

GC7.3000



© Copyright 2024 Gantner Electronic GmbH

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

Liability

Any claims against the manufacturer based on the hardware or software products described in this manual shall depend exclusively on the conditions of the guarantee. Any further-reaching claims are excluded, and 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: www.gantner.com/EN/locations.

Contact address of manufacturer

Gantner Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria
www.gantner.com/locations

Dear Customer,

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

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

Notation of safety information and safety symbols

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

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

1. Safety messages for personal injury

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



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

Format of safety messages that apply to an entire section:

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

CAUTION



Electrical shock

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

- Do not remove safety protection and covers.
- Do not touch the electrical connections while power is being supplied.

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



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

2. Property damage messages

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

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

NOTICE

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

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

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

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

3. Definition of the signal words

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

4. Definition of the safety symbols

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

Important Safety Information



- The installation, commissioning, and servicing of our products must be performed only by suitably trained personnel. 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 GC7.3000 controller 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/downloads-gc7.3000_f21b98B3p1



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



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

WARNING!

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



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 Information Statement

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

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.

Radiation exposure statement

This equipment complies with FCC & Canadian radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

CONTENTS

1	INTRODUCTION	11
1.1	About this manual	11
1.2	Target groups	11
1.3	Contact & inquiries	11
1.4	Formatting	12
1.4.1	Safety-critical information	12
1.4.1	General information	12
1.4.2	Instructions and results	12
1.5	Terminology	12
2	GENERAL INFORMATION	15
2.1	Intended use	15
2.2	Functional description	15
2.3	System overview	16
2.4	System components	17
2.5	Device dimensions and components	19
3	INSTALLATION	21
3.1	Target group	21
3.2	Installation instructions	21
3.3	Mounting the housing	21
3.3.1	Instructions for installing the GC7.3000	22
4	ELECTRICAL CONNECTIONS	23
4.1	Target group	23
4.2	Network connection (LAN / Ethernet)	23
4.2.1	Network connection via Ethernet LAN	23
4.2.2	Network connection via WLAN	25
4.3	Connecting a GR7 or GAT SR 7xxx / SLR 73xx RFID reader	26
4.3.1	Wire colors of the connection cable	27
4.3.2	Pin assignment of the RJ45 sockets of the RS-485 sub interfaces	27
4.4	Connection of relay outputs and optocoupler inputs	28
4.5	Connecting external devices via RS-232 (e.g. barcode scanners)	29
4.6	Connection of Wiegand interfaces	30
4.7	Connection of the power supply	31
4.7.1	Supply via Gantner power supply	31
4.7.2	Supply via the network using PoE (Power over Ethernet)	32

4.7.3	Supply via customer-specific power supply	32
4.8	Strain relief of the connection cables	33
5	CONFIGURATION	35
5.1	Target group	35
5.2	Configuration options of the GC7.3000 controller	35
5.3	Configuration via G7 Connect (Gantner Cloud)	35
5.3.1	Search device by serial number	37
5.3.2	Selecting a device from a project	37
5.4	Configuration via web interface	40
5.4.1	System overview	42
5.4.2	Device configuration - Network	43
5.4.3	Device configuration - G7 Connect	46
5.4.4	Device configuration - External web server	47
5.4.5	Device configuration - Web proxy	48
5.4.6	Device configuration - WLAN	49
5.4.7	Device configuration - Security and user	50
5.4.8	SCEP (Simple Certificate Enrollment Protocol)	51
5.4.9	Device configuration - Time	53
5.4.10	Device configuration - Display	54
5.4.11	Device configuration - Data carrier	56
5.4.12	Device configuration - Device	57
5.4.13	Device configuration - Fingerprint	58
5.4.14	Device configuration - Barcode interface	59
5.4.15	Device configuration - Sub controller (RFID)	60
5.4.16	App configuration	61
5.4.17	Installed apps	62
5.4.18	Cloud pairing	63
5.4.19	Licensing and coding points	66
5.4.20	Certificate management	68
5.4.21	Maintenance - Device	71
5.4.22	Maintenance - Update firmware	73
5.4.23	Maintenance - Addon bus (external devices)	74
5.4.24	Maintenance - Log viewer	75
5.4.25	Maintenance - Device state	76
5.4.26	Maintenance - Legal information	77
5.5	Integration in control software	77
6	OPERATION	79
6.1	Target group	79
6.2	Operation of the GC7.3000 and reader	79
6.3	Resetting the GC7.3000	80
7	TECHNICAL DATA	81

1 INTRODUCTION

1.1 About this manual

This manual contains a detailed description of how to install, configure, and commission the GC7.3000 controller. The instructions for completing the electrical connection of external devices and signals as well as the power supply and network connections are also included in the manual.

The GC7.3000 can operate with different apps. Apps are application programs that are installed and activated in the GC7.3000 and determine the operation of the controller. The default app for the GC7.3000 is the G7 Access app, which is used for access control, e.g., in gyms or leisure facilities. However, other apps can also be activated, e.g., the G7 Main Controller App to control locker locks. Separate manuals are available for each app that describe the configuration options, functionality, and operation for the end user.

Different devices, e.g., RFID readers, can be connected to the GC7.3000 for user identification or for the input and output of signals such as turnstile control and feedback. The basic functions and configuration settings are described in this manual. You will also find examples of typical applications. For a description of the supplementary devices and applications not listed in this manual, please refer to the manuals and documentation of these other devices.

1.2 Target groups

This manual contains information relevant for the different stages in the operating life of the GC7.3000 controller. Information about the installation, commissioning, and service/maintenance of the GC7.3000 controller 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 (installation, configuration).
- > Service technicians (configuration, operation).
- > End users of the GC7.3000 controller (operation).

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

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

1.3 Contact & inquiries

For all inquiries concerning the GC7.3000, 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.
 - 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.

App

An app in the context of Gantner devices refers to the software application that can be installed on the app-enabled devices of the GC7 and GT7 series. The enabled app determines the operation of the device.

G7 Access App

The name of the software (app) installed by default on the GC7.3000 and as described in this manual. This app can be used to control and monitor access to and from a facility.

Reader

To allow users to identify themselves in the system, RFID data carriers are used for the identification process. Gantner offers various types of RFID readers to read the data carriers. Barcode readers, which are also commonly referred to as "readers", are also possible.

PC software

Refers to device management software that allows or denies access based on user authorization, among other things.

User

In this manual, the term “user” refers to the person who is operating the GC7.3000, e.g., to gain access to an area.

Data carrier

Data carriers are used by users to identify themselves in the system and thus enable access if authorized. Data carriers with contactless RFID chips (Radio Frequency Identification) are available in various forms, e.g., cards, key tags, or wristbands, and for different identification systems (LEGIC, MIFARE® or ISO 15693). The data carriers are read by an RFID reader (e.g., GR7) connected to the GC7.3000. If a barcode reader is connected to the GC7.3000, barcode media can also be used for identification.

TLS

The term “TLS” (previously called “SSL”) is an encryption protocol for secure data transmission. For the GC7.3000, TLS can be enabled to encrypt the data transfer between PC/server/cloud server and GC7.3000 with TLS.

2 GENERAL INFORMATION

2.1 Intended use

Various apps can be installed on the GC7.3000 that determine the function and thus the area of application of the GC7.3000. Observe the intended uses as specified in the respective documentation of the app.

In this manual, the standard app for the GC7.3000 controller is described. The standard app is the G7 Access App, which allows the GC7.3000 to be used for access control in public facilities such as leisure centers or gyms.

2.2 Functional description

The GC7.3000 controller can operate with different apps, which provide flexibility for use with different applications. In this manual, the focus is on operation with the G7 Access App.

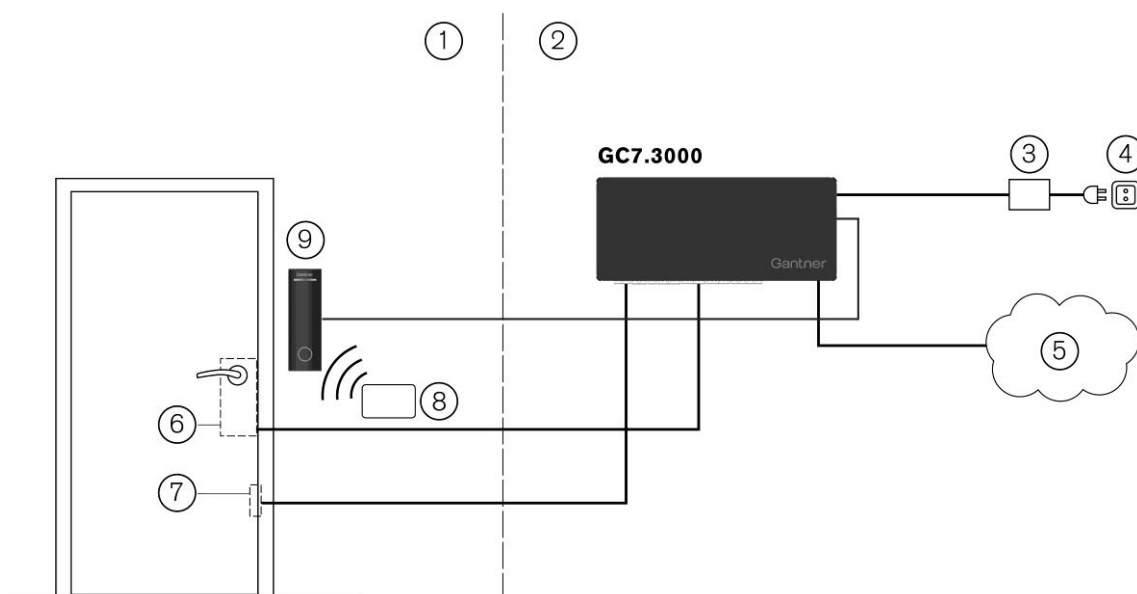
To control unlocking devices such as turnstiles or electronic door locks, the GC7.3000 has six relay outputs that are switched depending on the configuration and authorization. Status signals can be detected using the vier optocoupler inputs.

The identification of users is carried out by default using contactless data carriers at RFID readers, which can be connected to the GC7.3000. A wide variety of readers are available. Barcode readers or Wiegand readers can also be connected.

For configuration and the authorization control of users, the GC7.3000 connects to a LAN network via a network interface. Configuration can thus be completed via a web browser (web interface) or also conveniently via the Gantner Cloud (G7 Connect). Via the configuration, the functionality of the GC7.3000 can be adapted to the respective requirements.

2.3 System overview

The following figure shows schematically how the GC7.3000 controller is used for access control.



- 1 Unsecured area
- 2 Secured area
- 3 Power supply
- 4 Power outlet
- 5 Network connection (configuration, control)
- 6 Control electronic lock
- 7 Feedback door contact
- 8 User identification via RFID data carrier
- 9 Gantner RFID reader

Fig. 2.1 – System overview

2.4 System components

The following system components are available for the operation of the GC7.3000:

1. GC7.3000

2. GAT NET.Power Supply 7020-1 100-240 / VI

3. Power Cord 2m xxx – IEC 60320 C7

4. GAT NET.Power Supply 7020 PoE

5. GAT NET.Power Supply Cable OE

6. WLAN Stick Archer T2U

6. GR7 Reader
 GR7.1300 GR7.1310 GR7.2300 GR7.2310 GR7b.2300 GR7b.2310 GR7.7380

7. GAT IO 7054 GAT IO 7055

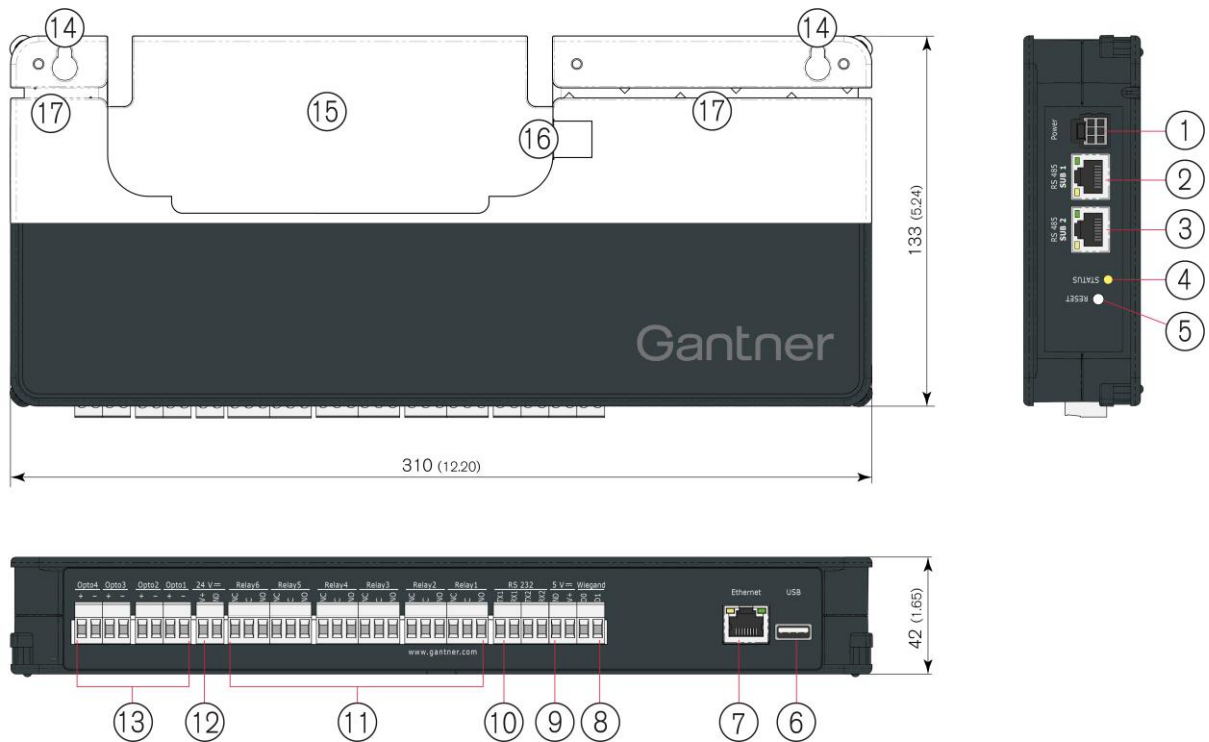
8. RJ45 Splitter 2port CAT 5
RJ45 Splitter 8port CAT 5



Fig. 2.2 - GC7.3000 with accessories and available system components

1. GC7.3000 (Part No. 1103557)
Multifunctional controller, Access App (see G7 App License Points), connections: 1 x Ethernet, 2 x RS-232, 2 x RS-485, 2 x USB, 1 x Wiegand, 4 x optocoupler inputs, 6 x relay outputs
2. GAT NET.Power Supply 7020-1 100-240 / VI (Part No. 1104784)
Power supply for powering the GC7.3000 controllers, with C7 socket for connecting a power cord (see position 3). The suitable power cable must be ordered separately.
3. Power Cord 2m xxx – IEC 60320 C7
2 m power cord for the GAT NET.Power Supply 7020 100-240 V/VI, suitable for different power outlet configurations:
 - Power Cord 2m EU CH – IEC 60320 C7 (Part No. 494181). For European power outlets.
 - Power Cord 2m UK – IEC 60320 C7 (Part No. 494282). For United Kingdom power outlets.
 - Power Cord 2m AUS – IEC 60320 C7 (Part No. 511474). For Australian power outlets.
 - Power Cord 2m USA – IEC 60320 C7 (Part No. 636835). For United States power outlets.
 - Power Cord 2m IND – IEC 60320 C7 (Part No. 636734). For Indian power outlets.
4. GAT NET.Power Supply 7020 PoE (Part No. 1106359)
Power supply for voltage supply of the GC7.3000 controllers with C7 socket for connection of a power cable (see 3). The first variant requires a separate voltage cable for connection to the GC7.3000. The second variant "PoE" can be used for supply via the Ethernet interface.
5. GAT NET.Power Supply Cable OE (Part No. 1106420)
Power supply cable for GC7 with 6-pin Molex connector on one side and open end on the other side to connect custom power supplies, length 15 cm.
6. WLAN Stick Archer T2U Nano (Part No. 1108854)
USB 2.0, suitable for use in the GC7.3000 controller for communication via WLAN, standards IEEE 802.11b/g/n/ac (2.4 GHz/5 GHz), with integrated antenna
7. GR7
13.56 MHz multi-technology RFID reader, RS485 interface, for connection to control devices, e.g., the GC7.3000 access controller.
GR7.1300 (Part No. 1105583) - slimline housing, without keypad
GR7.1310 (Part No. 1105584) - slimline housing, with keypad
GR7.2300 (Part No. 1105588) - standard wide housing, without keypad
GR7.2310 (Part No. 1105590) - standard wide housing, with keypad
GR7b.2300 (Part No. 1105601) - standard wide housing, without keypad, with fingerprint reader
GR7b.2310 (Part No. 1105602) - standard wide housing, with keypad, with fingerprint reader
GR7.7380 (Part No. 1106839) - with optional glass front or integrated in switch program with black or white front
Other variants are available. Go to www.gantner.com.
8. GAT IO 7054 (Part No. 1105454)
GAT IO 7055 (Part No. 1105456)
IO expansion unit with 4 outputs and 12 inputs (GAT IO 7054) or 8 outputs and 16 inputs (GAT IO 7055), RS-485 interface.
Other variants are available. Go to www.gantner.com.
9. RJ45 Splitter 2port CAT 5 (Part No. 430171)
RJ45 Splitter 8port CAT 5 (Part No. 1102453)
RS-485 distributor with 2 or 8 RJ45 outlets and a 20 cm RJ45 connection cable. All outlets are connected in parallel! Suitable to connect several sub controllers or GR7 readers to each GC7.3000.

2.5 Device dimensions and components



Measurements in mm (inches shown in brackets for reference only)

- | | | |
|---------------------------------|--------------------------------|----------------------------------|
| 1 Power supply connection | 7 Ethernet connector (network) | 13 Optocoupler inputs (4x) |
| 2 Serial interface RS-485 SUB 1 | 8 Wiegand interface | 14 Mounting holes |
| 3 Serial interface RS-485 SUB 2 | 9 Voltage output DC 5 V | 15 Power supply compartment |
| 4 STATUS display | 10 Serial interface RS-232 | 16 USB connector (optional WLAN) |
| 5 RESET button | 11 Relay outputs (6x) | 17 Cable holder |
| 6 USB port | 12 Voltage output DC 24 V | |

Fig. 2.3 – GC7.3000 controller overview

The GC7.3000 has removable screw terminals, which are supplied. There are no other individual parts.

There is a compartment (15) in the housing of the GC7.3000 where the power supply can be stored if required.

3 INSTALLATION

⚠ CAUTION



Electric Shock

- ➔ Touching live parts can lead to injuries from electric shock.
 - Before working on the device or mounting/dismounting, the device must be disconnected from the power supply.
 - The applicable safety and accident prevention regulations must be observed.
 - Protective devices must not be removed.

NOTICE



Damage to or malfunction of the GC7.3000

- ➔ Improper work on the device can damage the GC7.3000.
 - Read the information in this chapter carefully before installing the GC7.3000.
 - Installation and maintenance of this device may only be carried out by trained, competent personnel.
 - Observe the specified technical data and measurement diagrams of the device.
 - Use the correct tools for install the GC7.3000

3.1 Target group

This chapter contains information for the technicians responsible for installing the GC7.3000. Experience in mechanical work and basic electrotechnical knowledge is assumed. Previous knowledge of the GC7.3000 or the Gantner access system is not required.

3.2 Installation instructions

The GC7.3000 controllers are designed to be installed on a flat, smooth surface. Depending on the installation requirements, the GC7.3000 controllers can also be housed, e.g., in a server cabinet, without fastening.

CAUTION Risk of injury! If the GC7.3000 is not fastened and placed at a height of more than 2 m, precautions must be taken to prevent the controller from falling and injuring persons.

3.3 Mounting the housing

The GC7.3000 controllers must be placed close to the associated readers and locking elements to minimize the cable lengths to these devices/parts. Therefore, the controllers are usually installed near the doors or turnstiles being controlled.

The controllers must be placed in a secure location that is protected from unauthorized access. If the controller is installed higher than 2 m above the floor, the controllers must be installed with three screws attached to the mounting holes provided in the rear part of the housing.

