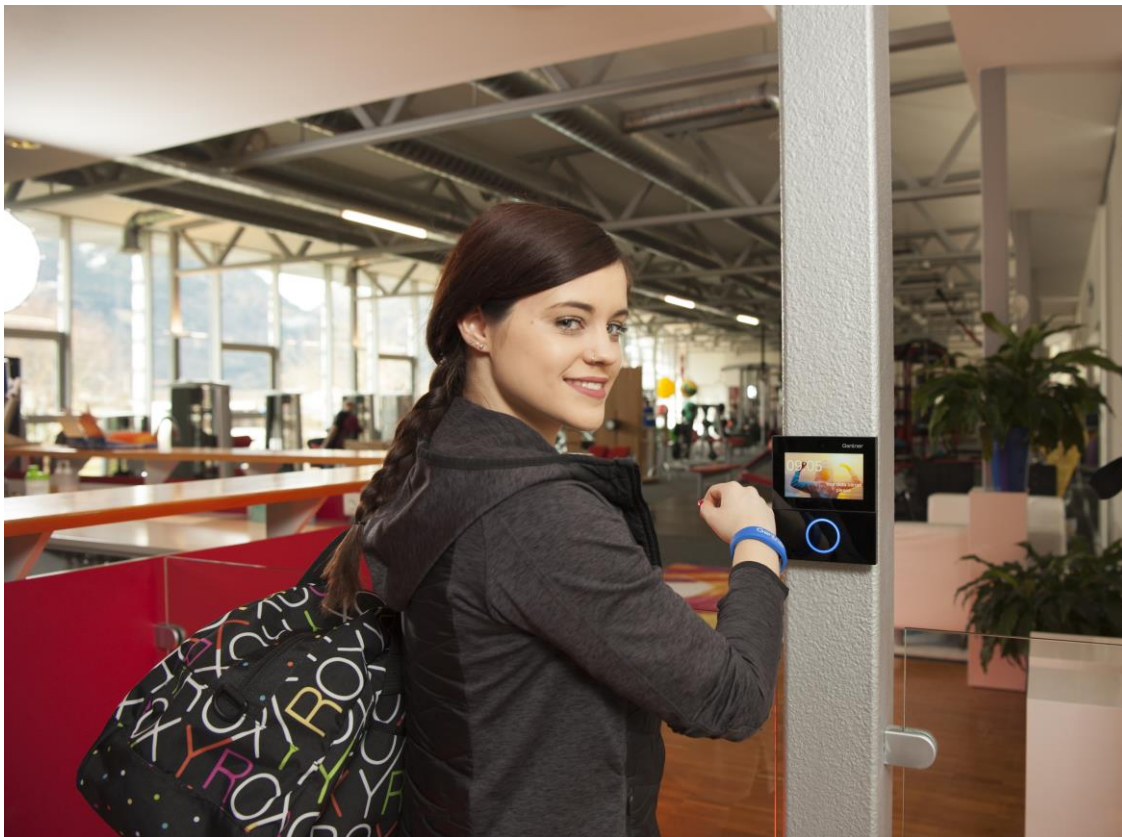


G7 Access and G7 Advanced Access App

App for GT7 Terminals and GC7 Controllers for Access Control of Recreational Facilities



Configuration & Operation

App Versions: G7 Access V 2.7.7, G7 Advanced Access V 1.5.1

Document Version 1.5

© Copyright 2023 GANTNER Electronic GmbH

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

Liability

Any claims against the manufacturer based on the hardware or software products described in this manual shall depend exclusively on the conditions of the guarantee. Any further-reaching claims are excluded, and in particular the manufacturer accepts no liability for the completeness or accuracy of the contents of this manual. The right is reserved to make alterations, and alterations may be made at any time without prior notice being given.

Trademarks

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

Contact

The contact information for questions regarding this product or for general enquiries is listed below:

Contact address of manufacturer

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

CONTENTS

1	INTRODUCTION	5
1.1	About this manual	5
1.2	Chapter overview	5
1.3	Target group	5
1.4	Formatting	6
1.4.1	Safety-critical information	6
1.4.2	Non safety-critical information	6
1.4.3	Instructions and results	6
1.5	Contact & inquiries	6
2	GENERAL INFORMATION	7
2.1	Intended use	7
2.2	Functional description	7
2.3	Information on the GT7 terminals and GC7 controllers	8
2.4	Terminology	8
3	TERMINAL AND APP INSTALLATION	9
3.1	App installation	10
3.2	Themes (design templates)	12
4	APP CONFIGURATION	13
4.1	Configuration options	13
4.2	General settings	17
4.3	Access	18
4.4	Reader settings	21
4.5	Check-in	22
4.6	Display texts	24
4.6.1	Editing languages and texts	25
4.7	Emergency mode	26
4.8	G6 compatibility mode	28
4.9	PIN	30
4.10	QR code	31
4.11	Design	33
5	OPERATION	35
5.1	Target group	35
5.2	Operation of the G7 Access Apps	35
5.2.1	Operation with display	35
5.2.2	Operation with a GC7 Controller without display	36
5.2.3	Checking the EU digital COVID certificate	37

1 INTRODUCTION

1.1 About this manual

This manual contains information on the configuration and operation of the G7 Access and G7 Advanced Access App operating on a GT7 terminal or GC7 controller.

i In this manual, the term "G7 Access Apps" is generally used when the respective information refers to both apps.

i For information on the installation and electrical connection of the GT7 terminal and GC7 controllers, refer to the respective manuals for these devices. Separate documentation is also available for related applications such as the other G7 apps available for the GT7 terminal and G7 Connect.

1.2 Chapter overview

In chapter "2. GENERAL INFORMATION" you will find information on the intended use and function of the GT7 terminal and GC7 controller with G7 Access and G7 Advanced Access App as well as a description of the terms frequently used in this manual.

Provided in chapter "3. TERMINAL AND APP INSTALLATION" are the details for where additional information on the installation and commissioning of the GT7 terminal can be found

Chapter "4. APP CONFIGURATION" describes all configuration settings specific to the G7 Access and G7 Advanced Access App. This chapter also describes in detail how to configure the G7 Access and G7 Advanced Access App according to the requirements of the application.

