the "Installed Apps" page of the GT7 web interface, all installed apps are listed with the currently active app indicated by the green "Active App" text.

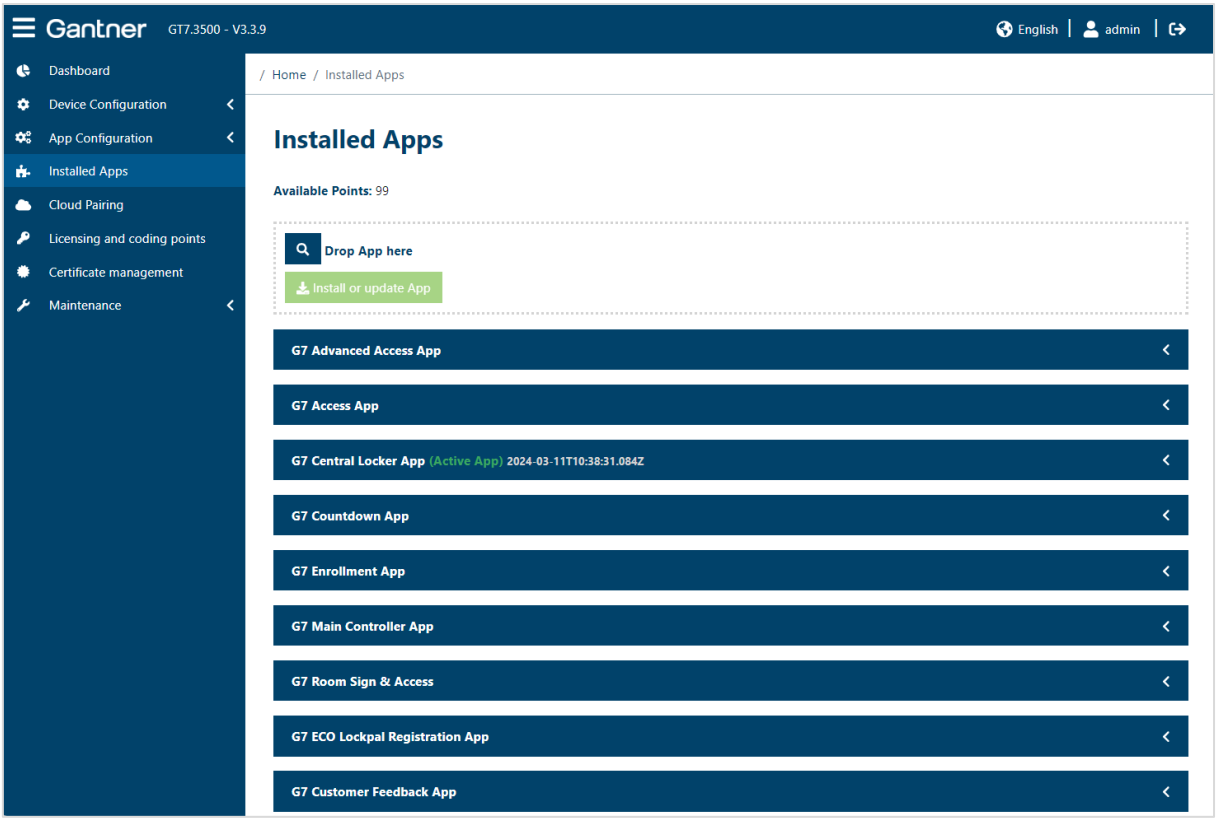


Fig. 5.40 – GT7 terminal web interface - Installed Apps

- ► 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 currently active app is automatically stopped.
- ► In the upper "Drop App here" field, additional apps can be loaded into the GT7 terminal. To do this, the app file is needed.
- ► An app can also be assigned a theme (Design Template). To do this, drag a theme file (ZIP file) from Windows Explorer directly into the "Drop Theme here" box.

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 terminal's screensaver function (see "5.6.10. Display"). The images are located in the screensaver subfolder in the archive file.

5.6.20 Cloud pairing

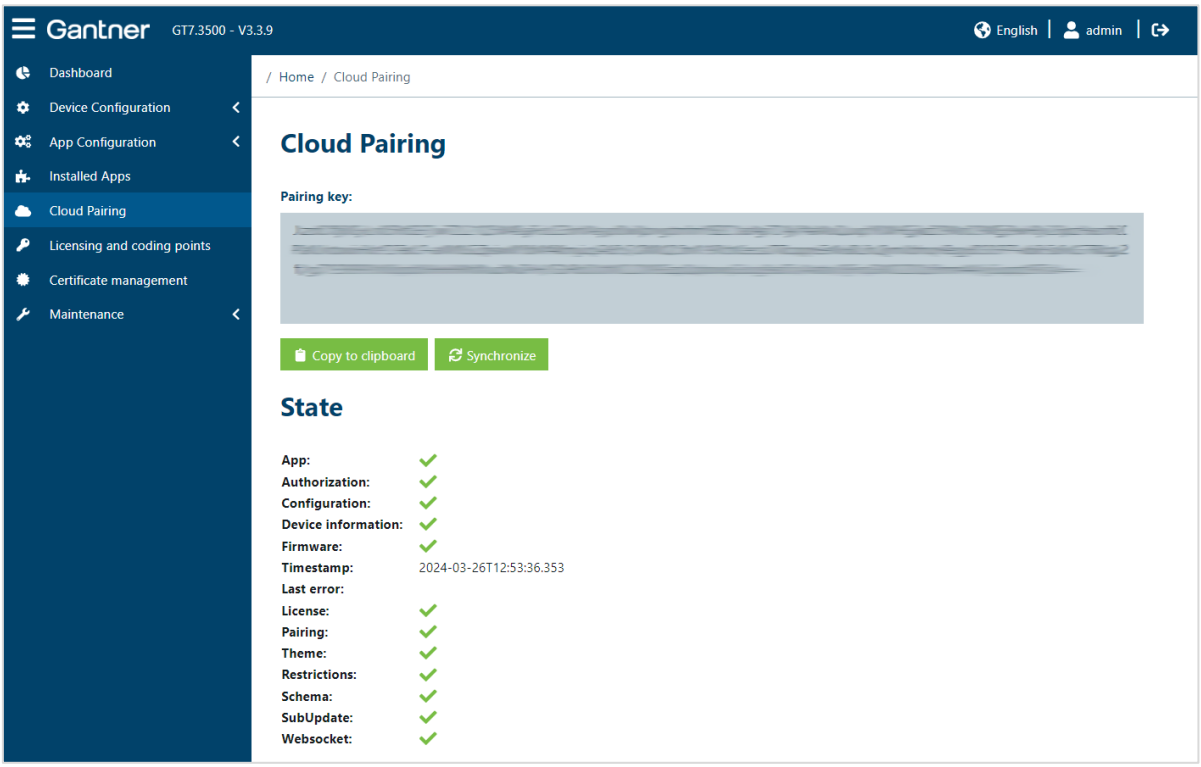


Fig. 5.41 – GT7 terminal web interface - Cloud Pairing

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.
  - o The home page ("Dashboard") is displayed.
- ► Click on "Projects".