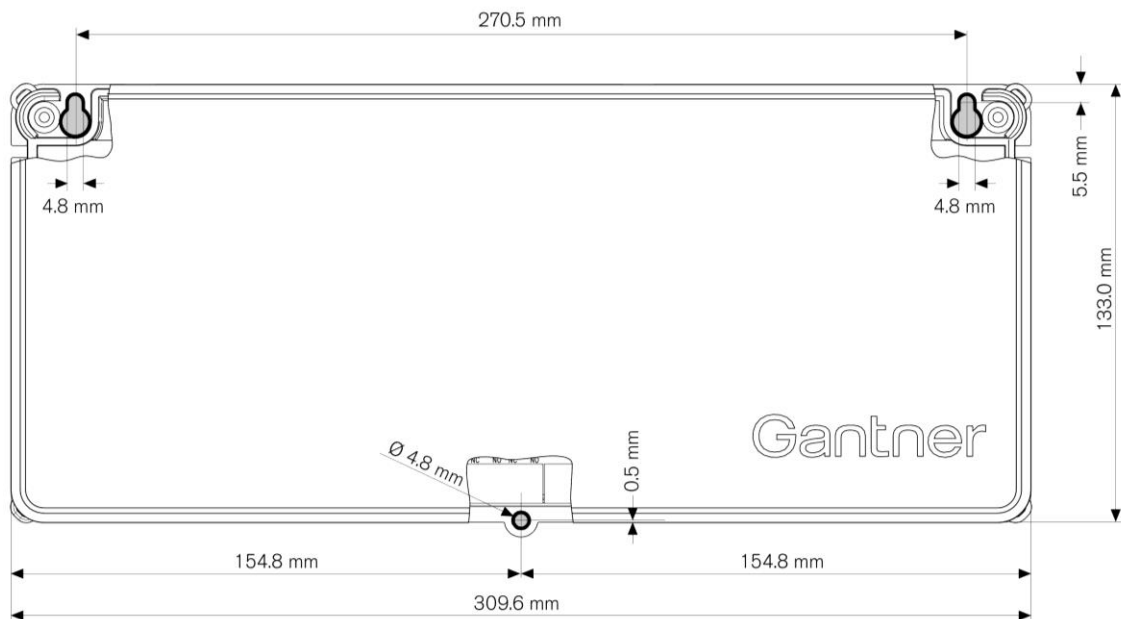
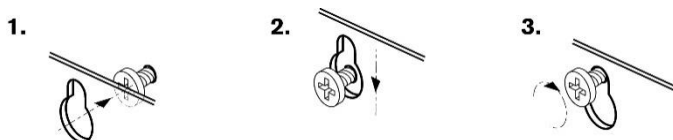


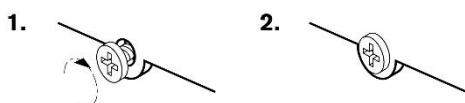
Fig. 3.1 – Mounting the GC7.3000 housing (dimensions in mm)

3.3.1 Instructions for installing the GC7.3000

- ▶ Drill the three mounting holes using the measurements as shown in Fig. 3.1.
Depending on the substrate, use the appropriate drill diameters for the screws and/or wall plugs (screws with a maximum diameter of 4.5 mm). Depending on the substrate, the screws and any wall plugs required must be selected so that they can withstand the weight of the controller (see “7 TECHNICAL DATA”). The 4 mm (0.16 in) thickness of the controller housing wall must also be considered when selecting the screw length.
- ▶ Screw in the top two screws until the head protrudes approximately 5 mm (0.19 in) out from the wall.
- ▶ Attach the controller housing to the top two screws and push down until the housing stops against the screws. If necessary, remove the controller and tighten the screws as required before rehanging.



- ▶ Screw the third screw into the central lower mounting hole and tighten firmly.



- ▶ Ensure that the controller is securely fastened and cannot be removed.

4 ELECTRICAL CONNECTIONS

The GC7.3000 controller is connected to a network via a LAN interface. This interface is used for configuration and communication during operation. The power can be supplied via a separate power supply or also via PoE with the suitable accessory - GAT NET.Power Supply 7020 PoE (Part No. 1106359).

⚠ CAUTION



Electric Shock

➔ Touching live parts can lead to injuries from electric shock.

- Before working on the device or mounting/dismounting, the device must be disconnected from the power supply.
- The applicable safety and accident prevention regulations must be observed.
- Observe the specified technical data and dimensional drawings of the device.
- Protective devices must not be removed.

4.1 Target group

This chapter contains information for the electricians responsible for completing the electrical connection of the GC7.3000. This work may only be carried out by qualified personnel. Previous knowledge of the GC7.3000 or the locker locking system from Gantner is not required.

4.2 Network connection (LAN / Ethernet)

For connection to a network, the LAN connection via Ethernet is recommended. Alternatively, communication via WLAN stick is also possible (see "2.4 System components").

4.2.1 Network connection via Ethernet LAN

Connecting the GC7.3000 to a PC/server via Ethernet is completed as follows.

- Plug the Ethernet cable (3) into the RJ45 socket labeled "Ethernet" (4) on the front of the GC7.3000.

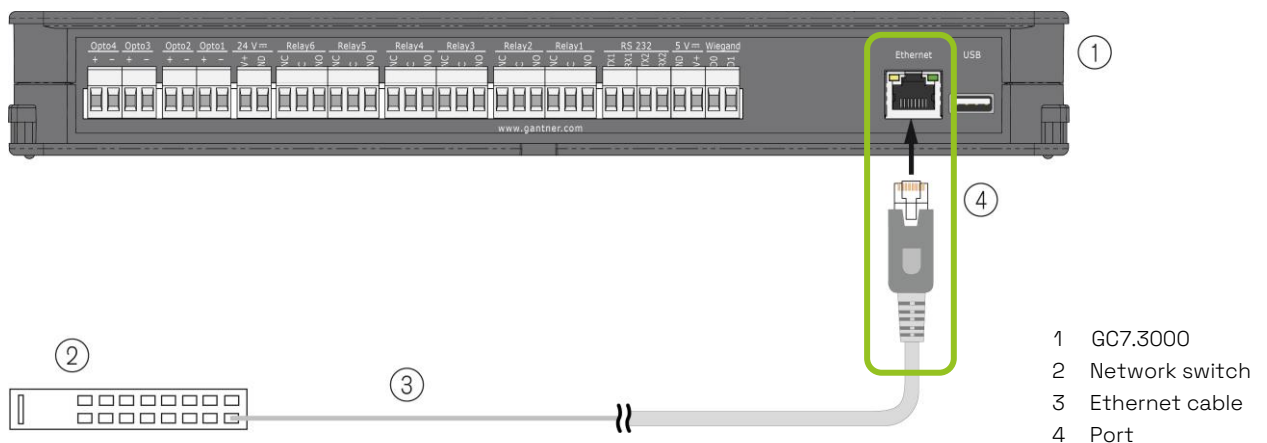


Fig. 4.1 – Network cable connection

Recommended cables / cable lengths for LAN Ethernet

- > Shielded and twisted data cable (recommendation min. CAT. 5 for 100 MBit)
- > Cable length max. 100 m.

► Connect the Ethernet cable (3) to a separate port on the network switch (2).

Depending on the standard used, the wire colors for the Ethernet cable are as follows:

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

Table 4.1 – Ethernet wire colors

4.2.2 Network connection via WLAN

The GC7.3000 does not have an integrated WLAN interface. To use the WLAN connection, a special WLAN USB stick can be used. Gantner offers the "WLAN Stick Archer T2U Nano" (Part No. 1108854) for this purpose.

- Open the cover (2) on the side of the GC7.3000 (1). This is held in place with tabs (3) at the top and bottom and can be pulled off towards the front.

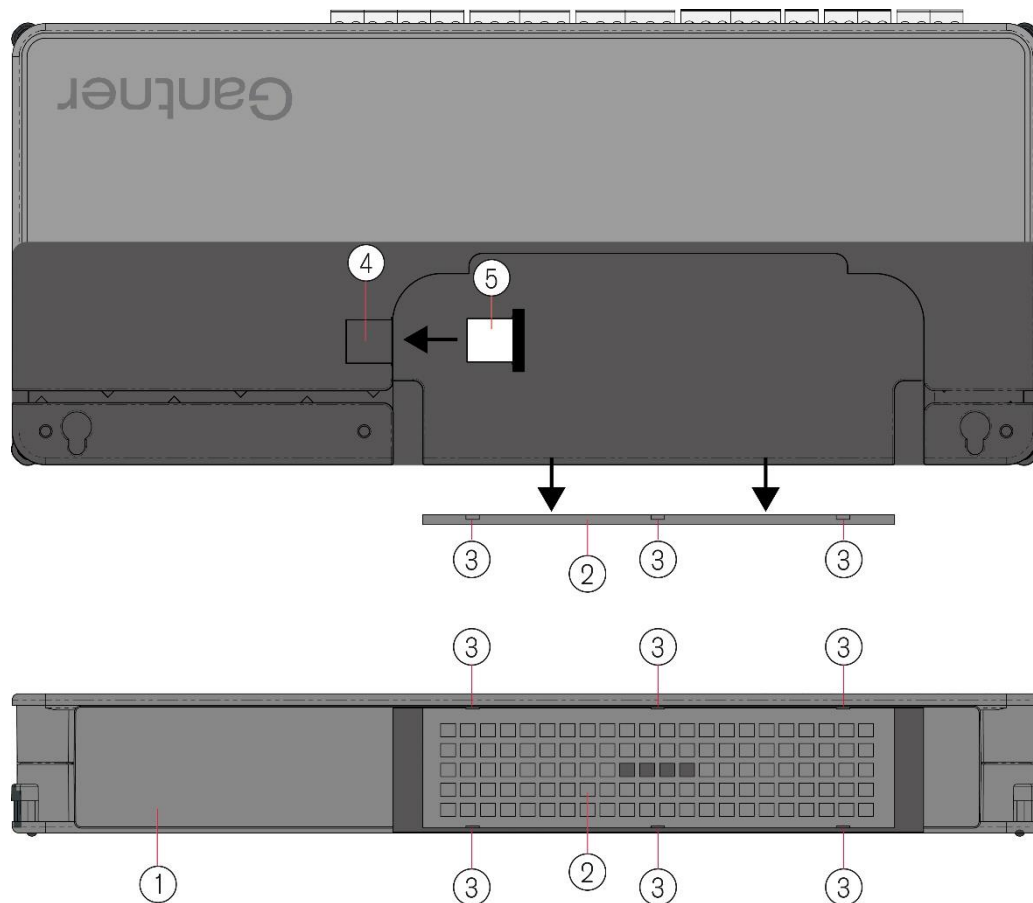


Fig. 4.2 – Inserting the WLAN stick

- Insert the WLAN stick (5) into the USB type-A socket (4) on the inside of the recess.
- Replace the cover (2) on the GC7.3000 (1) so that the tabs (3) snap into housing.
- Configure the WLAN connection in the configuration interface of the controller (see "5.4.6 Device configuration – WLAN").

4.3 Connecting a GR7 or GAT SR 7xxx / SLR 73xx RFID reader



The GAT SR 3xx readers are not supported.

RFID readers can be used to read the contactless data carriers of the users identifying themselves at the GC7.3000. Different reader types are available to suit the various data carrier types, e.g., MIFARE, LEGIC, etc.

NOTE! The number of readers that can be used with a GC7.3000 depends on the installed app. The GC7.3000 has two RJ45 ports available for two readers. However, more than two readers can be used simultaneously (depending on the app) by connecting an RS-485 splitter.

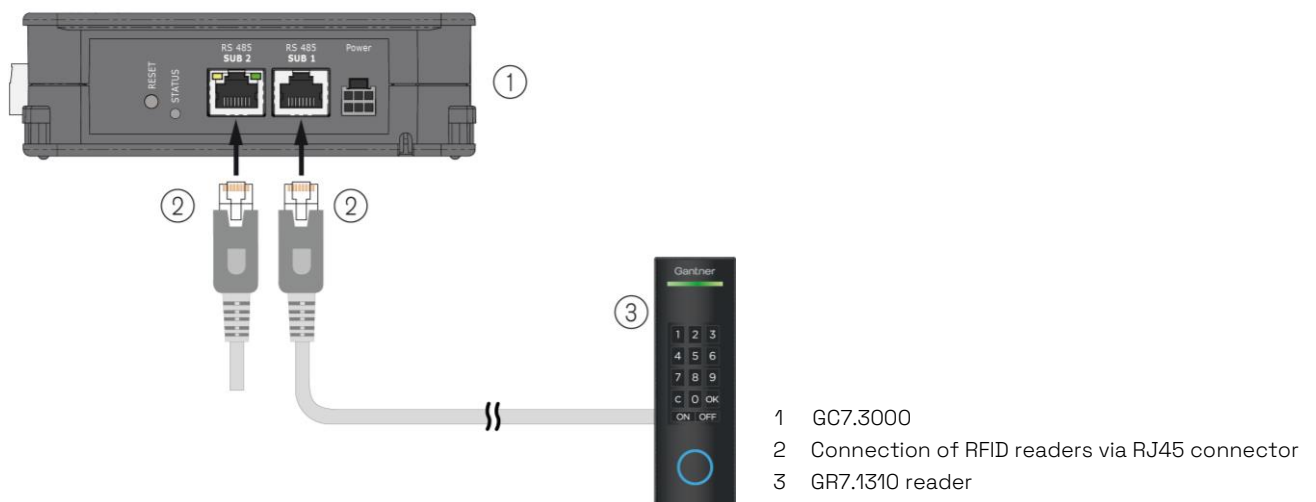


Fig. 4.3 – Connection of RFID readers to RJ45

Gantner readers of the GR7 and GAT SR 7xxx/SLR 73xx series can be connected directly to the RJ45 sockets on the GC7.3000 labelled "RS 485 SUB 1" and "RS 485 SUB 2" using an RS-485 cable.



The readers can be used in combination, e.g., a GR7 series reader connected to "SUB 1" and a GAT SR 7xxx/SLR 73xx series reader connected to "SUB 2".

- Connect the RS-485 cable of the reader to the RJ45 socket "RS 485 SUB 1" or "RS 485 SUB 2" on the GC7.3000 (1). The two ports are equivalent, and you can freely select between SUB 1 and SUB 2 as desired.

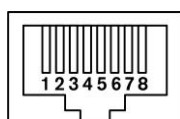
NOTE! For most readers of the GR7 and GAT SR 7xxx/SLR 73xx series, the connection cable is already attached to the reader, and it only needs to be plugged into the controller via the RJ45 connector. If the connection cable needs to be connected to the reader first (e.g., GR7.7380), please refer to the reader documentation.

4.3.1 Wire colors of the connection cable

Terminal	Signal	Wire color (31 cm cable)
VOut (24V)	Supply voltage for reader	Red + blue
A	Data line A	Yellow
B	Data line B	Gray
GND	Ground	Pink + green
IDENT	Reader recognition Plug&Play (only with RJ45 connection)	White

Table 4.2 – RS-485 wire colors

4.3.2 Pin assignment of the RJ45 sockets of the RS-485 sub interfaces



PIN	Signal	
1	-	Not used (reader recognition Plug&Play)
2	-	Not used
3	GND	Ground
4	A	Data line A
5	B	Data line B
6	GND	Ground
7	VOut+ (DC 12 - 24 V)	Supply voltage for reader
8	VOut+ (DC 12 - 24 V)	Supply voltage for reader

Table 4.3 – PIN assignment of the RJ45 socket

4.4 Connection of relay outputs and optocoupler inputs

The GC7.3000 has six floating relay outputs (1 in Fig. 4.4), which can be used to output signals when certain events occur. The controller also has four digital signal inputs in the form of optocouplers (2 in Fig. 4.4), which can be used, for example, to detect the feedback of the turnstile.

Gantner also offers the GAT IO 7054 and GAT IO 7055 expansion devices to increase the number of relay outputs and digital inputs.

- > GAT IO 7054: Additional 4 relay outputs and 12 digital inputs
- > GAT IO 7055: Additional 8 relay outputs and 16 digital inputs

These devices can be connected to the RS-485 interface "RS 485 SUB 1" or "RS 485 SUB 2". Please also refer to the separate documentation of these devices.

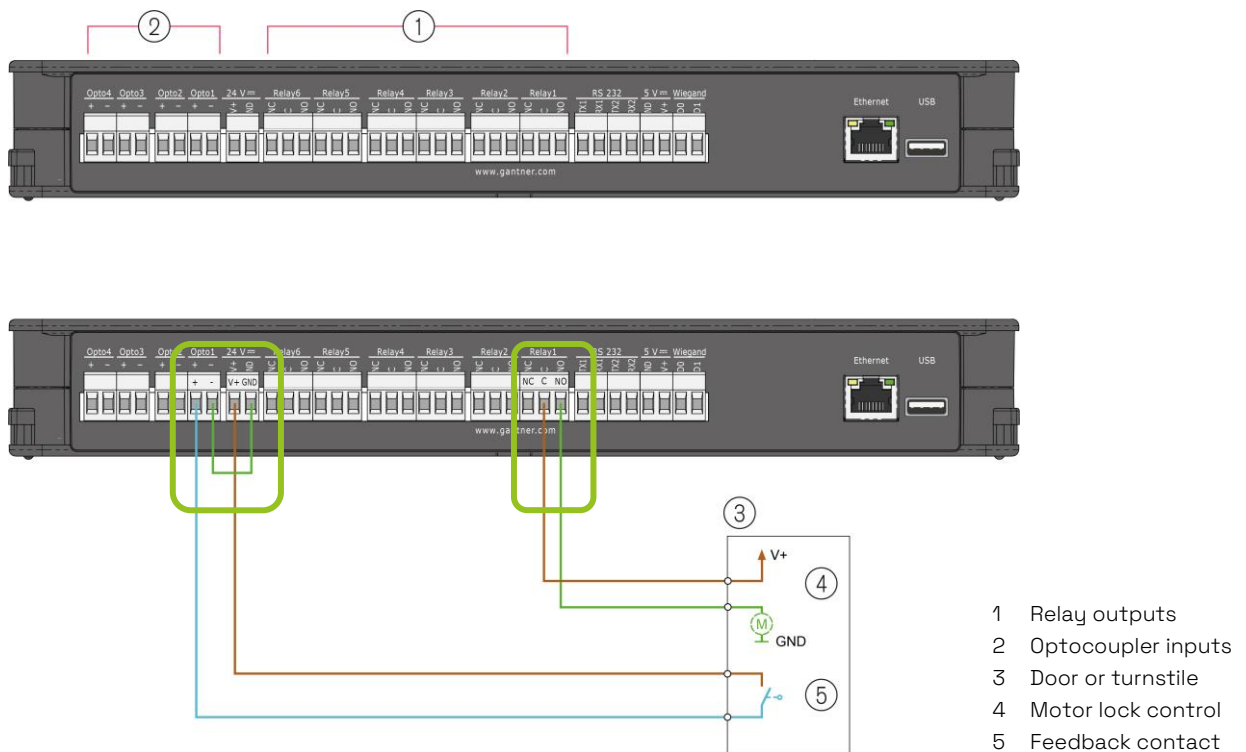


Fig. 4.4 – Connection of the relay outputs and optocoupler inputs (example)

A relay output can be used to control, for example, a turnstile or a door. When a user identifies themselves using a data carrier at a reader connected to the GC7.3000 and the user is subsequently granted access, the configured relay is activated and thus the connected turnstile is unlocked. The wiring (NO or NC) and configuration must be completed depending on the turnstile used.

The relay outputs are connected to the corresponding inputs of the devices to be controlled. The supply voltage for this can come from an independent voltage source (depending on the requirements of the device to be controlled).

Fig. 4.4 shows an example of how a door lock (3) with its own power supply can be connected to the relay output and a feedback contact (4) for status reporting is connected to an optocoupler input.

NOTE! Observe the max. permissible switching voltages and currents according to chapter "7 TECHNICAL DATA". Also read the instructions of the devices to be connected and observe the specifications of the connection options.

4.5 Connecting external devices via RS-232 (e.g. barcode scanners)

External devices, e.g., barcode scanners, can be connected to the two serial interfaces (RS-232) of the GC7.3000. The following example shows how to connect the barcode scanner ATR 110 from Gantner. The colors shown are the default colors of the ATR 110 connection cable.