In chapter "5. OPERATION" information on the operation of the G7 Access and G7 Advanced Access App for the end user is available.

1.3 Target group

Information for the following target groups is available in this manual:

- Installation personnel (installation, commissioning, configuration)
- Users of the G7 Access and G7 Advanced Access apps (operating instructions)
- Software partners

If the target group is not specifically stated, the information is intended for all target groups.

⚠ CAUTION! Injury and damage to property/equipment. The instructions in this manual that are intended for a specific target group may only be performed by this target group. The completion of activities by unqualified personnel can lead to injuries and/or damage to property/equipment.

1.4 Formatting

1.4.1 Safety-critical information

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

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

1.4.2 Non safety-critical information

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

 *The text accompanying this symbol contains interesting information relevant to the current chapter. This information is intended to help you understand the context in the section or provide interesting tips for the described device or software operation.*

1.4.3 Instructions and results

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

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

1.5 Contact & inquiries

If you have any questions concerning the G7 devices and the G7 Access or G7 Advanced Access app, please contact your local sales partner or one of the GANTNER branch offices directly. The contact details are available via the following link: www.gantner.com/locations

2 GENERAL INFORMATION

2.1 Intended use

The GT7 terminal and GC7 controller with the G7 Access or G7 Advanced Access app are used to control access to services and areas such as spas, locker rooms, pool areas, etc., in recreational facilities such as fitness clubs, swimming pools, or thermal baths.

2.2 Functional description

To control unlocking devices such as turnstiles or electronic door locks, the 2 relay outputs of the GT7 terminal or the 6 relay outputs of the GC7.3000 are switched depending on the configuration and authorization. Status messages can be received by up to 3 (GT7) or 4 (GC7) optocoupler inputs.

The identification of users is carried out using contactless data carriers at the RFID reader of the GT7 or at one of the RFID readers that can be connected to the GC7.3000 by default. A wide range of reader types are available for the connectable readers. Barcode readers or Wiegand readers can also be connected.

For configuration and the authorization control of users, the GT7 terminal and the GC7 controller are connected to a LAN network via a network interface. The configuration can thus be completed via a web browser (web interface) or also in a convenient way in the GANTNER Cloud (G7 Connect). Via the configuration, the function of the GT7 or GC7 can be adapted to the respective requirements.

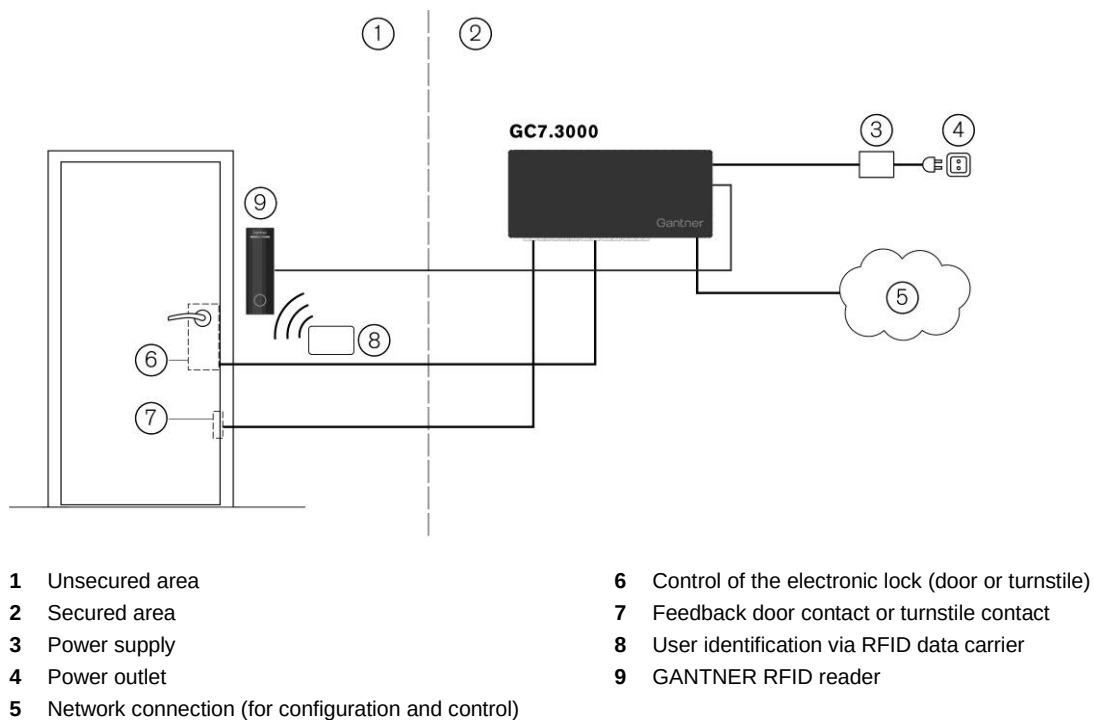


Figure 2.1 – System overview for using the G7 Access App (example with GC7.3000)

2.3 Information on the GT7 terminals and GC7 controllers

For information on the installation and commissioning as well as general settings for the GT7 and GC7 devices, please refer to the manual for the respective device. The manual you are currently reading only contains information about the configuration settings and operation of the G7 Access and G7 Advanced Access Apps.

2.4 Terminology

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

App

For GANTNER devices, this term refers to a software application that can be installed on the app-capable devices of the GC7 and GT7 series. The activated app determines the operation of the device.

G7 Access App, G7 Advanced Access App

The names of the software (apps) described in this manual. These apps can be used to control and monitor access. The G7 Advanced Access App includes the standard functions of the G7 Access App plus additional functions such as authorization list, EU Digital Covid certificate check, support of external GR7 readers connected to a GT7 or GC7, and encoding of MIFARE Classic data carriers.

User / Visitor

In this manual, these terms refer to the end user who interacts with the GT7 terminal or GC7 controller to gain access via the G7 (Advanced) Access App.

Computer / PC

These terms refer to all desktop and laptop computers used to configure the GT7 or GC7 devices and the G7 (Advanced) Access App.