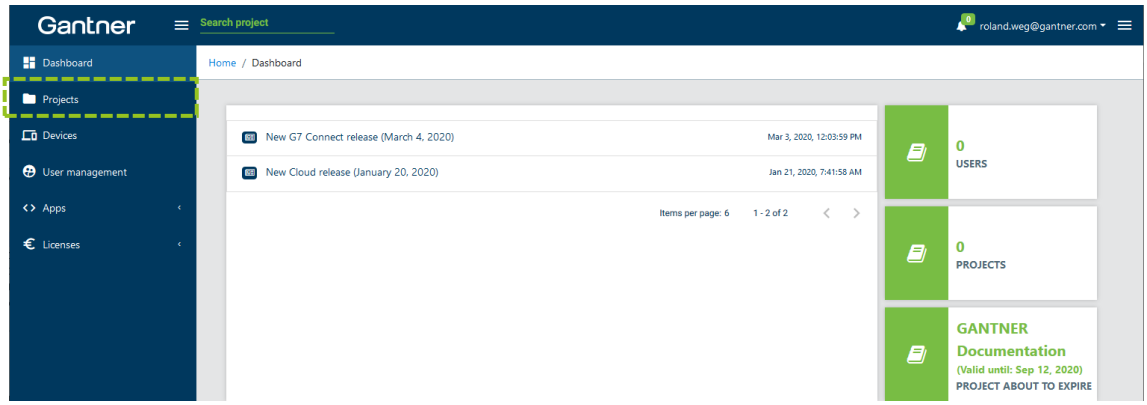


Fig. 5.42 – Cloud pairing – Dashboard

  - o Your available projects are displayed.

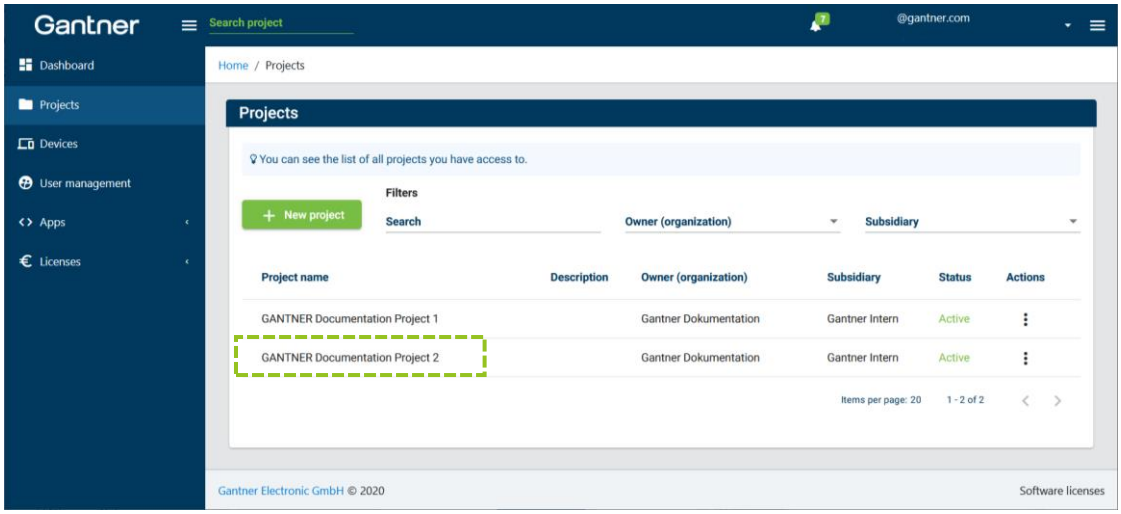


Fig. 5.43 – Cloud pairing – List of available projects

► Click on the project where the GT7 terminal is to be added.

► Click on “Device pairing”.

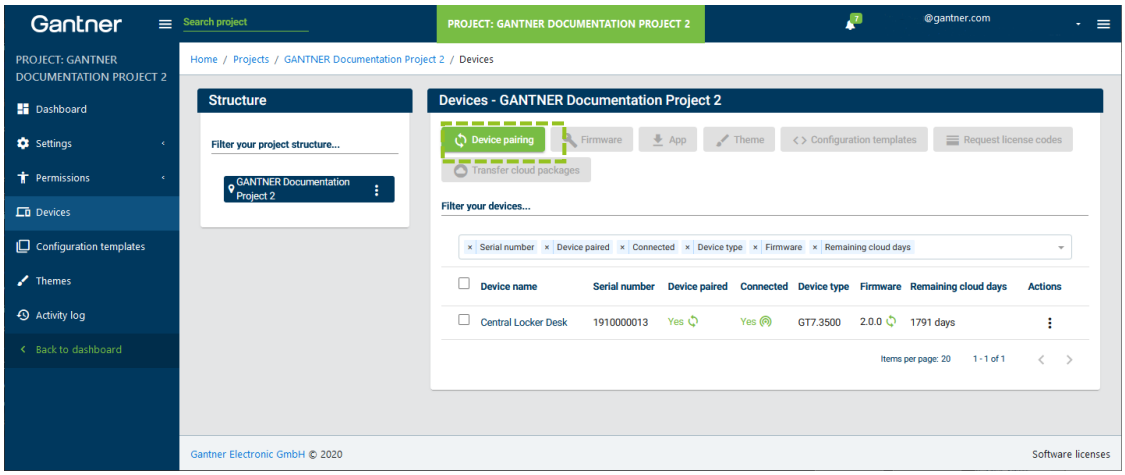


Fig. 5.44 – Cloud pairing – GT7 pairing

- A new window is displayed.

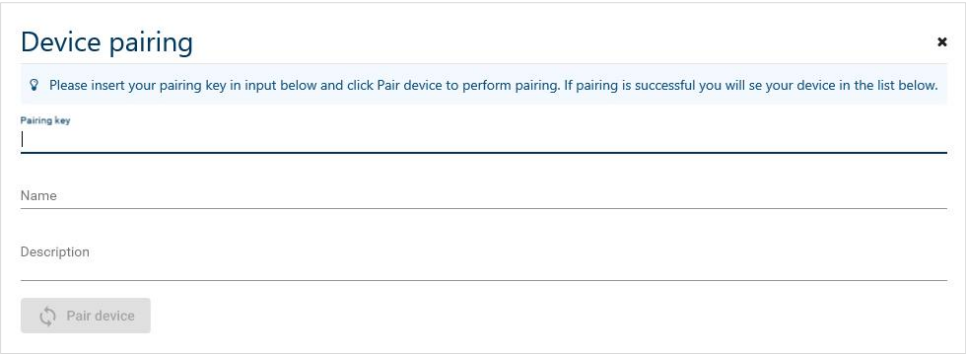


Fig. 5.45 – Cloud pairing – Enter pairing key

- Enter the pairing key, as displayed in the “Cloud Pairing” menu, into the configuration of the GT7 terminal.
- 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 terminal with the matching pairing key is searched for. This requires the GT7 terminal to be powered on and online, i.e., it must have an outgoing connection to the Internet (G7 Connect). Check the connections and firewall settings if pairing is unsuccessful.
  - When the GT7 terminal is found, it is displayed in the devices list of the project.
  - The status of the pairing process is displayed in the web interface. After pairing is completed, the different states are shown where you can see whether an update is required. For example, a red ”X” after ”Firmware” indicates that the firmware in the device is not up to date and a red ”X” after ”License” indicates that there are no license points in the device.