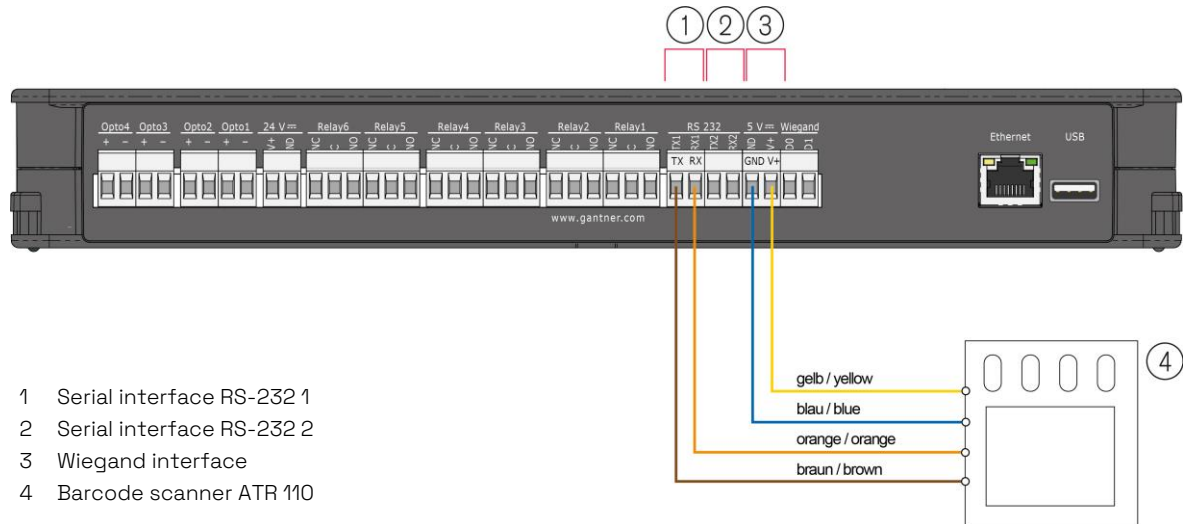


Fig. 4.5 – Connecting an ATR 110 barcode scanner to the RS-232 serial port

ATTENTION! Always refer to the documentation of the devices being connected and the technical data of the device and the GC7.3000 (see "7 TECHNICAL DATA"). The max. permissible voltages and currents must not be exceeded.

NOTE! Up to eight external devices can be connected to each GC7.3000 controller. The GR7 and GAT IO 705x devices can also be used together at one RS-485 bus.

4.6 Connection of Wiegand interfaces

Third-party readers that support the Wiegand protocol can be connected to the Wiegand interface.

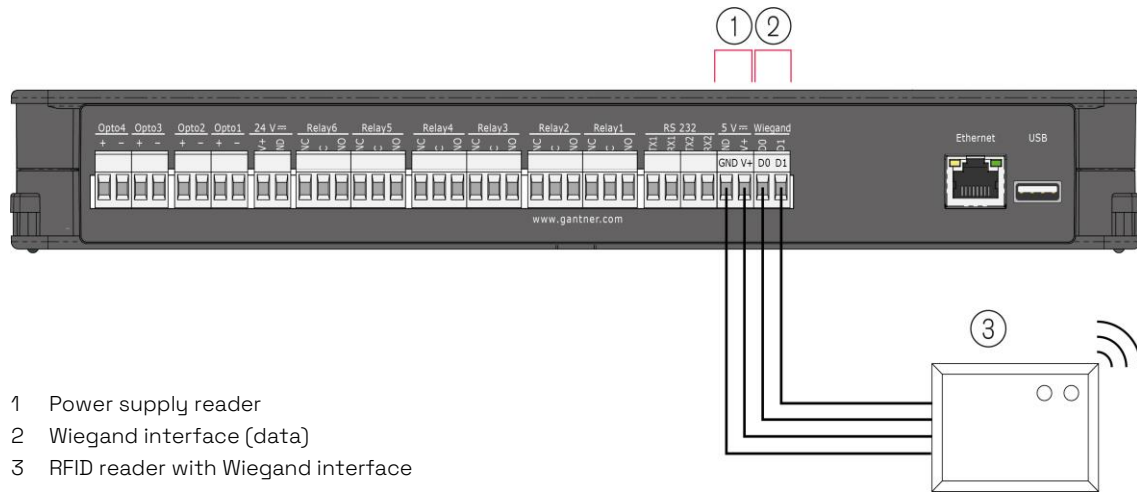


Fig. 4.6 – Connecting a Wiegand reader to the GC7.3000

ATTENTION! Always also observe the descriptions of the readers to be connected and the technical data of the reader and the GC7.3000 (see "7 TECHNICAL DATA"). The maximum permissible voltages and currents must not be exceeded.

4.7 Connection of the power supply

For the power supply of the GC7.3000, different possibilities are available:

- > Supply via a Gantner power supply.
- > Supply via the network using PoE (Power over Ethernet).
- > Supply via a customer-specific power supply and Gantner cable.

4.7.1 Supply via Gantner power supply

In this case, the GC7.3000 controller is connected to the mains voltage using the power supply GAT NET.Power Supply 7020-1 100-240V / VI (Part No. 1104784). A mains voltage of UAC 230 V or UAC 115 V can be used (depending on the application). See chapter "7 TECHNICAL DATA" for exact technical data on the voltage supply.

- Connect the power supply to the MOLEX connector marked "Power".

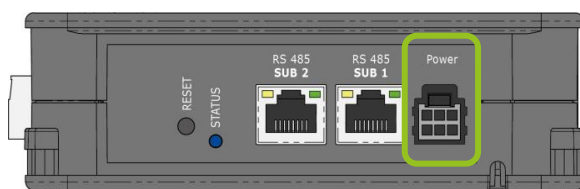


Fig. 4.7 – Power supply connection on the GC7.3000 controller

There is a compartment to store the power supply on the side of the controller if desired. Proceed as follows.

- Remove the compartment cover (1).
- Insert the power supply into the compartment and then insert the cables into the recesses provided on the underside of the controller.
- Replace the compartment cover.

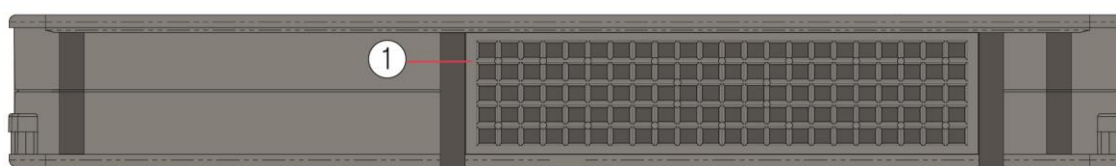


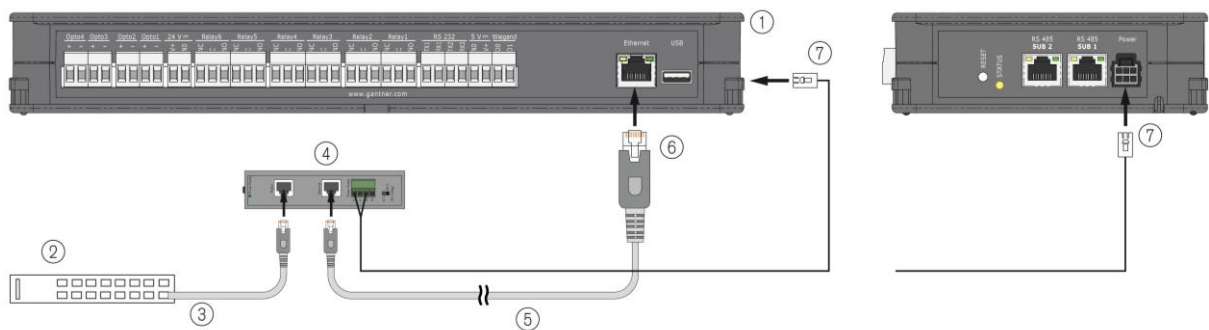
Fig. 4.8 – Storage compartment for the power supply

4.7.2 Supply via the network using PoE (Power over Ethernet)

It is also possible to power the GC7.3000 via Power over Ethernet (PoE) instead of using a power supply. For this purpose, the supplementary unit GAT.NET.Power Supply 7020 PoE (Part No. 1106359) is required. Please note the following requirements when operating via PoE:

PoE Switch Requirements

- > Compliant 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



- 1 GC7.3000
- 2 Ethernet switch with PoE
- 3 Ethernet PoE cable
- 4 GAT.NET.Power Supply 7020 PoE (separation Ethernet and power supply)
- 5 Ethernet cable
- 6 Network connection
- 7 Power supply connection

Fig. 4.9 – Connection of the supply with PoE

4.7.3 Supply via customer-specific power supply

It is possible to use any power supply to power the GC7.3000.

ATTENTION! The technical data for the supply of the GC7.3000 must be observed and adhered to (DC voltage supply 24 V (LPS/SELV), power consumption 3 W, see "7 TECHNICAL DATA").

ATTENTION! Complete the following connections only in a de-energized state.

- Use the GAT NET.Power Supply Cable OE (Part No. 1106420) from Gantner for connection.



- Connect the wire ends of the cable to the corresponding terminals of the power supply.

Wire color	Function
Black	Ground
Red	Supply DC +24 V

Fig. 4.10 – Wire colors of the GAT NET.Power Supply Cable OE

- Connect the Molex connector of the connection cable to the "Power" socket on the GC7.3000.

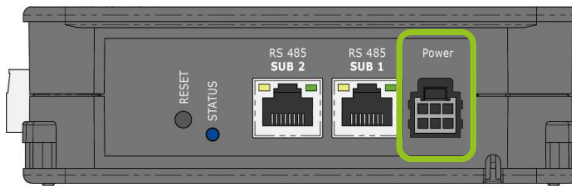
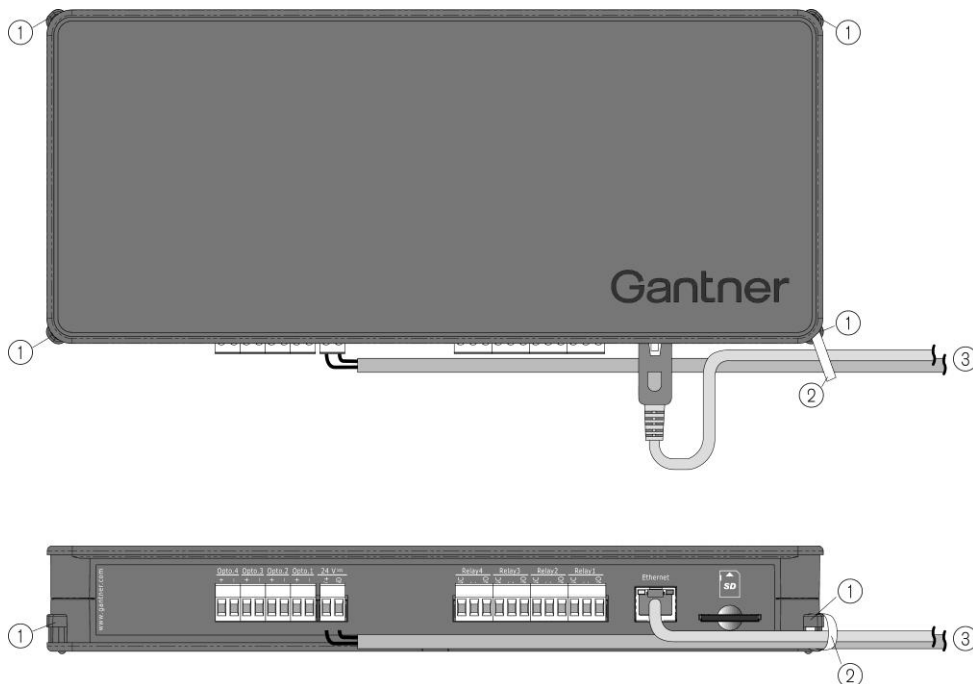


Fig. 4.11 – Supply voltage connection on the GC7.3000 controller

4.8 Strain relief of the connection cables

Eyelets are provided on the corners of the GC7.3000 housing that can be used for strain relief using cable ties.



- 1 ... Strain relief eyelets
- 2 ... Cable tie
- 3 ... Connection cable

Fig. 4.12 – Strain relief on the GC7.3000 housing

To ensure that the plug-in and screw connections of the cables are relieved from tensile forces on the cable, ensure to install the cable strain relief as follows.

- ▶ Run the cables past one of the eyelets.
- ▶ Use a cable tie to fasten the cables to the eyelet.
- ▶ Ensure that the cables are not bent and damaged.

5 CONFIGURATION

5.1 Target group

This chapter contains information for the technicians responsible for commissioning and configuring the GC7.3000 controller. A basic understanding of electrical engineering is assumed. Gantner recommends that only trained personnel carry out the system configuration. Gantner offers regular training courses for its partners.

5.2 Configuration options of the GC7.3000 controller

The configuration of the functionality of the GC7.3000 can be completed as follows:

- > Via G7 Connect (Gantner Cloud): the GC7 controllers in a facility are conveniently integrated in the Gantner Cloud. Here, the user can see all their G7 devices (GC7, GT7, etc.) displayed in an overview and if the devices are online, they can be configured directly within this platform.
- > Direct network connection via web interface: In a web browser, a http or https connection to the GC7.3000 controller is established, and the web server integrated in the GC7.3000 is displayed with all the configuration settings.

5.3 Configuration via G7 Connect (Gantner 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 GC7.3000 using G7 Connect is analogous to the direct configuration via web interface, which is described in chapter "5.4 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>
 - The login window for G7 Connect opens.

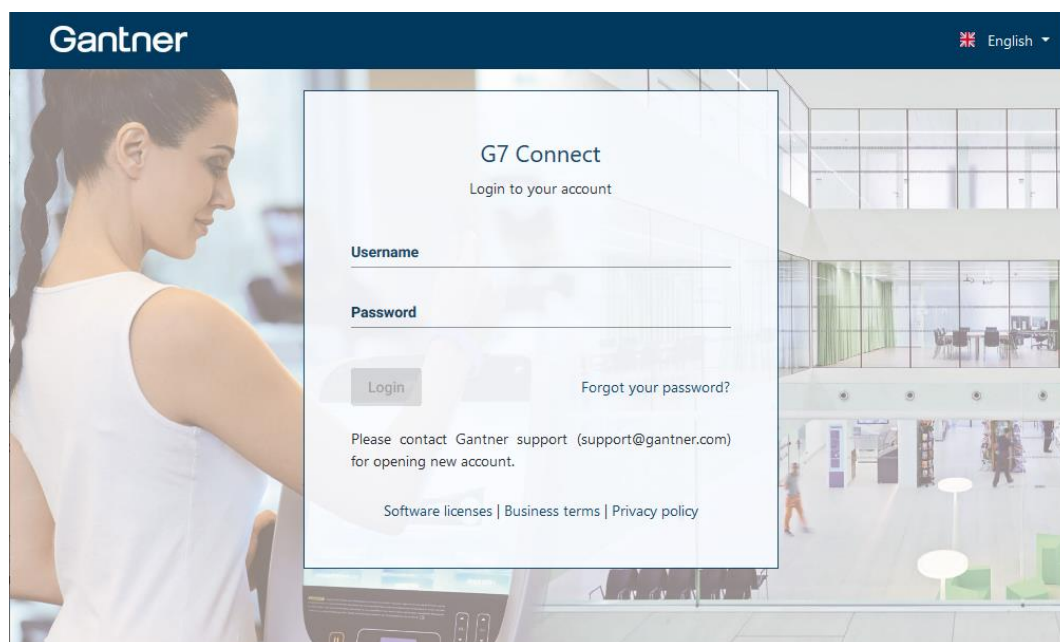


Fig. 5.13 – Login window for G7 Connect

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

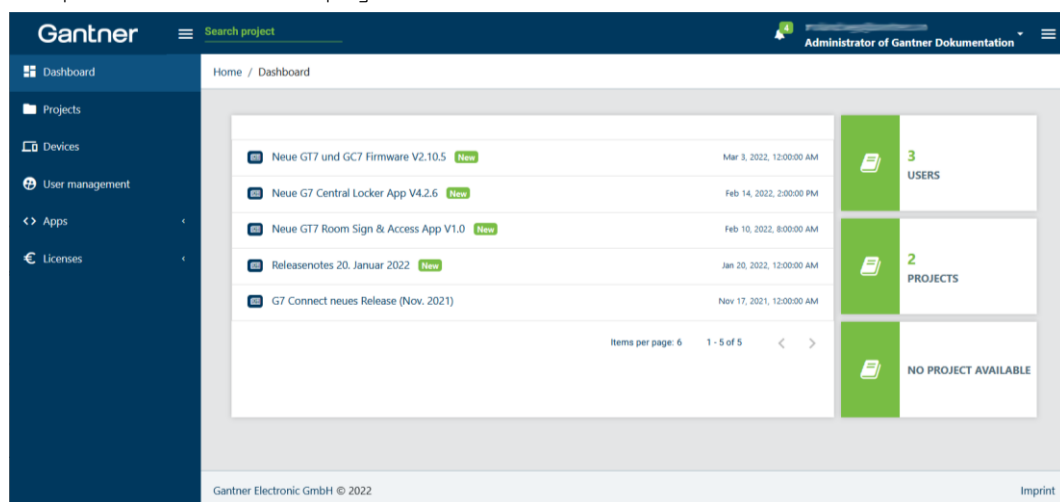


Fig. 5.14 – User dashboard

5.3.1 Search device by serial number

If you have already added a GC7.3000 controller to your G7 Connect project and know its serial number, you can search for the controller via its serial number and access it directly.

- Select "Devices" in the menu.
 - The following window is displayed.

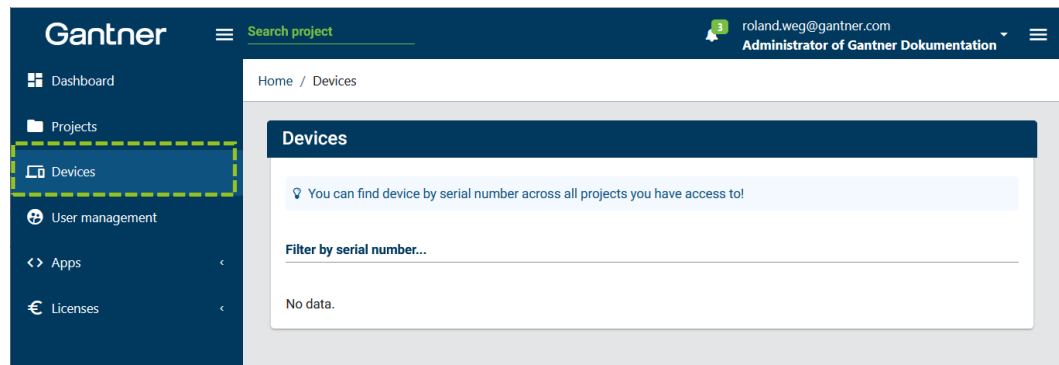


Fig. 5.15 – Device search via serial number

- Enter the serial number.

NOTE! The serial number must be entered in full. A partial number will not be found.

5.3.2 Selecting a device from a project

In a project, you can group together all the devices you want and assign them to your facility or to several facilities (locations).

- Click on "Projects" in the main menu on the left.
 - All projects that you have created or have been assigned to you are displayed.

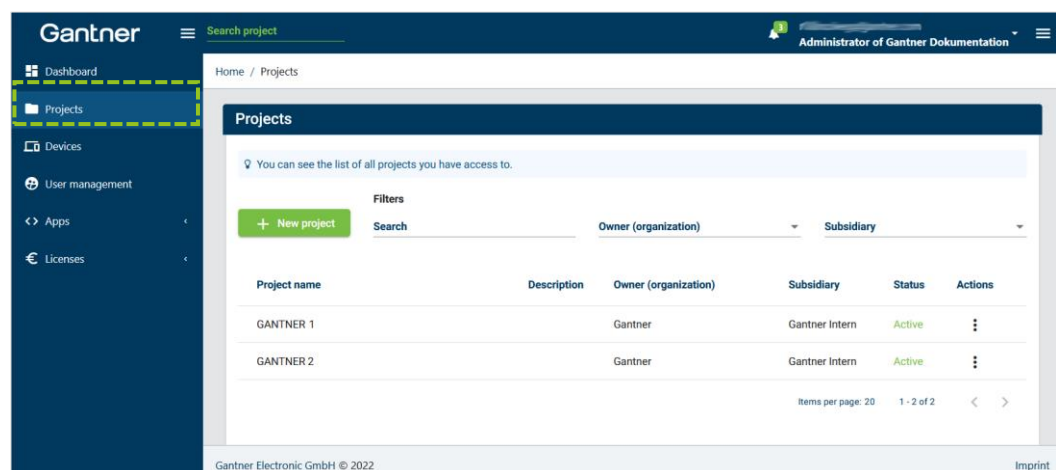


Fig. 5.16 – List of projects

- In the list, click on the project that contains the GC7.3000 to be configured.
 - The project dashboard opens.
 - The name of the project is displayed top left of the screen, above the menu.