GT7 terminal / GC7 controller

The devices running the G7 Access and G7 Advanced Access app. Other apps can also be installed and activated (provided the corresponding license points are available). These terms refer to the hardware, i.e., the device, regardless of which app is currently active.

Reader

RFID data carriers are used to identify users of the GT7 or GC7. The GT7 has a built-in RFID reader and GANTNER also offers external RFID readers to read the data carriers. Barcode readers or fingerprint readers are also available, which are also commonly referred to as "readers".

Data carrier

An identification medium (e.g., in the form of a key tag or chip card) with electronic memory and an ID number that the system users employ for identification in the system. The data carriers are available to suit different identification systems (LEGIC®, MIFARE™, ISO 15693).

RFID (Radio-Frequency Identification = identification via electromagnetic field)

In this manual, this term refers to the identification of a person via radio frequency at close range. An RFID data carrier, e.g., in the form of a key tag or chip card, serves as the identification medium.

FID (Company ID) and Site Key

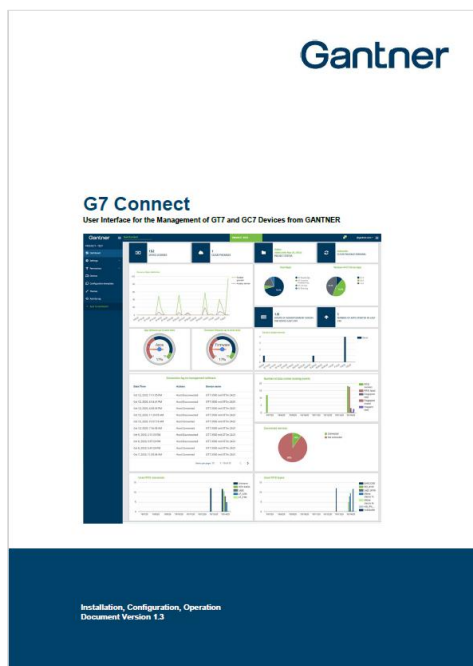
LEGIC systems use the FID number and in MIFARE systems the Site Key is used, which is a combination of FID and the read and write keys. The FIDs and the Site Keys are unique for each system. These numbers are encoded in all data carriers and devices thereby ensuring that data carriers can only be used in the designated facility.

3 TERMINAL AND APP INSTALLATION



The installation, electrical connection, and commissioning of the GT7 terminals and GC7 controllers are described in a separate device manual. For installation and commissioning, please read and carefully follow the information provided in the respective manual.

Figure 3.1 – GT7 and GC7 user manuals



G7 Connect (GANTNER Cloud) is a web browser based application that can be used for the convenient configuration and management of the GT7 terminals and GC7 controllers. This application is especially recommended for larger systems with multiple G7 devices. A separate manual with detailed information on all software functions is available for G7 Connect.

Figure 3.2 – G7 Connect manual

3.1 App installation

The GT7 terminal and GC7 controller are multi-purpose devices with the functionality determined by the app operating on the device. By default, the G7 Access app is preinstalled on the devices and the G7 Info and G7 Time apps are also preinstalled on a GT7 terminal. All other G7 apps are not available on the devices and must first be installed.

i The installation of apps and the transfer of device license points to the GT7 and GC7 are described in the G7 Connect manual.

To enable the G7 Advanced Access app for use, the 30 license points required for operation can be ordered from GANTNER via the article “G7 Device License Points Advanced Access” (Part No. 1107069). Each installed app can be viewed on the “Installed Apps” page of the device web interface.

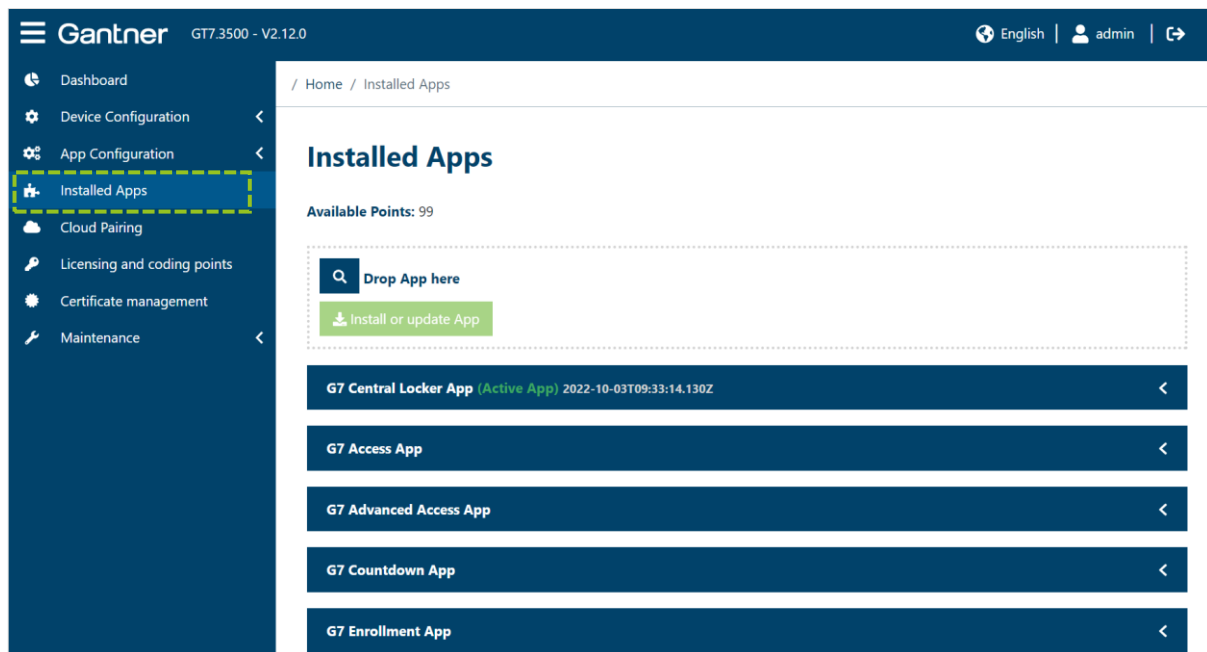


Figure 3.3 – GT7 web interface – “Installed Apps” page

- To view the details of an app, click on the arrow to the right of the app name.