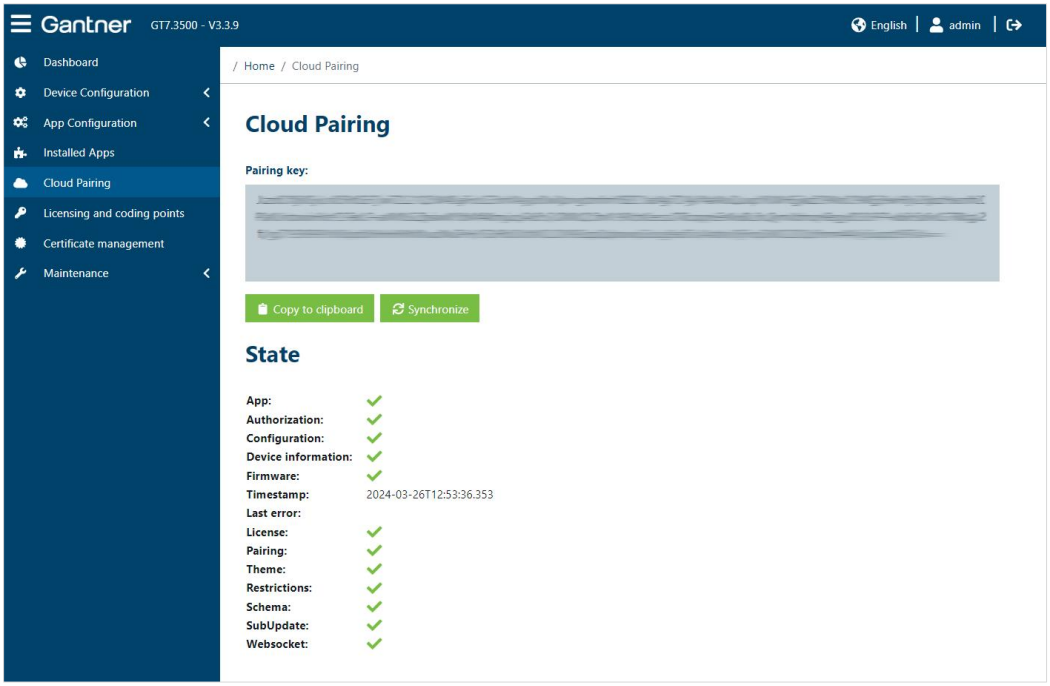


Fig. 5.46 – Cloud pairing – Status of the pairing process

5.6.21 Licensing and coding points

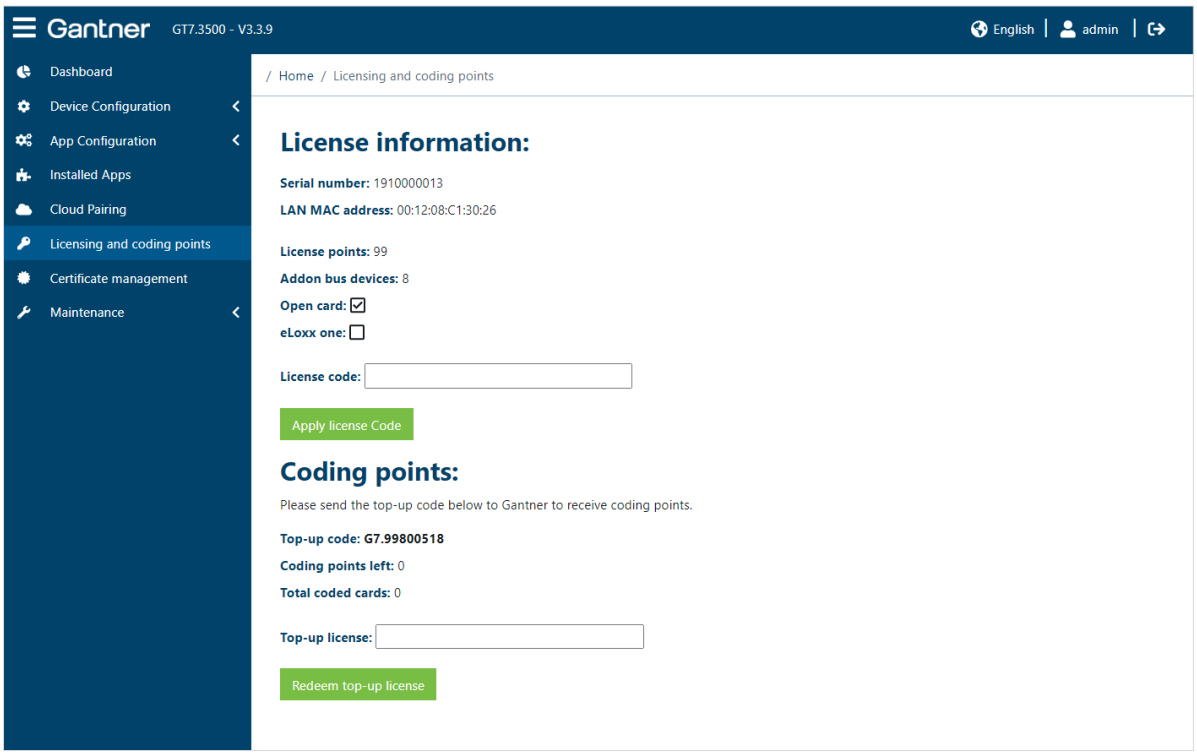


Fig. 5.47 – GT7 terminal web interface – Licensing and coding points

On this page, the network and license information for the GT7 terminal are displayed and you can also add new license points here. You can also add coding points, which can then be used to encode data carriers using the corresponding GT7 app.

License information

- Serial number:	The serial number of the GT7 terminal.
- LAN MAC address:	Unique, internal network address of the GT7 terminal.
- 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 terminal.
- Open card:	This field indicates whether the “Open Card” license is enabled. If the license is enabled, the certificate check is switched off, i.e., data carriers that were not supplied by Gantner can also be used.
- eLoxx One:	If the license for the eLoxx One software is activated, this field is marked with a tick. The eLoxx One can then be started in the overview (start screen).
- License code:	A license code for the installation of additional apps or to activate additional functions can be entered here.

Coding points

- Top-up code:	You can use this code to request the desired number of coding points from Gantner Electronic GmbH.
- Coding points left:	Here you can see how many coding points are currently still available in the terminal. As soon as you add new coding points using a top-up license, the new coding points are added here.
- Total coded cards:	The number of data carriers already encoded is displayed here.
- Top-up license:	If you request coding points from Gantner using a top-up code, you will receive a license code that you enter here. You can activate the coding points by clicking on "Redeem top-up license". These are then added to the "Coding points left" counter.

