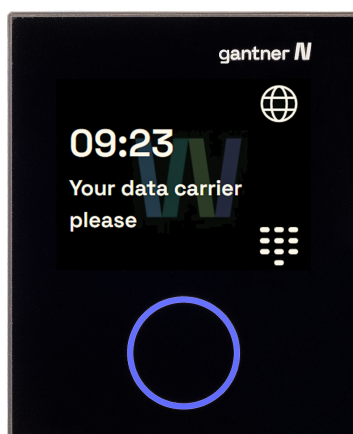


GT7 Lite

Multifunctional RFID Terminals GT7.0500, GT7.0510 and GT7.1300



Installation, Electrical Connections, Maintenance
Document version: 1.1



Copyright © 2026 Gantner Electronic GmbH

All rights reserved. Copying, reproducing, translating, converting to any electronic medium or machine-readable form, in whole or in part, is prohibited. The sole exception is the creation of a backup copy of software for your own use as a safeguard, insofar as this is technically possible and recommended by us. Any infringement will render the party committing such infringement liable to compensation payment.

Liability

Claims against the manufacturer based on the hardware and/or software products described in this manual shall depend exclusively on the provisions of the guarantee. Further claims are excluded, in particular the manufacturer assumes no liability for the completeness or accuracy of the content of this manual. We reserve the right to make changes and changes may be made at any time without prior notice.

Trademarks

Reference is made at this point to the identifications and registered trademarks used in this manual. All product or company names mentioned in this manual are for identification and explanation purposes only and, depending on the designation, may be trademarks or registered trademarks of the respective companies.

TABLE OF CONTENTS

1. Important information	5
1.1. Safety information	5
1.2. Certification information	6
1.3. Copyright information	7
1.4. Software license information	7
1.4.1. Send-in solution	8
1.5. Contact and inquiries	8
2. General information	9
2.1. About this manual	9
2.2. Target group	9
2.3. Terminology	9
2.4. Intended use	10
2.5. Functional description	10
2.6. System overview	11
2.7. Device overview	12
2.8. Device features and dimensions	13
3. Installation	15
3.1. Installation guidelines	15
3.2. Installation options	16
3.3. Surface installation with wall bracket	18
3.4. Surface installation with wall box	19
3.5. Semi-flush installation	21
4. Electrical connections	22
4.1. Power supply connection	22
4.2. Network connection (LAN/Ethernet)	23
4.3. Input and output connections	24
4.3.1. Relay connection	25
4.3.2. Optocoupler connection	25
4.4. USB connection (GT7.0510)	25
5. Configuration	27
5.1. Target group	27
5.2. Configuration options	27
5.3. Configuration via the terminal	27
5.3.1. Device information	29
5.3.2. Installed apps	30
5.3.3. Device configuration	31
5.3.4. Start active app / Reboot device	32
5.4. Configuration via web interface	33
5.4.1. System overview	35
5.4.2. Network	36
5.4.3. G7 Connect	39
5.4.4. External web server	39
5.4.5. Web proxy	40
5.4.6. Security and user	41
5.4.7. SCEP	42
5.4.8. Time	43
5.4.9. Display	44
5.4.10. Data carrier	45
5.4.11. Device	46
5.4.12. Barcode interface	47
5.4.13. App configuration	48
5.4.14. Installed apps	48
5.4.15. Cloud pairing	50
5.4.16. Licensing and coding points	55
5.4.17. Certificate management	56
5.4.18. Device	59
5.4.19. Update firmware	60
5.4.20. Log viewer	61
5.4.21. Device state	62

5.4.22. Legal information 63

5.5. Configuration via G7 Connect 63

5.6. Integration in system management software 64

6. Maintenance 65

6.1. Target group 65

6.2. Cleaning 65

7. Technical data 66

1. IMPORTANT INFORMATION

Dear customer,

To ensure that our product operates with safety and to your complete satisfaction, 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.
- Also observe information marked with the signal word "NOTE". These contain important information for avoiding damage to property.
- Pay attention to the symbols and warnings on the product.
- Read through all the information that affects your target group carefully before installing or operating the device.
- Unless specifically documented elsewhere, the installation, commissioning, and maintenance of the product is the responsibility of the customer.

1.1. Safety information

	<ul style="list-style-type: none"> - The installation, commissioning, and maintenance of our devices must only be performed by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association -> Work by unqualified personnel can lead to injuries (e.g. electric shock). - Unless otherwise stated, the installation and maintenance of our devices must only be carried out in a voltage-free state. This applies in particular to devices that are connected to the low-voltage network. -> If the device is not disconnected from the supply voltage, touching terminals or internal parts can result in minor injuries (electric shock).
	<ul style="list-style-type: none"> - It is forbidden to make alterations to the product (device, connection cable): - Do not remove protective shields and covers from devices. -> Removing protective shields and covers may result in personal injury or property damage. - Do not attempt to repair or recommission products yourself after a defect, fault, or damage has occurred. In such cases, be sure to contact your customer advisor or Gantner Electronic GmbH.
	<ul style="list-style-type: none"> - Installation, commissioning, operation, and maintenance of the purchased product must be carried out as intended, i.e., in accordance with the technical conditions of operation as described in the corresponding documentation. It is therefore essential that you read the relevant chapters in this manual and proceed accordingly. - If there are still some points that are not entirely clear, do not proceed. All queries can be clarified by your Gantner representative or the Gantner Support Team. - Immediately upon receipt of the goods, check the packaging and the product or data carrier visually to ensure that it is intact. Also check that the delivery is complete and includes all accessories, documentation, auxiliary devices, etc.

	<ul style="list-style-type: none"> - If the packaging was damaged during transport or if you suspect damage or a malfunction of the product, the product must not be put into operation. In this case, contact your Gantner representative who will endeavor to resolve the problem as quickly as possible. - Unless otherwise stated, the customer is responsible for the intended installation, commissioning, operation, and maintenance of the product. - Gantner Electronic GmbH assumes no responsibility for injuries or damage resulting from 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 if you have any suggestions for improvement, please contact your Gantner representative or Gantner Electronic GmbH directly.

We especially look forward to hearing from you even if you just want to let us know that everything is operating smoothly.

1.2. Certification information



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.



CAUTION

For security-relevant applications, the device may only be used in secure indoor areas. Alternatively, the device must be protected against manipulation by other measures (e.g. monitoring).

	<p>The GT7 Lite was developed and manufactured under the ISO 9001 quality management standard.</p>
	<p>Gantner Electronic GmbH is certified according to the ISO 14001 standard for environmental management systems (EMS).</p>
<p>CE</p>	<p>This product is in compliance with the following EC directives, including all applicable amendments:</p> <p>2014/53/EU (Radio Equipment Directive)</p> <p>The complete text of the CE Declaration of Conformity is available via the following link:</p> <p>https://www.gantner.com/en/qr_u9gfp3s2Y6</p>
	<p>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.</p>

	<p>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 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. For more information on recycling an item marked with the WEEE symbol, please contact your local city office or your household waste disposal operation.</p>
---	--

1.3. Copyright information

© Copyright 2026 Gantner Electronic GmbH

All rights reserved. Copying, reproducing, translating, converting to any electronic medium or machine-readable form, in whole or in part, is prohibited. The sole exception is the creation of a backup copy of software for your own use as a safeguard, insofar as this is technically possible and recommended by us. Any infringement will render the party committing such infringement liable to compensation payment.

Liability

Claims against the manufacturer based on the hardware and/or software products described in this manual shall depend exclusively on the provisions of the guarantee. Further claims are excluded, in particular the manufacturer assumes no liability for the completeness or accuracy of the content of this manual. We reserve the right to make changes and changes may be made at any time without prior notice.

Trademarks

Reference is made at this point to the identifications and registered trademarks used in this manual. All product or company names mentioned in this manual are for identification and explanation purposes only and, depending on the designation, may be trademarks or registered trademarks of the respective companies.

Contact address of manufacturer

Gantner Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria

1.4. Software license information

Free software remark

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

WARRANTY DISCLAIMER

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

WRITTEN OFFER

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

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

open-source@gantner.com

1.4.1. Send-in solution

The safety of this product is of great importance to us. For this reason, modified versions of the open source software used can generally only be installed if this is enabled by us. Please note that the installation of modified software may mean that any applicable security requirements for the product are no longer met and that it can no longer be used in the form originally intended.

If you still wish to install modified versions of the software components licensed under the GNU General Public License (GPL) and/or the GNU Lesser General Public License (LGPL), please contact **open-source@gantner.com** stating that you want to install customized versions of the software on your device and include the following information: device article number, serial number, firmware version and your contact details (name, address, city and state). You will then receive all the necessary information for returning the device to us.

We will then remove the security features used to fulfill our license obligations to the GPL and/or LGPL licensors, thereby enabling you to install GPL and/or LGPL software, remove our trademarks from the product and return the product to you. Removing the security features also results in functional restrictions.

However, redistribution of the product with modified software is not permitted as exhaustion of the distribution right cannot occur for the specific copy. Also the use of the product may be prohibited if it violates any legal provisions. It is your responsibility to check whether the use is permissible in the specific case or to obtain the required permits. The warranty is void for any defects related to the use of modified software.

1.5. Contact and inquiries

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

[Gantner Locations](#)

2. GENERAL INFORMATION

2.1. About this manual



NOTE

Henceforth, the term GT7 Lite is used to refer to all variants of the G7 Base series collectively. If information is only applicable to a specific variant, this will be noted.

This manual contains a detailed description of how to install, configure, and commission the GT7 Lite terminals.

Other Gantner devices and software as well as third party devices can operate with the GT7 Lite. For more information on the supplementary devices and applications mentioned in this manual, please refer to the respective documentation of these components.

2.2. Target group



CAUTION

Injury and property/equipment damage

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

This manual contains information relevant for the different stages in the operating life of the GT7 Lite. Information about the installation, commissioning, and configuration of the GT7 Lite 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, maintenance)

2.3. Terminology

GT7 Lite

A compact multipurpose RFID terminal that allows different functions to be implemented through the installation of apps. This term refers to all variants of the GT7 Lite in general, regardless of which app is currently active.

G7 Connect

G7 Connect is Gantner's cloud service for the configuration and management of projects that contain Generation 7 Gantner devices. G7 Connect is accessible via a web browser following registration and login.

G7 app

General term for the software (app) that is activated on the G7 device to provide the desired functionality. Several G7 apps are available.

Data carrier

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

RFID (Radio-Frequency Identification)

Identification over short distances using radio frequency. An RFID data carrier is used as an identification credential in the Gantner system.

User

This term refers to the end user who is using or operating the Gantner device to complete a function.

Web interface

A web browser accessible interface that allows the device and app settings to be viewed and configured.

2.4. Intended use

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

- The control of turnstiles and doors (G7 Access App and G7 Advanced Access App)
- The display of locker information or visitor information (G7 Info App)
- The display of a countdown for using time-limited services such as showers and power plates (G7 Countdown App)
- The reading and writing to/from RFID data carriers (G7 Writer App)

2.5. Functional description

The GT7 Lite is a compact RFID and NFC terminal designed for multiple applications in fitness centers, attractions, corporate environments, and educational facilities. Depending on the installed app, the device can function as an access control terminal (for doors and turnstiles), a countdown timer (to display the time remaining for using a device or service), or a universal read/write station.

To activate a function on the GT7 Lite, the user must first identify themselves at the terminal. Identification can be performed in a variety of ways: using an RFID data carrier, via NFC (Near Field Communication), or using a barcode scanner.

The identification data is forwarded via LAN Ethernet onto a system management application such as eLoxx Relaxx. Following identification, further operation is defined by the G7 app operating on the terminal.

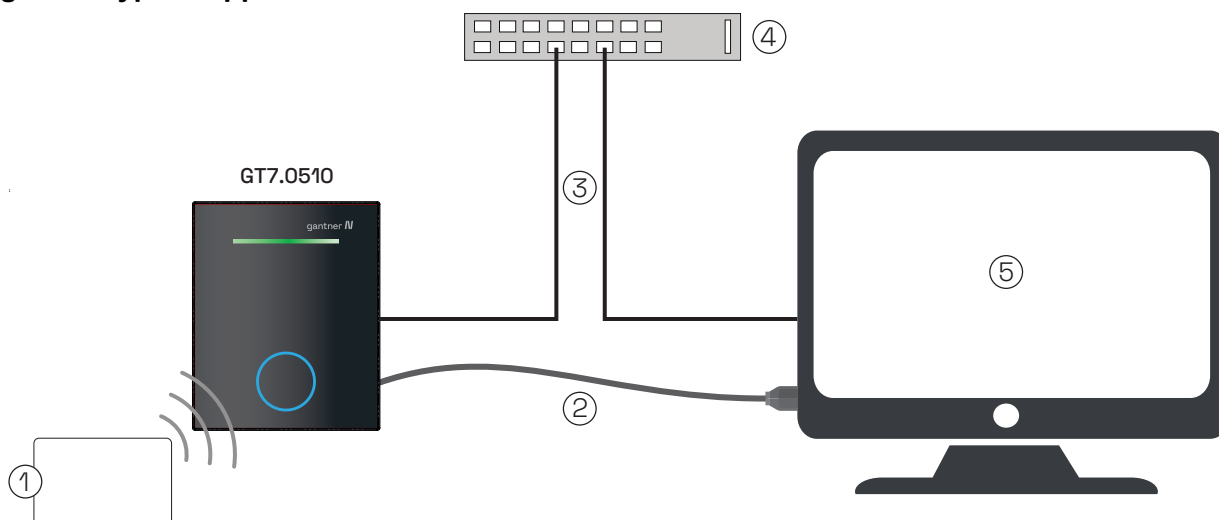
The terminals are suitable for indoor use. A metal wall bracket is included with each device for wall mounting. Alternatively, mounting clips are available to install the terminal in a cutout, e.g., in a desk or turnstile.

The full range of terminal settings can be configured via a web browser (web interface) or via Gantner's G7 Connect cloud solution. Through the configuration, the functionality of the terminal can be customized to the requirements.

2.6. System overview

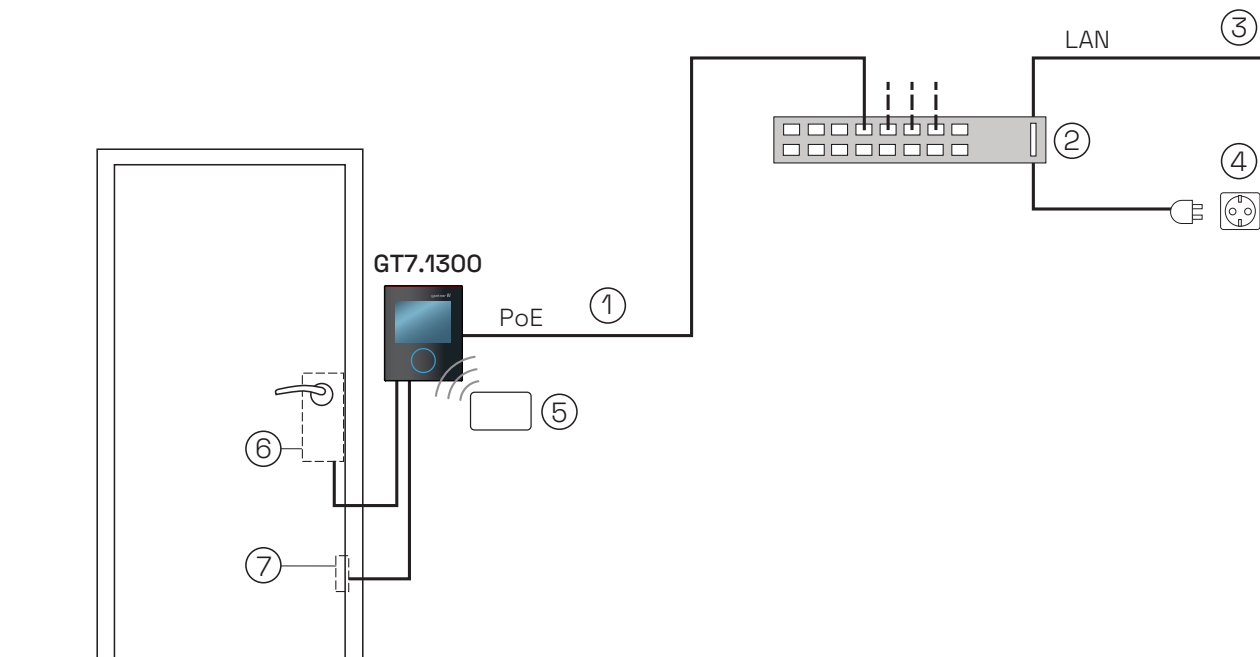
The following figure shows an example of how the GT7 Lite typically operates with the other components in the system.

Figure 1. Typical application of the GT7.0510



1. RFID data carrier
2. USB (HID interface)
3. Network
4. Network switch
5. Computer with Gantner software

Figure 2. Typical application of the GT7.0500 or GT7.1300



1. Connection to network and power supply (PoE)
2. Network switch with PoE injection
3. Network
4. Power supply for network switch
5. RFID data carrier
6. Electronic door lock
7. Door status feedback

2.7. Device overview

The different GT7 Lite variants provide flexibility for different applications. The functionality of each variant is as follows.