Figure 3.4 – List of installed apps

- Information on the app, e.g., the version and theme, are displayed.

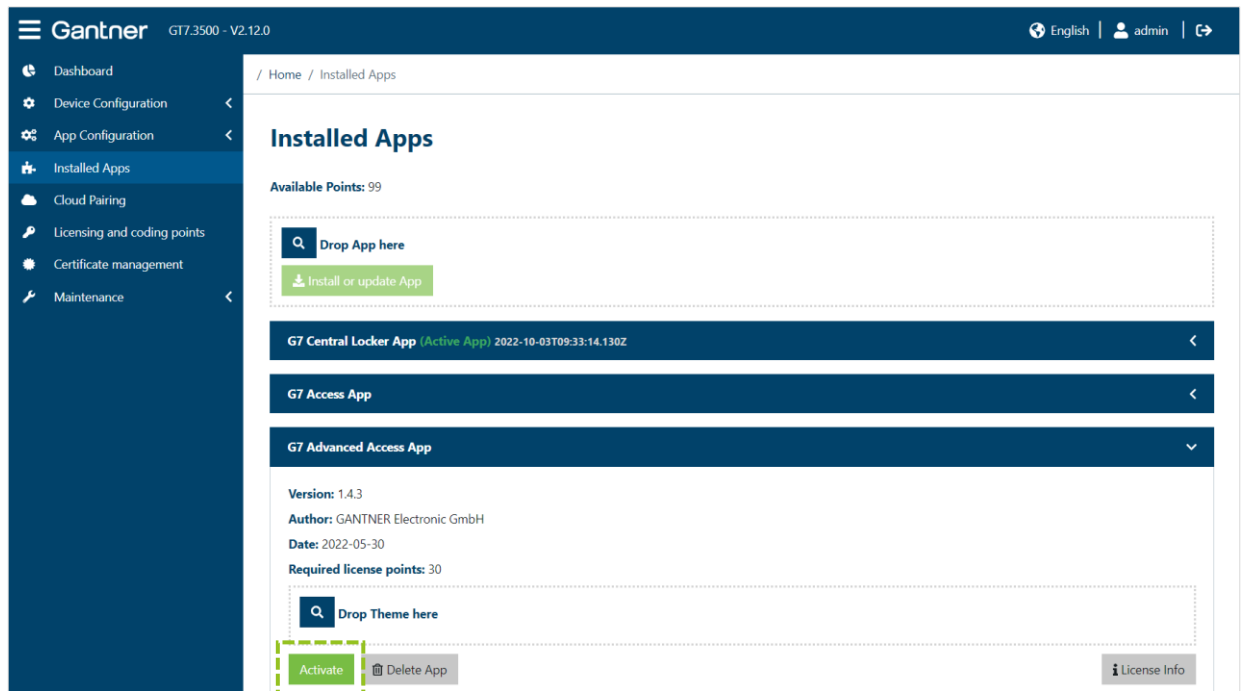


Figure 3.5 – Web interface with app configuration

- To enable the G7 Access App or G7 Advanced Access App for use on the device, open the details of the G7 Info App as described and click on "Activate".
- A suitable design template can also be selected here to customize the design of the display (background, colors, fonts, etc.). Design templates are called "themes" in the configuration. For more information, see "3.2 Themes (design templates)".

3.2 Themes (design templates)

Themes are design templates and provide a straightforward way to graphically customize the devices. Themes provided for the G7 Access and G7 Advanced Access app can easily be transferred to the device via G7 Connect. Without significant effort you can create your own themes using the Themes Editor in G7 Connect.

Some example screenshots of the default theme available for the G7 Access Apps app that can be used or further customized.



Figure 3.6 – Default theme of the G7 Access App

The color of the LED circle on the GT7 terminal as well as the display elements such as the background image, the size, position and type of the symbols, and the default design can be customized in the configuration. See chapter "4.11. Design" for more information.

i Since the GC7 controller does not have a display and LED indicator like the GT7 terminal, the design settings are not relevant when operating the G7 Access Apps on the GC7 controller.

4 APP CONFIGURATION

4.1 Configuration options

There are two options for configuring the settings of the GT7 terminal or GC7 controller and the G7 Access apps:

- G7 Connect:

G7 Connect is recommended for the convenient configuration of all GT7 and GC7 devices and G7 apps and especially for large systems with multiple devices. The GANTNER Cloud Platform is accessed via web browser at <https://gantner.cloud>. All projects and installations of the organization and their associated G7 devices are assigned here and, depending on the activation, the user can clearly manage and edit their G7 devices.

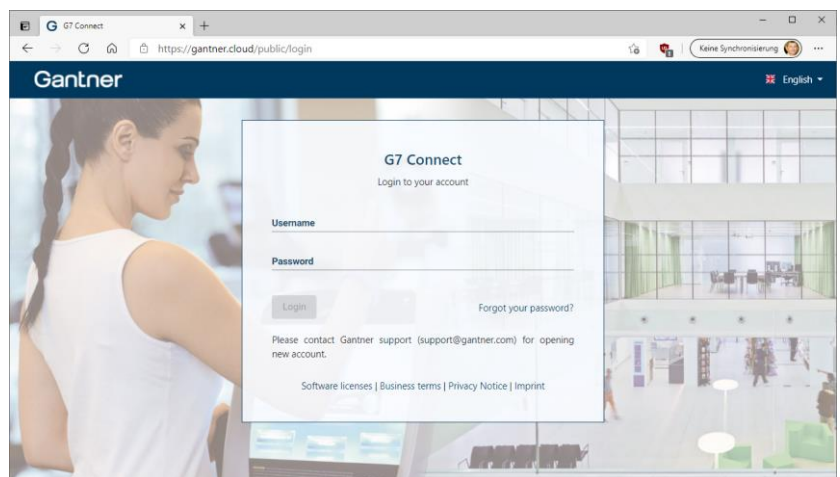


Figure 4.1 - G7 Connect login screen

Add devices:

To add a device to the G7 Connect environment so that it can be configured, the pairing process (also called "pairing") must be completed. For this purpose, the device pairing function is accessed in G7 Connect and the pairing key of the device is inserted there. This key can be found in the web interface (see next point) of the device on the "Cloud Pairing" page.