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

5.6.22 Certificate management

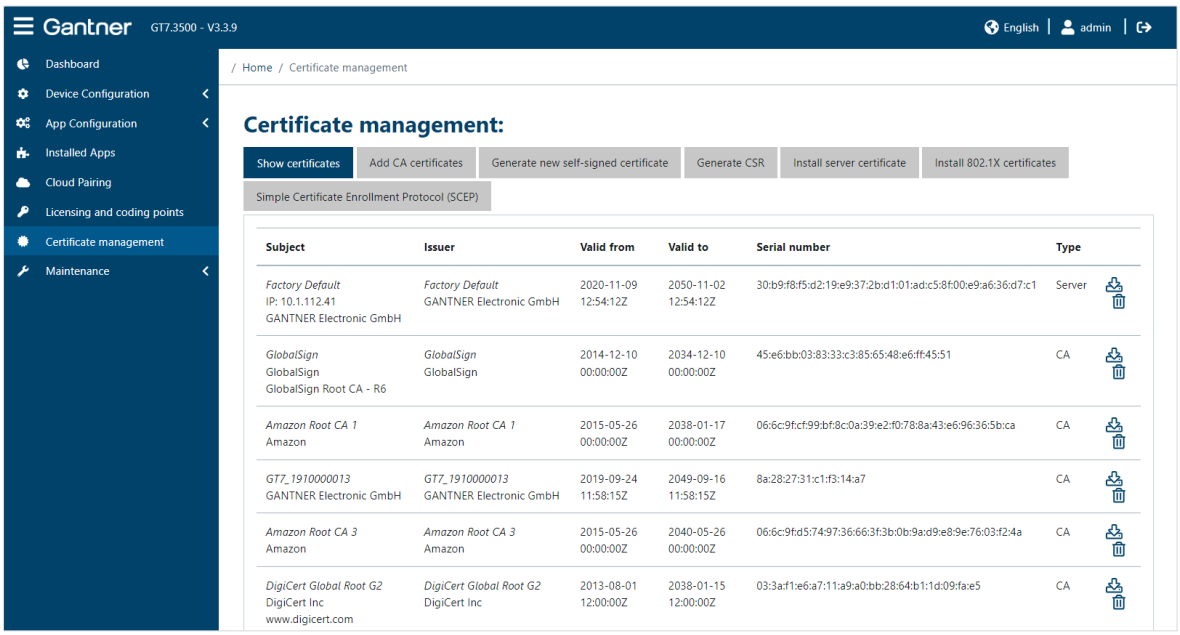


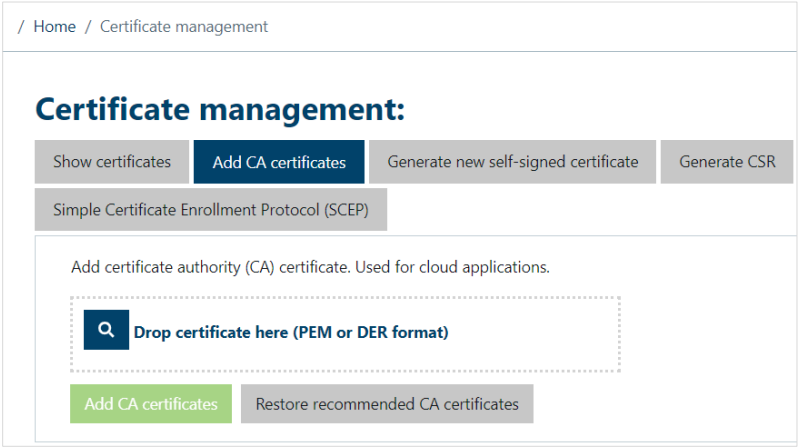
Fig. 5.48 – GT7 terminal web interface - Certificate management

Here, the certificates stored in the GT7 terminal 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 certificate". This way you can also install a certificate that was previously deleted for example.

- Generate new self-signed certificate:

  If encrypted communication between the GT7 terminal and the server is being used (via TLS over HTTPS or WSS), the GT7 terminal requires a certificate. It is recommended that you use a certificate issued by a certification authority. Alternatively, you can create a certificate yourself by clicking on “Create new self-signed certificate”. The GT7 terminal 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 an 802.1X user certificate created by a certification authority, you can create a Certificate Signing Request (CSR). Enter your data, e.g., company name, country, and IP, here.

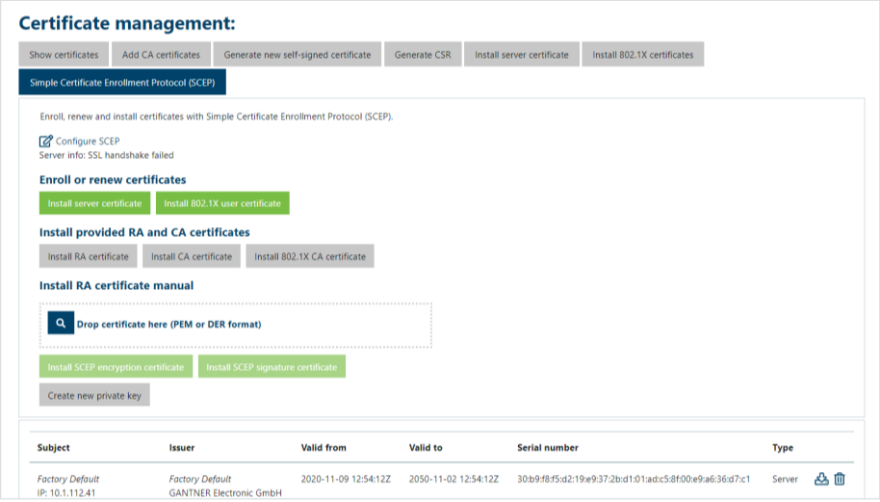
- Install server certificate: If the GT7 terminal is acting as a web server (e.g., when using eLoxx Relaxx, which acts as a “client” to establish the connection to the “server” GT7 terminal), a certificate for the server, i.e., on the GT7 terminal, is required for a secure connection via TLS. You can 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 CA certificate: 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 (SCEP):

  Certificates can be issued, renewed, and installed here using the Simple Certificate Enrollment Protocol (SCEP). The following window is displayed:



  Below the “Configure SCEP” link, the status of the SCEP connection (“Server Info”) is displayed. If “Disabled” is shown here, the SCEP function is not activated. If the SCEP function is enabled, a server notification is displayed, e.g., “Enabled” indicates a successful connection or “Host not found” if the server connection could not be established.

To enable SCEP and configure the server connection, click on the “Configure SCEP” link. This takes you directly to the SCEP configuration page in the device configuration menu. See chapter ”5.6.8. SCEP (Simple Certificate Enrollment Protocol)” for more information.

If SCEP is enabled and the connection to the SCEP server is active, you can perform the following actions:

- Install server certificate

  If the GT7 terminal is operating as a web server (e.g., when using eLoxx Relaxx, which acts as a “client” and establishes the connection to the “server” GT7 terminal, see ”5.8 Integration in eLoxx Relaxx”), a certificate is required for the server, i.e., on the GT7 terminal, for a secure connection using TLS. You can complete the installation by clicking on this button.

- Install 802.1X user certificate

  Here you can install a certificate for authentication via 802.1X.

- Install RA certificate

  Here you can install a certificate issued by a registration authority (RA).

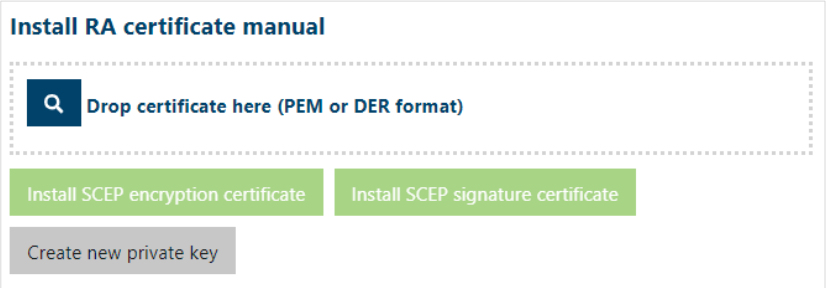
- Install CA certificate

  Here you can install a certificate issued by a certification authority (CA).

- Install 802.1X CA certificate

  This button allows you to install an official certificate from a certification authority for authentication using 802.1X.