Feature	GT7.0500	GT7.0510	GT7.1300
Ethernet interface	✓	✓	✓
1 x relay output	✓	✓	✓
1 x optocoupler input	✓	✓	✓
Acoustic beeper	✓	✓	✓
Power supply: PoE	✓	X	✓
Power supply: USB	X	✓	X
MIFARE reader	✓	✓	X
LEGIC advant reader	X	X	✓
LED bar	✓	✓	X
3.5 inch touchscreen	X	X	✓
USB HID interface	X	✓	X
Barcode scanner ready	X	X	✓

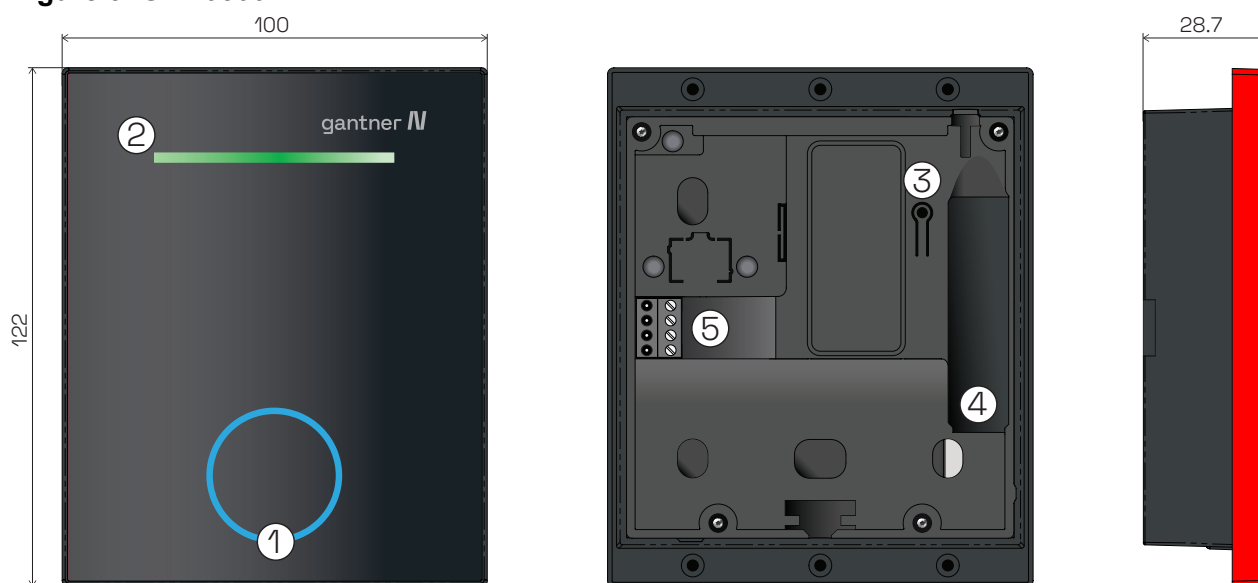
2.8. Device features and dimensions



NOTE

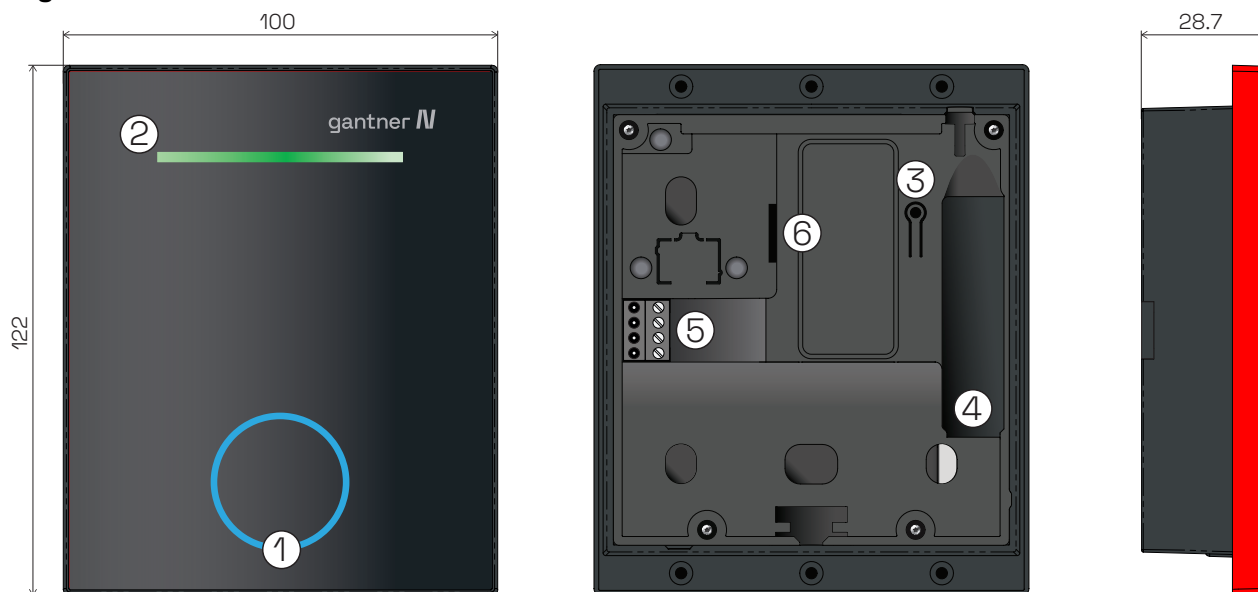
All measurements in millimeters.

Figure 3. GT7.0500



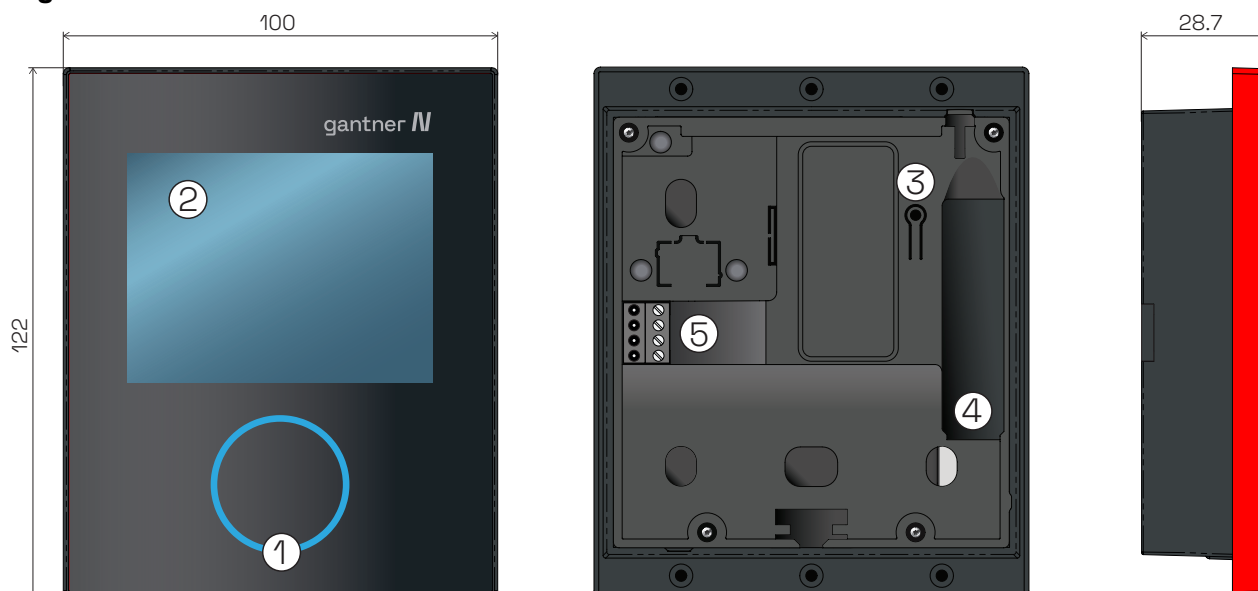
1. RFID reader with LED ring
2. LED bar (status display)
3. RESET button
4. RJ45 connector (network)
5. Input/output connector

Figure 4. GT7.0510



1. RFID reader with LED ring
2. LED bar (status display)
3. RESET button
4. RJ45 connector (network)
5. Input/output connector
6. USB-C connector

Figure 5. GT7.1300



1. RFID reader with LED ring
2. 3.5 inch touchscreen display
3. RESET button
4. RJ45 connector (network)
5. Input/output connector

3. INSTALLATION



CAUTION

Touching live parts can lead to injuries from electrical shock

- Disconnect the device from the power supply before working on the device or installation/disassembly.
- Observe the applicable safety and accident prevention regulations.
- Do not remove protective devices.



NOTICE

Improper work can lead to damage or malfunction of the device

- Installation and maintenance of this device may only be carried out by suitably trained technicians.
- Read the information in this chapter carefully before installing the device.
- Observe the specified technical data and measurement diagrams of the device.
- Always use the correct tools for installation.



NOTICE

RF exposure statement

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

3.1. Installation guidelines

The GT7 Lite terminals are designed to be installed onto a flat, smooth surface. The terminals can be surface mounted, e.g., onto a wall, or semi-flush mounted into a cutout in a desktop or metal turnstile.

Pay attention to the following points during installation:

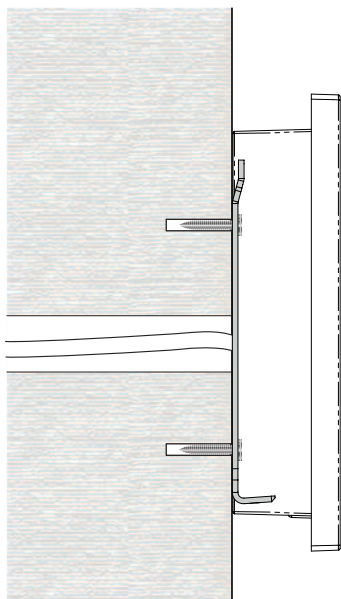
- Recommended mounting height for wall mounting: 1.3 m to the middle of device display.
- The **GT7.1300** should not be exposed to direct sunlight. Otherwise, limitations in the readability of the display can occur.

3.2. Installation options

There are three options for installing the GT7 Lite.

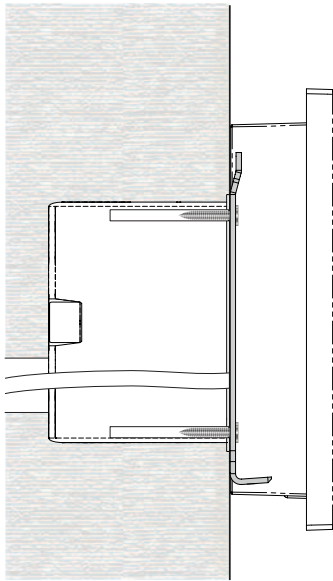
1. Surface installation with wall bracket

This method uses a metal wall bracket (included with each terminal) to mount the terminal onto a wall or door frame. The entire terminal housing is visible after installation. For instructions see [Surface installation with wall bracket \[18\]](#).



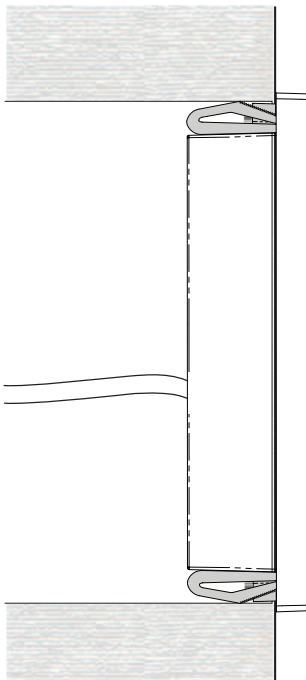
2. Surface installation with wall box

This method also uses the metal wall bracket but instead of attaching the bracket directly to the wall, the wall bracket is attached to a flush-mounted wall box. The entire terminal housing is visible after installation. For instructions see [Surface installation with wall box \[19\]](#).



3. Semi-flush installation

A semi-flush installation allows the terminal housing to be installed into a desk or countertop or metal turnstile. After installation, only the front part (7.5 mm) of the terminal is visible. Four mounting clips are attached to the terminal housing that hold the terminal in the cutout. For instructions see [Semi-flush installation \[21\]](#).



3.3. Surface installation with wall bracket



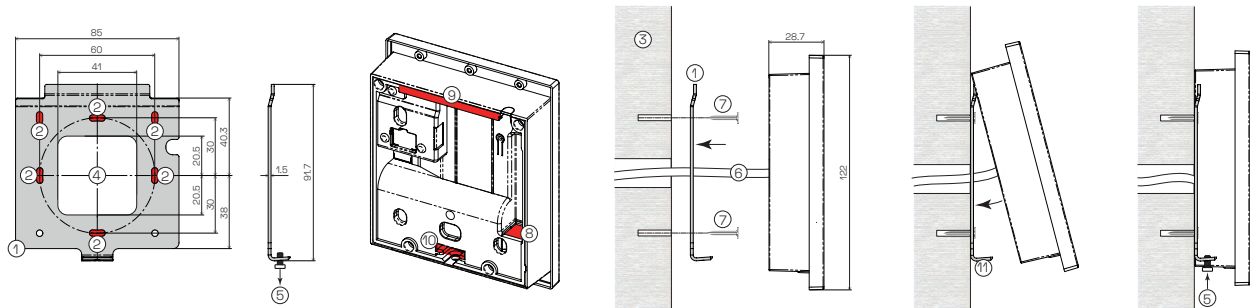
NOTE

All measurements in millimeters.

The terminal can be surface-mounted onto a flat surface such as a wall or door frame. A metal wall bracket and mounting hardware (two screws and wall plugs) are included with each terminal. The type of mounting hardware must be selected depending on the wall material.

Complete the following steps:

Figure 6. Installation with wall bracket



1. Wall bracket
2. Mounting hole
3. Wall
4. Opening for electrical cabling
5. Fixing screw
6. Electrical cabling
7. Mounting screw
8. RJ45 socket (Ethernet)
9. Upper mounting part
10. Lower mounting part
11. Lower bracket part

1. Use the wall bracket (1) to mark out and drill two mounting holes (2) in the desired location on the wall (3).



NOTE

The recommended mounting height is 1.3 m to the middle of the device.

2. The wall bracket is delivered with the terminal fixing screw (5) attached. Unscrew and remove the fixing screw from the wall bracket and retain for later.
3. Feed the electrical cabling (6) through the opening (4) in the wall bracket.
4. Attach the wall bracket to the wall using two screws (7). Ensure that the wall bracket is level and securely attached to the wall.

**NOTE**

Use the correct type of screws and wall plugs according to the wall material. Do not use countersunk screws.

5. Complete the required electrical connections (see [Electrical connections \[22\]](#) for instructions). Plug the Ethernet cable into the RJ45 socket (8) on the rear side of the terminal and connect any other electrical cabling if required.
6. Hook the upper mounting part (9) of the terminal onto the top of the wall bracket then carefully swing the terminal forward onto the wall bracket. Ensure that the lower bracket part (11) aligns with the lower mounting part (10) and that the cabling is not damaged during this process.
7. To secure the terminal onto the wall bracket, tighten the fixing screw (5) from below.

3.4. Surface installation with wall box

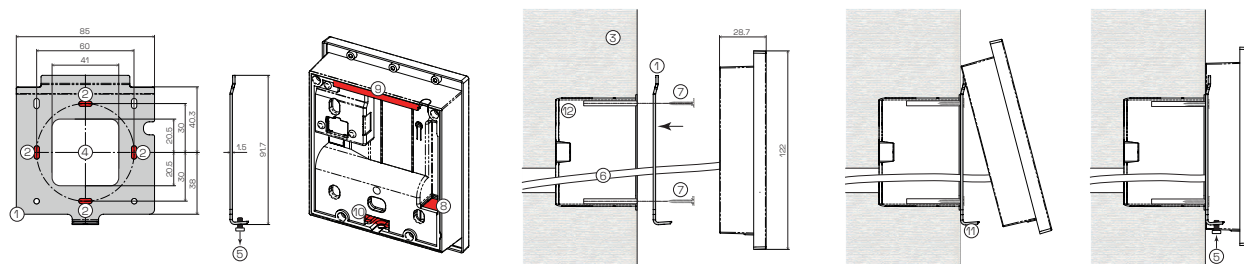
**NOTE**

All measurements in millimeters.

The terminal can be surface mounted onto a flat surface in combination with a flush-mounted wall box. The metal wall bracket that is included with each terminal is attached to the wall box. The wall box and required mounting hardware are not included in the scope of supply and must be selected depending on the wall material.

Complete the following steps:

Figure 7. Installation with wall box



1. Wall bracket
2. Mounting hole for wall box
3. Wall
4. Opening for electrical cabling
5. Fixing screw
6. Electrical cabling
7. Mounting screw
8. RJ45 socket (Ethernet)
9. Upper mounting part
10. Lower mounting part
11. Lower bracket part
12. Flush-mounted wall box

1. Install the wall box (12) according to the manufacturer's instructions.



NOTE

The recommended mounting height is 1.3 m to the middle of the device.

2. The wall bracket (1) is delivered with the fixing screw (5) attached. Unscrew and remove the fixing screw from the wall bracket and retain for later.
3. Feed the electrical cabling (6) through the opening (4) in the wall bracket.
4. Attach the wall bracket (1) to the wall box (12) via two of the wall bracket mounting holes (2) and two screws (7). Ensure that the wall bracket is level and securely attached to the wall box.



NOTE

Use the correct type of screws suitable for the wall box. Do not use countersunk screws.

- Complete the required electrical connections (see [Electrical connections \[22\]](#) for instructions). Plug the Ethernet cable into the RJ45 socket (8) on the rear side of the terminal and connect any other electrical cabling if required.
- Hook the upper mounting part (9) of the terminal onto the top of the wall bracket then carefully swing the terminal forward onto the wall bracket. Ensure that the lower bracket part (11) aligns with the lower mounting part (10) and that the cabling is not damaged during this process.
- To secure the terminal onto the wall bracket, tighten the fixing screw (5) from below.

3.5. Semi-flush installation



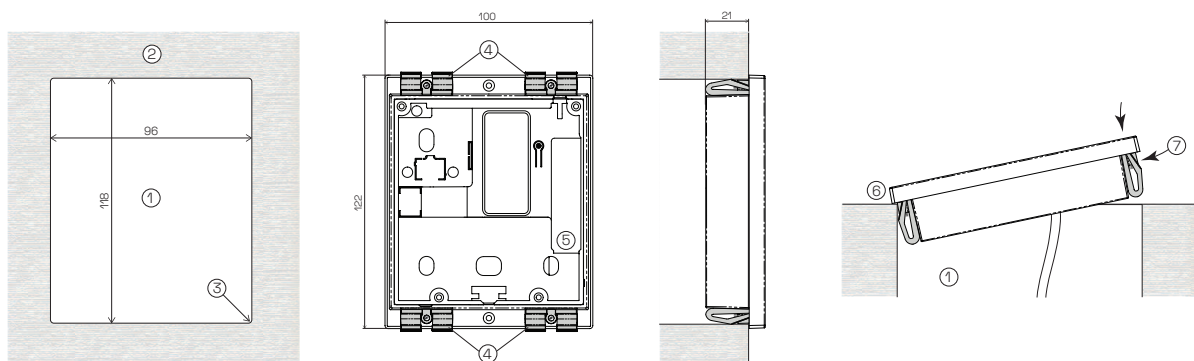
NOTE

All measurements in millimeters.

A semi-flush installation allows the terminal to be installed on a flat surface, e.g., into a desk or countertop or metal turnstile. Four clips are attached to the terminal housing that hold the terminal securely in the cutout. The mounting clips are available to order from Gantner as an accessory (Part No. 1115190). No other installation accessories apart from the clips are required for this method.

Complete the following steps:

Figure 8. Semi-flush installation



1. Cutout (W: 96 mm, H: 118 mm)
 2. Installation surface
 3. Corner radius = max. 5 mm
 4. Mounting clips
 5. RJ45 socket (Ethernet)
1. Cut out and remove a section (1) of the installation surface (2) according to the measurements above.



NOTE

A corner radius of max. 5 mm is possible for the edges of the cutout.

2. Attach the four mounting clips (4) to the holes in each corner of the terminal housing using the supplied screws.
3. Complete the required electrical connections (see [Electrical connections \[22\]](#) for instructions). Plug the Ethernet cable into the RJ45 socket (4) on the rear side of the terminal and connect any other electrical cabling if required.
4. Insert one side of the terminal (6) into the cutout (1). While pushing the clips in on the other side of the terminal (7), insert the terminal into the cutout.

4. ELECTRICAL CONNECTIONS



WARNING

Touching live parts can lead to serious injury or death from electrical shock

- Disconnect the power supply before working on the device or installation/deinstallation.
- Observe the applicable safety and accident prevention regulations.
- Observe the specified technical data and technical drawings of the device.
- Protective devices must not be removed.

4.1. Power supply connection

Depending on the variant, there are two options for supplying power to the terminal:

1. GT7.0500 and GT7.1300

For these variants, power is supplied via **Power over Ethernet (PoE)**. The following requirements for PoE switches must be considered.

- Must comply with IEEE 802.3af
- Power class: 0
- Min. 15.4 W per PoE port
- Total power budget: min. 15.4 W x number of ports
- Be aware that some PoE switches do not transmit the supply voltage on separate wires (DC+ and DC-) but superimpose it on the transmit and receive lines (RX+/- and TX +/-). In this case, the terminal is supplied with voltage even if only RX and TX are connected.



NOTE

See [Network connection via Ethernet LAN](#) for information on the Ethernet wiring required for power supply via PoE.