- Web interface:

If the PC and the GT7 terminal or GC7 controller are on the same network, the configuration can also be directly accessed via web browser by entering the IP address or network name of the device. After entering the IP address, the login screen opens in the browser.

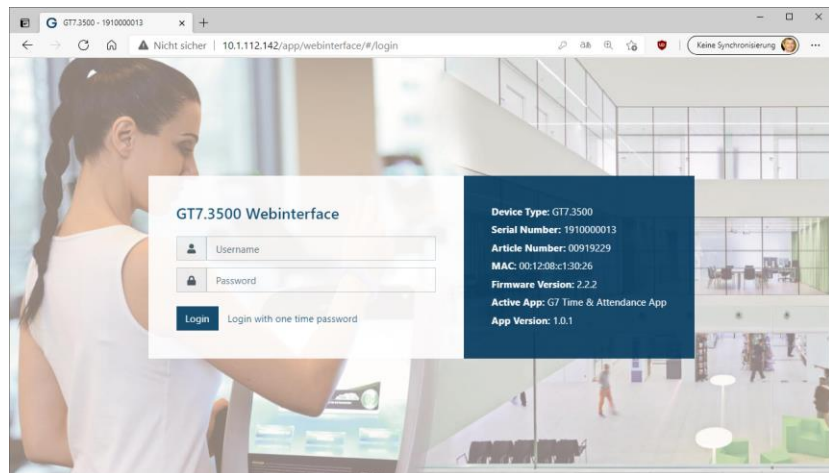


Figure 4.2 - Web interface login screen

IP address or network name:

A GC7 controller uses DHCP by default to automatically obtain an IP address on the network. Ask your network administrator for the IP address.

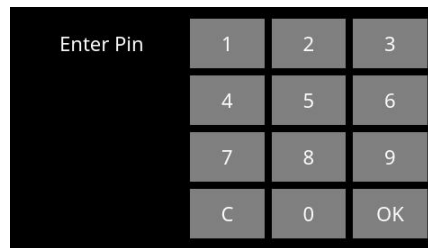
i Alternatively, you can use GANTNER's GAT Device Finder software to scan the network for devices. A GC7.3000 is displayed there with the device type "GC7.3000" and the IP address. GAT Device Finder can be downloaded from the partner page of the GANTNER website. In addition, GAT Device Finder is also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

The IP address of a GT7 terminal is shown on the display when the device is powered on. It can also be accessed via the configuration menu of the GT7 terminal as follows.

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



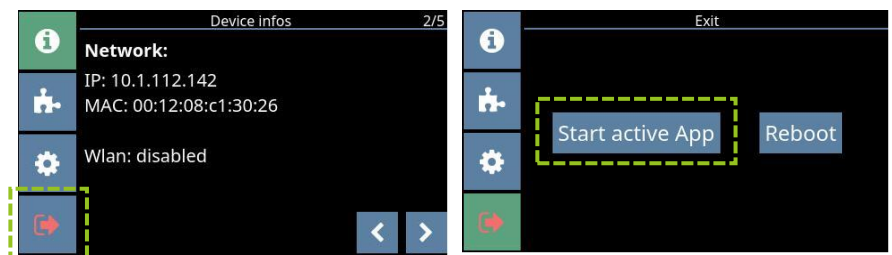
- Enter the PIN code to access the configuration menu. The default code is 0815, which should be changed in the configuration for security reasons after commissioning the GT7 terminal (see the GT7 terminal manual).



- The IP address can be found in the “Info” menu on page 2.



- Exit the configuration menu by clicking on the “Exit” button and selecting “Start active App”.



All configuration settings and information for the GT7 terminal or GC7 controller are divided into groups and shown on different pages, each page being displayed via the menu in the sidebar on the left-hand side.

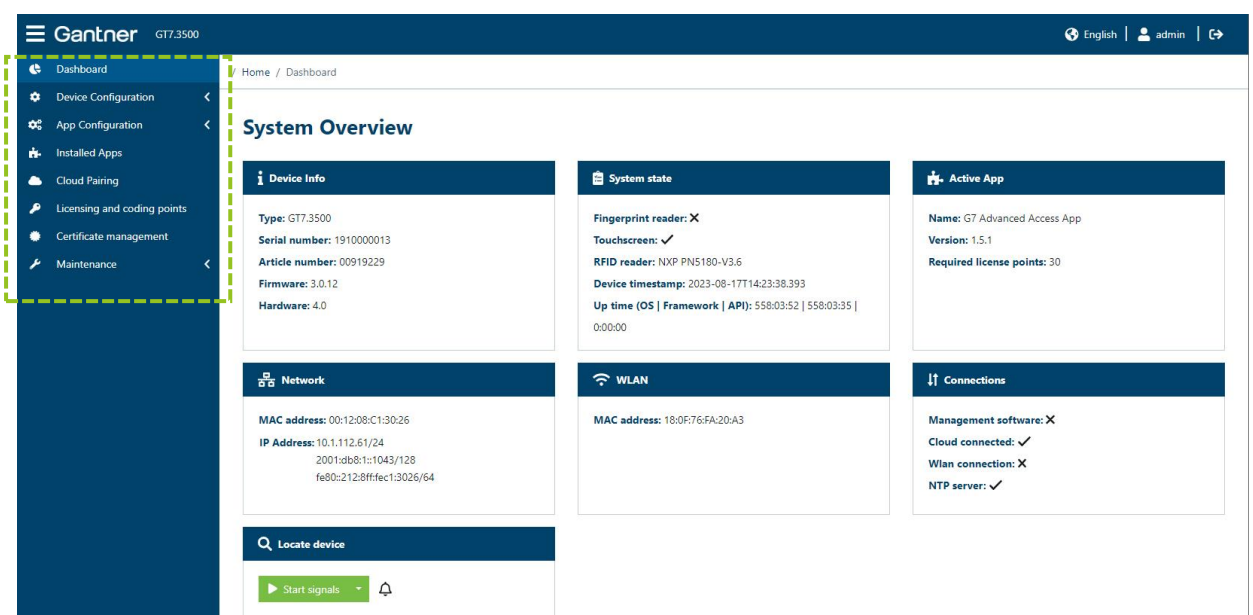


Figure 4.3 - Configuration and information pages in the GT7 terminal web interface

The settings specific to the G7 Access app can be found under “App Configuration” in the menu.