The certificates (encryption and signature) for the registration authority (RA) can also be installed manually from a file without using the SCEP server. This can be done in the “Install RA certificate manually” section.



Drag the file with the certificate into the dotted field and click on “Install SCEP encryption certificate” or “Install SCEP signature certificate”.

5.6.23 Device maintenance

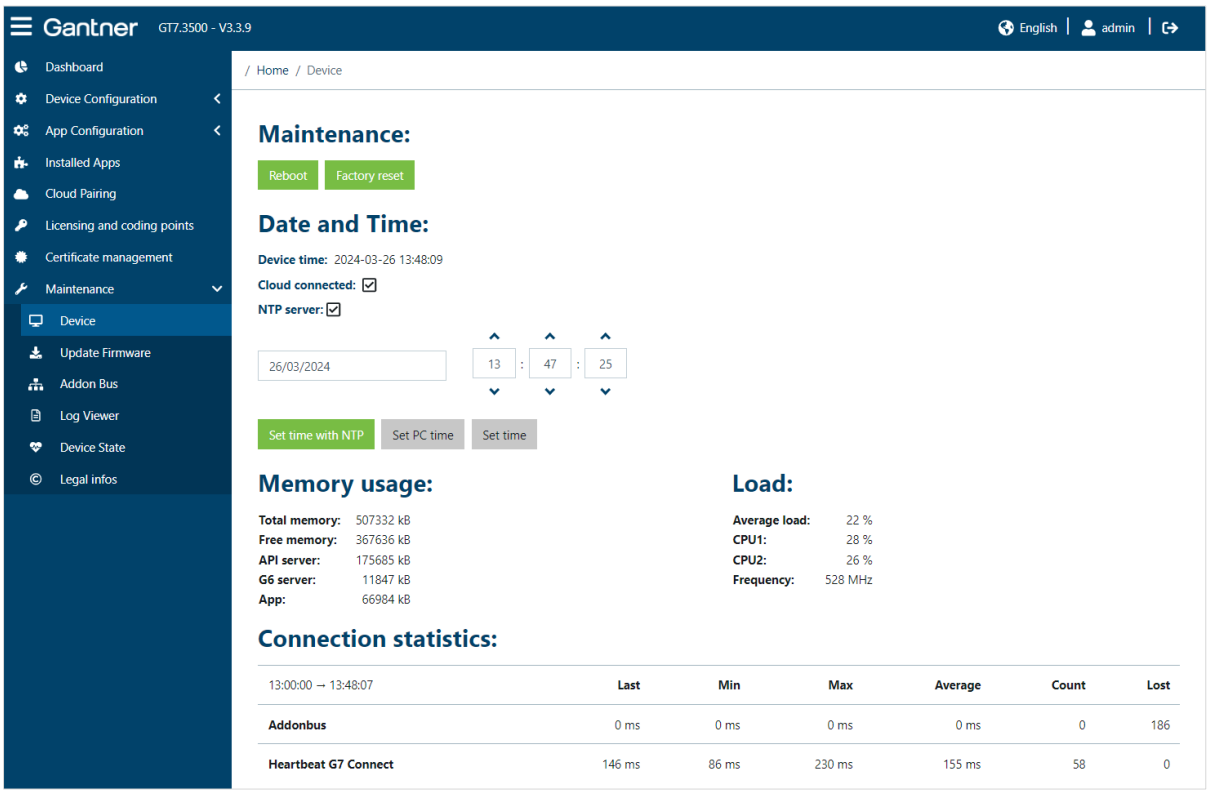


Fig. 5.49 – GT7 terminal web interface - Maintenance

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

Maintenance

- ► Click on the "Reboot" button to restart the GT7 terminal.
  - o 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 terminal to its default settings, click on the "Factory reset" button.
  ATTENTION! All settings in the device are deleted during the reset process.
  - o After resetting to the default settings, the device is in same functional state it was upon delivery.

Date and Time

- Device time:	The current time in the GT7 terminal is displayed here. This time is updated every second. The time can be changed in the device configuration (see "5.6.9 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 "5.6.3. G7 Connect").
- NTP server:	This setting defines whether an NTP server is used for automatic time synchronization in the GT7 terminal (tick = enabled). The setting for using an NTP server is provided in the configuration menu of the GT7 Central Locker (see "5.6.9 Time").

► To reset the time in the GT7 terminal, 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 terminal.
- 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 terminal.

Memory usage

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

Load

These values show how much the processor cores of the GT7 terminal are being used. The frequency refers to the clock frequency of the processors. These values are mainly of interest to maintenance personnel.

Connection statistics

Displayed here are the connection statistics of the system components that interface with the GT7 terminal.

5.6.24 Update firmware

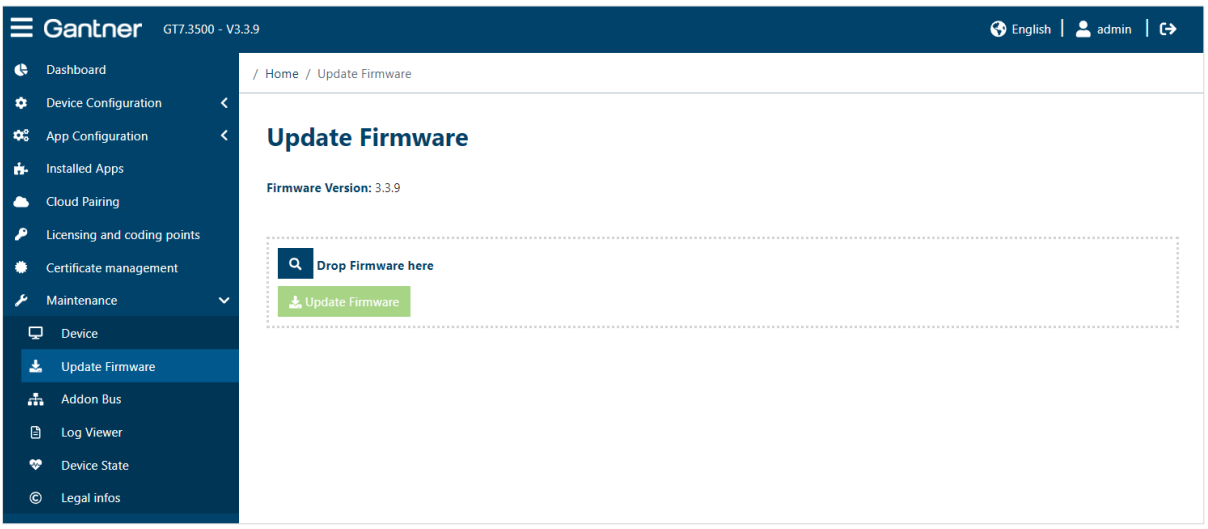


Fig. 5.50 – GT7 terminal web interface – Update firmware

Here, the firmware currently installed in the GT7 terminal is displayed.

- ► To install new firmware, drag the firmware file to the "Drop Firmware here" field.
- ► Click on "Update Firmware".
  - o The new firmware is loaded into the GT7 terminal and the device restarts.
    ATTENTION! During the firmware update, ensure that the power supply to the GT7 terminal is not disconnected.