2. GT7.0510

For this variant power is supplied via **USB**. The **GT7.0510** is delivered with a USB cable that is connected to the USB port on the rear of the terminal. See [USB connection \(GT7.0510\) \[25\]](#) for instructions.



NOTE

A network connection is required for all variants including the **GT7.0510**. However, as the **GT7.0510** is powered via USB, the power over Ethernet instructions (as described in [Network connection \(LAN/Ethernet\) \[23\]](#)) are not applicable.

4.2. Network connection (LAN/Ethernet)



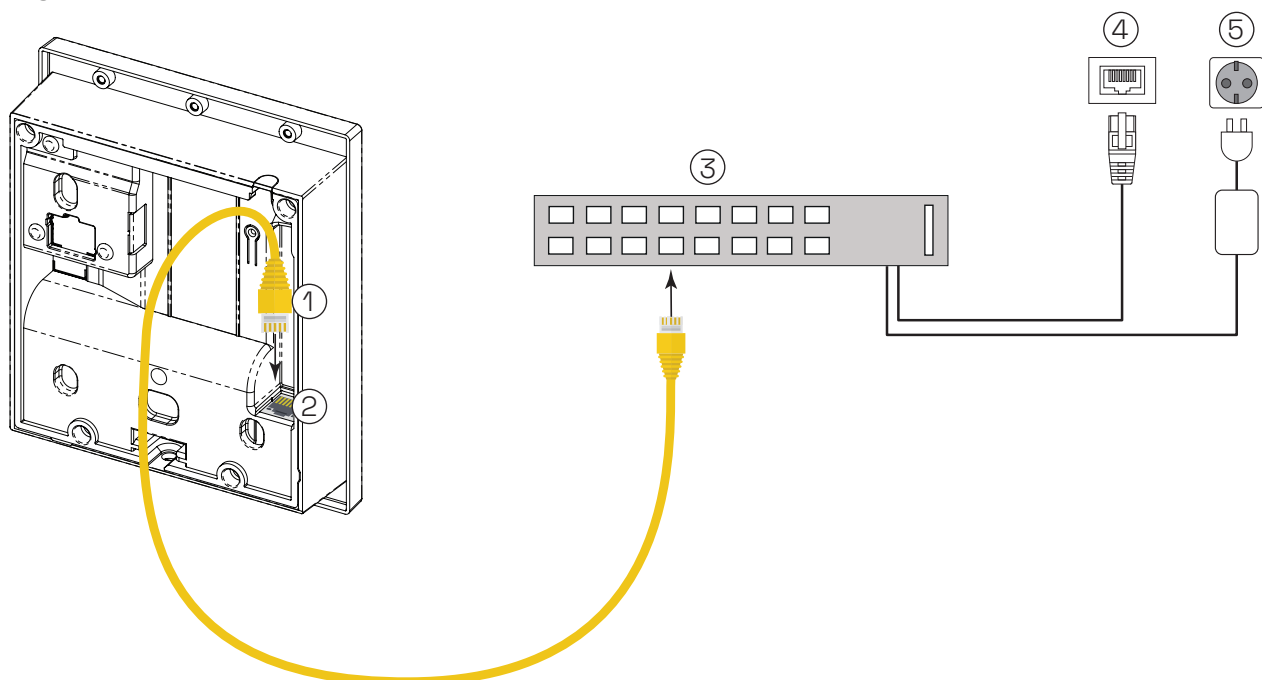
NOTE

Recommended cabling for LAN Ethernet

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

Connect the GT7 Lite to the network as follows.

Figure 9. Network connection



1. Ethernet cable
2. Rj45 connector
3. Network switch with PoE
4. LAN Ethernet connection
5. Mains power supply

1. Connect the Ethernet cable (1) to the RJ45 connector (2) on the rear side of the terminal.
2. Connect the Ethernet cable (1) to a separate port on the network switch (3). Depending on the Ethernet standard used, the wire colors for the Ethernet cable are as follows:

Table 1. Ethernet wire colors

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	-	-
DC+	PoE supply +	blue/white	blue/white
DC+	PoE supply +	blue	blue
DC-	PoE supply -	brown/white	brown/white
DC-	PoE supply -	brown	brown



NOTE

The connections for supplying power to the terminal via PoE are also provided in the table. A suitable PoE switch is required for this option. See [Power supply connection](#) for more information.

Be aware that power for the **GT7.0510** is supplied via USB. PoE is not available for this variant.

4.3. Input and output connections



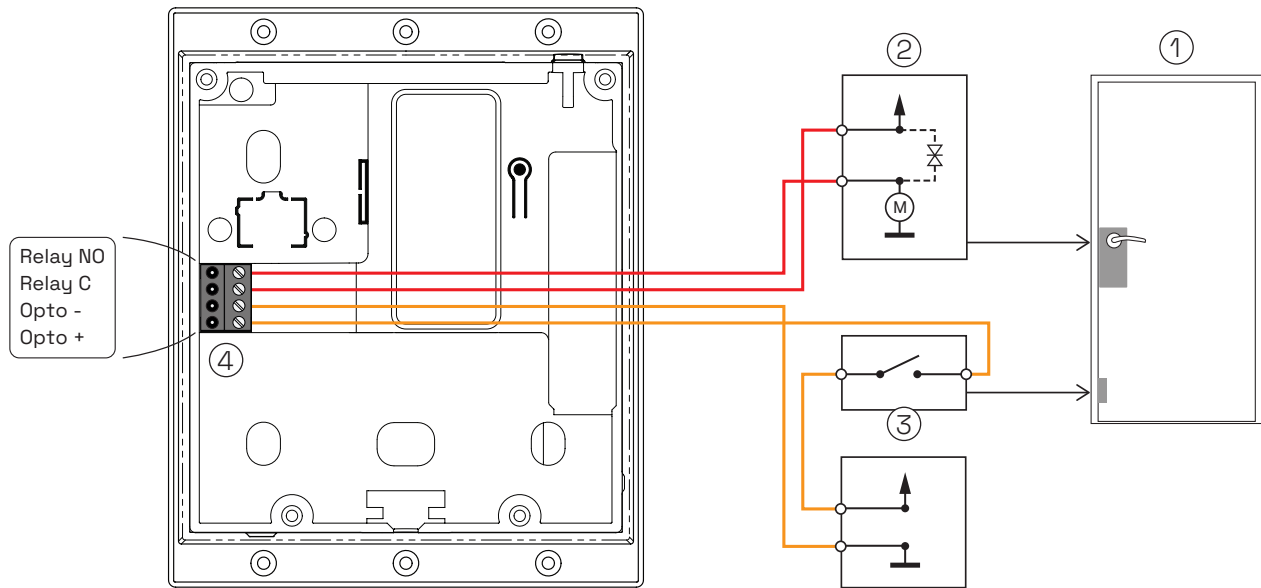
NOTICE

Observe the permitted voltage and power values of the relay and optocoupler (see [Technical data](#)).

External components, e.g., turnstiles and doors, can be controlled by the GT7 Lite via the relay output and status information can be acquired via the optocoupler input.

After connection, the desired function for the relay and optocoupler must be configured in the configuration settings of the G7 app that is operating on the terminal. These settings are not available with every app as not all apps require this functionality.

Figure 10. Example connection of the relay and optocoupler



- 1 ... Door
- 2 ... Door opener
- 3 ... Door feedback contact
- 4 ... Input/output connector

4.3.1. Relay connection

All terminals have one relay output (**Relay**) that can be used to output digital signals to control external components such as door openers. The reader's relay can be activated independently. Connected devices must comply with the applicable electrical safety standard (IEC 60950-1 or 62368-1). When connecting inductive loads (e.g., door openers), a suitable free-wheeling diode must be used.

The desired function, such as unlock door, deny access, or block external device, must be selected and the activation time of the relay set in the **App configuration** settings. The activated app (e.g., Access App) must provide this option in order to use the relays.

4.3.2. Optocoupler connection

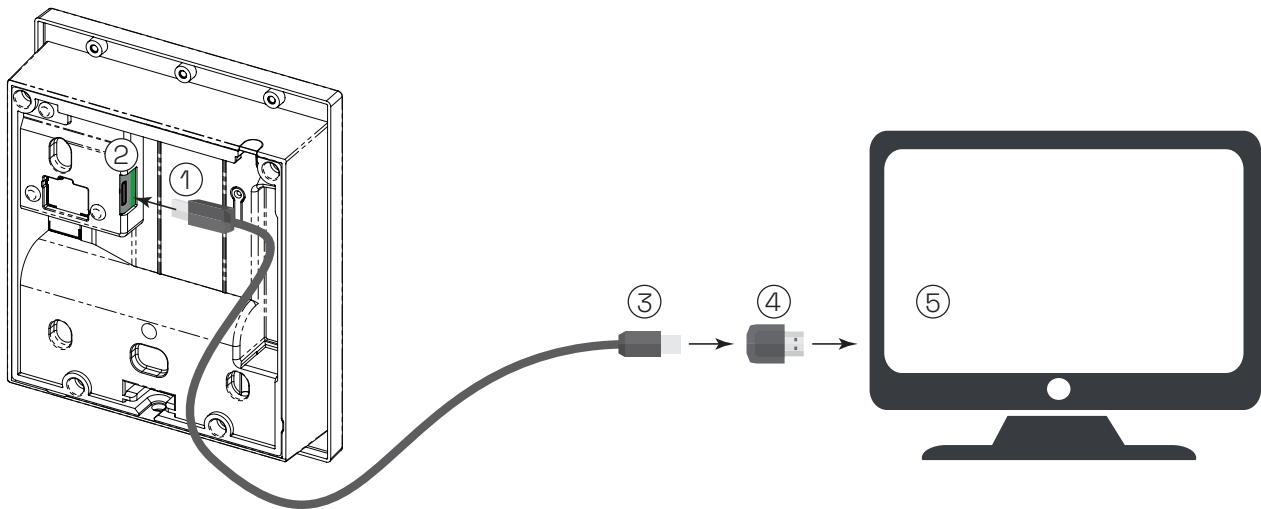
The optocoupler input (**Opto**) is used for feedback, e.g., status acquisition from the connected door. Connected devices must comply with the applicable electrical safety standard (IEC 60950-1 or 62368-1).

4.4. USB connection (GT7.0510)

The **GT7.0510** is equipped with a USB-C port on the rear side of the terminal. After connecting a USB cable to this port and connecting the other end to a computer, the **GT7.0510** can operate as a USB Human Interface Device (HID) to read and write data carriers of all types.

A USB-C to USB-C cable and a USB-C to USB-A adapter are delivered with the **GT7.0510** for this purpose. Connect the USB cable to the **GT7.0510** as follows.

Figure 11. USB connection



1. USB-C cable (terminal end)
2. USB port
3. USB-C cable (computer end)
4. USB adapter
5. Computer

1. Connect the USB-C cable (1) to the USB port (2) on the rear side of the terminal.
2. If your computer only has a USB-A connection, connect the other end of the USB-C cable (3) to the USB adapter.
3. Connect the other end of the USB-C cable (3), or the USB adapter (4), to a spare USB port on your computer (5).
4. To configure the **GT7.0510** as a read/write device, log in to the web interface via a web browser. Refer to [Configuration via web interface \[33\]](#). The configuration can also be completed in G7 Connect. Refer to the G7 Connect manual for instructions.

5. CONFIGURATION



NOTICE

RF exposure statement

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

Requirements for use

- To use all the information described in this chapter, ensure that the latest firmware is installed in the GT7 Lite.



NOTE

The firmware can be updated in G7 Connect.

5.1. Target group

This chapter contains information for the technicians responsible for commissioning and configuring the GT7 Lite. 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

There are three options for configuring the functionality of the GT7 Lite:

1. Via the terminal

Basic information and settings are directly accessible and configurable at the display of the device (if equipped) via the integrated device configuration menu.

2. Via the web interface

In a web browser, an HTTP/HTTPS connection to the GT7 Lite is established and the web server integrated in the device is displayed. After login, all the device settings as described in the following chapters can be viewed and configured.

3. Via G7 Connect

The GT7 Lite integrates conveniently into the Gantner Cloud. Here you can see all of your G7 devices displayed in an overview and if the devices are online, they can be configured directly within this platform.

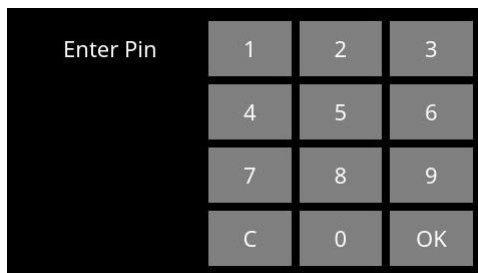
5.3. Configuration via the terminal

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

1. Write a large **M** on the touchscreen with your finger without removing it.



↪ A keypad for PIN entry is displayed.



2. Enter the PIN code **0815**, and then press **OK**.



NOTICE

For security reasons, change the default PIN code to a secret code. This can be done via the **Device Configuration** settings of the web interface.

After entering the PIN code, the configuration menu is displayed.

3. Via the icons to the left, you can select the desired information or configuration page.



1 ... Display of general device settings

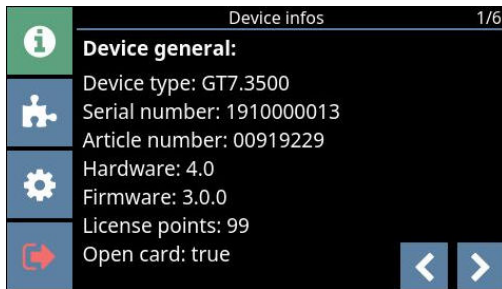
2 ... Display and selection of installed apps

3 ... Configure device settings

4 ... Start active app or restart device

4. Each configuration page has sub-pages (page displayed top right). Use the arrow buttons in the lower-right corner of the screen to scroll through the sub-pages.

5.3.1. Device information



General device information is displayed on the sub-pages of this menu. Most of the settings shown here can be configured via the device configuration page.

Device type: The type/model of the terminal.

Serial number / Article number: The serial number and article number of the GT7 Lite are displayed here.

Hardware / Firmware: The version of the hardware / firmware installed in the device.

License points: License points are required to activate certain G7 apps and enable other features. License points can be purchased from Gantner. The available license points are displayed here.

Open card: If **true** is shown here, the terminal can read the UID number of third-party data carriers, i.e., those not supplied by Gantner. To activate this function, the product **G7 Device License Points Open Card** must be purchased and the license code entered into the web interface.

Ethernet



MAC: The MAC address of the device.

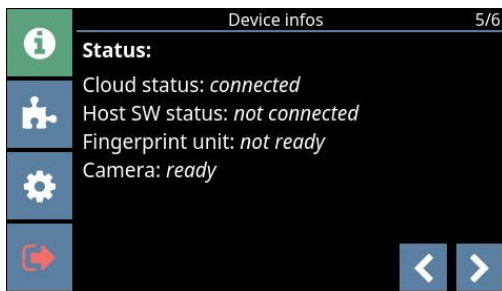
IP: The IP address of the device. The first line shows the IPv4 address. If IPv6 is enabled (possible via configuration menu or web interface), the IPv6 address is also displayed in the second line.

Network routing



Here you can see the routing settings for the network connection. The top two lines show the information for the IPv4 settings. The settings for IPv6 are shown below if IPv6 has been enabled in the settings. These settings are assigned automatically and cannot be changed.

Status

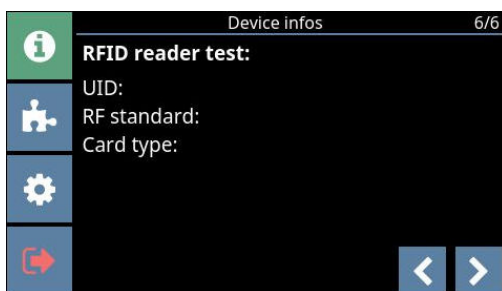


Cloud status: If **connected** is shown here, the connection to G7 Connect is functioning.

Host SW status: If **connected** is shown here, the connection to the host software (e.g., locker management software) is functioning. The text “not connected” means that there is no connection to any host software.

Fingerprint unit / Camera: If **ready** is shown in these fields, the fingerprint reader/integrated camera (if applicable) of the terminal is ready for operation.

RFID reader test



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

- Hold a data carrier next to the reading field (LED ring) of the GT7 Lite.
↳ The data carrier is read, and the respective data is displayed in the **UID**, **RF standard**, and **Card type** fields.

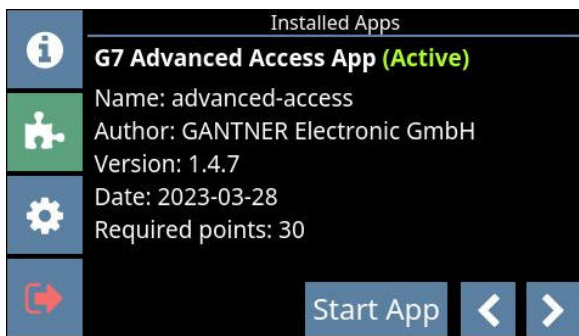
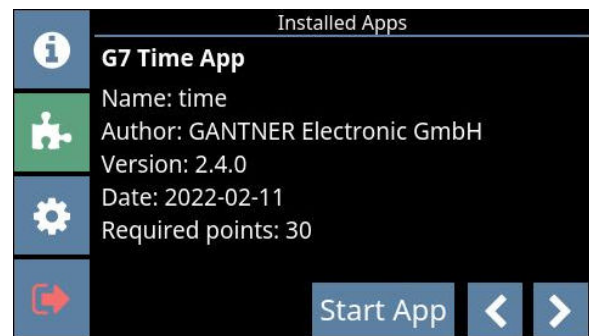
5.3.2. Installed apps

On the **Installed Apps** page, all apps that have been installed in the GT7 Lite are displayed. Information, e.g., which app version is installed and the required license points, is provided here.



NOTE

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



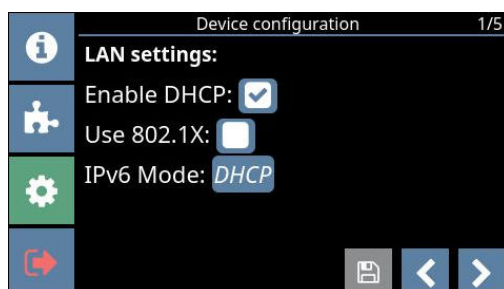
1. To scroll through each installed app, press the arrow buttons in the bottom right of the display.
 2. To begin using an app, press the **Start App** button.
- ↪ The app is loaded (this takes a few seconds), and the default page of the app is displayed after restarting.

5.3.3. Device configuration

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

1. To enable a setting, press the box so that a **tick** is displayed.
2. To define a setting that has numbers (e.g., the IP address), press the **wrench** icon.
3. Once you have defined the settings on a page, press the **disc** icon to save the settings.

LAN settings



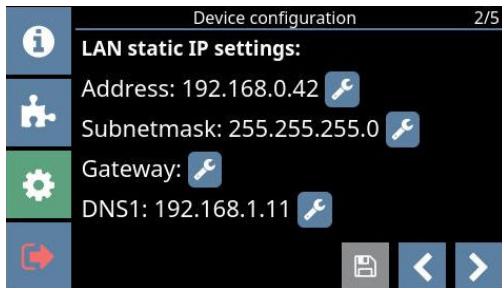
Enable DHCP: When this option is enabled, the network router will assign a dynamic IP address to the GT7 Lite. When not enabled, the **LAN static IP settings** (page 2) are used to determine LAN communication.