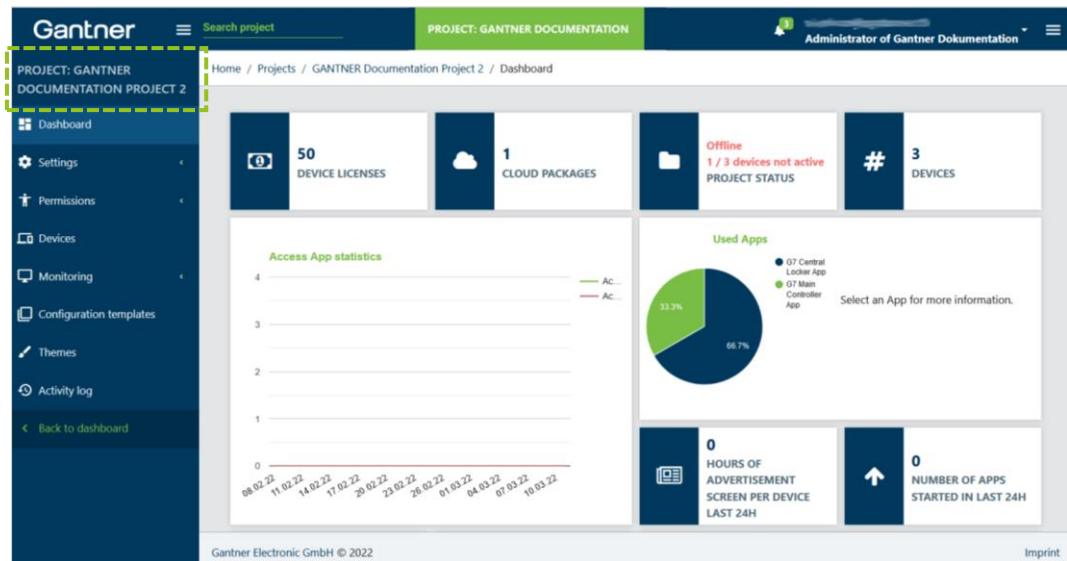


Fig. 5.17 – Project dashboard (current project shown top left)

- Click on "Devices".
 - The list of all devices in the project is displayed.

Gerätename	Seriennummer	Gerät gepairt	Verbunden	Gerättyp	App	Firmware	Geräteversion	Restlaufzeit	Cloud Tage	Aktionen
Central Locker Desk	1910000013	Ja	Ja	GT7.3500	G7 Time & Attendance App (1.1.0)	2.4.0	99	1504 Tage	✓	
BoR GT7	1920000082	Ja	Ja	GT7.3300	G7 Central Locker App (3.1.0)	2.2.2	50	92 Tage	✓	
Zutritt Rezeption	2039030053	Ja	Ja	GC7.3000	G7 Main Controller App (1.1.1)	2.6.0	0	364 Tage	✓	

Fig. 5.18 – List of devices in the project

- In the "Structure" area, a project structure with different levels of hierarchy, e.g., to separate the devices according to their location can be defined. Click on the location to which the device being configured is assigned.
- Click on the device.
 - The device information with configuration settings for the GC7.3000 is displayed.

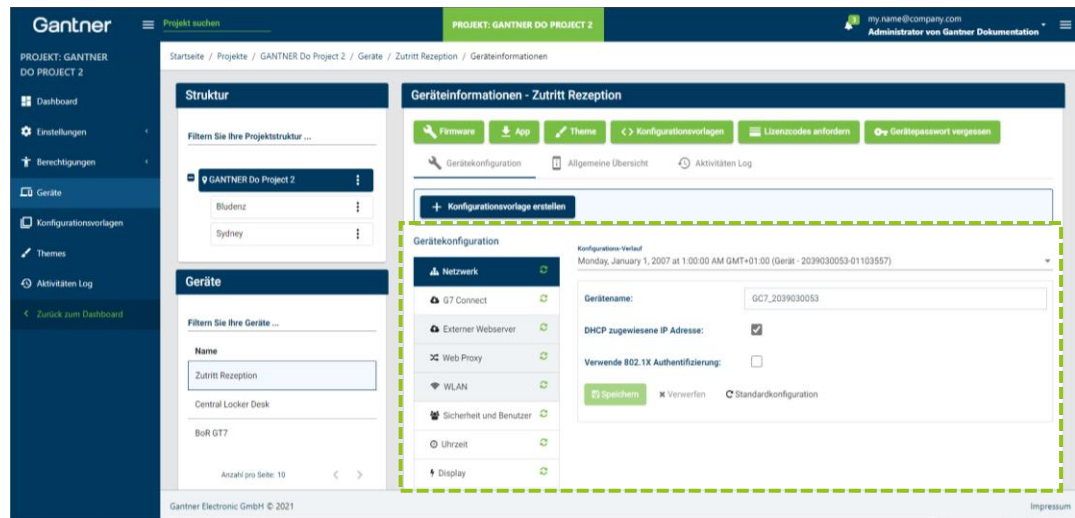


Fig. 5.19 – Device configuration settings

- The configuration settings are displayed in the marked area and can be edited there.
- ▶ After editing settings, click "Save" to apply them in the GC7.3000.
- ▶ Another possibility is to use configuration templates. A configuration template saves the configuration settings that are transferred to the GC7.3000 controller, and the template can then be applied to other devices when the template is selected. To apply a configuration template, click on the green "<> Configuration Templates" button.
 - The "Configuration" popup window opens.
- ▶ Select a configuration template and confirm with "Apply configuration".

The configuration of a GC7.3000 is analogous to the direct configuration via web interface, which is described in the following section.



A detailed description of how to create an account as well as instructions on using the G7 Connect Cloud Service can be found in the G7 Connect manual. There you will also find a description of how configuration templates are created.

5.4 Configuration via web interface

Provided that it is reachable via the network, a GC7.3000 controller can be directly accessed via a web browser. All settings for the device and the installed G7 apps are available for configuration in the web interface.

- Open a web browser.
- Enter the IP address (IPv4 or IPv6) of the GC7.3000 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



Alternatively, you can use Gantner's GAT Device Finder software to scan the network for devices. A GC7.3000 will be displayed there with the device type "GC7.3000" and the IP address. The GAT Device Finder software is available on the partner page of the Gantner website. In addition, GAT Device Finder is also included in the GAT Config Manager software.

- The login page of the GC7.3000 web interface opens.

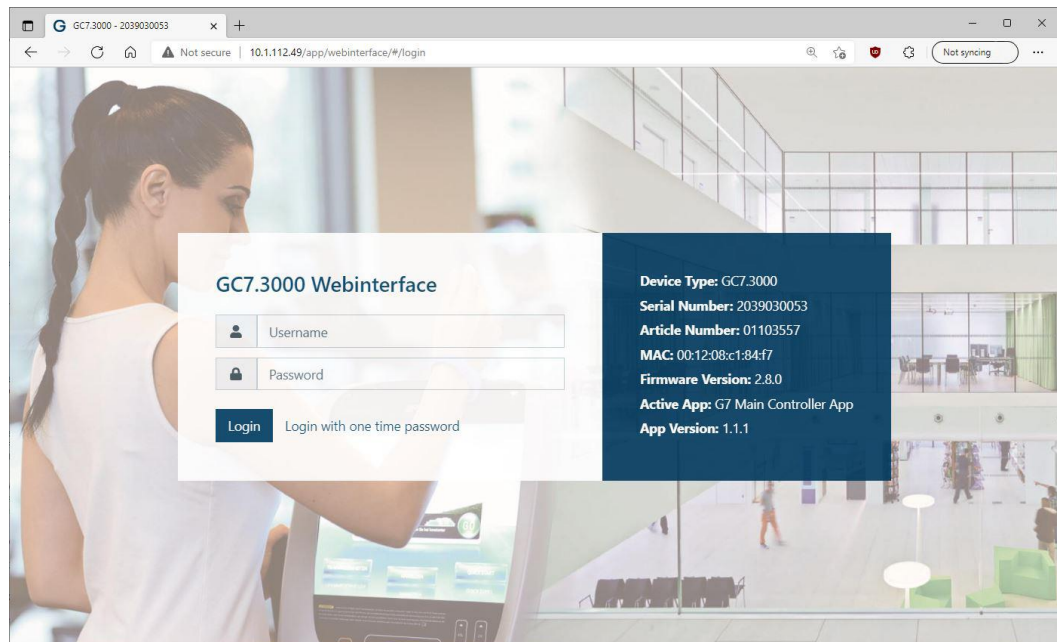


Fig. 5.20 – Login screen of the GC7.3000 web interface

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

NOTE! The default username is "admin" and the default password is "GAT". Please change this data to a secure, secret password after the initial login (see "5.4.7. Device configuration - Security and user").

- The configuration page of the GC7.3000 opens with an overview of the system settings.

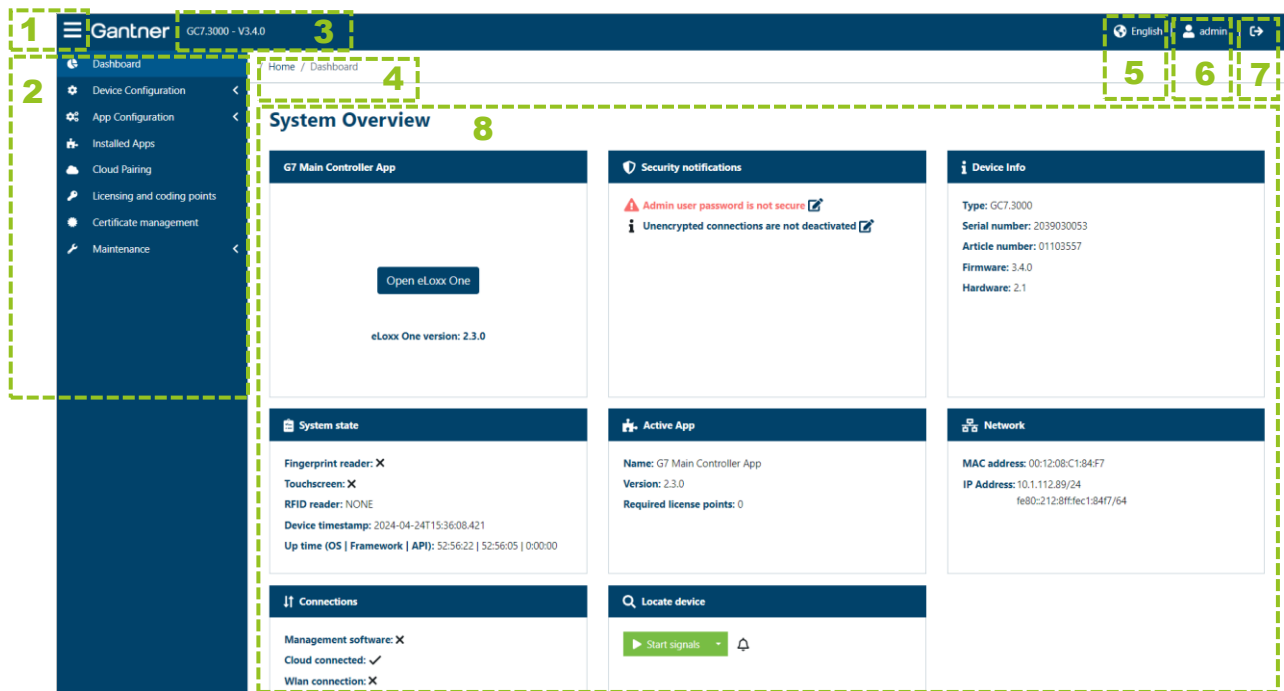


Fig. 5.21 – GC7.3000 configuration - System overview

The following areas and functions are available in this window.

- | | |
|-------------------------|---|
| 1 – Show/hide menu: | Use this button to show/hide the configuration menu. |
| 2 – Configuration menu: | Here you will find all the menu items that can be used to access the relevant settings pages of the GC7.3000. |
| 3 – Firmware version: | Version of the firmware operating in the GC7.3000. |
| 4 – Current path: | Displays a navigation aid with the name of the menu that is currently displayed. |
| 5 – Language selection: | The display language can be selected here. |
| 6 – User: | The logged-in user is displayed here. |
| 7 – Logout: | Clicking on this symbol will log out the current user. |
| 8 – Display area: | All information and settings of the selected menu option are displayed in this area. |

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

5.4.1 System overview

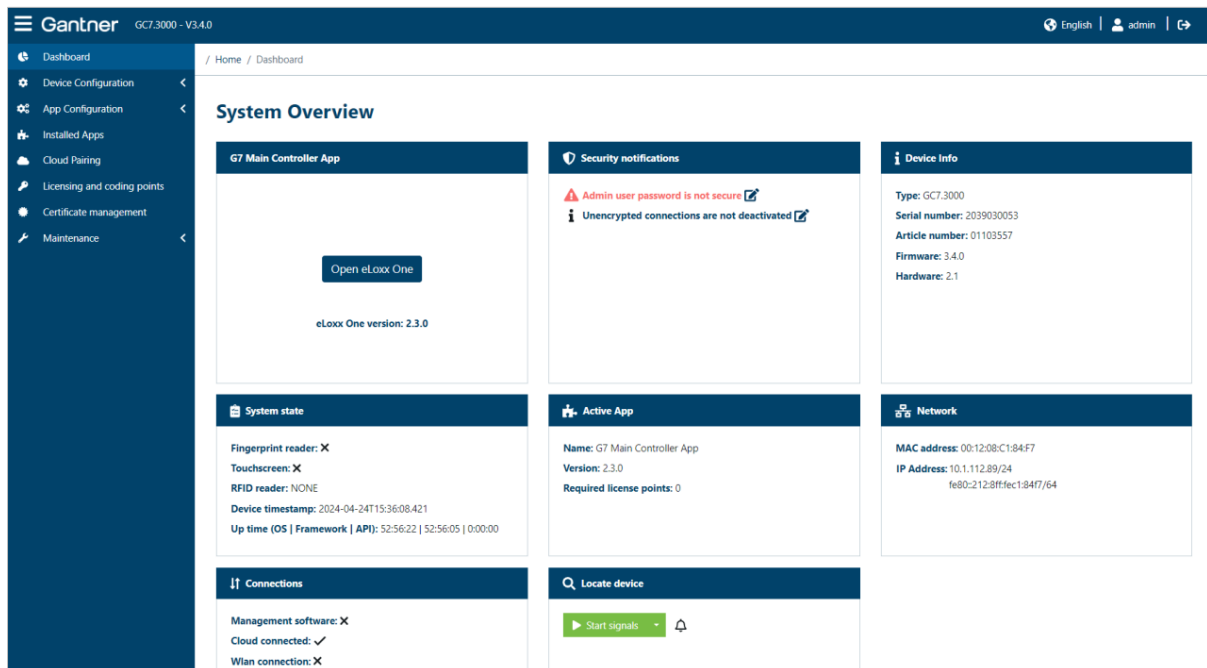


Fig. 5.22 – GC7.3000 configuration - System overview

An overview of the most important settings and status information of the GC7.3000 is displayed here.

- G7 Main Controller App: If the G7 Main Controller App is the active app, the button for starting eLoxx One is displayed here.
- Security notifications: Useful information, e.g., login warnings, relating to the security of the GC7.3000 is displayed here.
- Device info: The device type, the serial and part numbers, and the versions of the GC7.3000 hardware and firmware are displayed here.
- System state: Display of which functions are enabled or being used. The time set in the GC7.3000 and how long the GC7.3000 has been running continuously since the last startup are also displayed.
- Active app: Various apps can be installed in a GC7.3000, whereby only one app can be active at a time. The active app with version and the required license points is displayed here. In this manual, the default G7 Access App is used as an example. Separate documentation explaining the configuration and operation is available for each app.
- Network: The network addresses of the GC7.3000 are displayed here.
- Connections: Shown here are the available network connections and whether they are active (tick icon) or inactive ("X").
 - Management software: Connection to a PC software that then controls the GC7.3000. The software in question depends on the app being used. For example, the eLoxx Relaxx software can be used for the G7 Main Controller app to control locker locks.

- Cloud connected:
Displayed as active (tick symbol) if the GC7.3000 is connected to G7 Connect (see "Cloud Pairing") and can also be configured via the Gantner Cloud.
- Wlan connection:
Displayed as active if the GC7.3000's network connection is via WLAN instead of LAN.
- NTP server:
Connection to a time server that automatically sends and sets the time on the network.
- Locate device:
This button has no function with the GC7.3000.

5.4.2 Device configuration - Network

The screenshot displays the 'Network' configuration page for the GC7.3000 device. The interface is in English, with the user logged in as 'admin'. The left sidebar lists various configuration options: Dashboard, Device Configuration (selected), Network (selected), G7 Connect, External Webserver, Web Proxy, WLAN, Security and user, SCEP, Time, Display, Data Carrier, Device, Fingerprint, Barcode Interface, Barcode Interface 2, Sub Controller, Sub Controller RFID, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area shows the 'Network' settings. The 'Device name' is set to 'GC7_2039030053'. The 'DHCP assigned IP address' checkbox is unchecked. The 'Static IPv4' section is expanded, showing fields for 'Static IP' (192.168.0.42), 'Static subnet mask' (255.255.255.0), 'Static default gateway' (empty), 'Static primary DNS' (8.8.8.8), and 'Static secondary DNS' (1.1.1.1). The 'IPv6 mode' is set to 'disabled'. The 'Use 802.1X authentication' checkbox is checked. The 'Select authentication' dropdown is set to 'TLS'. The 'TLS' section is expanded, showing an 'Identity' field (empty) and a 'Verify CA certificate' checkbox which is checked. At the bottom, there are buttons for 'Save', 'Discard', and 'Default'.

Fig. 5.23 – GC7.3000 configuration - Network

Here the network settings for the connection to the GC7.3000 controller can be displayed and changed.

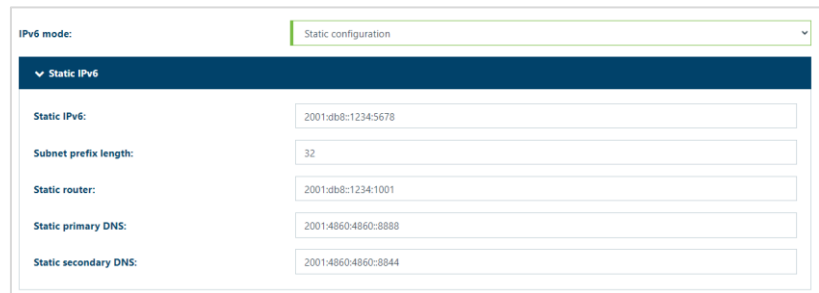
- Device name:
An arbitrary name for the GC7.3000 can be entered here. When the network is scanned for devices, the device with this name is displayed.
- DHCP assigned IP address:
If this option is enabled, the IP address of the GC7.3000 is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, disable this option and enter the network settings into the "Static IPv4 configuration" area. The "Static IPv4 configuration" area is only displayed if the 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:



The screenshot shows the 'IPv6 mode' dropdown set to 'Static configuration'. Below it, the 'Static IPv6' section is expanded, displaying the following fields:

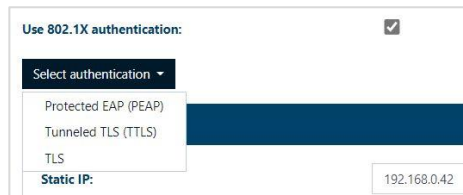
Static IPv6:	2001:db8:1234:5678
Subnet prefix length:	32
Static router:	2001:db8:1234:1001
Static primary DNS:	2001:4860:4860:8888
Static secondary DNS:	2001:4860:4860:8844

Enter the IPv6 address of the GC7.3000 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 GC7.3000 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.



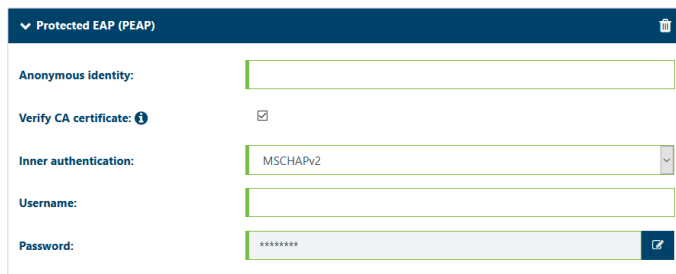
The screenshot shows the 'Use 802.1X authentication:' checkbox checked. Below it, the 'Select authentication' dropdown menu is open, showing the following options:

- Protected EAP (PEAP)
- Tunneled TLS (TTLS)
- TLS

The 'Static IP:' field is set to 192.168.0.42.