5.6.25 Addon bus (external devices)

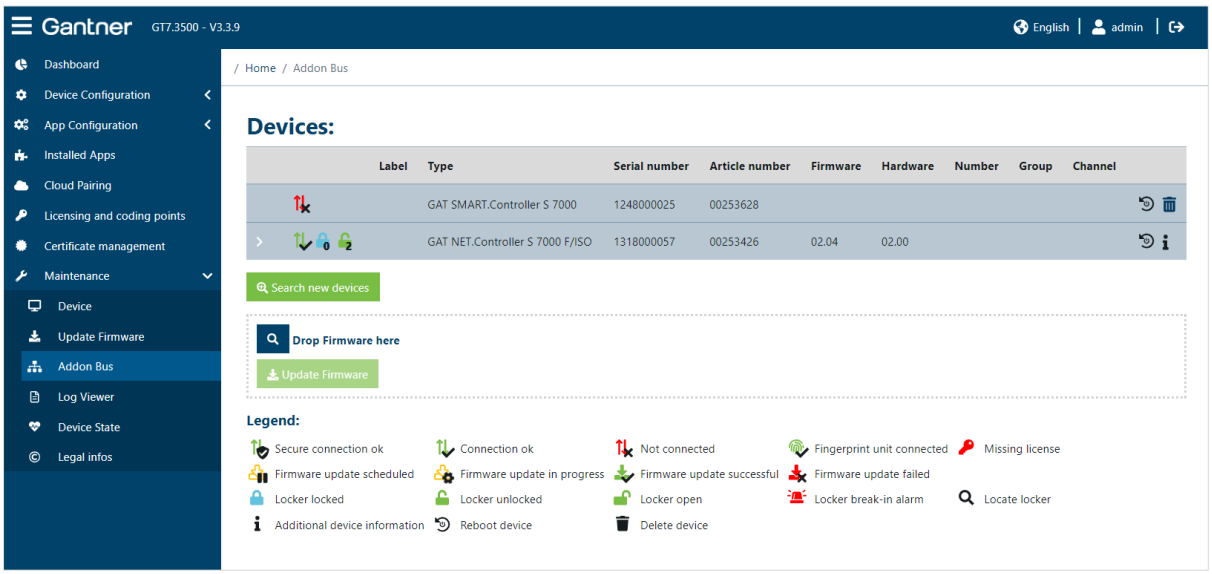


Fig. 5.51 – GT7 terminal web interface – Addon Bus

Information about the external devices connected to the GT7 terminal 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 hides the list.

- ► To search for new devices that were connected to the GT7 terminal, click on “Search new devices”.
  - o The terminal searches for new devices at the addon bus and shows them in the list. This may take one minute.
- ► To install new firmware for the devices, drag the firmware file to the “Drop Firmware here” field.
- ► Click on “Update Firmware”.
  - o The new firmware is loaded to all devices of the appropriate type and the devices are restarted. **ATTENTION!** During the firmware update, ensure that the power supply to the external device and the connected device are not disconnected.

5.6.26 Log viewer

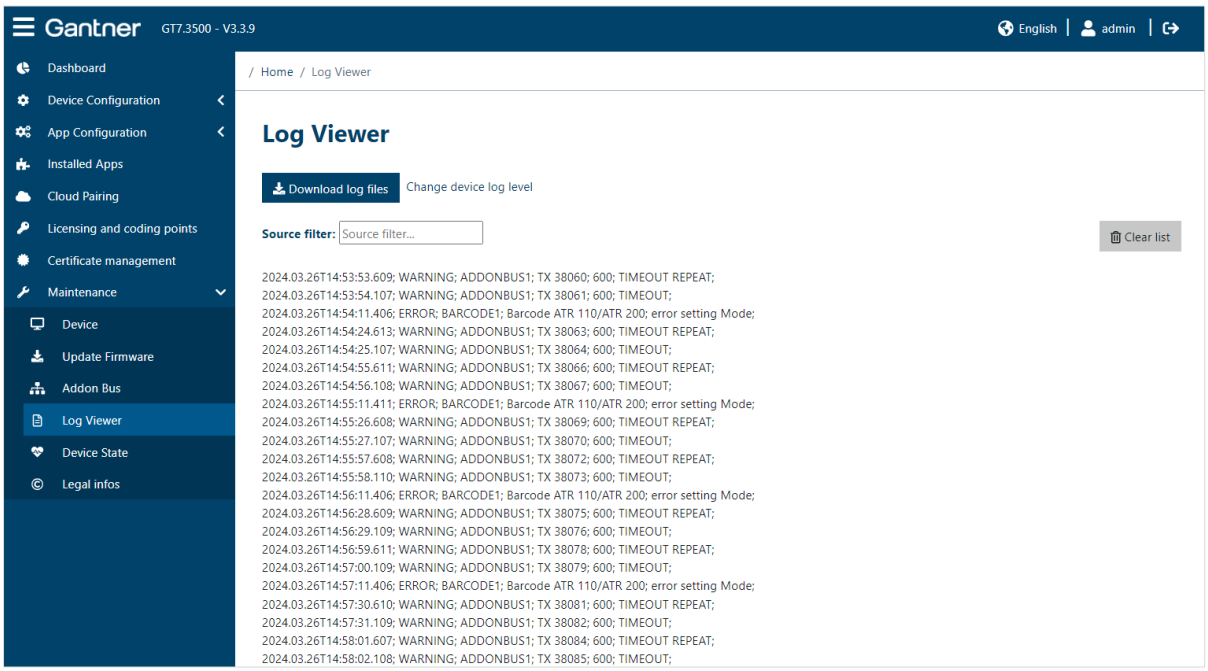


Fig. 5.52 – GT7 terminal web interface – Log Viewer

All events such as door openings, data carrier identifications, and even error messages are recorded by the GT7 terminal and 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 terminal, 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.

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 ”5.6.12 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.).