Use 802.1X: When this option is enabled, the GT7 Lite will use the 802.1x protocol for identification.

IPv6 mode: If your network supports using the IPv6 protocol for device addresses, you can select one of the following options to use the protocol.

- **DHCP assigned IP address:** When this option is enabled, the IP address of the GT7 Lite is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, disable this option and enter the network settings into the **Static IPv4 configuration** section.
- **Static configuration:** Select this option and enter the network settings into the **Static IPv6** section to assign a static address to the device.
- **Stateless address autoconfiguration:** Stateless address autoconfiguration is the process that IPv6 nodes (hosts or routers) use to automatically configure IPv6 addresses for interfaces.

LAN static IP settings



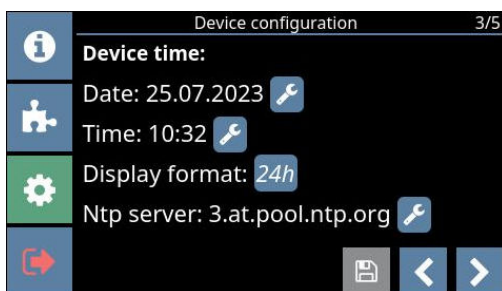
Address: The static IP address of the GT7 Lite for LAN communication.

Subnet mask: The static subnet mask of the GT7 Lite for LAN communication.

Gateway: The static gateway address of the GT7 Lite for LAN communication.

DNS1: The address of the primary DNS server for LAN communication.

Time settings

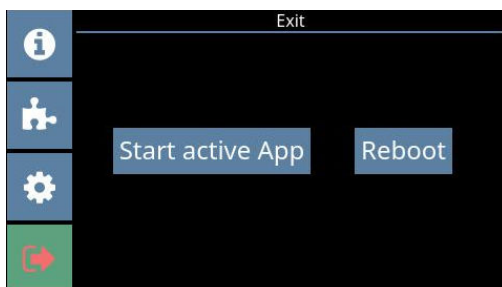


Date / Time: The date and time can be manually set here.

Display format: Select between **12h** or **24h** time format or select **None** to not display the time.

NTP server: The location of the NTP server from which the time is taken automatically. The default server is displayed. To change this address, use the web interface, as only numbers can be entered in the configuration menu on the GT7 Lite.

5.3.4. Start active app / Reboot device



1. To exit the configuration menu, press the exit icon at the bottom left of the display.
2. Press **Start active App** to start the last active app.
 - ↪ The active app is loaded and after a few seconds the app's home screen is displayed.

- Alternatively, press the **Reboot** button if you would like to restart the terminal.

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

5.4. Configuration via web interface

You can use a web browser to directly access a GT7 Lite that is reachable via the network.

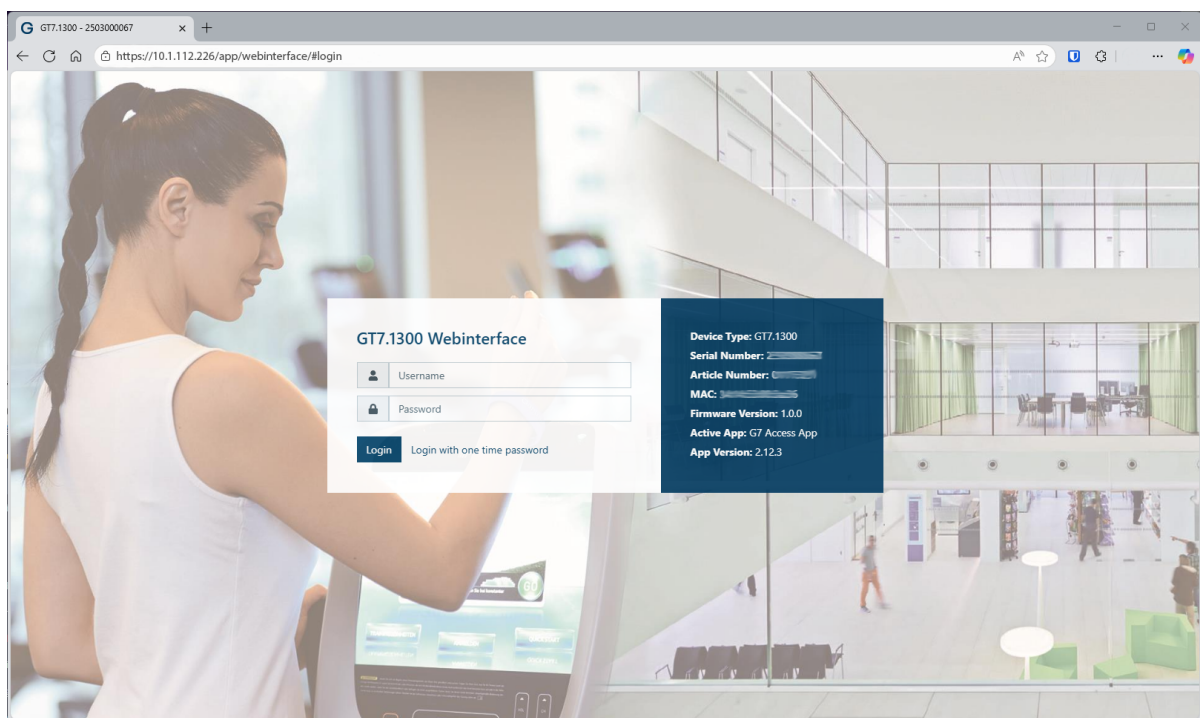
- Open a web browser (e.g., Chrome or Firefox) on a PC or mobile device.
- Enter the IP address of the GT7 Lite into the address line.



NOTE

The GT7 Lite uses DHCP by default to automatically obtain an IP address from the network. You can use the GAT Device Finder software to scan the network for Gantner devices and see their IP addresses. This software can be downloaded from the Gantner website (login required). Alternatively, ask your network administrator for the IP address.

↪ The login page of the web interface opens.



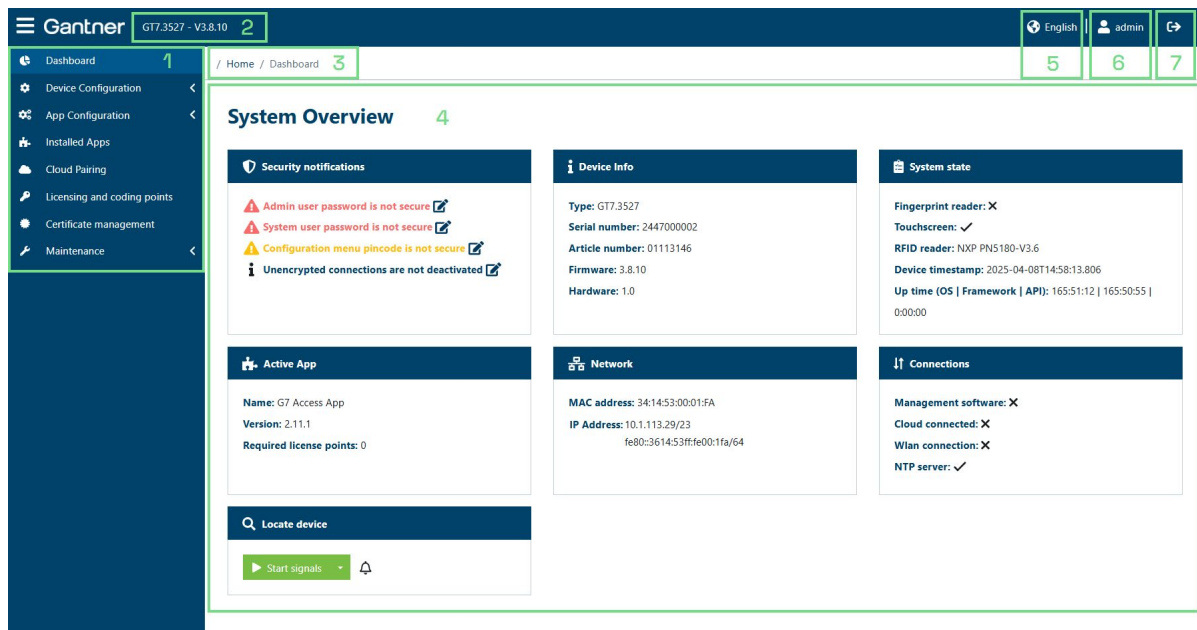
- Enter your **Username** and **Password**. Click **Login**.



NOTICE

For the initial login, the default username **admin** and the default password **GAT** can be used. After the initial login, a new admin password and PIN code must be set for configuration in the web interface (see **Security and user**).

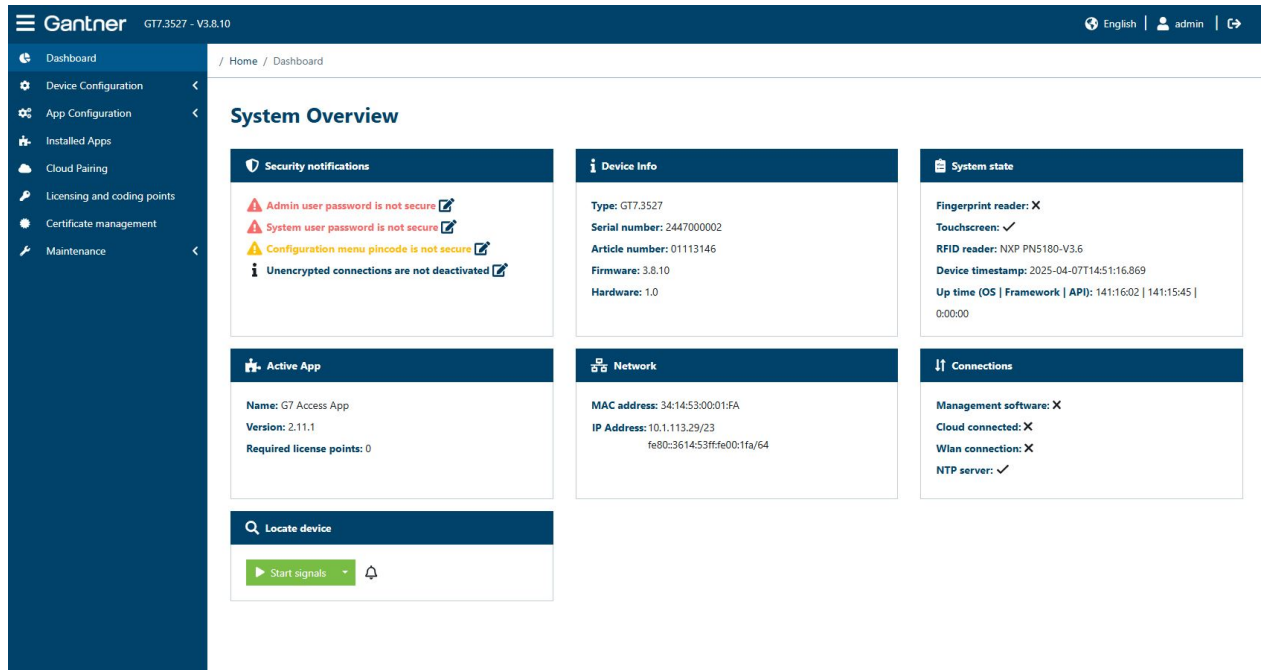
↪ The dashboard of the web interface opens with an overview of the system.



The following areas and functions are available in this window.

1. Use the **configuration menu** to access the settings of the GT7 Lite. Click on the menu button in the top left corner to **show/hide** the configuration menu.
2. The **device type** and **firmware version** are shown here.
3. **Path** of the currently displayed screen.
4. Main **information** screen for the selected configuration menu option.
5. You can change the display **language** here.
6. The logged-in **user** is displayed here.
7. Click on this symbol to **log out** of the web interface.

5.4.1. System overview



An overview of the most important settings and status information of the GT7 Lite is displayed here.

Security notifications: In this field, important security related information are displayed. If the default administrator password for accessing the web interface has not been changed yet, a notification is shown like in the example above.

Device info: The device type, the serial and article numbers, and the hardware/firmware versions of the GT7 Lite are displayed here.

System state: Display of which functions are enabled or being used. The time set in the GT7 Lite and how long the device has been running continuously since the last startup are also displayed.

Active App: The active app with the installed version and the required license points are displayed here. Depending on the device type only certain apps are relevant, for example the G7 Return App for the G7 Return and the G7 Access App for the G7 Ticketing Terminal.

Network: The addresses of the GT7 Lite on the network are displayed here.

Connections: Shown here are the available network connections and whether they are active (✓) or inactive (X).

- Management software: Connection to a PC software that controls the device. The management software can vary depending on the app being used.
- Cloud connected: Displayed as active (✓) if the GT7 Lite is connected to G7 Connect.
- Wlan connection: Displayed as active (✓) if the device's network connection is via WLAN instead of LAN.
- NTP server: Displayed as active (✓) if there is a connection to a time server that automatically sets the time in the device.

Locate device: Click this button to activate sound signals for the time defined in the drop-down menu. This function allows you to identify the terminal who you are currently connected with. Depending on the terminal the signal LED

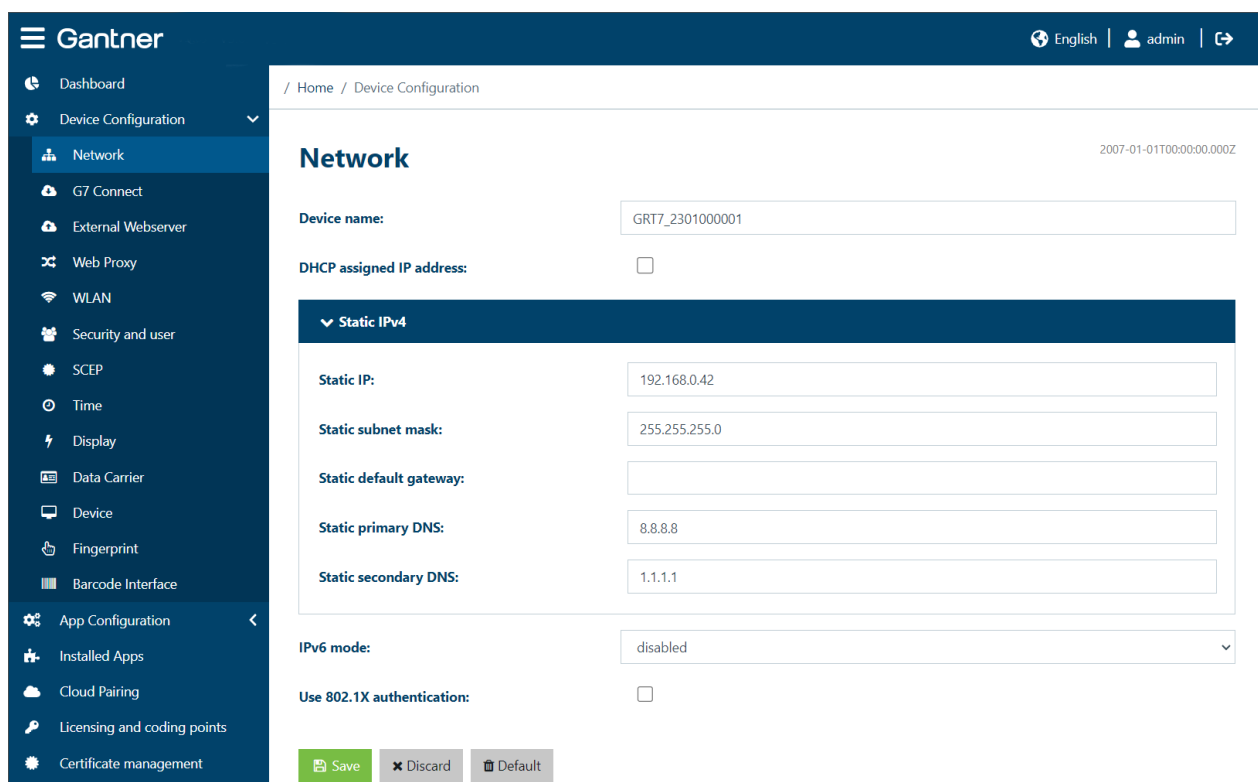
may also be lit up. If you press this button without selecting a time, only a short sound signal is generated. Note that for some devices like the G7 Return this button may have no function.

5.4.2. Network



NOTE

Please also consult with your system administrator for assistance with configuring these settings.



The screenshot shows the Gantner web interface for network configuration. The sidebar on the left lists various settings categories. The main content area is titled 'Network' and includes the following fields and options:

- Device name:** A text input field containing 'GRT7_2301000001'.
- DHCP assigned IP address:** A checkbox that is currently unchecked.
- Static IPv4 configuration:** A section with a dropdown arrow, containing:
 - Static IP:** Text input field with '192.168.0.42'.
 - Static subnet mask:** Text input field with '255.255.255.0'.
 - Static default gateway:** Empty text input field.
 - Static primary DNS:** Text input field with '8.8.8.8'.
 - Static secondary DNS:** Text input field with '1.1.1.1'.
- IPv6 mode:** A dropdown menu currently set to 'disabled'.
- Use 802.1X authentication:** A checkbox that is currently unchecked.
- Buttons:** At the bottom, there are three buttons: 'Save' (green), 'Discard' (grey with an 'X'), and 'Default' (grey with a trash icon).

The network settings for the connection to the GT7 Lite are displayed and can be configured here.

Device name: An arbitrary name can be entered for the GT7 Lite here. When the network is scanned for devices, e.g., when adding a device to Relaxx, the device is shown with this name.

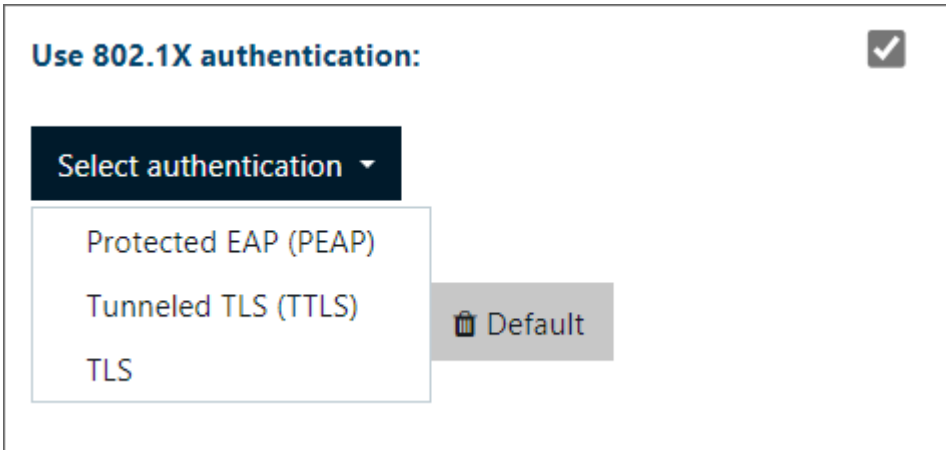
DHCP assigned IP address: When this option is enabled, the IP address of the GT7 Lite is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, disable this option and enter the network settings into the **Static IPv4 configuration** section.

IPv6 mode: If your network supports using the IPv6 protocol for device addresses, you can select one of the following options to use the protocol.