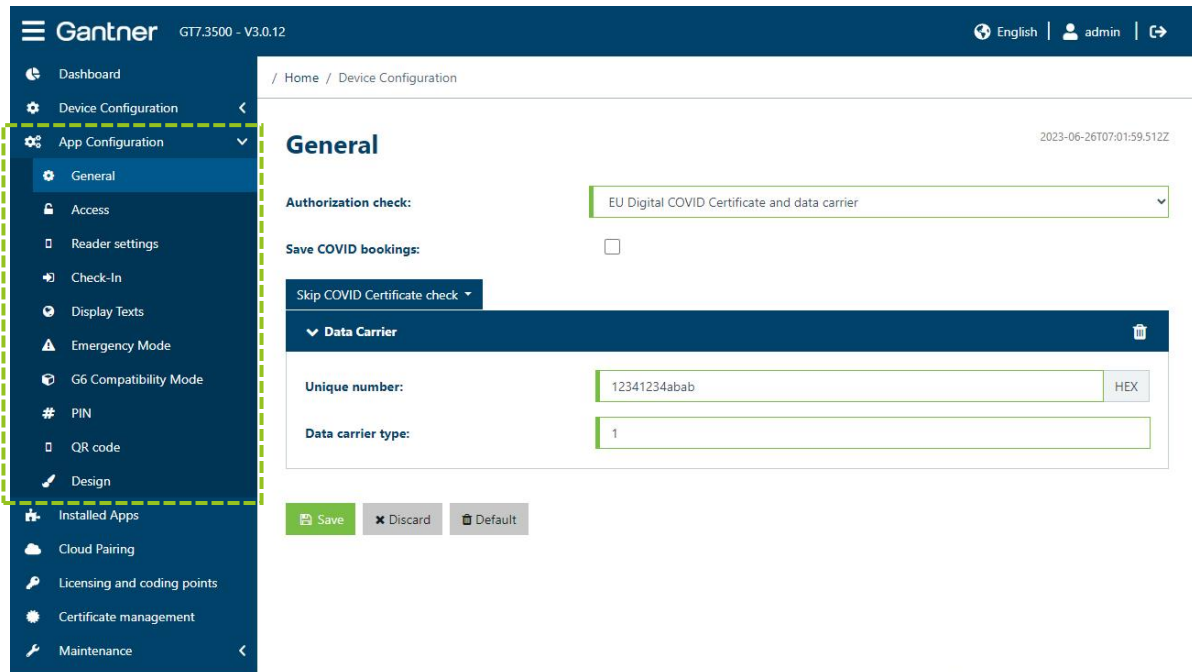


Figure 4.4 – App-specific configuration settings

4.2 General settings

NOTE! These settings are only applicable for the G7 Advanced Access App.

For the G7 Advanced Access app, it is possible to select the EU digital COVID certificate for the authorization check in addition to the RFID data carriers.

► Open the "App Configuration" -> "General" configuration page.

Figure 4.5 – G7 Advanced Access App – General settings

► In the "Authorization check" field, you can select whether identification is allowed at the GT7 or GC7 device using a data carrier (default), using an EU digital COVID certificate, or both.

- If "Data carrier" is selected, no further settings are possible or necessary here.
- If you select "EU Digital COVID Certificate" or "EU Digital COVID Certificate and data carrier", the following settings can be configured.

NOTE! Please also observe the applicable local data protection regulations!

- "Save COVID bookings": If this option is enabled, the GT7 or GC7 will save the read COVID certificates.
- "Delete after": Enter the number of days the read COVID certificates are kept before being deleted.
- "Add day of birth": If this option is enabled, the date of birth is also saved with the read certificate.
- "Add vaccination/recovered/test type and date": If this option is enabled, the date of the last injection, or the recovery or test status is saved.
- "Skip COVID certificate check" -> "Data carrier": Here you can click on "Data carrier" to add one or more data carriers that will be excluded from the COVID certificate check at the device. For each data carrier, the unique number (in hexadecimal format) and the data carrier type must be entered.

4.3 Access

Here you can define the time settings for the access functions, e.g., the unlocking time, and the functions of the relay outputs and optocoupler inputs of the GC7.3000.

The screenshot displays the 'Access' configuration page in the Gantner G7.3000 - V2.11.0 web interface. The left sidebar contains a menu with options like Dashboard, Device Configuration, App Configuration, General, Access (highlighted), Reader settings, Check-in, Display Texts, Emergency Mode, G6 Compatibility Mode, PIN, Design, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main content area is titled 'Access' and shows various settings for access control. The 'Unlocking time' is set to 5000 ms. The 'Release device at' dropdown is set to 'Start feedback / open door'. The 'Deny time' is set to 5000 ms. The 'Double door system' checkbox is checked, and the 'Double door system timeout' is set to 60 s. Below these are sections for 'Relay 1' through 'Relay 6' and 'Optocoupler 1' through 'Optocoupler 4'. Each section has a 'Use for' dropdown (set to 'All readers'), a 'Function' dropdown (set to 'Unlock' for relays and 'Feedback' for optocouplers), and a 'Mode' dropdown (set to 'Normally open contact'). At the bottom, there is an 'IO extensions' dropdown and three buttons: 'Save', 'Discard', and 'Default'.

Figure 4.6 – G7 Access Apps – Access

► Define the following settings for access control in the upper area.

- Unlocking time:

This setting determines the time (in seconds) that the unlocking process is active for after a user with valid access authorization identifies themselves at the GT7 or GC7. If a signal is detected by the feedback contact during the unlocking time, the unlocking process is terminated, and the device returns to its default state.