NOTE! For assistance in configuring these settings, please contact your system administrator.

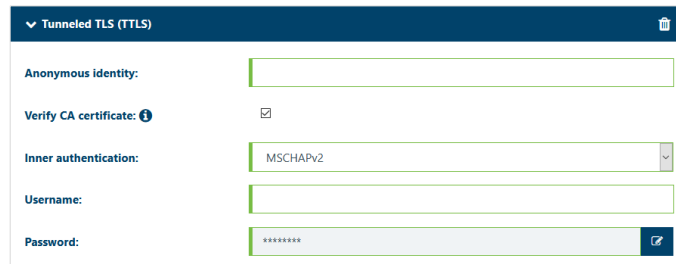
Protected EAP (PEAP)



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:

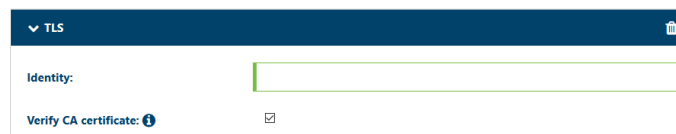
- Anonymous identity: An anonymous identity can be entered here for systems that support a separate authentication outside of a secure tunnel. If no anonymous identity is provided, the default is to use the "Username" for outer and inner authentication.
- Verify CA certificate: It is recommended to enable this option. Certificates are managed via the "Certificate management" page (see chapter "5.4.20 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 "5.4.20 Certificate management").

5.4.3 Device configuration - G7 Connect

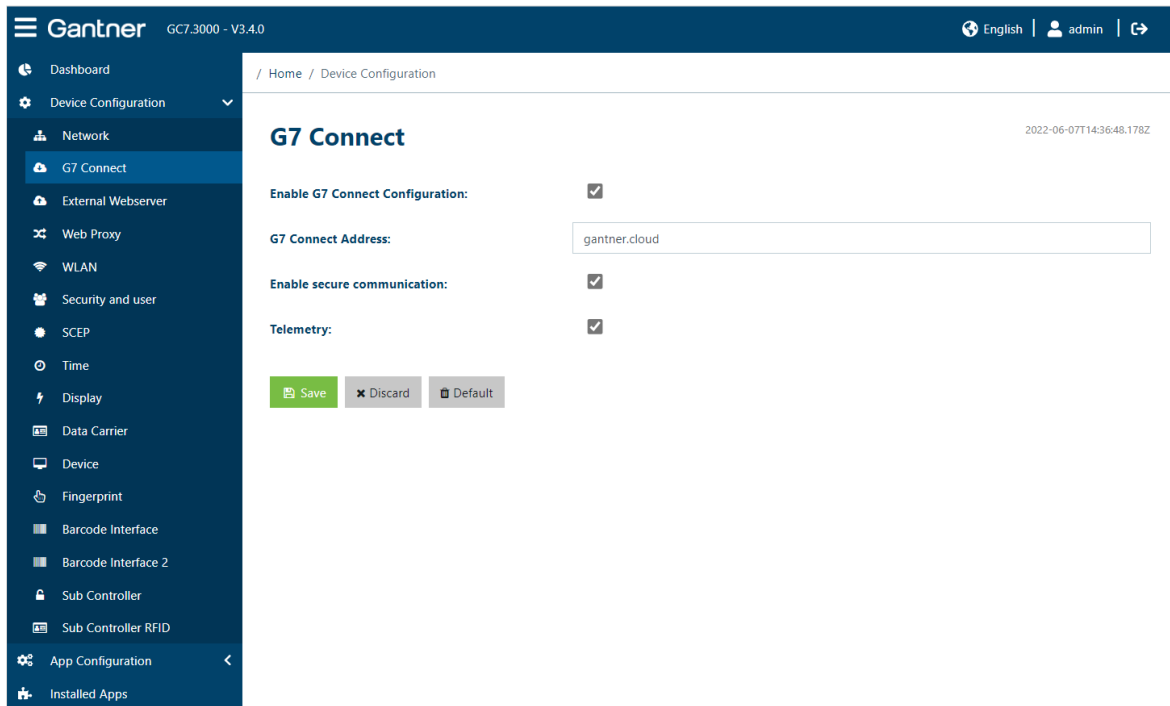


Fig. 5.24 – GC7.3000 configuration - G7 Connect

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

- Enable G7 Connect Configuration: Enable this option if you want to use the configuration of the GC7.3000 from G7 Connect.
- G7 Connect Address: Enter the Internet address of G7 Connect here.
- Enable secure communication: Enable this option to encrypt the communication using TLS.
- Telemetry: Enable 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).

5.4.4 Device configuration - External web server

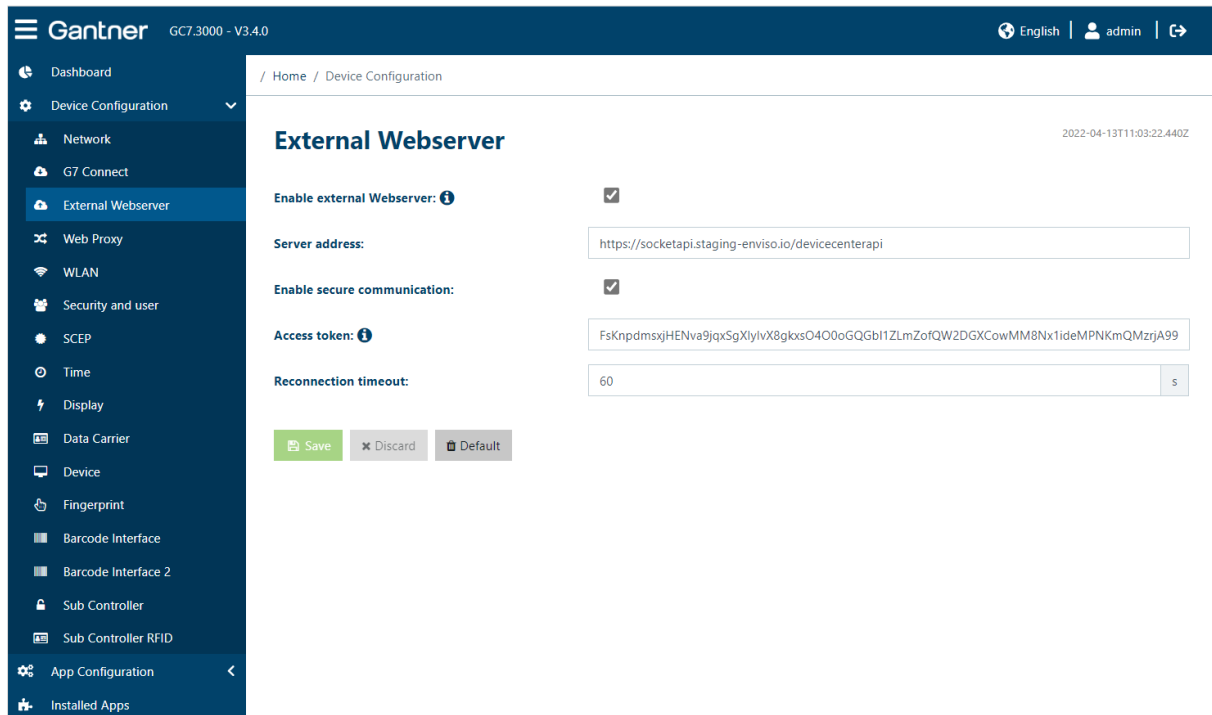


Fig. 5.25 – GC7.3000 configuration - External web server

The GC7.3000 controller can operate as a client or server. In the configuration described here, the GC7.3000 operates as a server, i.e., the PC establishes the connection to the GC7.3000. If the GC7.3000 is to operate as a client, an external web server can be used. In this case, the communication will be carried out via this web server.

- Enable external web server: Enable this option if a web server is to be used for communication. After selection, the following settings are displayed.
- Server address: IP address of the web server (IPv4 format).
- Enable secure communication: When this option is enabled, TLS is used for the web socket connection.
- Access token: In this field, an additional value for authentication can be specified, which is entered in the authorization field of the HTML header. What must be entered here depends on the implementation by the third-party software.
- Reconnection timeout: In this field, enter the waiting time in seconds until reconnection is attempted after the connection between the GC7.3000 and the management software has been interrupted.

5.4.5 Device configuration - Web proxy

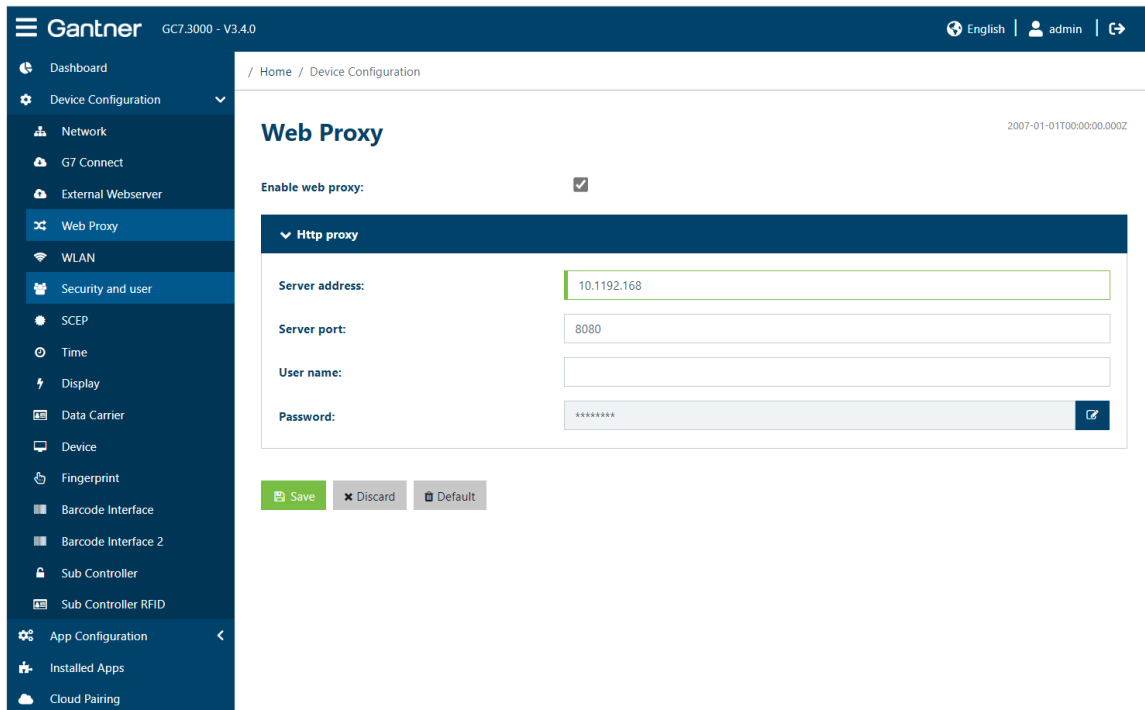


Fig. 5.26 – GC7.3000 configuration - Web proxy

A web proxy server can be configured in order to direct all outgoing connections via this web proxy server.

- Enable web proxy: Enable 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.

5.4.6 Device configuration – WLAN

Fig. 5.27 – GC7.3000 configuration - WLAN settings

A GC7.3000 controller can also communicate using WLAN instead of via the LAN network. When WLAN is enabled, additional options are displayed.

- Enable WLAN: With this option, WLAN can be enabled or disabled.
- DHCP assigned IP address: The method for assigning the IP address is defined here. Enable this option to obtain the address automatically from a DHCP server. If disabled, the static IP addresses must 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).
- Ip6 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 “5.4.2 Device configuration - Network”.
- Standard gateway selection: Select whether the GC7.3000 should always use the WLAN or Ethernet connection or whether the interface itself should be selected via “Autodetection”.
- Preferred frequency: If WLAN is being used for the network connection, you can select the preferred frequency (2.4 GHz or 5 GHz) can be selected here.

5.4.7 Device configuration - Security and user

Fig. 5.28 – GC7.3000 configuration – Security and user

Here, you can define the users who are allowed to access the GC7.3000 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, for example, by the management software eLoxx Relaxx.

- 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, the eLoxx Relaxx software creates a new, secure password for communication. If the password is changed here, it must also be entered into the eLoxx Relaxx software.

- Enable FTP access: Here, the FTP server in the GC7.3000 controller can be enabled or disabled (disabled by default).
- Add eLoxx One user: The two pre-defined users for eLoxx One can be configured here, e.g., defining the login details. You can also configure additional users via the "Add eLoxx One user".

5.4.8 SCEP (Simple Certificate Enrollment Protocol)

The screenshot shows the Gantner GC7.3000 V3.4.0 configuration interface. The sidebar on the left contains navigation options: Dashboard, Device Configuration (selected), Network, G7 Connect, External Webserver, Web Proxy, WLAN, Security and user, SCEP (selected), Time, Display, Data Carrier, Device, Fingerprint, Barcode Interface, and Barcode Interface 2. The main content area is titled 'SCEP' and shows the following configuration options:

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

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

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

At the bottom of the form are three buttons: **Save**, **Discard**, and **Default**.

Fig. 5.29 – GC7.3000 configuration - SCEP

SCEP is a protocol for requesting and issuing digital certificates quickly and easily. These certificates are used to establish secure communication between the GC7.3000 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 GC7.3000 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 GC7.3000 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.

5.4.9 Device configuration - Time

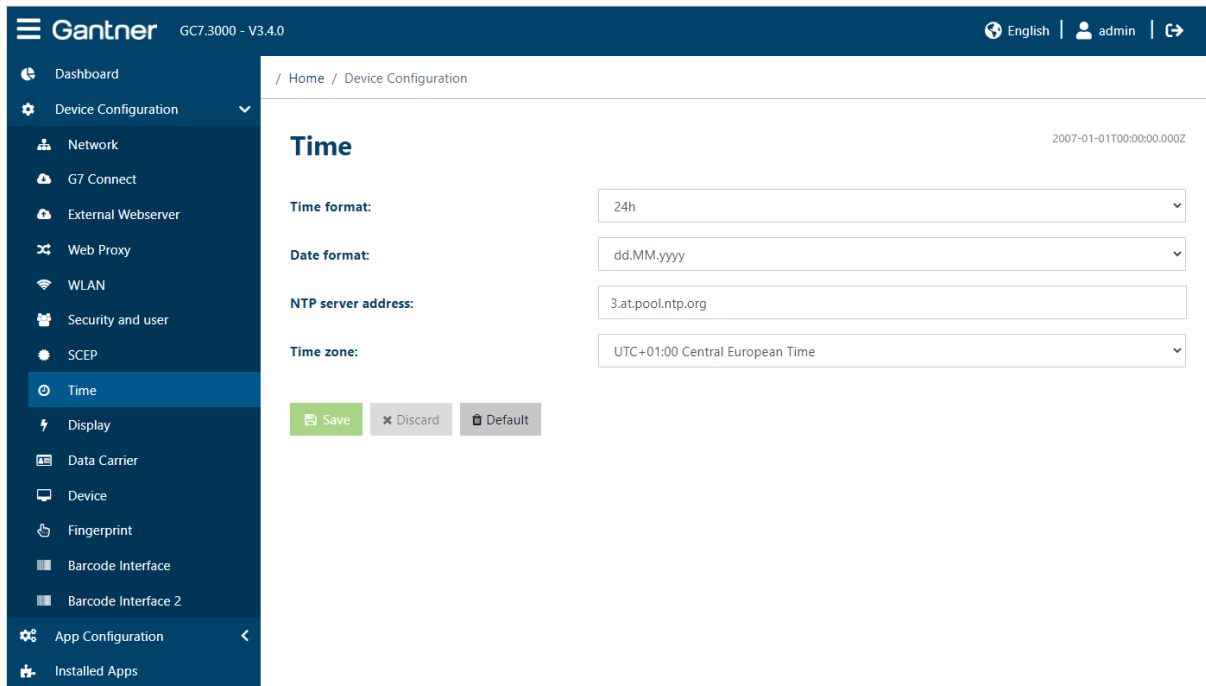


Fig. 5.30 – GC7.3000 configuration – Time

With these settings you can define how the time should be set and used in the GC7.3000.

- 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.
- 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 displayed.
- NTP server address: An NTP server can be used to supply the time in a network to the users/devices. You can enter the address of the NTP server here. If an address is not entered here (empty field), the NTP server will not be used.
- Time zone: Select here the time zone in which the GC7.3000 controller is operating.

5.4.10 Device configuration - Display

Fig. 5.31 – GC7.3000 configuration – Display

These settings are used when an external display is connected to the GC7. These settings can be used to adjust the brightness of the display and to set the times when the display should switch to the screensaver or advertising display.

- 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 "5.4.17. 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.

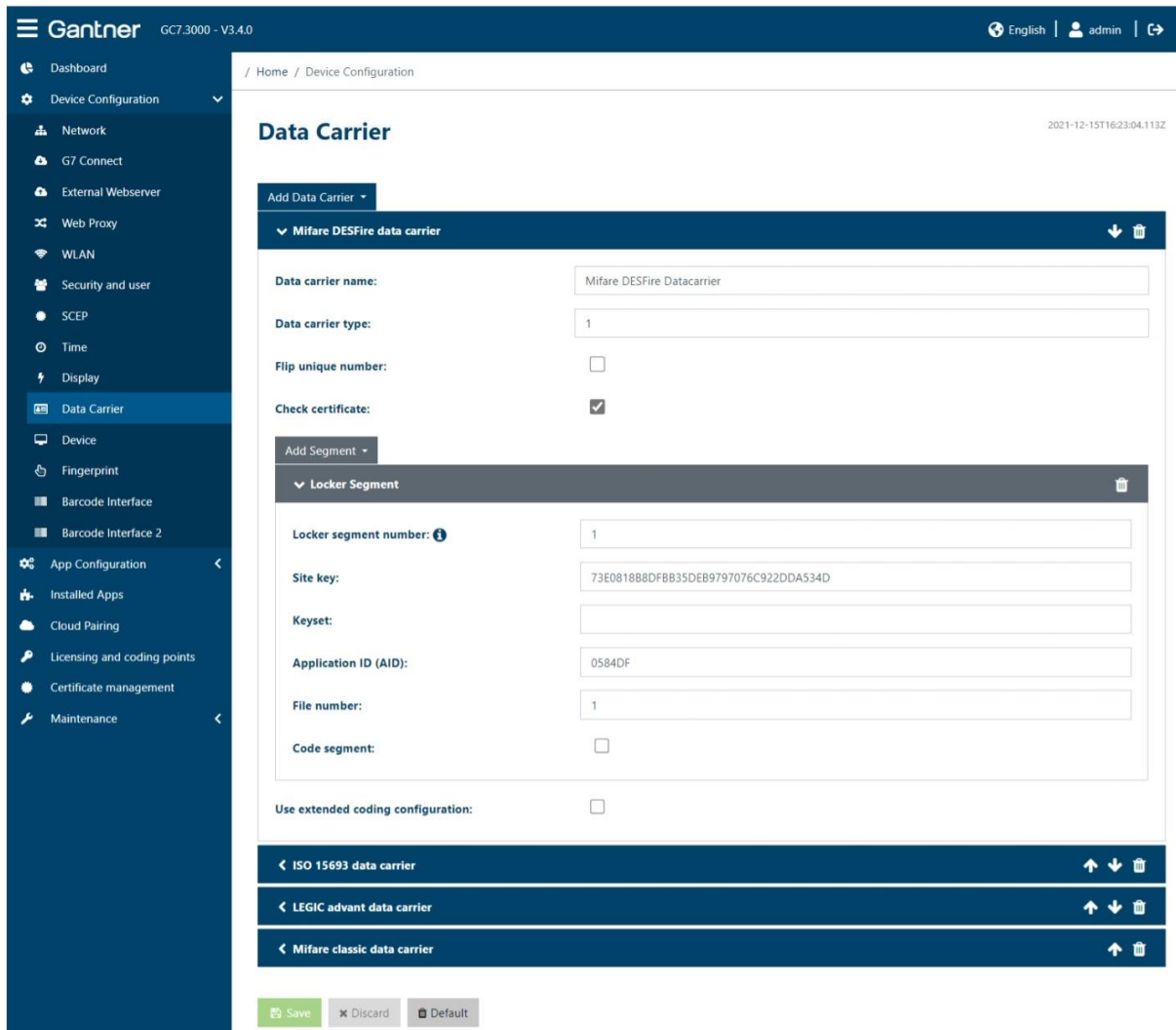
- External screen:

If an external screen is connected to the GC7.3000, the settings for the screen can be configured here.