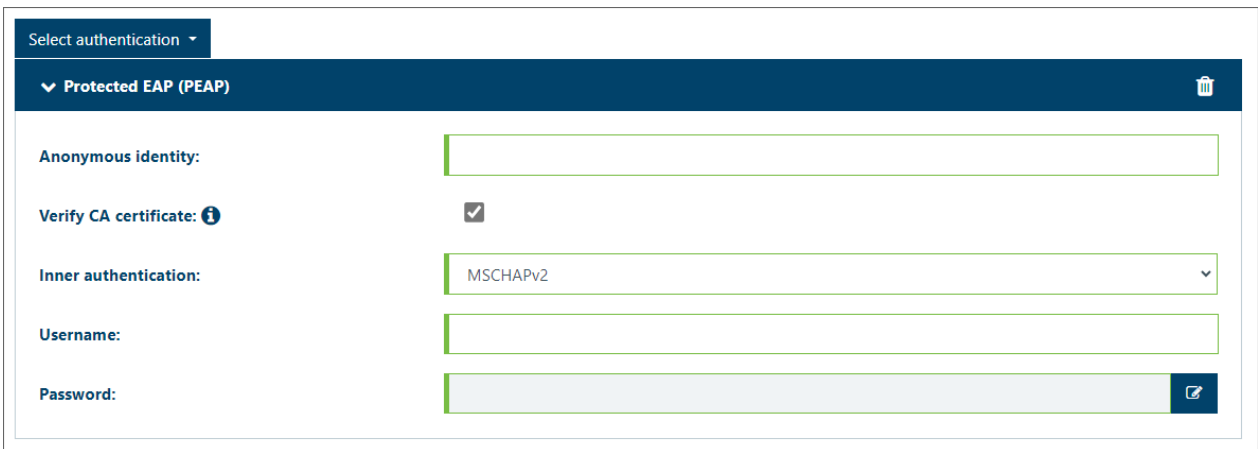
- **DHCP assigned IP address:** When this option is enabled, the IP address of the GT7 Lite is automatically assigned by a DHCP server. If you do not want to or cannot use a DHCP server, disable this option and enter the network settings into the **Static IPv4 configuration** section.
- **Static configuration:** Select this option and enter the network settings into the **Static IPv6** section to assign a static address to the device.

- **Stateless address autoconfiguration:** Stateless address autoconfiguration is the process that IPv6 nodes (hosts or routers) use to automatically configure IPv6 addresses for interfaces.

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.



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 servers. 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.
- **Inner authentication:** Select the type of protocol to use for inner authentication from the menu.
- **Username / Password:** Enter the username and password that will be used for authentication into the respective fields.

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. Define the following settings:

Select authentication ▼

▼ Tunneled TLS (TTLS)

Anonymous identity:

Verify CA certificate: ⓘ
☒

Inner authentication:
MSCHAPv2 ▼

Username:

Password:

- **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.
- **Inner authentication:** Select the type of protocol to use for inner authentication from the menu.
- **Username / Password:** Enter the username and password that will be used for authentication into the respective fields.

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.

Select authentication ▼

▼ TLS

Identity:

Verify CA certificate: ⓘ
☒

- **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.

5.4.3. G7 Connect

The screenshot shows the 'G7 Connect' configuration page in the Gantner IV interface. The left sidebar is expanded to 'Device Configuration' > 'Network' > 'G7 Connect'. The main content area has a title 'G7 Connect' and a timestamp '2007-01-01T00:00:00.000Z'. Below the title are four settings, each with a checkbox: 'Enable G7 Connect Configuration:' (checked), 'G7 Connect Address:' (text field with 'gantner.cloud'), 'Enable secure communication:' (checked), and 'Telemetry:' (checked). At the bottom are three buttons: 'Save' (green), 'Discard' (grey), and 'Default' (grey).

The settings for the device's connection to G7 Connect are configured here.

Enable G7 Connect Configuration: Enable this option if you want to use the configuration set via G7 Connect for the GT7 Lite.

G7 Connect Address: Enter the address of G7 Connect here (default = gantner.cloud).

Enable secure communication: Select this option to encrypt the communication using TLS.

Telemetry: Select this option if you want to send telemetry data to G7 Connect. This data does not contain any personal data (see the terms and conditions of G7 Connect for more information).

5.4.4. External web server

The screenshot shows the 'External Webserver' configuration page in the Gantner IV interface. The left sidebar is expanded to 'Device Configuration' > 'Network' > 'External Webserver'. The main content area has a title 'External Webserver' and a timestamp '2007-01-01T00:00:00.000Z'. Below the title are five settings: 'Enable external Webserver:' (checked), 'Server address:' (text field with a red border and error message 'Please enter a value!'), 'Enable secure communication:' (checked), 'Access token:' (text field), and 'Reconnection timeout:' (text field with '60' and a unit selector 's'). At the bottom are three buttons: 'Save' (green), 'Discard' (grey), and 'Default' (grey).

The GT7 Lite can operate as a client or server. In the configuration described here, the device operates as a server, i.e., the PC establishes the connection to the device. If the device 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 Webserver: Select 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/SSL is used for the web socket connection.

Access token: An additional value for authentication, which is entered in the authorization field of the HTML header, can be specified in this field. The data that must be entered here depends on the implementation by the third-party software.

Reconnection timeout: In this field, enter the waiting time in seconds until reconnection is attempted after the connection between the GT7 Lite and the management software has been interrupted.

5.4.5. Web proxy

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

Enable web proxy: Select this option to use a web proxy server for communication. After selection, the following settings are displayed.

Server address: IP address of the web proxy server (IPv4 format).

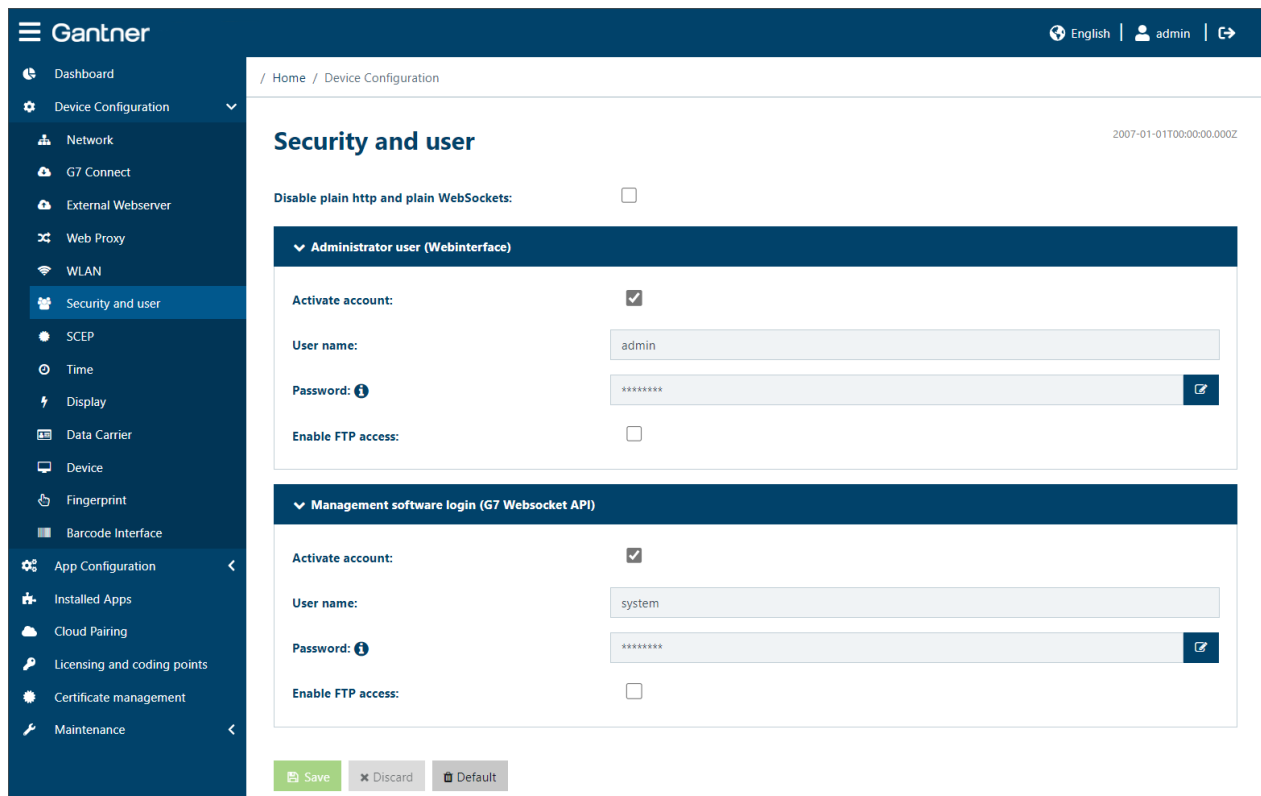
Server port: Port of the web proxy server.

Username / Password: The username and password used to access the web proxy server.

Use for G7 Connect: Enable this option is you want to use the configured web proxy to connect to G7 Connect.

Use for external web server: Enable this option is you want to use the configured web proxy to connect to an external web server.

5.4.6. Security and user



The screenshot shows the 'Security and user' configuration page in the Gantner interface. The page is titled 'Security and user' and has a timestamp '2007-01-01T00:00:00.000Z'. The page is divided into two main sections: 'Administrator user (Webinterface)' and 'Management software login (G7 Websocket API)'. Each section has a form with the following fields: 'Activate account' (checkbox), 'User name' (text input), 'Password' (password input with a blue edit button), and 'Enable FTP access' (checkbox). The 'Administrator user' section has 'Activate account' checked, 'User name' set to 'admin', and 'Enable FTP access' unchecked. The 'Management software login' section has 'Activate account' checked, 'User name' set to 'system', and 'Enable FTP access' unchecked. At the top of the page, there is a checkbox for 'Disable plain http and plain WebSockets'. At the bottom of the page, there are three buttons: 'Save', 'Discard', and 'Default'.

Here you can define the users who are allowed to access the GT7 Lite via its web interface (**Administrator user (Webinterface)**) and the G7 WebSocket API (**Management software login (G7 Websocket API)**). The **Management Software Access (G7 Websocket API)** user is used, e.g., by the eLoxx Relaxx management software. Only the **Administrator user** is activated by default.

Disable plain http and plain WebSockets: This option is enabled by default (security by default). If this option is disabled, the GT7 Lite may use an unencrypted connection (e.g., HTTP instead of HTTPS) for communication.

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. This name cannot be changed.

Enable FTP access: Enable or disable access to the FTP server in the GT7 Lite via this setting. FTP access is deactivated by default.

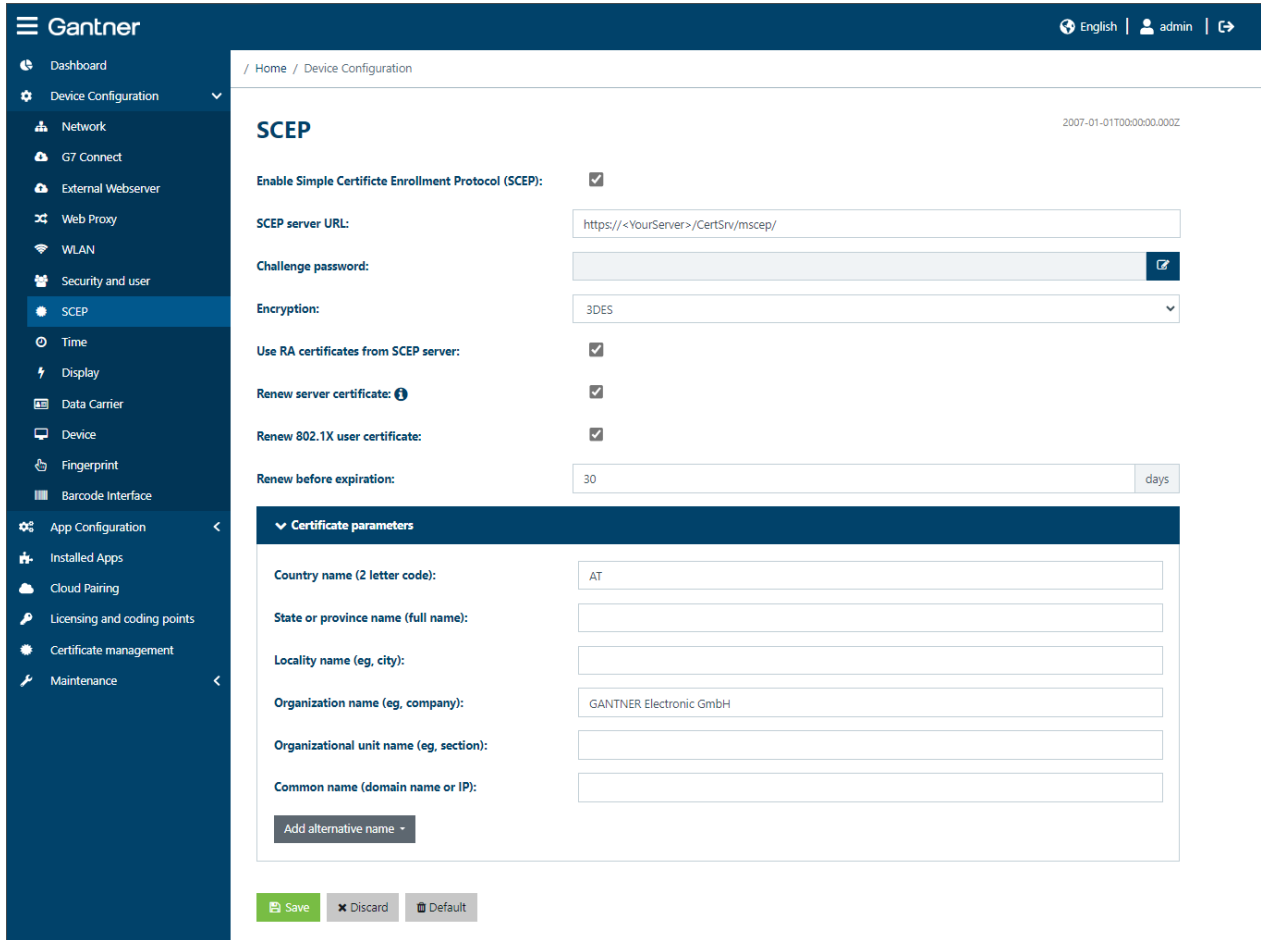
Password: Enter a password for the user. Click on the blue edit button to the right.



NOTE

If the **Management Software Access (G7 Websocket API)** password is changed here, it must also be entered into the eLoxx Relaxx software.

5.4.7. SCEP



SCEP

2007-01-01T00:00:00.000Z

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

▼ Certificate parameters

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):

SCEP (Simple Certificate Enrollment Protocol) is a protocol to quickly and simply request and issue digital certificates. The digital certificates are used for establishing a secure communication between the GT7 Lite and a host computer or server.

Enable Simple Certificate Enrollment Protocol (SCEP): Enable this option to use SCEP. Additional settings are then displayed below.

SCEP server URL: The address (URL) of the server where the certificates are located.

Challenge password: The password that is used to access the SCEP server.

Encryption: Select the desired encryption type (AES or 3DES).

Use RA certificates from SCEP server: With this option the certificates from 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 / Renew 802.1X user certificate: These options are used for the communication between the device web interface and the management software. If an option is enabled, the device will restart after installing or renewing the certificate on the server or the device.

Renew before expiration: The number of days entered here defines when the certificate will be renewed (x days before expiration).

Certificate parameters: Enter the data for the certificate into this area. The data must correspond to the parameters that were used to generate the certificate.

5.4.8. Time

Adjust these settings to define how to display and use the time in the GT7 Lite.

Time format: Select either 24-hour format (example: 15:48) or 12-hour format (example: 3:48 pm).

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. Enter the address of the NTP server here. If this field is empty, no NTP server will be used.

Time zone: Select the time zone that the GT7 Lite is operating in.

5.4.9. Display

The screenshot shows the Gantner web interface for device configuration. The left sidebar lists various configuration categories, with 'Display' currently selected. The main panel displays the 'Display' settings for a specific device. The settings are as follows:

Setting	Value	Unit
Display Brightness:	70	%
Display Brightness (Screensaver):	20	%
Slideshow after:	3600	s
Next image after:	20	s
Screensaver after:	7200	s
Screensaver Text:	Gantner	

At the bottom of the settings panel, there are three buttons: 'Save' (green), 'Discard' (grey), and 'Default' (grey).

These settings are relevant when the GT7 Lite has a display or if an external display is connected to the device. The 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 is enabled (see screensaver settings).

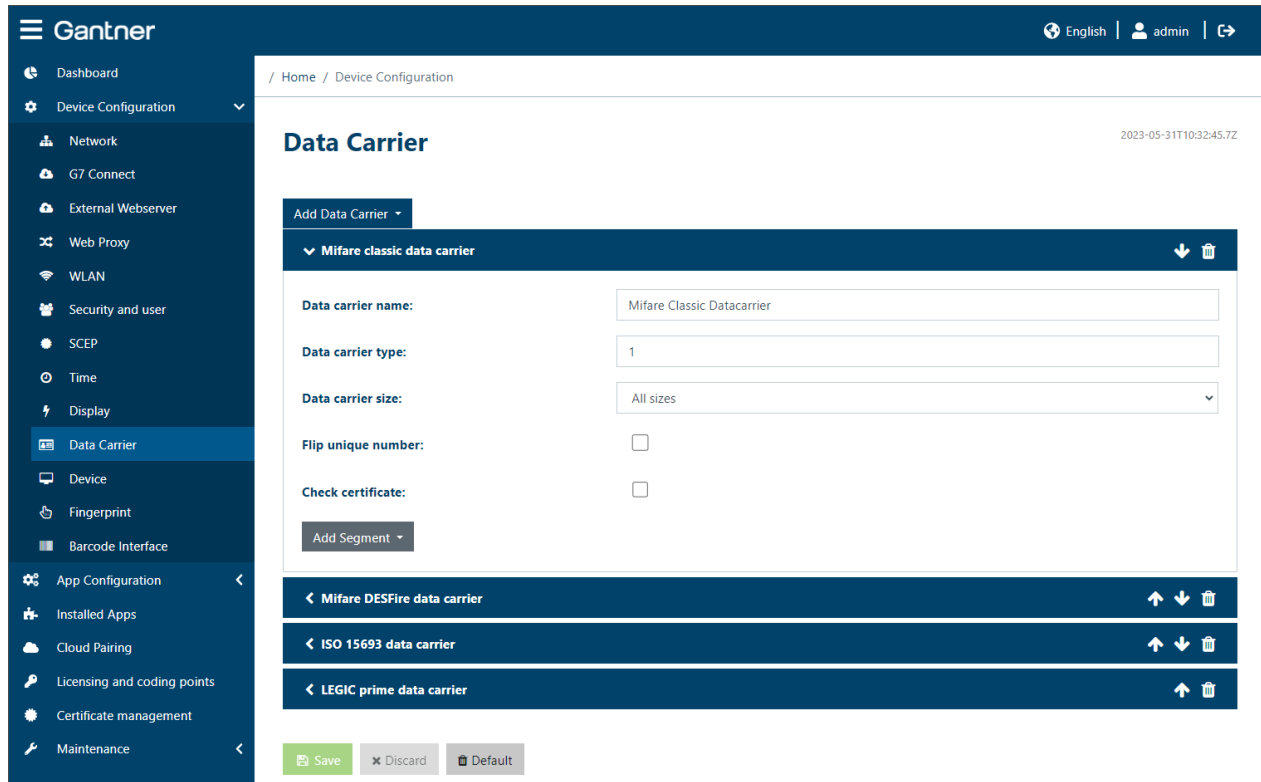
Slideshow after: Time (in seconds) of device inactivity after which an image slideshow (e.g., pictures from the theme) is displayed.