- Release device at: Here you configure when the unlocking process is considered to be completed by the GT7 or GC7. This is possible either as soon as the door is opened or the turnstile is turned (start of the feedback signal) or only when the feedback signal is deactivated again or the door is closed.
 - Deny time: This setting determines the time (in seconds) that the denial process is active for after a user with invalid access authorization identifies themselves at the GT7 or GC7.
 - Double door system (timeout): With this locking function, the status of two doors is considered. After passing through the first door, the GT7 or GC7 will continue to block access until the feedback from the second door is deactivated (see optocoupler "Lock feedback"). If the feedback from the second door is not deactivated within the timeout time entered here, the GT7 or GC7 aborts the access process and returns to its default state.
- Under the general settings, you can configure the relay outputs and optocoupler inputs.
- Relay x: Here you can define the function for each relay of the device (i.e., "Relay 1" to "Relay 6" for the GC7.3000 and "Relay 1" or "Relay 2" for the GT7).
 - Use for: This function is only available for the GC7 controllers. Here you can select the readers for which the respective relay configuration is to be used. The options are "All readers", for the internal reader of the GC7 only, for a specific barcode reader, or for an external reader.
 - Function: Select how the relay should function.
 - Transparent: The relay has no function.
 - Unlock: The relay is always activated when a valid authorization has occurred at the GT7 or GC7, e.g., when a user reads their data carrier at the reader and the data carrier is authorized for access.
 - Denied: The relay is always activated when an invalid authorization has occurred at the GT7 or GC7, e.g., when a user reads their data carrier at the reader and the data carrier is currently not authorized for access.
 - External locking: The relay will be activated during a process at the GT7 and GC7 (e.g., an identification via data carrier and granting of access). This signal can be used, for example, to lock a terminal or reader on the opposite side during the process.
 - Mode: Here you can select whether the normally open (NO) or normally closed (NC) contact of the relay is used. This selection must correspond to the wiring connections of the relays. The NO contact is open in the idle state and is closed when the relay is "activated" (depending on the set function). The NC contact is closed at rest and is opened when the relay is activated.
 - Relay active time: The length of time that the relay is triggered for during an activation.

- Optocoupler x:

Here you can define the function for each digital input of the device ("Optocoupler 1" to "Optocoupler 4" for the GC7 controller and "Optocoupler 1" to "Optocoupler 3" for the GT7).

- Function:

Select here how the output should function.

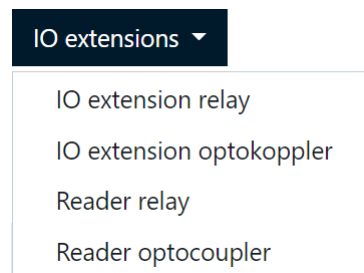
- Transparent: The input has no function.
- Feedback: The input serves as a status message for the access process, i.e., the input is active when the door or the turnstile has been opened or turned after valid identification.
- Lock: If this input is active, access is not possible. This can be used to temporarily block access, e.g., using a push button.
- Unlock: If this input is active, the relays set to the "Unlock" function are activated. This allows, e.g., an unlocking via a push button.
- Unlock permanent: If this input is active, access is permanently enabled, i.e., all relays set to the "Unlock" function are permanently activated. This means that access can be enabled generally via a connected switch as long as the switch is closed.

- Mode:

Here you can select whether the selected function of the optocoupler input is active when a voltage is applied ("make contact") or when the voltage is not applied ("break contact").

- IO extensions:

When you click on this button, the following menu is displayed:



Here you can add the relays or optocouplers of a connected IO expander or reader. Each time you select a menu option, the corresponding entry is inserted below. The settings for the relays and optocouplers are identical to the GT7 or GC7 relays and optocouplers (see above).

4.4 Reader settings

NOTE! These settings are only applicable for the G7 Advanced Access App.

On the "App Configuration" -> "Reader Settings" page, support for multiple doors can be activated thereby allowing two or more readers to operate together at the GT7 or GC7 device. Door in this case means, for example, an access door or also a turnstile. The multiple door function can be used for access, e.g., to use one reader for entry and a second reader for exit.

A maximum of 8 readers can be connected, which can also operate in parallel depending on the configuration settings.

i This function is only possible for GC7 controllers operating with an activated G7 Advanced Access App. The G7 Access App does not offer this possibility.

Figure 4.7 – G7 Advanced Access App – Reader settings

- ▶ To activate support for multiple doors, enable the option on this page.
 - The "Reader Groups" menu is displayed.
- ▶ Select the desired reader from the "Reader Groups" menu.
 - A reader group is inserted for each reader where the following settings can be configured:
 - Doors / turnstile: The number of the door can be entered here. By adding several reader groups, it is possible to configure several doors that are differentiated by the number.
 - Direction: Define here whether the reader in question is used for entry or exit. "Undefined" means that the direction is not defined or distinguished.

NOTE! If a reader within a group reads a data carrier, the remaining readers of this group are blocked. For example, if a data carrier is read at the entry reader, the exit reader is blocked at this time.

4.5 Check-in

The configuration page for the locker check-in function can be accessed via the “App Configuration” -> “Check-In” menu. The locker check-in function is disabled by default.

The screenshot shows the Gantner App Configuration interface. The left sidebar contains a menu with options: Dashboard, Device Configuration, App Configuration, General, Access, Reader settings, Check-In (highlighted with a yellow dashed box), Display Texts, Emergency Mode, G6 Compatibility Mode, PIN, Design, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main area displays the 'Check-In' configuration page. The page title is 'Check-In' and the breadcrumb is '/ Home / Device Configuration'. The page is dated 2022-09-09T12:13:45.601Z. The 'Locker Check-In' section contains the following settings:

- Number lock group: 1
- Clear Locker number: ☒
- "Check use time" flag: Unchanged
- Valid Until: Offset to Midnight
- Offset in hours and minutes: 24:00
- Use for: All readers

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

Figure 4.8 – G7 Access Apps – Locker Check-In

The locker check-in function is used to automatically authorize the user data carriers for lockers (e.g., changing rooms) that are equipped with battery-powered, electronic locker locks from GANTNER. With the check-in, the authorization data for the lockers within the facility is also written to the user's data carrier when it is read by the GT7 terminal or GC7 controller (e.g., during an access attempt). The user can then use the lockers directly without an additional check-in at the reception desk. Which lockers can be used is defined using locker groups. In addition, the time-based authorization can also be defined.