The following settings are possible for the external screen:

- Resolution: Select the correct resolution for the screen from one of the listed resolutions (width x height in pixels).
- Screen size: Enter the size of the screen. The specification is the diagonal in inches as well as the width to height ratio (e.g., 16:9).
- Custom touchscreen calibration: If you enable this option, you can calibrate the touchscreen yourself. The calibration data is provided in the following text box.
- Calibration data: Displayed only when the "Custom touchscreen calibration" option is selected.

5.4.11 Device configuration - Data carrier



The screenshot shows the 'Data Carrier' configuration page in the Gantner GC7.3000 V3.4.0 interface. The left sidebar contains a navigation menu with options like Dashboard, Device Configuration, Network, G7 Connect, External Webserver, Web Proxy, WLAN, Security and user, SCEP, Time, Display, Data Carrier (selected), Device, Fingerprint, Barcode Interface, and Barcode Interface 2. The main content area is titled 'Data Carrier' and includes a timestamp '2021-12-15T16:23:04.113Z'. It features an 'Add Data Carrier' button and a dropdown menu for 'Mifare DESFire data carrier'. Below this, there are input fields for 'Data carrier name' (Mifare DESFire Datacarrier), 'Data carrier type' (1), 'Flip unique number' (checkbox), and 'Check certificate' (checkbox, checked). A 'Locker Segment' section is also present, with fields for 'Locker segment number' (1), 'Site key' (73E081888DFB835DEB9797076C922DDA534D), 'Keyset' (empty), 'Application ID (AID)' (0584DF), 'File number' (1), and 'Code segment' (checkbox). At the bottom, there are buttons for 'Save', 'Discard', and 'Default'. A list of data carrier types is shown at the bottom: 'ISO 15693 data carrier', 'LEGIC advant data carrier', and 'Mifare classic data carrier', each with up/down arrows and a delete icon.

Fig. 5.32 – GC7.3000 configuration – Data carrier

The settings for the different types of data carriers that will be used with the GC7.3000 or the connected readers are configured here. These settings must be set correctly so that the data carriers can be used. Multiple data carrier types can also be configured.

- Add data carrier: To configure a new data carrier type, click on this field 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 using the icons   on the right.

The settings for the data carrier types are different depending on the type of data carrier used. Please speak to your sales partner if you have any questions regarding the exact settings.

If the GC7.3000 is used for locker control via the G7 Main Controller App, configure the data carrier settings for the sub controllers in the "Sub Controller RFID" menu item.

5.4.12 Device configuration – Device

Fig. 5.33 – GC7.3000 configuration – Device settings

Here you will find the basic settings related to the GC7.3000. These are:

- Location: A location can be entered here. This name is displayed to assist the user to distinguish between multiple GC7.3000 controllers. Special characters are not allowed. When entering these characters, you will be informed with a message.
- Serial/Article number: The serial number and article number of the GC7.3000 are displayed here.
- Sound volume: This setting has no function with the GC7.3000.
- Pin code configuration menu: This setting has no function with the GC7.3000.
- Configuration menu mode: This setting has no function with the GC7.3000.
- Log level: In this field, the types of events to be recorded by the GC7.3000 can be defined. This log can be displayed and read out with the menu item "Log Viewer" (see "5.4.24. Maintenance - Log viewer"). Depending on the setting here, different messages are logged:
 - ERROR: All errors are displayed. These include, e.g., connection errors to G7 Connect.
 - WARNING: Warning messages are displayed. These include, e.g., logins in the web interface.
 - INFO: Information messages are displayed, e.g., when a data carrier is in the read field and when it has been read.
 - DEBUG: Detailed debug messages are displayed for service purposes.

5.4.13 Device configuration - Fingerprint

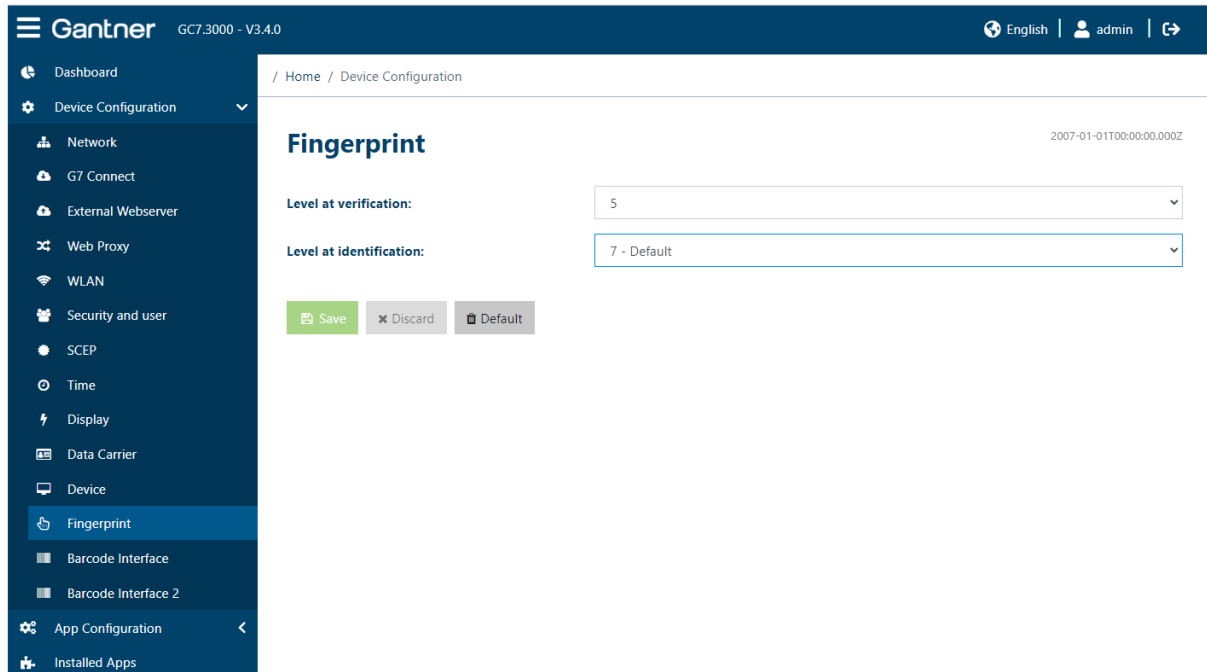


Fig. 5.34 – GC7.3000 configuration – Fingerprint settings

This setting is only relevant when a fingerprint reader, e.g., a GR7 with fingerprint reader, is being used with the GC7.3000.

- Level at verification: This value determines the accuracy of the fingerprint reader for verification, i.e., when the fingerprint is used as an additional confirmation of an identification by means of data carrier or similar. 1 = lowest level, 10 = highest level. Certain people (e.g., tradespeople who work with their hands) may have weaker fingerprints than others. If many users have difficulty reading their fingerprint, it may be helpful to lower the verification level.

- 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.

NOTE! This feature is only supported with certain apps.

5.4.14 Device configuration – Barcode interface

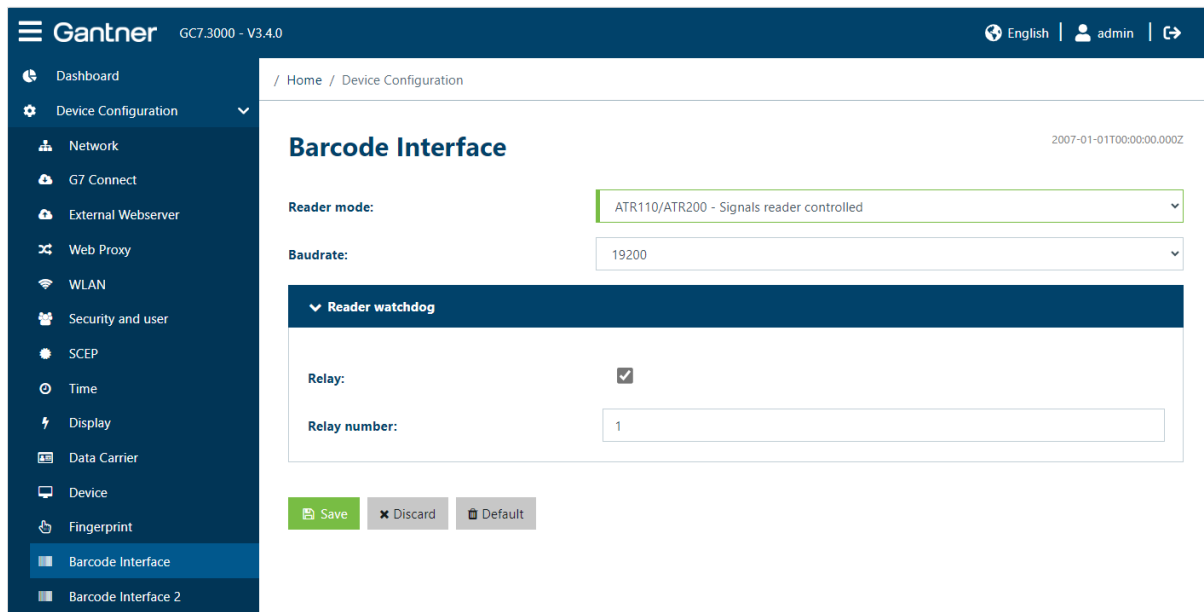


Fig. 5.35 – GC7.3000 configuration – Settings for the barcode interface

These settings are only relevant if a barcode reader is being used with the GC7.3000 (see “4.5. Connecting external devices via RS-232 (e.g. barcode scanners)”). Up to two barcode readers can be connected with separate configuration settings possible for each reader (“Barcode Interface” and “Barcode interface 2”).

- Reader mode:
 - If a barcode reader is connected to the GC7.3000, 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.
- Baud rate:
 - The transmission rate of the barcode reader.
- Reader watchdog:
 - This section is displayed if one of the “ATR110/ATR220” settings is selected for the “Reader mode” option.
 - The settings for “Internal 5V switch” and “Relay” with the relay number relate to the barcode reader monitoring. If the communication connection from the GC7.3000 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).

5.4.15 Device configuration - Sub controller (RFID)

The “Sub Controller” and “Sub Controller RFID” pages are only displayed if the G7 Main Controller App is activated in the controller.

Sub Controller

Emergency mode: Full

Locking timeout: 10 s

Auto close free locker: ☐

Auto lock personal/dynamic locker: ☐

Push to Open - Personal Locker: ☐

Push to Open - Dynamic Locker: ☐

Push to Open - Free Locker: ☐

Push to Open timeout: 30 s

Enable locker light: ☒

Light on duration time: 240 s

Enable USB charging: ☒

Lock manipulation detection: ☒

Alarm mode: ☒

Locker signalling

Beeper: ☒

Acoustic alarm: ☐

Advanced Acoustic Signaling Mode: ☐

Beeper volume: 100 %

GAT Lock 5xxx compatibility: ☐

Show rented: ☒

Color unlocked / not reserved: Deep green

Intensity unlocked / not reserved: 70 %

Color locked / reserved: Deep red

Intensity locked / reserved: 70 %

One time signaling (Eco.Lock compatibility): ☐

Save Discard Default

Fig. 5.36 – GC7.3000 configuration – Settings for the sub controller

The settings refer to the sub controllers connected to the GC7.3000. For instructions on these settings, please refer to the G7 Central Locker manual.

5.4.16 App configuration

In this menu, the settings for the active app in the GC7.3000 controller are defined. The sub-menu items and settings change depending on the activated app. The following example shows the menu for the G7 Access app.

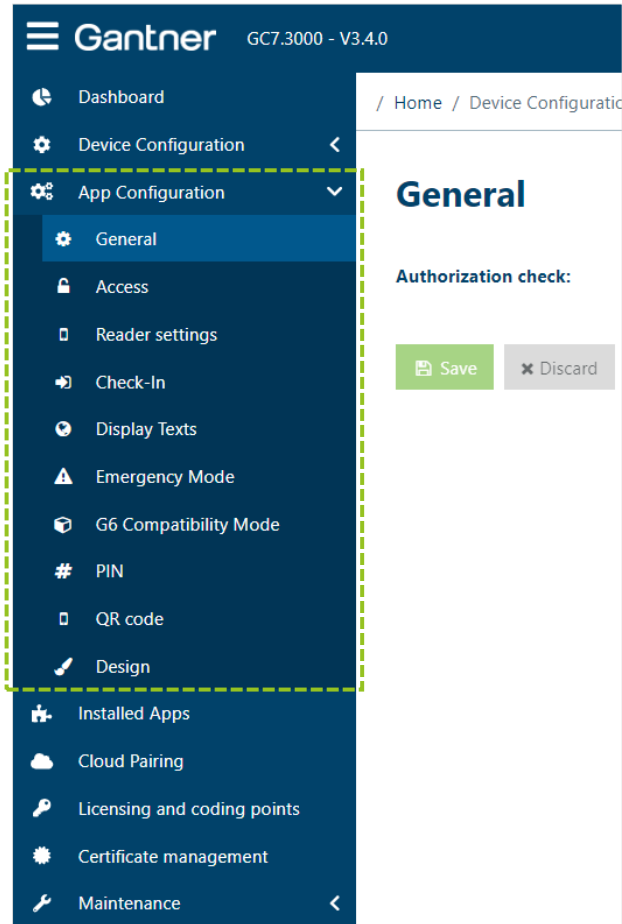


Fig. 5.37 – GC7.3000 configuration – App configuration menu (e.g., G7 Access App)

A separate manual is available for each G7 app. Information on the G7 Access App, which is pre-installed in the GC7.3000 upon delivery, and the settings available for this app can be found in the G7 Access App manual.

5.4.17 Installed apps

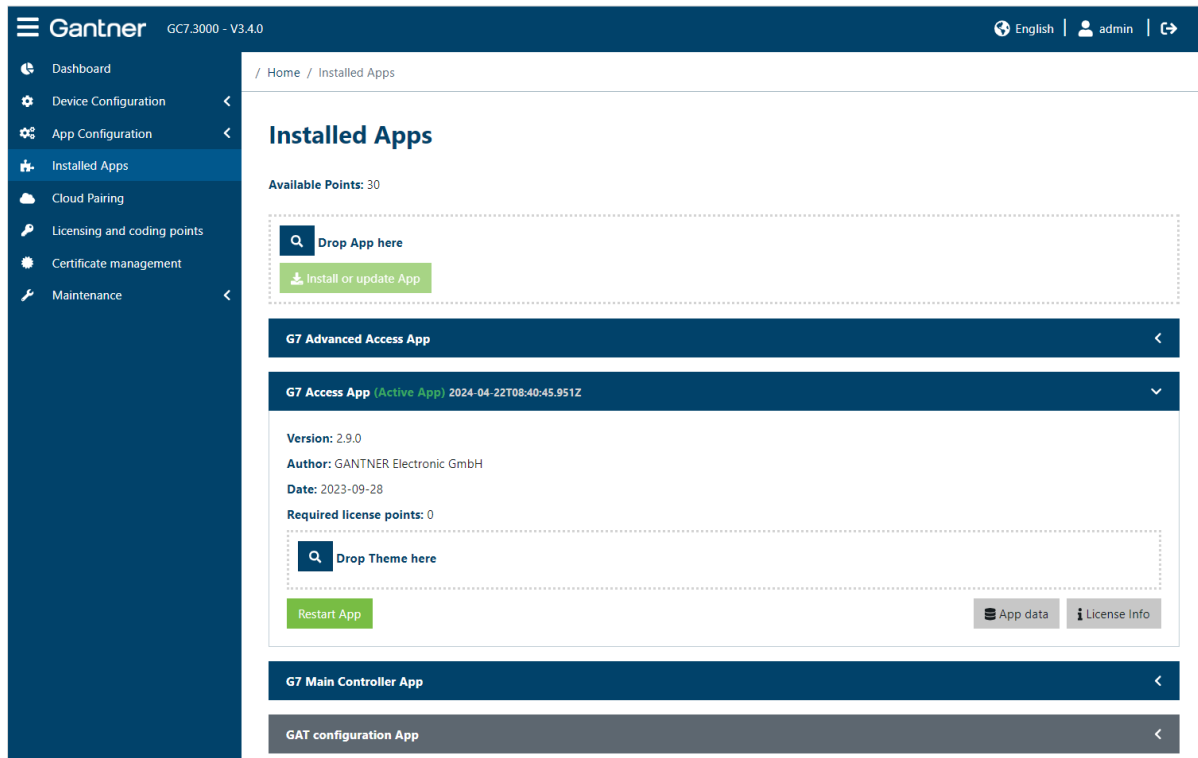


Fig. 5.38 – GC7.3000 configuration - Installed apps

Different apps can run on a GC7.3000. Since the GC7.3000 is designed for access control, the default app used for the GC7.3000 is the G7 Access App. This app is already installed and activated in the GC7.3000 upon delivery.

Additional apps can be subsequently installed in this window. For most apps, license points are required for this, which can be purchased from Gantner.

All installed apps are listed in this window and the currently active app is indicated with the green “Active App” text.

- To start another app, click on the “Activate” button for the desired app.
 - The app starts, which can take up to one minute, and the GC7.3000 then 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 field “Drag App here”, a new app or a new version of an already installed app can be uploaded to the GC7.3000 controller. The app file is required for this, which must be dragged and dropped onto this field.
- 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.



Themes have no effect on the GC7.3000 without an external display. A theme is a template file (ZIP archive) that determines the format of the display (e.g., text types, colors, positions, etc.). The theme formatting is done using CSS, which offers a lot of freedom in the design of the themes. In addition, a theme archive can also contain images that can be displayed on a screen when using the “Advertising” function. These images are located in the “screensaver” subfolder of the archive file.

5.4.18 Cloud pairing

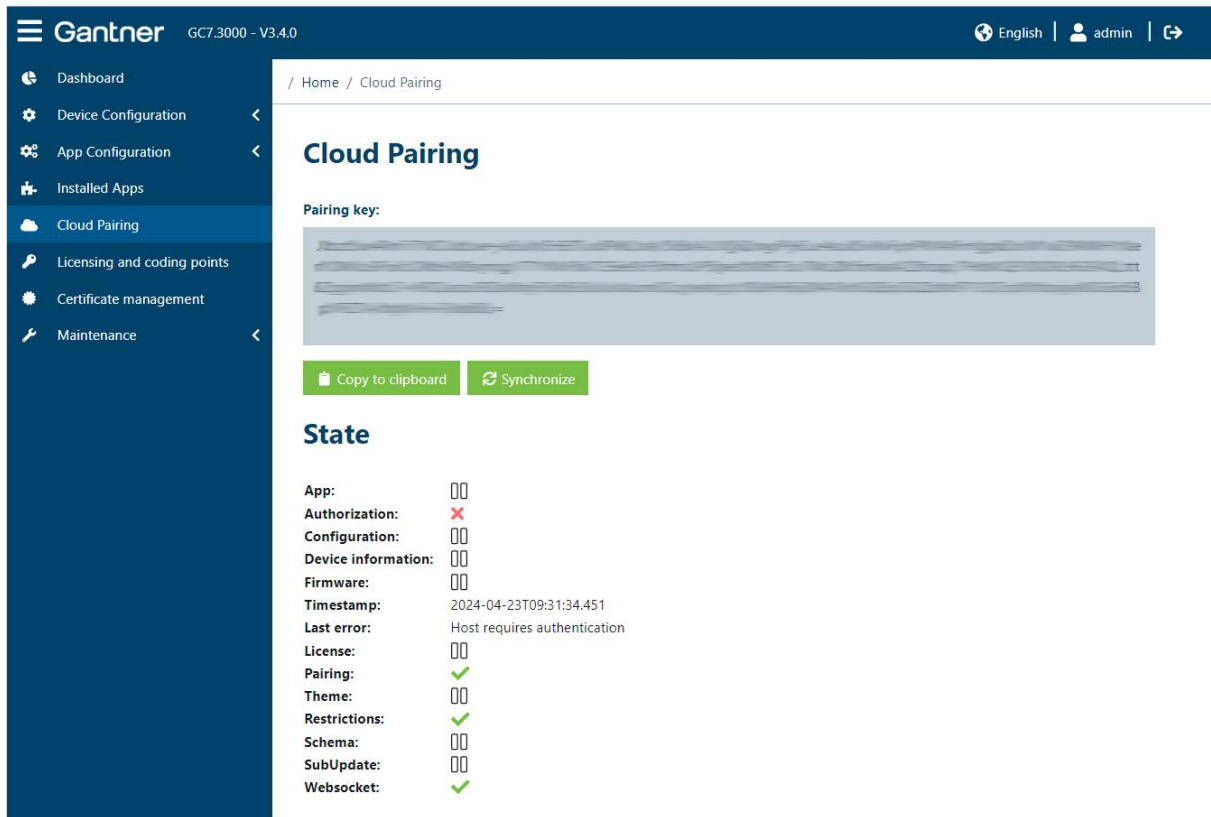


Fig. 5.39 – GC7.3000 configuration – Cloud pairing

G7 Connect is an online platform that allows operators to conveniently manage all their projects and facilities. The Gantner Generation G7 devices used in the facilities can also be conveniently managed and configured here.