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 count down as soon as the slideshow is activated.

Screensaver text: Text that is displayed when the screensaver is active. If no images are selected for the slideshow, this text will also be displayed when the slideshow is activated.

5.4.10. Data carrier



The settings for the different types of data carrier technologies that will be used with the GT7 Lite are configured here. These settings must be set correctly so that the data carriers can be used, i.e., read by the device.

Multiple data carrier types can be configured. The settings for each data carrier type differ depending on the type of technology being used.

Add data carrier: To configure a new data carrier type, click on this field and select the desired type from the list.

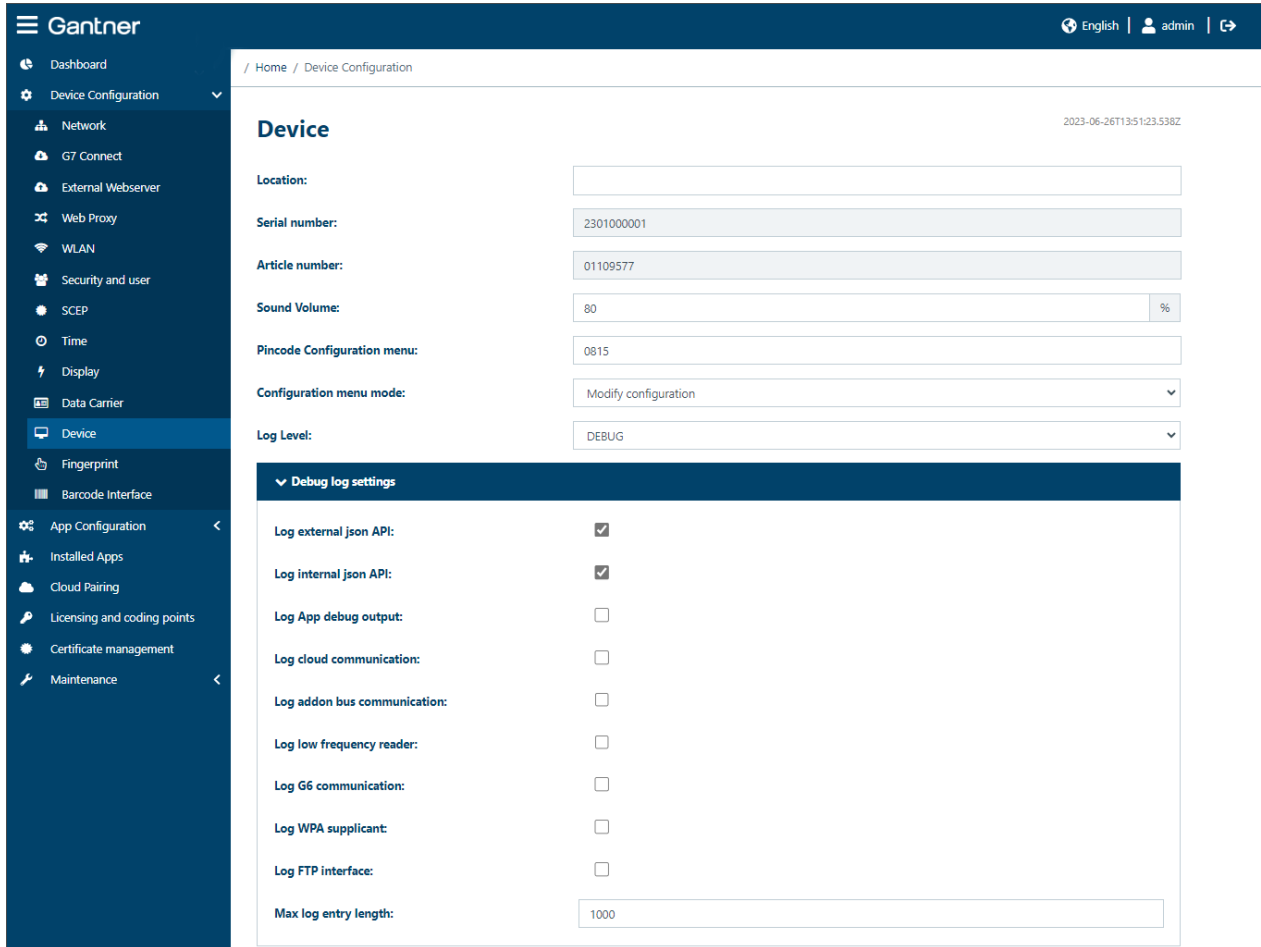
Delete data carrier: You can delete an existing data carrier type or a segment in the data carrier via the trash can icons on the right.



NOTE

Please speak to your Gantner representative if you have any questions regarding the settings.

5.4.11. Device



The screenshot shows the Gantner Device Configuration web interface. The sidebar on the left contains navigation links: Dashboard, Device Configuration (selected), Network, G7 Connect, External Webserver, Web Proxy, WLAN, Security and user, SCEP, Time, Display, Data Carrier, Device (selected), Fingerprint, Barcode Interface, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'Device' and displays the following settings:

- Location:** A text input field.
- Serial number:** A text input field containing '2301000001'.
- Article number:** A text input field containing '01109577'.
- Sound Volume:** A text input field containing '80' and a percentage symbol.
- Pincode Configuration menu:** A text input field containing '0815'.
- Configuration menu mode:** A dropdown menu with 'Modify configuration' selected.
- Log Level:** A dropdown menu with 'DEBUG' selected.

Below these settings is a 'Debug log settings' section with the following options:

- Log external json API:** ☒
- Log internal json API:** ☒
- Log App debug output:** ☐
- Log cloud communication:** ☐
- Log addon bus communication:** ☐
- Log low frequency reader:** ☐
- Log G6 communication:** ☐
- Log WPA supplicant:** ☐
- Log FTP interface:** ☐
- Max log entry length:** A text input field containing '1000'.

Here you will find the basic device settings, which include:

Location: The location of the device can be entered here. This name is displayed to help you to distinguish between multiple devices.



NOTE

Some special characters are not allowed. A message is displayed if an unusable special character is entered.

Serial number / Article number: The serial number and article number of the GT7 Lite are displayed here.

Sound volume: Adjusts the volume of the acoustic signal of the device from 0 to 100%. Entering 0% mutes the sound.

PIN code configuration menu: This code is used to access the configuration menu on the display of the device. The code can be entered after writing an **M** on the display with your finger.

Configuration menu mode: The GT7 Lite has an integrated configuration menu that allows certain settings to be adjusted on-site. The menu is accessed via the PIN code as defined in the **PIN code configuration menu** setting.

- **Modify configuration:** The configuration menu can be accessed and the settings can be viewed and edited.
- **Show configuration:** The configuration menu can be accessed and the settings can be viewed only.
- **Configuration menu disabled:** The configuration menu cannot be accessed.

Log level: Here you can define which types of events should be recorded by the device. This log can be downloaded and read via the **Log Viewer** page. Different messages are logged depending on the setting configured here:

- **Error:** All errors are displayed. This includes, e.g., connection errors to G7 Connect.
- **Warning:** Warning messages are displayed. This includes, e.g., logins in the web interface.
- **Info:** Information messages are displayed, e.g., when a data carrier is within the reading field and when it has been read.
- **Debug:** Detailed debug messages are displayed for service purposes.

Debug log settings: Select here which messages are to include in the log file. There are also two more settings in this area:

- **Max log entry length:** This is the number of debug log entries that are stored by the device. Default = 500.
- **Debug log duration:** The time period selected here defines how long the debug log entries are stored for. Select either 4 hours, one day (24 hours) or one week (7 days) from the menu.

5.4.12. Barcode interface

These settings are relevant when a barcode reader is being used with the GT7.1300.

Reader mode: Select the type of reader or interface from the menu.

- **Default:** General/undefined barcode reader.
- **GBS7.1xxx – Signals reader controlled:** For the GBS7.1xxx barcode readers 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:** For the GBS7.1xxx 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.

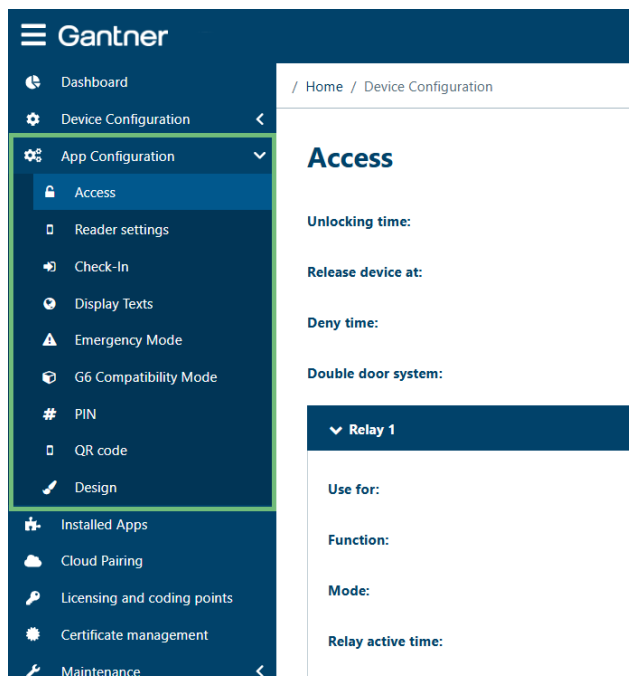
- **GBS7.1xxx - Signals host controlled, USB:** For the GBS7.1xxx barcode readers from Gantner, which are connected via USB. With this setting the signaling on the barcode reader is not set until the approval or rejection is made by the management software.

Baud rate: The transmission rate of the barcode reader.

Enable beeper: If a barcode reader of type GBS7.1xxx with signals host controlled is used, the beeper of the barcode reader can be activated or deactivated.

5.4.13. App configuration

The settings pages displayed in the **App Configuration** section of the web interface apply to the app currently running on the GT7 Lite. Only one app can be active at a time. If you want to run another installed app, the desired app can be started via the **Installed Apps** page of the web interface (see [Installed apps \[48\]](#)).



NOTE

As the settings pages displayed in the sidebar vary depending on which app is operating, these configuration settings are described in the corresponding user manual of the active app. Please refer to the manual of the respective app for more information.

5.4.14. Installed apps

Different apps can be installed on the GT7 Lite with one app being operable at a time, i.e., not multiple apps simultaneously. License points are required to activate some apps, and these are available to purchase from Gantner.

When you order license points, the desired number of points are transferred to your organization in G7 Connect. You can then transfer the points in G7 Connect to the projects and respective devices as required.



NOTE

See the G7 Connect manual for detailed information on how to transfer license points in G7 Connect.

There are also some extensions for the apps. The extension **G7 Open Card** can be used to disable certificate checking on the GT7 Lite so that third-party data carriers can work with the device. G7 Open Card requires 10 license points and can be applied to apps with 0 license points.

On the **Installed Apps** page of the web interface, all installed apps are listed with the currently active app indicated by the green **Active App** text.

1. To start another app, click on the **Activate** button for the desired app.
↳ The app starts, which can take up to a minute, and the GT7 Lite 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.
2. In the upper **Drop App here** field, additional apps can be loaded into the GT7 Lite. To do this, the app file is needed.
3. 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.



NOTE

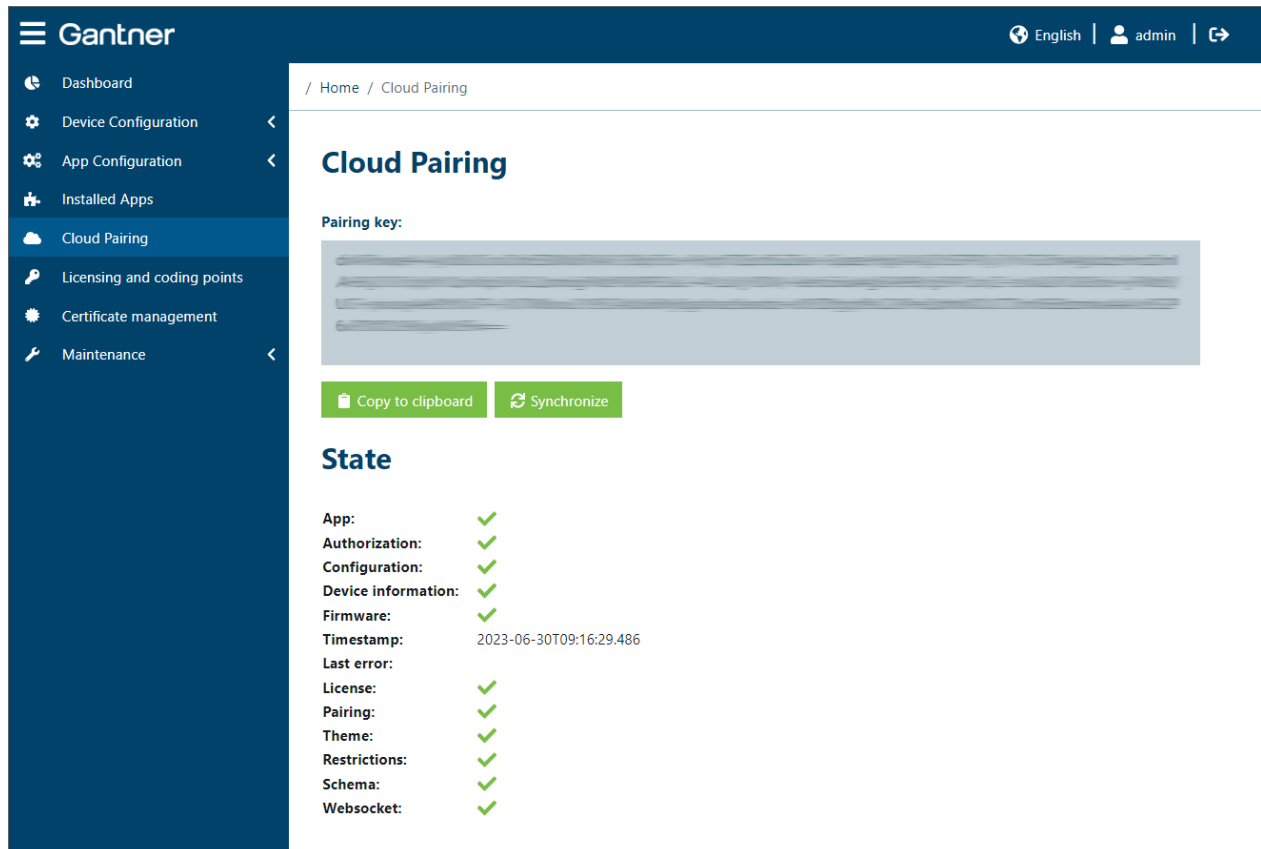
A theme is a template file (ZIP file) that defines the format and appearance of the app on the display (e.g., text types, colors, positions, etc.). The formatting in a theme is done using CSS, which offers a lot of freedom in the design of the themes. In addition, a theme archive may contain images that can be viewed using the screensaver function. The images are located in the archive file of the screensaver sub-folder.

Table of G7 Apps

Table 2. G7 App functionality and required license points

App	Function	License Points
G7 Access App (default app)	For access control to an area separated by a door or turnstile, etc. Access is granted or denied after identification with the user's data carrier, fingerprint, or barcode.	0
G7 Advanced Access App	Enables the standard access app functions as well as additional functions such as an authorization list, support for multiple GR7 readers per terminal/controller, and coding of MIFARE Classic data carriers.	30
G7 Countdown App	Displays a configurable countdown timer (e.g., 5 mins) to show the user when the use of a time-limited device, e.g., a shower or power plate, will expire.	0
G7 Info App	For the display of customer information after their data carrier is read. The information displayed is configurable, e.g., the customer's locker number or the validation date.	20
G7 Writer App	This app is designed exclusively for the GT7.0510 (GT7 Lite Terminal) with a USB HID Mode interface. It is used as a universal read/write app for RFID data carriers.	0

5.4.15. Cloud pairing



The screenshot shows the Gantner G7 Connect web interface. The left sidebar contains navigation links: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing (selected), Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'Cloud Pairing' and shows a 'Pairing key' field with a blurred key value. Below the key are two buttons: 'Copy to clipboard' and 'Synchronize'. The 'State' section lists various system parameters with their status indicated by green checkmarks:

- App: ✓
- Authorization: ✓
- Configuration: ✓
- Device information: ✓
- Firmware: ✓
- Timestamp: 2023-06-30T09:16:29.486
- Last error:
- License: ✓
- Pairing: ✓
- Theme: ✓
- Restrictions: ✓
- Schema: ✓
- Websocket: ✓

G7 Connect is Gantner's online platform that allows you to configure and manage all your G7 devices in one convenient location.

To add a GT7 Lite to a project in G7 Connect, the device must be paired with G7 Connect once. This process requires a pairing key, which is displayed on this page.

1. To open G7 Connect in your default web browser, click on the link: [G7 Connect](#), and log in with your username and password.



NOTE

See the G7 Connect manual for information on creating an account.

↪ The G7 Connect dashboard is displayed.

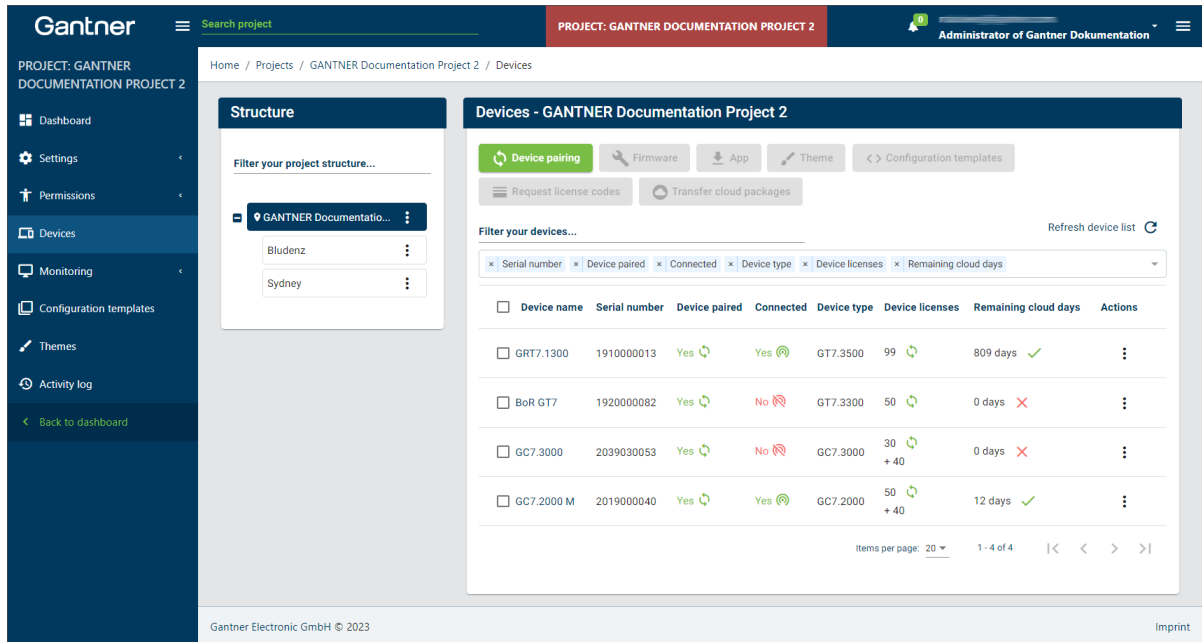
- Click on **Projects** in the sidebar.