5.6.27 Device state

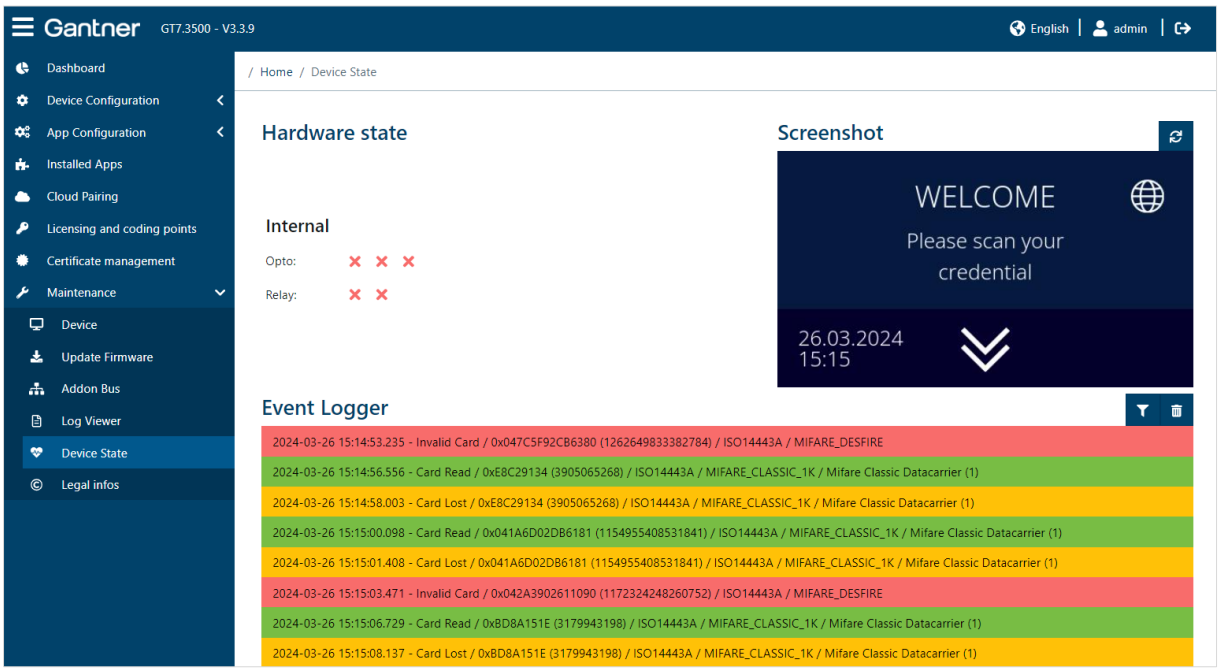


Fig. 5.53 – GT7 terminal web interface – Device State

Depending on the model, a GT7 terminal has either one or 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 hardware state is the screenshot function for the GT7 terminal.

► 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 terminal (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 .

5.6.28 Legal information

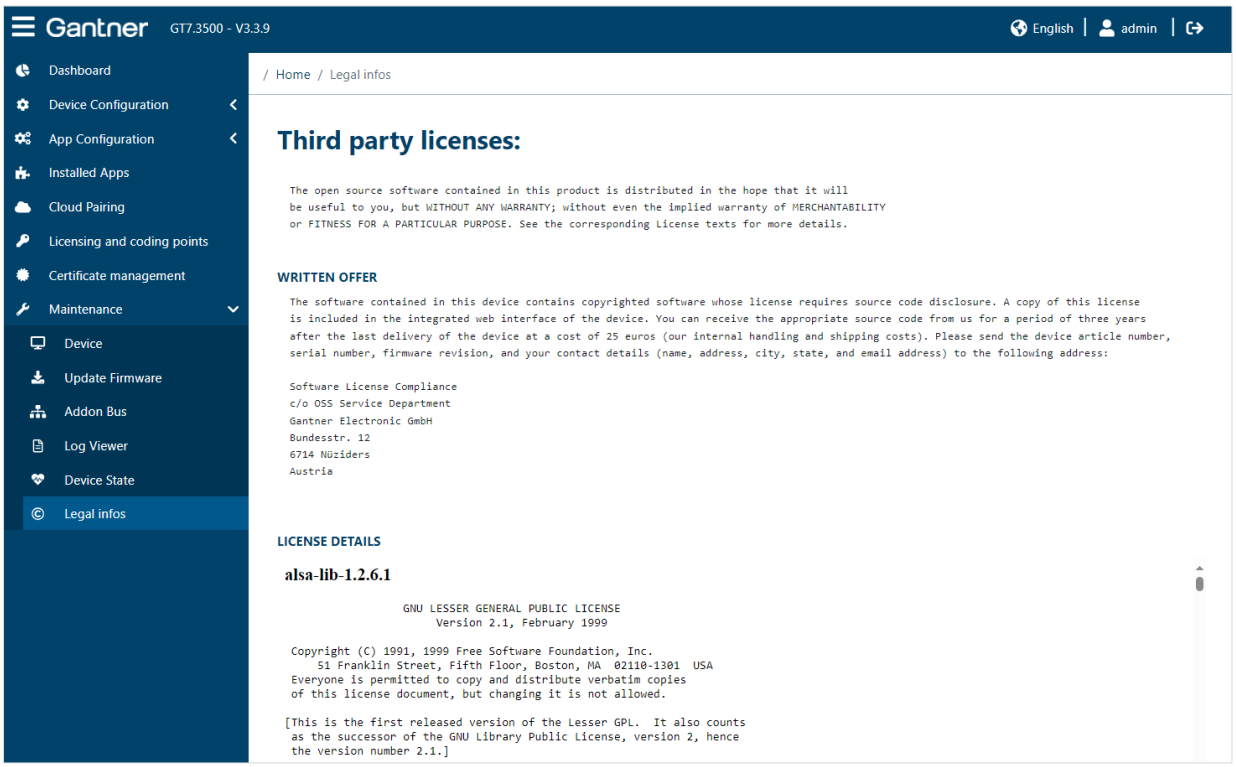


Fig. 5.54 – GT7 terminal web interface – Legal Info

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

5.7 Authorizing the GT7 terminal

In systems that use LEGIC advant RFID technology with specific access to protected data, the GT7 terminals must be authorized once to allow the terminal to access (write to) the protected data areas of the data carrier. The authorization process is completed using the GAT Authorization Tag 400 BA card (Part No. 368029).

The use of GAT Authorization Tag 400 BA requires special care to maintain system securtiy. As such, Gantner requires an assumption of liability form to be signed when ordering. Speak to your Gantner representative for details.

- ► To authorize a terminal, hold the GAT Authorization Tag 400 BA for your system next to the reader until the authorization process is completed (approx. 15 seconds).
  - During authorization, the circular LED flashes red and green alternately.
- ► The read authorization data are displayed in the web interface under “Maintenance” > “Device”.

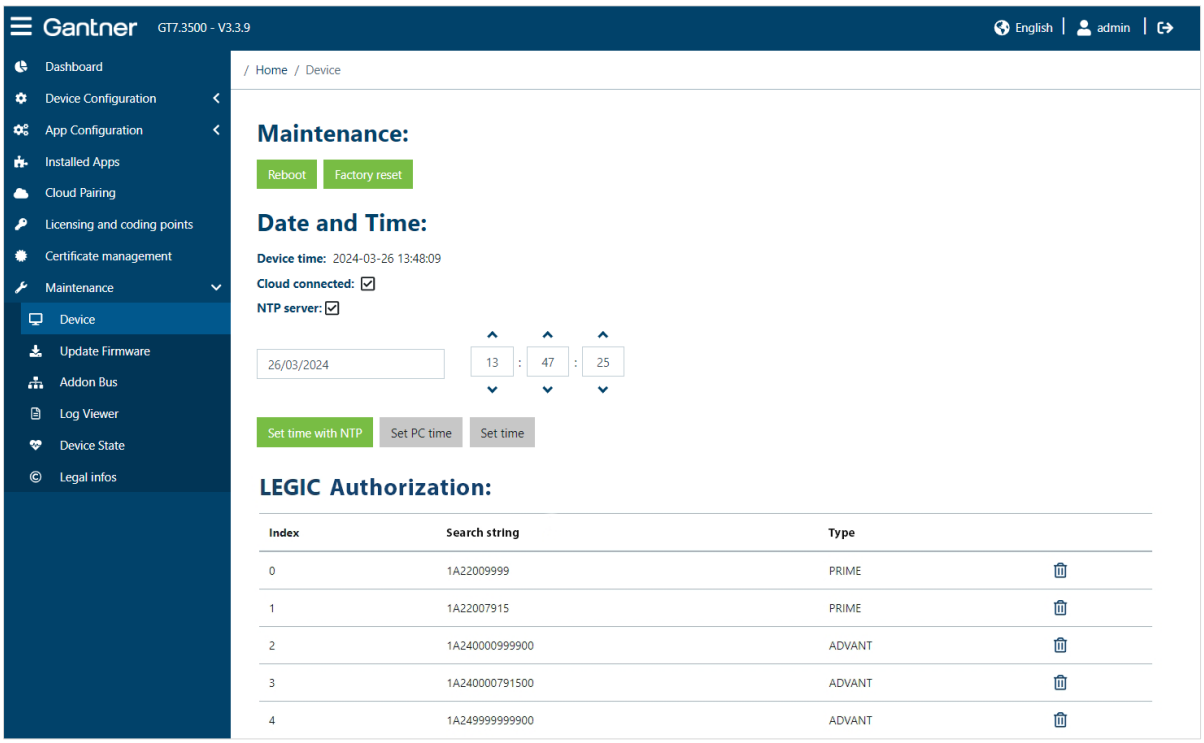


Fig. 5.55 – Web interface – LEGIC authorization data

- ► To delete the authorization data, click on the trash can symbol next to the respective data.