To add a GC7.3000 controller to a project in G7 Connect, the GC7.3000 must be connected ("pairing") to the Gantner Cloud once. This process requires a pairing key, which is displayed in this window.

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

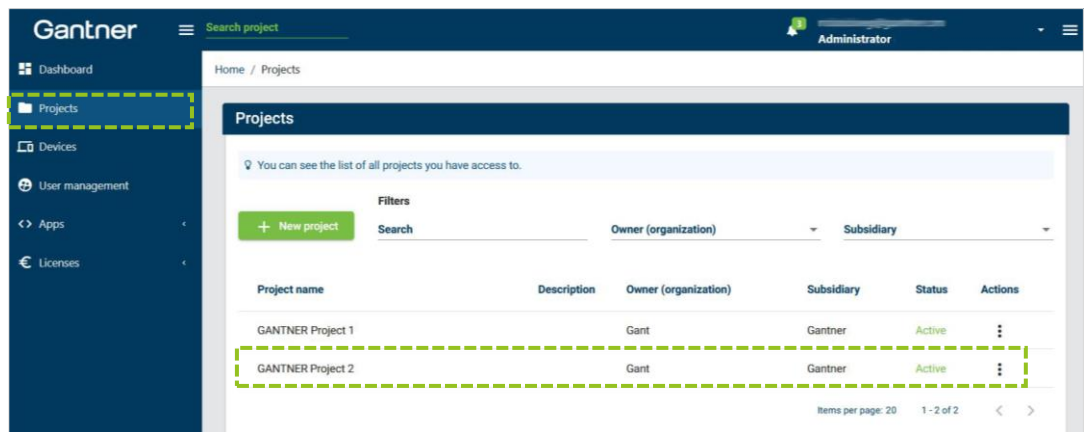


Fig. 5.40 – List of projects in G7 Connect

- Click on the project where the GC7.3000 is to be added.
 - The project page opens. The selected project is displayed above the menu on the left.
 - The devices already assigned to the project are listed on the right.

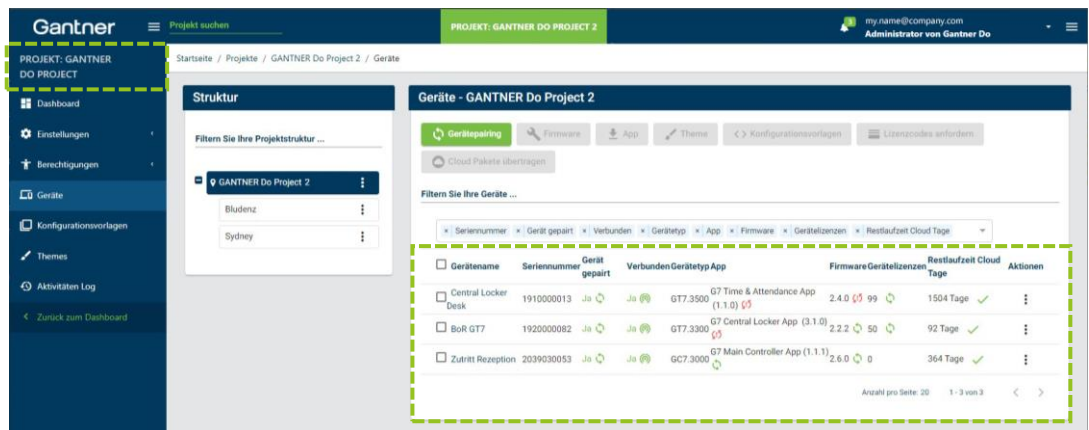


Fig. 5.41 – List of devices in the project

- Click on "Device pairing" here.

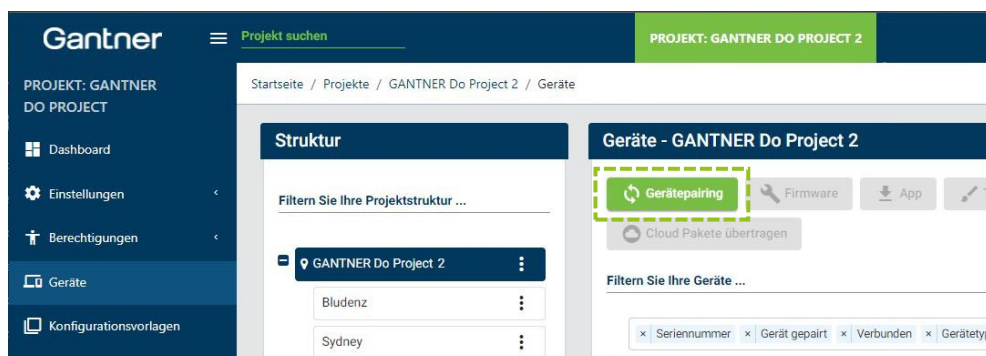


Fig. 5.42 – Pairing a GC7.3000

- The device pairing window opens.

Device pairing [X]

Please insert your pairing key in input below and click Pair device to perform pairing. If pairing is successful you will see your device in the list below.

Pairing key
12345678

Name

Description

Pair device

Fig. 5.43 – Cloud pairing – Enter pairing key

- ▶ Enter the pairing key, as displayed in the “Cloud Pairing” menu, into the configuration of the GC7.3000.
- ▶ 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 GC7.3000 attempts to establish an outgoing connection to G7 Connect via the Internet. The GC7.3000 must therefore be switched on and online, i.e., it must be connected to the Internet (G7 Connect). Check the connections and firewall settings if pairing and synchronization does not work.
 - When the GC7.3000 is found, it is displayed in the devices list of the project.
 - In the web interface, the status of the pairing process along with other indicators are displayed. A green tick next to “Pairing” indicates that the device has been successfully paired.

Gantner GC7.3000 - V3.4.0 English admin

/ Home / Cloud Pairing

Cloud Pairing

Pairing key:

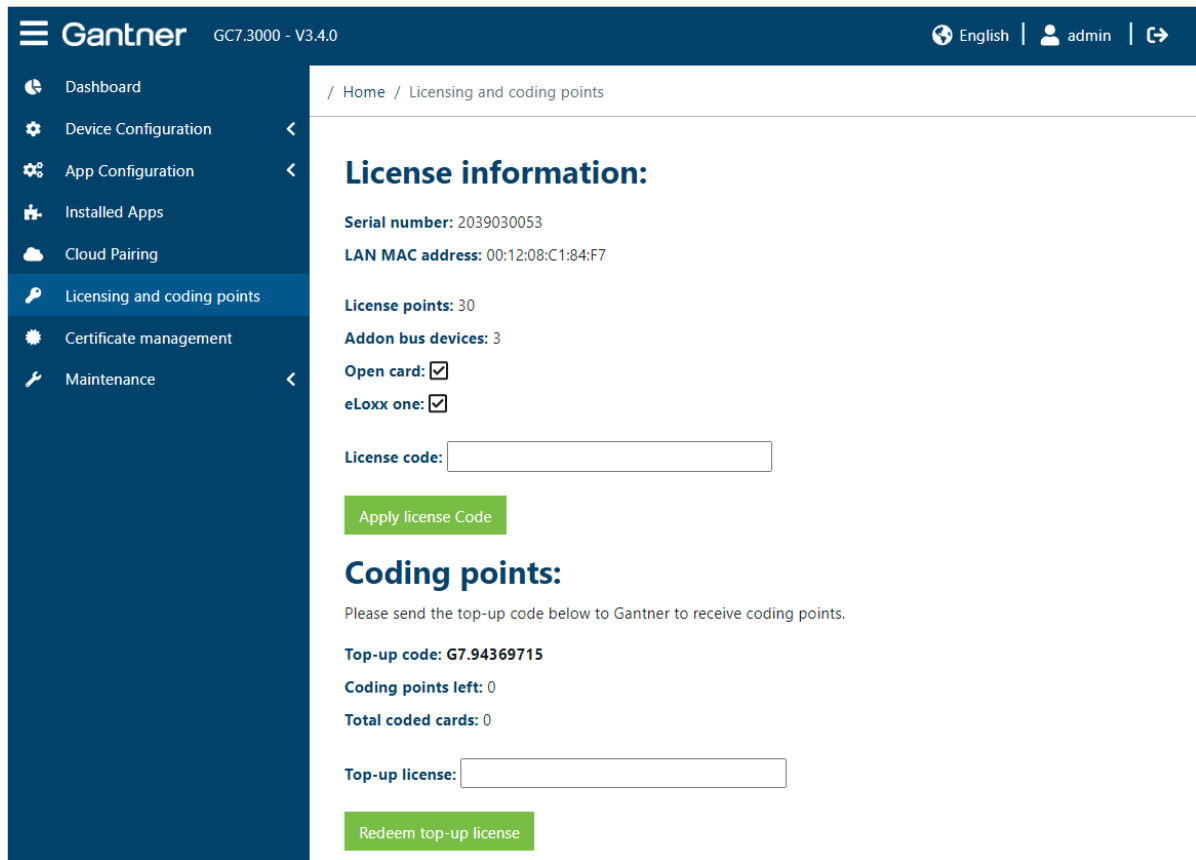
Copy to clipboard Synchronize

State

App:	00
Authorization:	✗
Configuration:	00
Device information:	00
Firmware:	00
Timestamp:	2024-04-23T09:31:34.451
Last error:	Host requires authentication
License:	00
Pairing:	✓
Theme:	00
Restrictions:	✓
Schema:	00
SubUpdate:	00
Websocket:	✓

Fig. 5.44 – Cloud pairing – Status of the pairing process

5.4.19 Licensing and coding points



The screenshot shows the Gantner GC7.3000 configuration interface. The left sidebar contains a menu with options: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points (selected), Certificate management, and Maintenance. The main content area is titled 'License information:' and displays the following details:

- Serial number:** 2039030053
- LAN MAC address:** 00:12:08:C1:84:F7
- License points:** 30
- Addon bus devices:** 3
- Open card:** ☒
- eLoxx one:** ☒
- License code:**
- Apply license Code** (button)

Below the license information, there is a section titled 'Coding points:' with the following details:

- Please send the top-up code below to Gantner to receive coding points.
- Top-up code:** G7.94369715
- Coding points left:** 0
- Total coded cards:** 0
- Top-up license:**
- Redeem top-up license** (button)

Fig. 5.45 – GC7.3000 configuration – Licensing and coding points

On this page, the network and license information for the GC7.3000 are displayed, and you can also add new license points here.

- | | |
|----------------------|---|
| - Serial number: | The serial number of the GC7.3000. |
| - MAC address LAN: | Unique, internal network address of the GC7.3000. |
| - 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: | The maximum number of devices (controller and I/O extensions) that can be connected to the expansion bus of the GC7.3000. |
| - Open card: | A tick in this field indicates that the "Open Card" license has been enabled and the certificate check is switched off, i.e., data carriers that were not coded by Gantner can also be used. |
| - eLoxx One: | A tick here indicates that the license for the eLoxx One locker system management software has been activated. Provided that the G7 Main Controller App is the active app, eLoxx One can then be started on the "Dashboard" page. |
| - License code: | Here you can enter a license code to manually load license points onto the device. |

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 GC7.3000. 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 must be entered 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 G7 Connect and allocated to the individual devices.

5.4.20 Certificate management

Certificate management:

Show certificates Add CA certificates Generate new self-signed certificate Generate CSR Install server certificate Install 802.1X certificates

Simple Certificate Enrollment Protocol (SCEP)

Subject	Issuer	Valid from	Valid to	Serial number	Type
Factory Default IP: 192.168.2.20 GANTNER Electronic GmbH	Factory Default GANTNER Electronic GmbH	2019-01-01 00:01:10Z	2048-12-24 00:01:10Z	23:da:80:f2:cad:c5:1:9a:43:31:f1:7a:09:5c:a3:74:ab:ce:7a:fc	Server
GlobalSign GlobalSign GlobalSign Root CA - R6	GlobalSign GlobalSign	2014-12-10 00:00:00Z	2034-12-10 00:00:00Z	45:e6:bb:03:83:33:c3:85:65:48:e6:ff:45:51	CA
Baltimore CyberTrust Root Baltimore CyberTrust	Baltimore CyberTrust Root Baltimore	2000-05-12 18:46:00Z	2025-05-12 23:59:00Z	02:00:00:b9	CA
D-TRUST Root Class 3 CA 2 EV 2009 D-Trust GmbH	D-TRUST Root Class 3 CA 2 EV 2009 D-Trust GmbH	2009-11-05 08:50:46Z	2029-11-05 08:50:46Z	09:83:f4	CA

Fig. 5.46 – GC7.3000 configuration – Certificate management

The certificates stored in the GC7.3000 are displayed here. The certificates are used to verify the authenticity and integrity of 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).

Certificate management:

Show certificates Add CA certificates Generate new self-signed certificate Generate CSR

Simple Certificate Enrollment Protocol (SCEP)

Add certificate authority (CA) certificate. Used for cloud applications.

Drop certificate here (PEM or DER format)

Add CA certificates Restore recommended CA certificates

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 GC7.3000 and the server is being used (via TLS over HTTPS or WSS), the GC7.3000 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 "Generate new self-signed certificate". The GC7.3000 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 GC7.3000 acts as a web server, e.g., when using eLoxx Relaxx, which acts as a "client" and establishes the connection to the GC7.3000 "server", a certificate is required on the server, i.e., on the GC7.3000 controller, for a secure connection using TLS. You can create this using CSR and then install it here. To do this, drag the certificate file onto the field provided and click on "Install server certificate".

- Install 802.1X CA certificate:

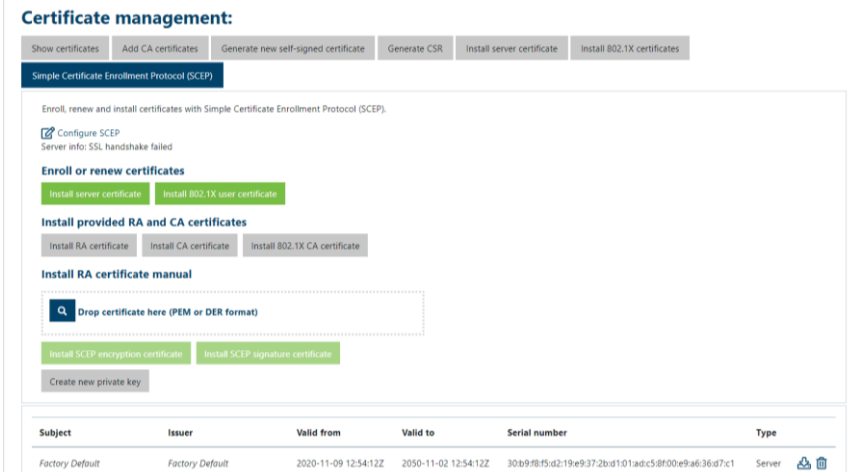
Here, you can install an official certificate from a certification authority for authentication using 802.1X. To do this, drag the file with the certificate to the field provided and click "Install 802.1X CA Certificate".

- 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:



Certificate management:

Show certificates | Add CA certificates | Generate new self-signed certificate | Generate CSR | Install server certificate | Install 802.1X certificates

Simple Certificate Enrollment Protocol (SCEP)

Enroll, renew and install certificates with Simple Certificate Enrollment Protocol (SCEP).

 **Configure SCEP**
Server info: SSL handshake failed

Enroll or renew certificates

Install server certificate | Install 802.1X user certificate

Install provided RA and CA certificates

Install RA certificate | Install CA certificate | Install 802.1X CA certificate

Install RA certificate manual

 Drop certificate here (PEM or DER format)

Install SCEP encryption certificate | Install SCEP signature certificate

Create new private key

Subject	Issuer	Valid from	Valid to	Serial number	Type
Factory Default IP: 10.1.112.41	Factory Default GANTNER Electronic GmbH	2020-11-09 12:54:12Z	2050-11-02 12:54:12Z	30b9dbf5d219e9372bd101adc58f00e9a636d7c1	Server

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 “5.4.8. 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 GC7.3000 is operating as a web server (e.g., when using the eLoxx Relaxx software, which acts as a “client” and establishes the connection to the “server” GC7.3000, a certificate is required for the server, i.e., on the GC7.3000, 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.

Install RA certificate manual


Drop certificate here (PEM or DER format)

Install SCEP encryption certificate

Install SCEP signature certificate

Create new private key

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

5.4.21 Maintenance - Device

The screenshot shows the 'Maintenance' section of the Gantner GC7.3000 V3.4.0 web interface. The left sidebar contains navigation links: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance (expanded). The 'Maintenance' section includes 'Device' (selected), Update Firmware, Addon Bus, Log Viewer, Device State, and Legal infos.

Maintenance:

Reboot Factory reset

Date and Time:

Device time: 2024-04-23 14:24:57
 Cloud connected: ☒
 NTP server: ☒

23/04/2024 11 : 15 : 55

Set time with NTP Set PC time Set time

Memory usage:

Total memory: 507332 kB
 Free memory: 402740 kB
 API server: 168068 kB
 G6 server: 11826 kB
 App: 63171 kB

Load:

Average load: 6 %
 CPU1: 5 %
 CPU2: 7 %
 Frequency: 144 MHz

Connection statistics:

14:00:00 → 14:24:56	Last	Min	Max	Average	Count	Lost
Addonbus	0 ms	0 ms	0 ms	0 ms	0	97
Heartbeat G7 Connect	41 ms	36 ms	44 ms	40 ms	30	0
Heartbeat management software	90 ms	73 ms	151 ms	99 ms	25	0

Fig. 5.47 – GC7.3000 configuration – Maintenance settings

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

Maintenance

- Click on the “Reboot” button to restart the GC7.3000.
 - 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 GC7.3000 to its default settings, click on the “Factory reset” button.

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

 - After resetting to the default settings, the controller functionally returns to the state it was upon delivery. Most of the data is deleted, however, the license points for example are still available.

Date and time

- Device time: The current time in the GC7.3000 is displayed here. This time is updated every second. The time can be changed in the device configuration (see “5.4.9. Device configuration - 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 “5.4.3. Device configuration - G7 Connect”).
- NTP server: This setting defines whether an NTP server is used for automatic time synchronization in the GC7.3000 (tick = enabled). The setting for using an NTP server is provided in the configuration menu of the GC7.3000 (see 5.4.9. Device configuration - Time).

► To reset the time in the GC7.3000, 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 GC7.3000. |
| - 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 GC7.3000. |

Memory usage

Information about the memory in the GC7.3000, 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 GC7.3000 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 GC7.3000.