- Click on the project that you want to assign the device to.

↪ The project dashboard is displayed. The selected project is displayed above the menu on the left.

- Click on **Devices** in the sidebar.

↪ The devices already assigned to the project are displayed.

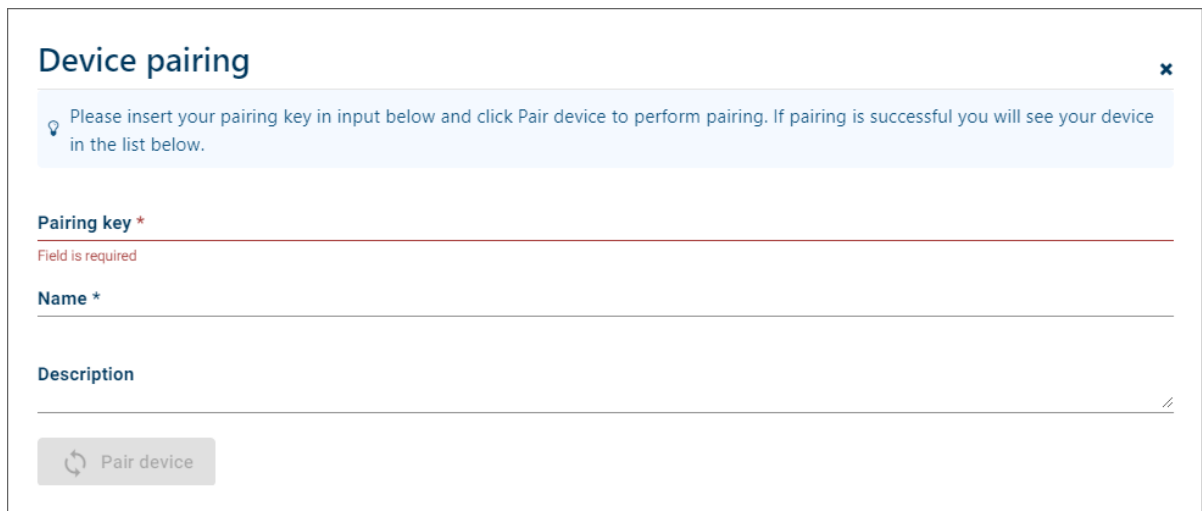


The screenshot shows the Gantner web interface for 'PROJECT: GANTNER DOCUMENTATION PROJECT 2'. The left sidebar contains navigation options like Dashboard, Settings, Permissions, Devices, Monitoring, Configuration templates, Themes, and Activity log. The main content area is titled 'Devices - GANTNER Documentation Project 2' and features a 'Device pairing' button, 'Request license codes', and 'Transfer cloud packages' buttons. Below these is a table of devices with the following data:

Device name	Serial number	Device paired	Connected	Device type	Device licenses	Remaining cloud days	Actions
GRT7.1300	1910000013	Yes	Yes	GT7.3500	99	809 days	
BoR GT7	1920000082	Yes	No	GT7.3300	50	0 days	
GC7.3000	2039030053	Yes	No	GC7.3000	30 + 40	0 days	
GC7.2000 M	2019000040	Yes	Yes	GC7.2000	50 + 40	12 days	

5. Click on the **Device pairing** button.

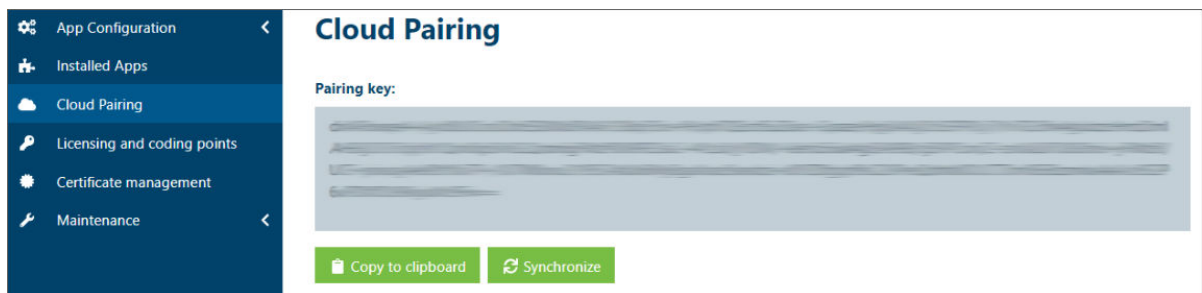
↪ The **Device pairing** window opens.



The 'Device pairing' window is a modal dialog with a close button (X) in the top right corner. It contains the following fields and buttons:

- Pairing key ***: A text input field with a red error message 'Field is required' below it.
- Name ***: A text input field.
- Description**: A text input field.
- Pair device**: A button with a circular arrow icon.

6. On the **Cloud pairing** page of the the web interface, copy the **Pairing key**.



The 'Cloud Pairing' page has a sidebar with navigation options: App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'Cloud Pairing' and contains a 'Pairing key:' label followed by a blurred key value. Below the key are two buttons: 'Copy to clipboard' and 'Synchronize'.

7. In the **Device pairing** window of G7 Connect, paste the **Pairing key** into the respective field. Enter a **name** for the device, which can be selected freely. You can also enter an optional descriptive text in the **Description** field.

Device pairing ✕

 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 *

Name *
 G7 Device

Description

 Pair device

8. Click on **Pair device**.

- The device attempts to establish an outgoing connection to G7 Connect via the Internet. The device must therefore be switched on and connected to the Internet (G7 Connect). Check the connections and firewall settings if pairing and synchronization does not work.
- When the device is found, it is displayed in the devices list of the project.
- In the web interface, the status of the pairing process is displayed. After pairing is completed, the different states are displayed to indicate whether an update is required.

 App Configuration <

 Installed Apps

 Cloud Pairing

 Licensing and coding points

 Certificate management

 Maintenance <

Cloud Pairing

Pairing key:

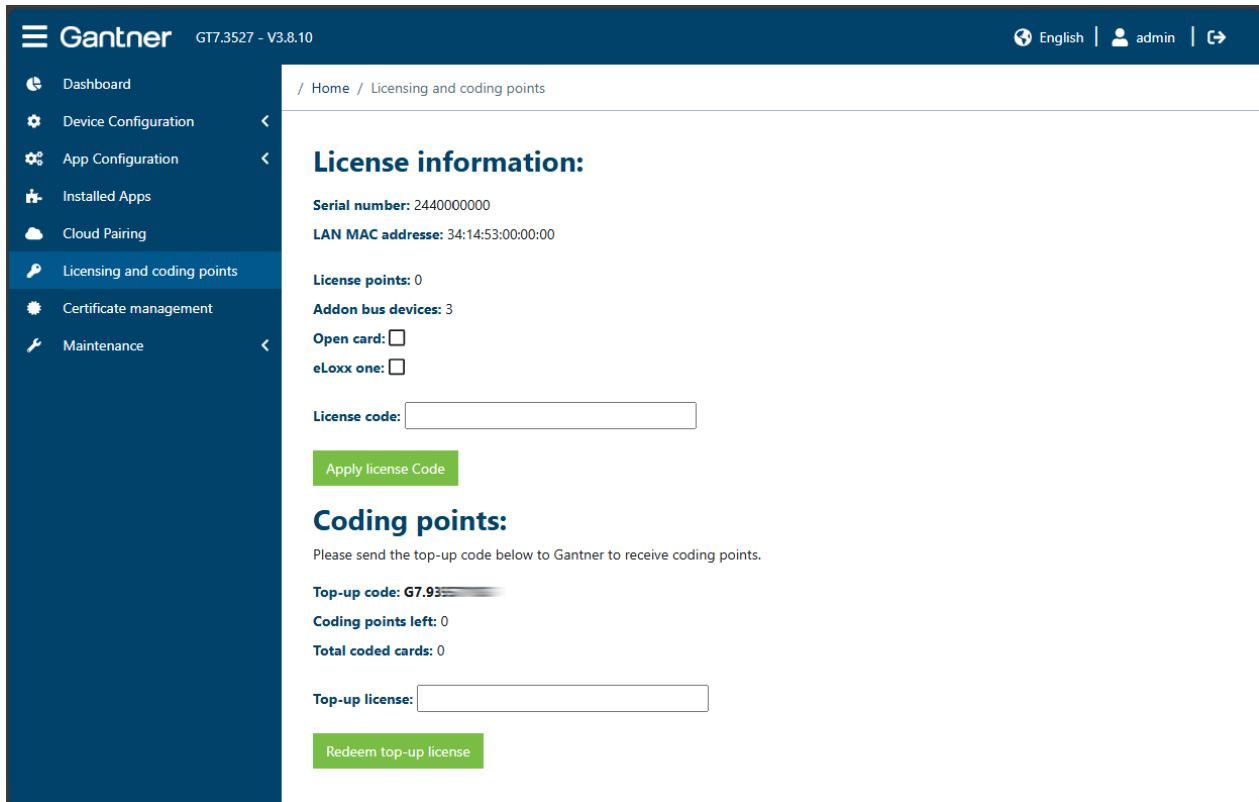
Copy to clipboard

Synchronize

State

App:	✓
Authorization:	✓
Configuration:	✓
Device information:	✓
Firmware:	✓
Timestamp:	2023-06-30T09:16:29.486
Last error:	
License:	✓
Pairing:	✓
Theme:	✓
Restrictions:	✓
Schema:	✓
Websocket:	✓

5.4.16. Licensing and coding points



The screenshot shows the Gantner web interface for a GT7.3527 - V3.8.10 device. The left sidebar contains navigation 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:** 2440000000
- LAN MAC address:** 34:14:53:00:00:00
- License points:** 0
- Addon bus devices:** 3
- Open card:** ☐
- eLoxx one:** ☐
- License code:**
- Apply license Code** (button)

Below the license information, the 'Coding points:' section is displayed. It includes the instruction: 'Please send the top-up code below to Gantner to receive coding points.' The details shown are:

- Top-up code:** G7.93
- Coding points left:** 0
- Total coded cards:** 0
- Top-up license:**
- Redeem top-up license** (button)

On this page, the network and license information for the GT7 Lite are displayed and you can also add new license points here. The coding points that are used to encode data carriers using the corresponding G7 app can also be added.

License information

Serial number: The serial number of the GT7 Lite.

LAN MAC address: Unique, internal network address of the GT7 Lite.

License points: License points are required to activate certain G7 apps and enable other features. License points can be purchased from Gantner. The available license points are displayed here.

Open card: A tick in this field indicates that the **Open Card** license has been enabled and the certificate check is disabled, i.e., data carriers that were not coded by Gantner can also be used.

License code: Here you can enter a license code for the installation of additional apps or to activate additional functions can be entered here.



NOTE

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

Coding points

Coding points left: Here you can see how many coding points are currently still available in the terminal. As soon as you add new coding points, the new coding points are displayed here.

Total coded cards: The number of data carriers that have already been encoded is displayed here.

5.4.17. Certificate management

The screenshot shows the Gantner web interface for Certificate management. The left sidebar contains navigation options: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management (selected), and Maintenance. The main content area has a breadcrumb trail: / Home / Certificate management. Below the breadcrumb, there's a section titled "Certificate management:" with several buttons: "Show certificates", "Add CA certificates", "Generate new self-signed certificate", "Generate CSR", "Install server certificate", and "Install 802.1X certificates". A sub-section titled "Simple Certificate Enrollment Protocol (SCEP)" contains a table of certificates.

Subject	Issuer	Valid from	Valid to	Serial number	Type
Factory Default, GANTNER Electronic GmbH	Factory Default, GANTNER Electronic GmbH	2022-01-01 00:01:11Z	2051-12-25 00:01:11Z	67:ac:32:8b:d0:ed:10:b8:f1:93:a4:14:83:14:fa:48:88:8a:e2:40	Server
COMODO ECC Certification Authority, COMODO CA Limited	COMODO ECC Certification Authority, COMODO CA Limited	2008-03-06 00:00:00Z	2038-01-18 23:59:59Z	1f47:afaa:62:00:70:50:54:4c:01:9e:9b:63:99:2a	CA
Amazon Root CA 3, Amazon	Amazon Root CA 3, Amazon	2015-05-26 00:00:00Z	2040-05-26 00:00:00Z	06:6c:9fd5:74:97:36:66:3f:3b:0b:9a:d9:e8:9e:76:03:f2:4a	CA
DST Root CA X3, Digital Signature Trust Co.	DST Root CA X3, Digital Signature Trust Co.	2000-09-30 21:12:19Z	2021-09-30 14:01:15Z	44:afb0:80:d6:a3:27:ba:89:30:39:86:2e:f8:40:6b	CA
Amazon Root CA 4, Amazon	Amazon Root CA 4, Amazon	2015-05-26 00:00:00Z	2040-05-26 00:00:00Z	06:6c:9fd7:c1:bb:10:4c:29:43:e5:71:7b:7b:2cc8:1a:xc:10:e	CA
ISRG Root X2, Internet Security Research Group	ISRG Root X2, Internet Security Research Group	2020-09-04 00:00:00Z	2040-09-17 16:00:00Z	41:d2:9d:d1:72:eae:ea7:80:c1:2c:6c:e9:2f:87:52	CA

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

This screenshot shows the "Add CA certificates" window within the Certificate management interface. It features a search bar with the text "Drop certificate here (PEM or DER format)". Below the search bar, there are two buttons: "Add CA certificates" (highlighted in green) and "Restore recommended CA certificates". The window also includes a description: "Add certificate authority (CA) certificate. Used for cloud applications."

Various options are displayed above the list. Click on the **Show certificates** option to display the installed certificates. To add a new certificate, simply drag the certificate file (file extension .PEM) to the **Drop certificate here (PEM format)** field in the corresponding window (depending on the selected function, e.g. **Add CA certificates** like in the image above).

The following functions can be performed via the other options in this menu.

Add CA certificates: Add a certificate issued by a certification authority (CA). To do this, drag the file with the certificate (in PEM format) onto the one provided in this window and click **Add CA certificates**.

If you click on **Restore recommended CA certificates**, the certificates are reset to or restored to the default certificates installed when the device was delivered.

Generate new self-signed certificate: If encrypted communication between the device and the server is being used (via TLS over HTTPS or WSS), the device 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 device 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 device is acting as a web server, which acts as a "client" and establishes the connection to the "server", a certificate is required on the server, i.e., on the GT7 Lite, for a secure connection using TLS.

You can create this certificate 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 certificates: Here, you can install an official certificate from a certification authority for authentication using 802.1X. To do this, drag the file with the certificate to the field provided and click **Install 802.1X certificates**.

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 using the Simple Certificate Enrollment Protocol (SCEP) can be installed here. 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



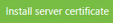
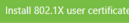
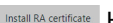
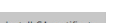
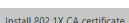
Drop certificate here (PEM or DER format)

[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	30:b9:f8:f5:d2:19:e9:37:2b:d1:01:ad:c5:8f:00:e9:a6:36:d7:c1	Server  

Below the **Configuring 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.

1. 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 "[SCEP](#)". for more information. If SCEP is enabled and the connection to the SCEP server is active, you can perform the following actions:
2.  If the GT7 Lite is operated as a web server (e.g. when using the eLoxx Relaxx software, which acts as a "client" and establishes the connection to the "server" GT7 Lite, a certificate is required for the server, i.e. on the GT7 Lite, for a secure connection using TLS. You can complete the installation by clicking on this button.
3.  Here you can install a certificate for authentication via 802.1X.
4.  Here you can install a certificate issued by a registration authority (RA).
5.  Here you can install a certificate issued by a certification authority (CA).
6.  This button allows you to install an official certificate from a certification authority for authentication using 802.1X.
7. The certificates (encryption and signature) for the registration authority (RA) can also be manually installed from a file without using the SCEP server. This can be done in the **Installing RA certificate manual** section.

Install RA certificate manual



Drop certificate here (PEM or DER format)

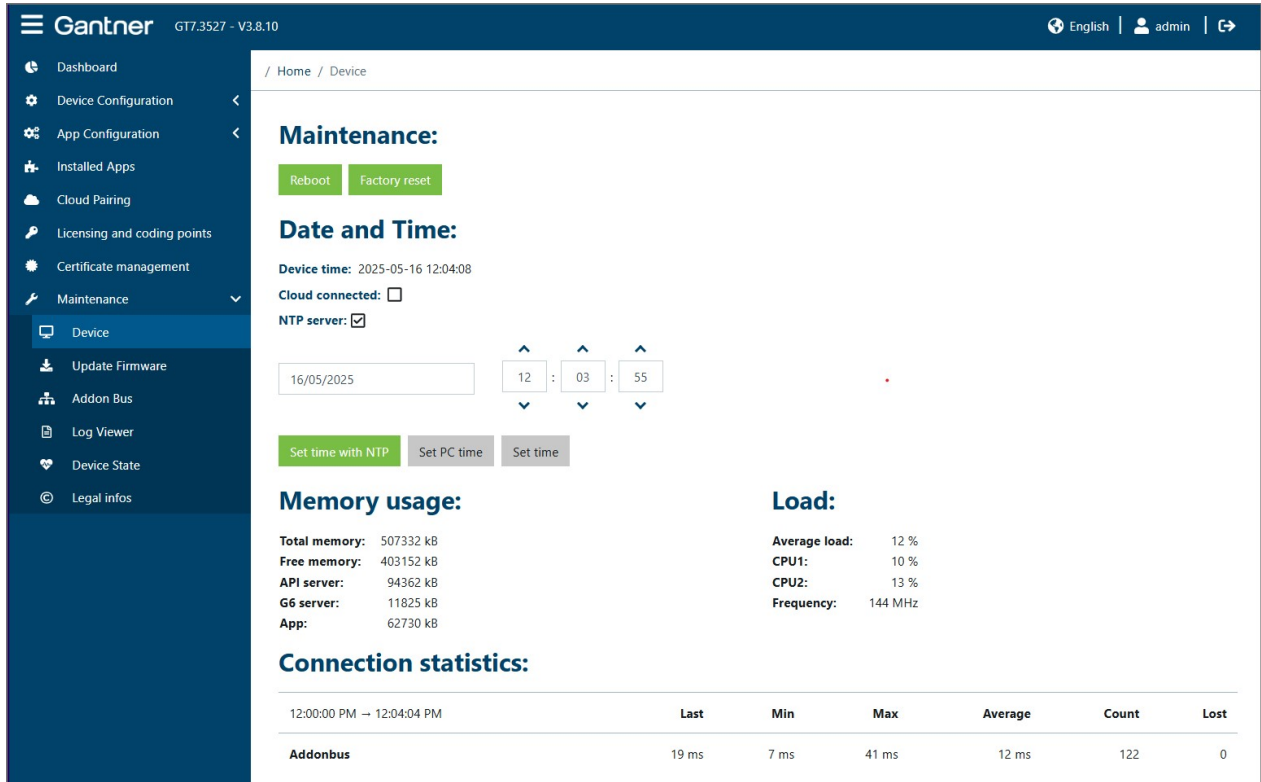
Install SCEP encryption certificate

Install SCEP signature certificate

Create new private key

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

5.4.18. Device



The screenshot shows the Gantner web interface for device configuration. The left sidebar contains navigation options like Dashboard, Device Configuration, App Configuration, etc. The main content area is titled 'Maintenance' and 'Date and Time'. Under 'Maintenance', there are buttons for 'Reboot' and 'Factory reset'. The 'Date and Time' section shows the device time as 2025-05-16 12:04:08, with checkboxes for 'Cloud connected' and 'NTP server'. Below this is a date and time picker. The 'Memory usage' section lists various memory metrics. The 'Load' section shows average load and CPU usage. The 'Connection statistics' section includes a table for addons.