5.8 Integration in eLoxx 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 terminal can be integrated into the eLoxx Relaxx management software.

A detailed description of eLoxx Relaxx is provided in the "Operation Manual", which is available to download from the Gantner website (login required).

Basically, the following steps are necessary:

1. Add your GT7 terminal (Central Locker, Info, Access) to eLoxx Relaxx
2. Configure the terminal depending on its application
3. Authorize the users

Adding a GT7 terminal to eLoxx Relaxx

NOTE! Before adding the GT7 terminal, it is important that the terminal already has the desired app enabled (e.g., Central Locker, Info, Access), and that this app is the active app.

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

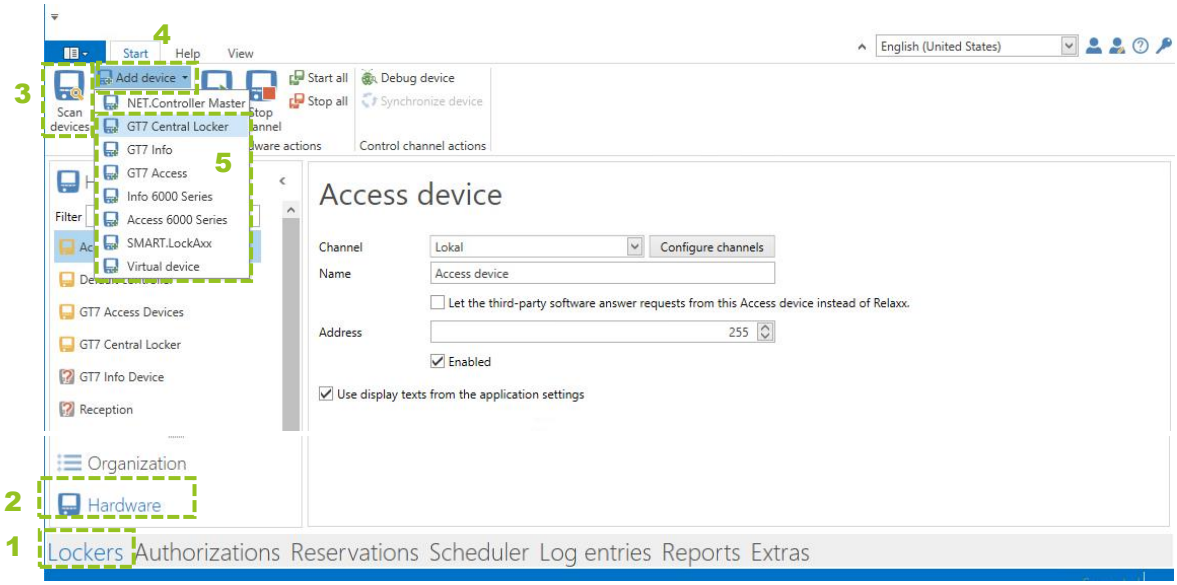


Fig. 5.56 – Adding a new GT7 terminal to eLoxx Relaxx

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

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

6 MAINTENANCE

⚠CAUTION

Electrical Shock

Touching current-conducting parts may result in injury due to electrical shock.

- Always disconnect the power supply before working on the device or installation/deinstallation.
- The applicable safety and accident prevention regulations must be observed.
- Carefully observe the measurement diagrams and technical specifications.
- Do not remove safety protection and covers.

The GT7 terminal does not require regular maintenance for operation; however, it is recommended to periodically clean the device and update the apps and device firmware (see "5.6.24. Update firmware").

Also refer to the Gantner document "Cleaning and care instructions" for detailed instructions.

6.1 Target group

This chapter contains information for the service technicians and cleaning personnel, who clean and maintain the GT7 terminal. Previous knowledge of the GT7 terminal or other Gantner devices is not required.

6.2 Cleaning

Periodically cleaning the GT7 terminal ensures that the device can perform its intended function properly and trouble-free operation is possible.

ATTENTION! Do not use cleaning agents that contain solvents, alcohol, surfactants, acids or abrasive ingredients. In addition, the components of the GT7 terminal must not be cleaned with a high-pressure or steam cleaner, or otherwise they could be damaged! Water or liquids must not penetrate the housing of the GT7 terminal.

Follow these steps to clean the GT7 terminal:

- ► Wipe off dirt and dust on the outside of the GT7 using a soft, lint free and dry cloth.
- ► For extreme dirt, the GT7 terminal can be cleaned using a slightly moistened cloth.

7 TECHNICAL DATA

7.1 Power supply

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

7.2 Reading field

Reader type	
- GT7.x**3**00	LEGIC advant and Proxy (125 kHz) reader
- GT7.x**5**00	MIFARE Classic (1k and 4k), MIFARE Ultralight®, MIFARE DESFire EV1®, EV2® and EV3®, MIFARE Plus, ISO 15693
- GT7.x**7**00	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.x**3**00 and GT7.x**7**00 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)

7.3 Inputs & outputs

Signal input	
- Optocoupler	1 x optocoupler input, potential-free, function configurable Input voltage: DC 0 to 30 V (U_{Low} < 2 V, U_{High} > 6 V)
- Wiegand (D1, D0)	2 x input, with potential, function configurable Input voltage: open or GND (e.g., push button connected to GND)
Signal output	GT7.**2**x00: 1 x relay GT7.**3**x00: 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

7.4 Memory and time management

Data storage	Flash memory for configuration and booking data, screensaver, and advertisement pictures.
Internal clock	Time retention without voltage = 1 hour

7.5 User guidance

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

7.6 Interfaces

Host interface	
- Ethernet	10/100 Mbps, IPv4 and IPv6
- 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)

7.7 Housing

Front/rear part	Plastic PC black gray
Reader cover	Plastic PC In-mold technology
Display	Hardened glass
Weight	370 g (13 oz)

7.8 Environmental conditions

Permitted ambient temperature	-10 to +50 °C (+14 to +122 °F)
Storage temperature	-25 to +70 °C (-13 to +158 °F)
Protection type	IP54 (installed state)
Protection class	III (Safety Extra-Low Voltage)
Environment class (VdS 2110)	III (outdoor conditions, weather protected)
Certification	
- GT7.x**3**00	CE
- GT7.x**5**00	CE, CB, FCC, IC, ETL, EAC
- GT7.x**7**00	CE, FCC, IC

gantner

INSPIRED ACCESS

SALTO WECOSYSTEM

SCAN FOR CONTACT

© 2025 Gantner
Gantner reserves the right to change technical specifications, designs and services without prior notice.
Photos: GANTNER / SALTO Systems / Shutterstock