5.4.22 Maintenance – Update firmware

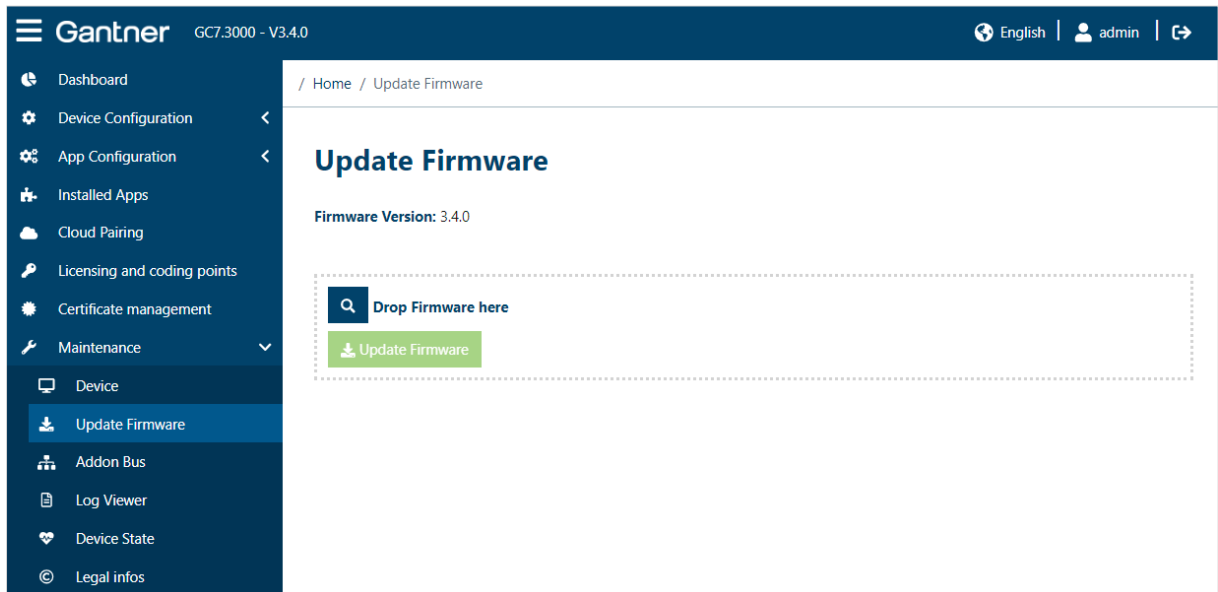
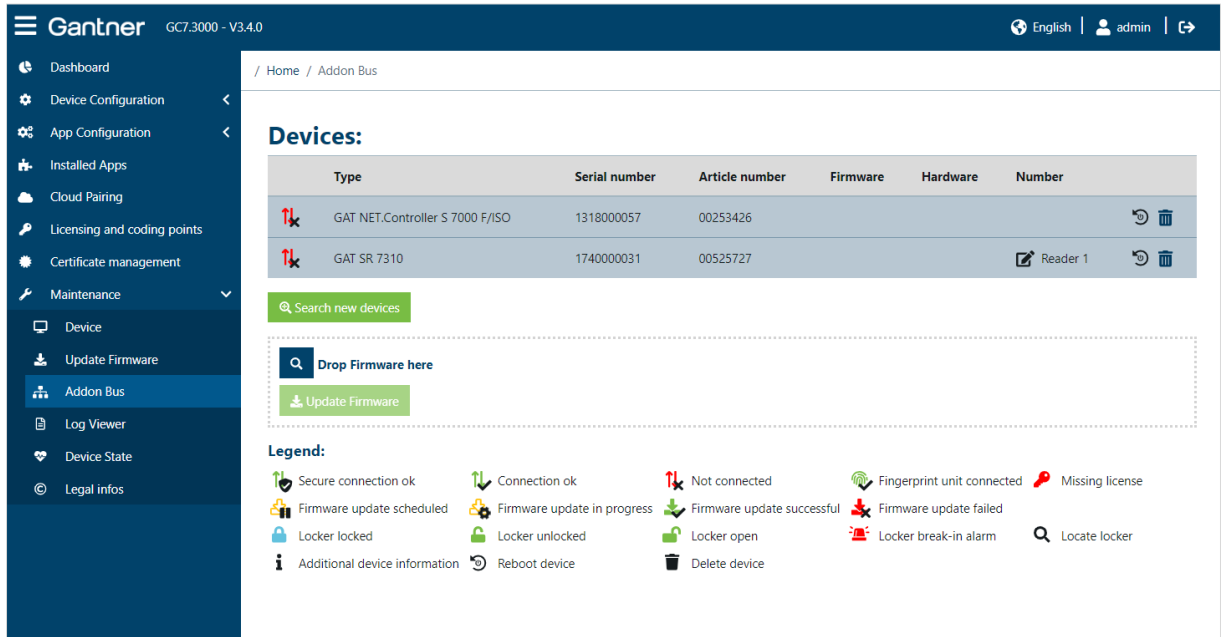


Fig. 5.48 – GC7.3000 configuration – Update firmware

Here, the firmware currently installed in the GC7.3000 is displayed.

- To update the firmware, drag the firmware file onto the “Drop Firmware here” field.
 - Click on “Update Firmware”.
 - The new firmware is loaded into the GC7.3000 and the device restarts.
- ATTENTION!** During the firmware update, ensure that the power supply to the GC7.3000 is not disconnected.

5.4.23 Maintenance – Addon bus (external devices)



The screenshot shows the Gantner GC7.3000 configuration interface. The sidebar on the left contains navigation options: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'Devices:' and displays a table of connected devices. The table has columns for Type, Serial number, Article number, Firmware, Hardware, and Number. Two devices are listed: GAT NET.Controller S 7000 F/ISO and GAT SR 7310. Below the table are buttons for 'Search new devices' and 'Drop Firmware here'. A legend at the bottom explains various status icons: Secure connection ok, Connection ok, Not connected, Fingerprint unit connected, Missing license, Firmware update scheduled, Firmware update in progress, Firmware update successful, Firmware update failed, Locker locked, Locker unlocked, Locker open, Locker break-in alarm, Locate locker, Additional device information, Reboot device, and Delete device.

Fig. 5.49 – GC7.3000 configuration – Addon bus

Information about the external devices connected to the GC7.3000 via the expansion bus are displayed here. These include the RFID readers connected to the RJ45 sockets “RS 485 SUB 1” and “RS 485 SUB 2” (see “4.3. Connecting a GR7 or GAT SR 7xxx / SLR 73xx RFID reader”). In Fig. 5.49, one reader is used. The symbol on the left in front of the respective device indicates whether the connection is OK (green symbol ) or whether the connection has been interrupted (red symbol ) , e.g., due to a defective cable.

Also displayed here are, e.g., expansion modules such as the GAT IO 705x relay expander.

- ▶ If a new device such as a reader is connected to the GC7.3000, it is not automatically displayed in the list. Click on “Search new devices” to search for and display all devices.
- ▶ A reader that is no longer connected to the device can be deleted by clicking on the trash can icon.
- ▶ You can change the numbering of a reader by clicking in the “Number” column.
- ▶ To install a new firmware for these devices, drag the firmware file to the “Drop Firmware here” field, then click on “Update Firmware”.
 - The new firmware is loaded to all connected devices of the matching type and the devices are restarted.

ATTENTION! The voltage supply to the external device must not be interrupted during the update process.

5.4.24 Maintenance - Log viewer

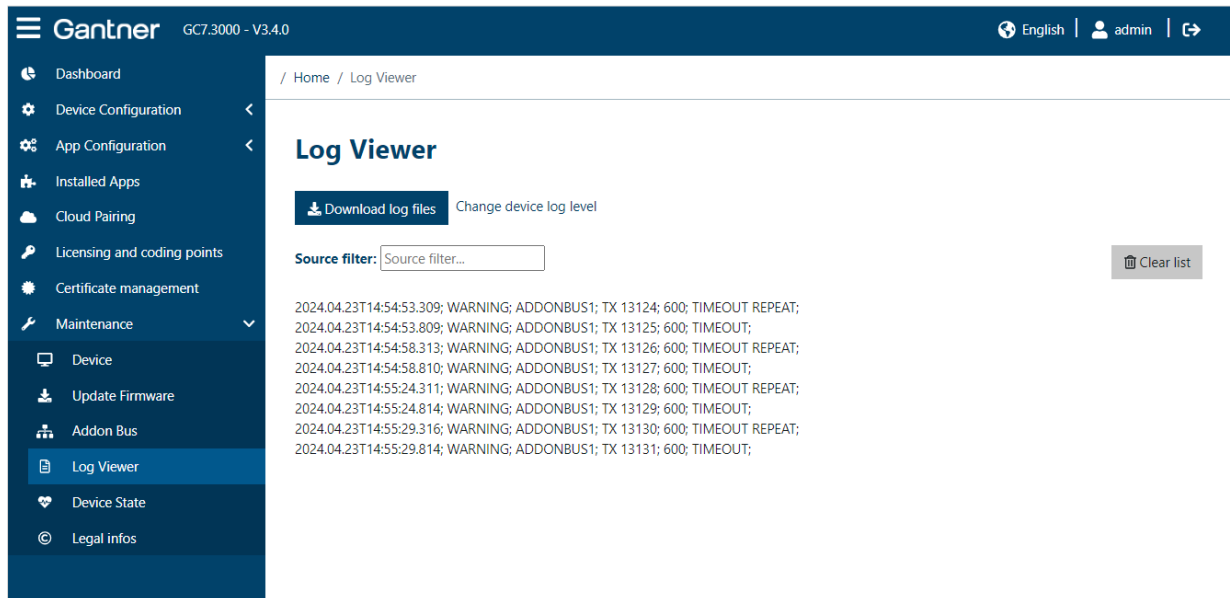


Fig. 5.50 – GC7.3000 configuration – Log viewer

All events and error messages are stored in the GC7.3000 as log files. The stored log files can be loaded from the device to the PC (file format = .csv).

If the “Log Viewer” page is open, all occurring events are displayed live. As soon as you close this page by opening another configuration page, the displayed events are sent out again and the next time you select the Log Viewer, the display is empty. However, the events are always recorded and can be downloaded.

- To load the log files from the GC7.3000, click on “Download log files”.
 - A file window opens in which you must specify the storage location.
 - The log files of the last 8 days are transferred to a ZIP file and saved in the selected location.



The events that will be recorded can be configured via the “Log Level” option (see “5.4.12. Device configuration – Device”).

- Clicking on the “Change device log level” text opens the device settings (see “5.4.12. Device configuration – Device”). Here you can change the log level, which defines the types of events that will be displayed in the live view (e.g., all info + warnings or only errors, etc.).

5.4.25 Maintenance - Device state

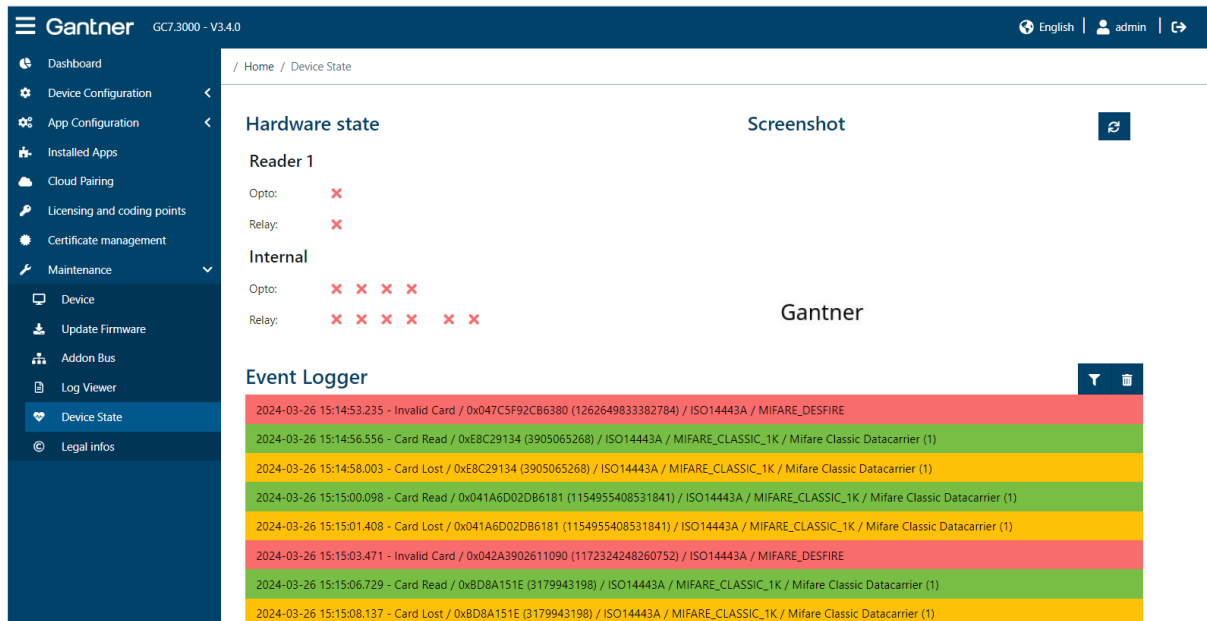


Fig. 5.51 – GC7.3000 configuration – Device state

A GC7.3000 controller has six digital relay outputs and two digital optocoupler inputs. These can be used for specific status detection and/or control. The status of these inputs and outputs is displayed here under “Hardware state”. These inputs and outputs do not have to be used. In Fig. 5.51 above, they are inactive. In addition, the inputs and outputs of connected readers are also displayed here, if present.

To the right of the hardware status display is the screenshot function for the GC7.3000. Since the controller does not have an integrated display, this display is not relevant for on-site operation. However, the G7 Access App supports a display, and the “internal” display texts are shown here. In addition, an external display can also be connected to the GC7.3000.

- ▶ To show a screenshot of the current display, press the refresh key  so that it is displayed in green and animated. The current live display is then always shown.
- ▶ Click the icon again to stop the live display . The currently displayed screen is then shown continuously.

The event logger is located in the lower area. Here, events recorded by the device can be displayed live.

- ▶ A corresponding entry is displayed as soon as an event occurs at the GC7.3000 (e.g., read data carrier) or the state of an optocoupler or relay changes.
- ▶ The filter button  displays all event types. Clicking on these events toggles them between active (green) and inactive (red). Only the events displayed in green are shown in the list.
- ▶ To clear the list, click on the trash can icon .

5.4.26 Maintenance – Legal information

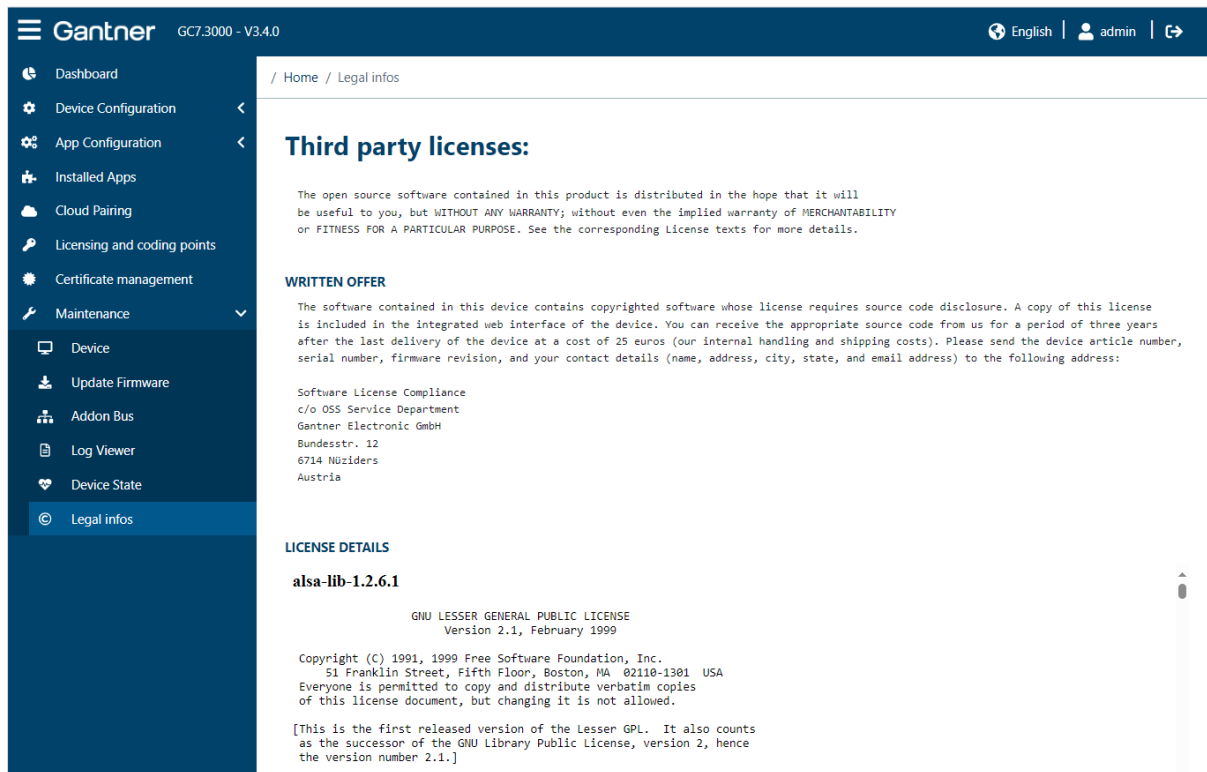


Fig. 5.52 – GC7.3000 configuration – Legal info

Displayed here is the license information for the third-party software included with the GC7.3000. For example, the GNU license information for the operating system in the GC7.3000.

5.5 Integration in control software

PC software can be used to control the GC7.3000. With this software, the data carriers and authorizations of the users are managed and thus the accesses for the doors or accesses of the system are enabled or blocked. When a data carrier is read at a GC7.3000, the controller transmits the information to the software, which makes the opening decision and sends the relevant commands to the controller to enable or deny access.

The GC7.3000 can also operate in emergency mode without communication with the PC software, e.g., in the event of a network failure. In this case, the GC7.3000 decides autonomously based on the saved authorization data as to which data carriers are authorized for access.

6 OPERATION

6.1 Target group

This chapter is intended for the system administrator and the operating personnel for the access system. It contains information on the operation of the GC7.3000 and the connected readers.

6.2 Operation of the GC7.3000 and reader

A major function of the GC7.3000 is the processing of identification requests when users read their credential at a connected reader. Therefore, the operation depends on the type of reader being used and its functionalities. The following example describes the operational process for a GR7.7310 reader.

In the idle state, the reader's reading field illuminates blue (1), and the LED bar is red (2) -> i.e., access is not permitted.



- ▶ Hold the data carrier near the reading field.
 - The data on the data carrier is read and transferred to the GC7.3000.
 - ▶ Depending on the configuration, it may also be necessary to subsequently enter a PIN code or scan a fingerprint.
 - This data is also transmitted to the GC7.3000.
 - - In emergency operation, the GC7.3000 checks the authorization based on the stored configuration.
 - - In normal operation, the data is sent from the GC7.3000 via the network interface to a higher-level PC software, which checks whether the data carrier is authorized to access the current door at the current time and sends the result to the GC7.3000 controller.
 - - If the authorization is valid, the GC7.3000 activates the relay(s) defined as the unlocking relay. This activates the door or turnstile and enables access.
 - - If the authorization is invalid, access is denied.
 - The LED bar (2) and the reading field (1) use colors to indicate the information for the user (e.g., green = access permitted, red = access denied). In addition, acoustic signals are emitted by means of a beeper.
- NOTE!** LEDs and beepers can be used to signal a wide variety of information. A detailed description can be found in the respective user manual of the readers.
- ▶ If the authorization is valid, the user must open the door or turnstile within the set unlocking time.
 - The GC7.3000 then returns to the idle state, depending on the door feedback.

6.3 Resetting the GC7.3000

It is possible to delete the configuration settings of a GC7.3000 and thus reset the controller to the default settings. This is completed using the RESET button on the side of the controller.

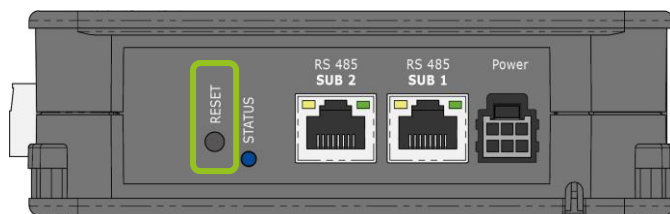


Fig. 6.1 – Button for resetting a GC7.3000

To perform the reset, complete the following steps.

- ▶ Press and hold the RESET key for approx. 12 seconds.
 - The "STATUS" LED starts to flash blue.
- ▶ Release RESET key within 3 seconds and press again briefly.
 - The configuration parameters are reset.

7 TECHNICAL DATA

Nominal voltage	DC 24 V (LPS/SELV)
Power supply	GAT NET.Power Supply 7020-1 100-240V / VI
Average power consumption	ca. 3 W
Authentication	802.1x
Security	SSL/TLS
Interface to the server	Ethernet
Serial interface for ext. devices	2 x RS-232
Connector	
- Server (Ethernet)	RJ45
- Supply	6-pin MOLEX
- Relay, optocoupler, RS-232, etc.	Screw terminal
Digital inputs	
- Quantity	4 x optocouplers (function configurable)
- Switching voltage	0 to 30 V DC ($U_{Low} < 2 \text{ V}$, $U_{High} > 18 \text{ V}$)
Digital outputs	
- Quantity	6 x relays (NO/NC, function configurable)
- Switching voltage	max. 30 V AC/DC
- Continuous current	max. 2 A
- Switching capacity	max. 60 VA
Weight	Approx. 600 g
Housing material	Plastic (ABS - VO)
Perm. ambient temperature	0 to +60 °C
Protection type	IP40
Protection class	I
Environment class (VdS 2110)	II (indoor conditions)
Compliance	CE, FCC, IC, ETL



gantner 
INSPIRED ACCESS

SALTO  **ECOSYSTEM**

SCAN FOR CONTACT

© 2024 Gantner
Gantner reserves the right to change technical specifications,
designs and services without prior notice.
Photos: GANTNER / SALTO Systems / Shutterstock