	Last	Min	Max	Average	Count	Lost
12:00:00 PM → 12:04:04 PM						
Addons	19 ms	7 ms	41 ms	12 ms	122	0

The following settings and information are available on this page.

Maintenance

Reboot: Click on this button to restart the device. The web interface remains connected to the device and further work can be completed in the web interface after the restart is completed.

Factory reset: Click on this button to reset the device to its default settings.



NOTICE

All settings in the device are deleted during the reset process. After the reset, the device is in same functional state it was upon delivery.

Date and time

Device time: The current time in the device is displayed here. This time is updated every second. Go to **Device Configuration > Time** to configure the time settings.

Cloud connected: A tick in this checkbox indicates that the device is paired with G7 Connect. Go to **Device Configuration > G7 Connect** to configure these settings.

NTP server: A tick in this checkbox indicates that the device is using an NTP server to automatically synchronize the time. Go to **Device Configuration > Time** to configure the time settings.

- To reset the time in the device, select one of the following options:

- **Set time with NTP:** The time is automatically obtained from an NTP server in the network. Go to **Device Configuration > Time** to define the address of the server.
- **Set PC time:** The current time of the PC being used to configure the device is used.
- **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 device.

Memory usage / Load

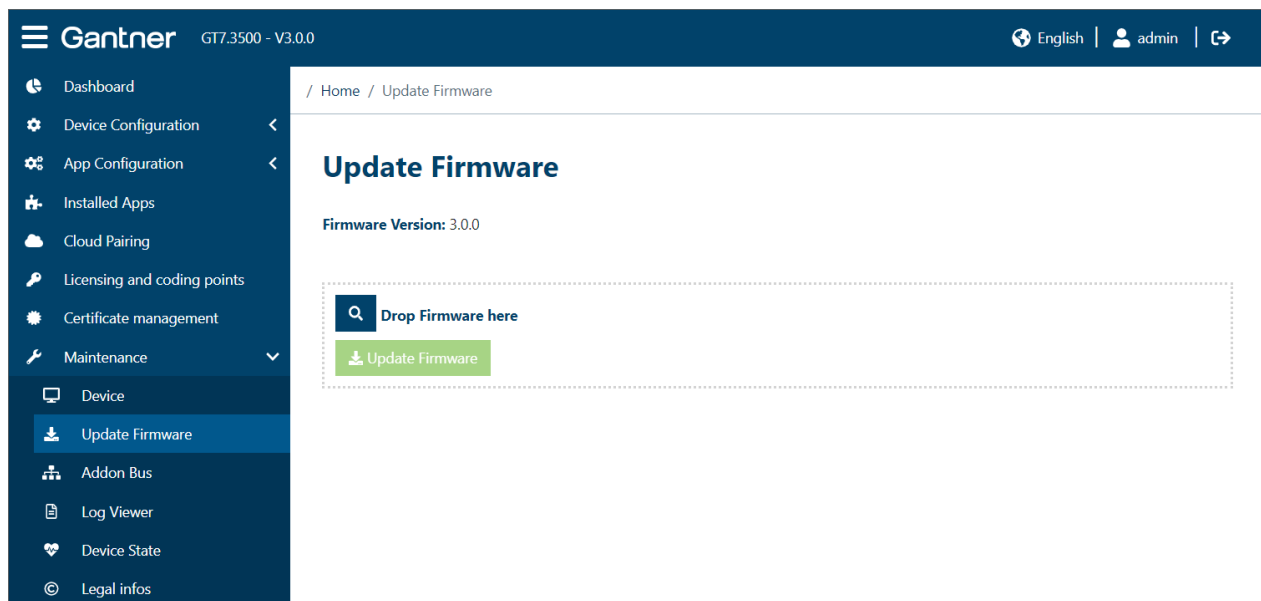
Information about the memory in the device, i.e., the total memory, free space, and memory used by each component, is shown here.

Shown in the load section is information on the current load and clock frequency of the CPUs. These values indicate how much the processor cores are being used and are mainly relevant for service personnel. If the average load is at a high value (>90%), an operation is using a lot of computing time and the device should be restarted.

Connection statistics

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

5.4.19. Update firmware



The firmware currently installed in the device is displayed here.

1. To update the firmware, drag the firmware file onto the **Drop firmware here** field.



NOTICE

During the firmware update, ensure that the power supply to the device is not disconnected.

2. Click on **Update Firmware**.

The new firmware is uploaded and the device restarts.

5.4.20. Log viewer

The screenshot shows the Gantner Log Viewer interface. The sidebar on the left contains navigation links: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, Maintenance, Device, Update Firmware, Addon Bus, Log Viewer (selected), Device State, and Legal infos. The main content area is titled 'Log Viewer' and includes a search bar, a 'Download log files' button, and a 'Change device log level' link. Below these is a table of log entries with columns for Timestamp, Level, and Source. The table contains five entries, all with a level of 'INFO' and a source of 'EVENT'. The first entry has a source of 'IO.BarcodeRead' and a timestamp of '2025.06.02 14:15:38.022'. The second entry has a source of 'IO.TagInReader' and a timestamp of '2025.06.02 14:15:38.026'. The third entry has a source of 'App.UnlockProcessResult' and a timestamp of '2025.06.02 14:15:39.348'. The fourth entry has a source of 'App.NewBookingAvailable' and a timestamp of '2025.06.02 14:15:39.787'. The fifth entry has a source of 'App.AppStateChanged' and a timestamp of '2025.06.02 14:15:39.788'. There is also a 'Clear list' button at the bottom of the table.

All events and error messages are stored in the GT7 Lite 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 currently occurring events are displayed live. If you close the **Log Viewer** page and then reopen it, the display of live events is restarted. However, the events are always recorded and can be downloaded at any time.

1. To load the log files from the device, click on **Download log files**.
↳ The log files from the previous 8 days are transferred to a compressed file (GZ) and automatically downloaded to the **Downloads** folder of your web browser.
2. Click on **Change device log level** to open the device settings. Here you can change the log level, which defines the types of events that are displayed in the live view (e.g., all info + warnings or only errors, etc.). For more information see "[Device configuration \[31\]](#)".
3. If you want to delete the displayed log entries to start a fresh session, click on **Clear list**.

5.4.21. Device state

The screenshot shows the Gantner GRT7.1300 - V3.0.0 web interface. The sidebar on the left contains navigation links: Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, Maintenance, Device, Update Firmware, Addon Bus, Log Viewer, Device State (selected), and Legal infos. The main content area is titled 'Device State' and includes a breadcrumb '/ Home / Device State'. It features three main sections: 'Hardware state' showing internal status for Opto and Relay with green and red checkmarks; 'Screenshot' showing a photo of a roller coaster; and 'Event Logger' showing a list of events with timestamps and descriptions.

Hardware state

Shown here is the state of the relay outputs and optocoupler inputs of the device, which can be used to receive status information and/or for control. A green tick indicates that the input/output is being used. The number of inputs and outputs available depends on the type of device (see technical data).

Screenshot

This image shows a screenshot of the currently displayed screen on the device display.

- To show the screen that is currently displayed on the device, click the refresh  button.
 - ↪ The refresh button turns green and the screen is automatically updated every second.
- When the live update shall be stopped, click again on the button.
 - ↪ The refresh button turns blue and the image shows the screen, that was displayed when the button was clicked. This image will not be updates until the refresh button is activated again.

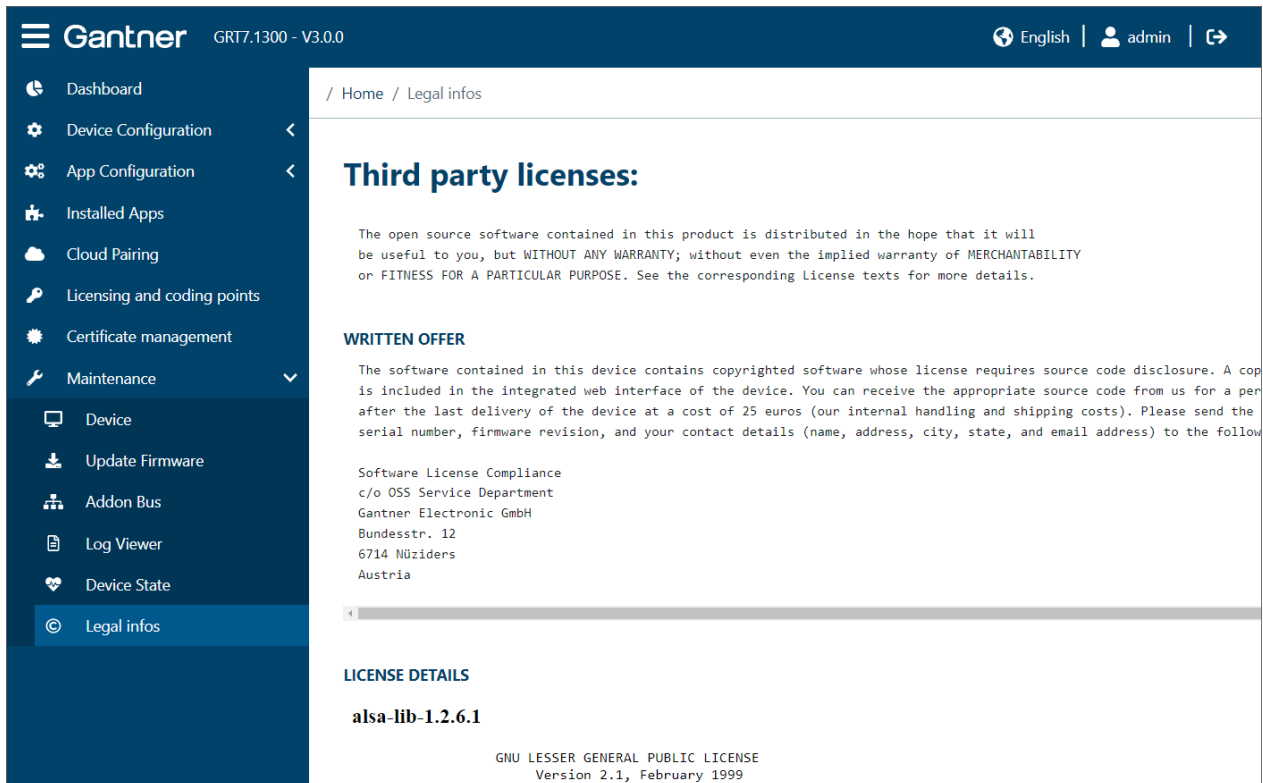
Event logger

When an event occurs at the device (e.g., data carrier read) or when the optocoupler input state or one of the relay states changes, a corresponding entry is displayed.

The live events occurring at the device are listed here. To clear the list, click on the trash can icon.

The filter icon displays all event types. By clicking on an event you can switch between active (green) and inactive (red). Only the active events are displayed in the list.

5.4.22. Legal information



The screenshot shows the Gantner web interface. The left sidebar contains a menu with options like Dashboard, Device Configuration, App Configuration, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The 'Legal infos' option is selected. The main content area displays the 'Third party licenses:' section. It includes a paragraph about open source software distribution, a 'WRITTEN OFFER' section with details about source code disclosure, and a 'LICENSE DETAILS' section for 'alsa-lib-1.2.6.1' under the GNU Lesser General Public License.

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

5.5. Configuration via G7 Connect

G7 Connect is Gantner's cloud service for managing and controlling all of an organization's Gantner G7 devices in a simple and convenient way. The system administrator and operators log in to G7 Connect via their personal accounts to configure the device settings.

It is also possible to create subordinate areas (e.g., different locations of a fitness chain) by organizing the locations into a hierarchical structure. The devices can then be assigned to the applicable area in the structure. An administrator can also create projects and assign each device to a project.

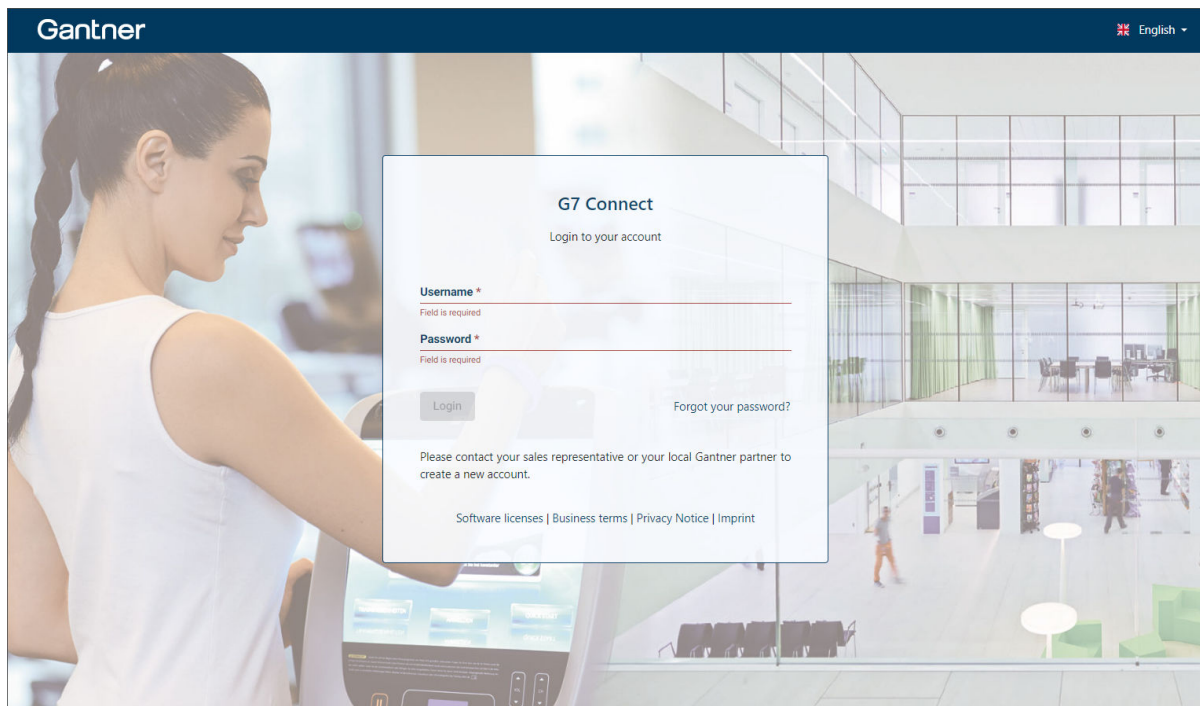


NOTE

A detailed description of how to create an account as well as instructions on using G7 Connect can be found in the G7 Connect manual.

1. Click on the following link to open G7 Connect: <https://gantner.cloud>

↪ The login window for G7 Connect opens in your default web browser.



2. Enter your **Username** and the corresponding **Password**. Next click **Login**.

↪ Your personal dashboard is displayed.

5.6. Integration in system management software

A local PC software or a cloud service can be used to control the GT7 Lite and manage the system. With this software, the data carriers and authorizations of the users are managed thus enabling or blocking the access for the doors in the system. When a data carrier is read by a device, the device transmits the information to the software that then decides whether to grant or deny the request, e.g., for access.



NOTE

See the documentation of the respective software for more information on software integration.

If so configured, the GT7 Lite can also operate in emergency mode if communication to the PC software is interrupted, e.g., during a network failure. In this case, the device decides autonomously on the basis of the saved authorization data as to which data carriers are authorized for access.

6. MAINTENANCE



WARNING

Touching live parts can lead to serious injury or death from electrical shock

- Disconnect the power supply before working on the device or installation/deinstallation.
- Observe the applicable safety and accident prevention regulations.
- Observe the specified technical data and technical drawings of the device.
- Protective devices must not be removed.

The GT7 Lite does not require periodic maintenance for operation. However, regular cleaning of the terminal is recommended to maintain hygiene standards.

6.1. Target group

This chapter contains information for the service technicians and cleaning personnel responsible for maintaining and cleaning the GT7 Lite. Previous knowledge of Gantner devices is not required.

6.2. Cleaning



NOTICE

- Do not use cleaning benzine, diluents or any other strong detergents.
- Do not clean the components of the device with a high-pressure or steam cleaner. Doing so will damage the device.
- Water or other liquids must not penetrate the device housing.

The periodical cleaning of the GT7 Lite is recommended and ensures that the device can perform its intended function properly.

Follow these steps to clean the GT7 Lite:

1. Wipe off any dirt and dust from the outside of the GT7 Lite using a soft, lint-free and dry cloth.
2. For extreme dirt, the terminal can be cleaned using a slightly moistened cloth.

7. TECHNICAL DATA

Nominal voltage	PoE: PoE conf. to IEEE 802.3af, performance class 0 USB (GT7.0510): DC 5 V
Permitted input voltage	PoE: DC 36 - 57 V USB (GT7.0510): DC 4.4 - 5.25 V
Power consumption	PoE: 60 mA USB (GT7.0510): 500 mA
Nominal power consumption	4 W
Reader type	GT7.05x0: ISO 14443 (MIFARE®) Classic (1k and 4k), DESFire, Ultralight ISO 15693 Gantner Smartpass GT7.1300: LEGIC advant ISO 14443 (MIFARE®) Classic (1k and 4k), DESFire, Ultralight ISO 15693 Gantner Smartpass
Reader frequency	RFID: 13.56 MHz Wireless interface: 2.4 GHz
Max. transmission power	RFID: 500 mW Wireless interface: 3.7 dBm (2.344 mW)
Reading range	2 - 8 cm (depending on the data carrier)
Data storage	Flash memory for configuration and booking data, screensaver and advertisement pictures (GT7.1300)
User guidance	GT7.05x0: Multi-colored LED status display, multi-color LED ring, acoustic beeper GT7.1300: 3.5" color display with capacitive touchscreen, resolution 320 x 240 px, multi-color LED ring, acoustic beeper
Host interface	Ethernet: 10/100 Mbps, IPv4 and IPv6
Connection	Screw terminals, 0.5 - 1.5 mm
Software integration	JSON interface Generation 6 compatibility adapter (limited functions)
Signal inputs	1 x optocoupler input, potential-free, function configurable Input voltage: 0 to 30 V DC, $U_{Low} < 2 \text{ V DC}$, $U_{High} > 6 \text{ V DC}$

Signal outputs	<p>1 x relay</p> <p>Type: NO contact, function/timing configurable</p> <p>Switching voltage DC: max. 30 V (SELV)</p> <p>Switching voltage AC: max. 15 V (SELV)</p> <p>Continuous current: max. 1.8 A</p> <p>Switching capacity: max. 54 W, 27 VA</p>
Housing material	<p>Front/rear part: Plastic PC anthracite gray</p> <p>Display: Hardened glass</p>
Weight	300 g (10.5 oz)
Permitted ambient temperature	-10 to +50 °C (+14 to +122°F)
Permitted storage temperature:	-25 to +70 °C (-13 to +158 °F)
Protection type	IP40
Protection class	III (Safety Extra-Low Voltage)
Environment class (VdS 2110)	II (indoor conditions)
Certification	CE



This page is intentionally left blank.