- ▶ To define a locker check-in, select the “Locker Check-In” option from the “Segments” menu.
 - A new “Locker Check-In” area is displayed with the settings as shown in the figure.
- ▶ Configure the following settings.
 - Number lock group: Enter the number of the locker group as configured for the data carrier type in the device configuration (Device Configuration -> Data Carrier -> Locker segment number). See the GT7 manual for more information on the device configuration settings.
 - Clear locker number: When a data carrier locks a locker, the locker number is written onto the data carrier. If this option is enabled, the locker number on the data carrier is deleted during check-in, which allows another locker to be used.

NOTE! The previously used locker must be unlocked before check-in is completed, otherwise it can no longer be opened.

- "Check use time" flag:

During the locker check-in, the "Check Use Time" flag on the data carrier can also be set, cleared, or left unchanged.

When the flag is enabled on the data carrier, the locker can only be opened again for a certain time after it has been locked. This time can be configured in the lock and is set to 1 hour by default.
- Valid until:

Here you can configure how the validity period for the data carrier is to be defined during a locker check-in.

 - Unchanged: The validity date on the data carrier is not changed.
 - Offset to midnight: The validity period is calculated by the offset time (set in the next field) from midnight.
 - Offset to check-in time: The validity period is calculated by the offset time (as defined in the next option) from when the locker check-in is completed.
 - Unlimited valid: The data carrier is valid without any time limit.
- Offset in hours and minutes:

If "Offset to midnight" is selected for "Valid until", this time determines the time until which a locker can be locked. If "Offset to check-in time" is selected, this time determines the validity period, which is always calculated from the respective locker check-in.
- Use for:

This option is only available for the G7 Advanced Access App and the GC7 controller. When multiple readers are connected to the controller, you can select here for which readers the locker check-in function is enabled.

4.6 Display texts

The G7 Access Apps can be operated in several languages. The languages German and English are available by default for ease of use. Other user-specific languages can be easily expanded.

If multiple languages are activated, the user can switch between the languages on the display via the language icon.

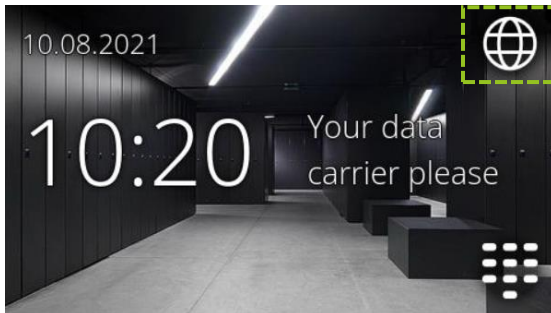


Figure 4.9 – Language selection icon on the GT7



The GC7 controller does not have a display for showing information. However, an external display can be connected. In this case, the display on the screen can also be in several languages.

- To define the display languages, select “App Configuration” -> “Display Texts” from the menu.

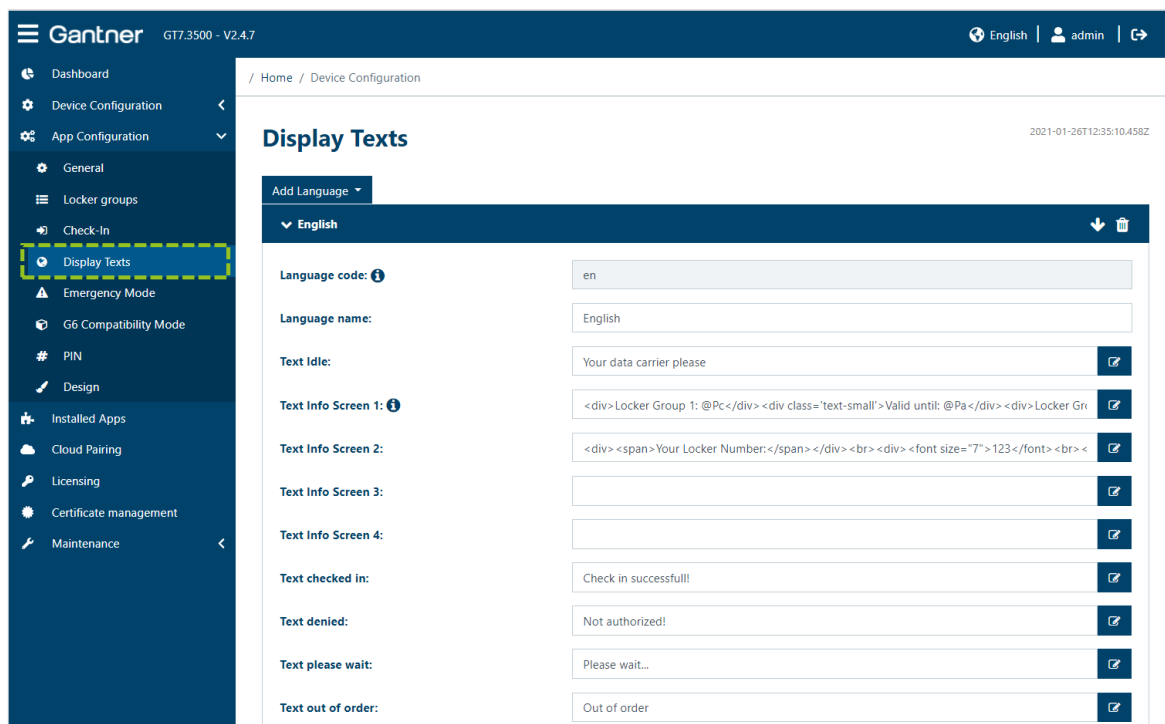


Figure 4.10 – G7 Access Apps - Configuring languages for the display texts

4.6.1 Editing languages and texts

The predefined texts, which are automatically displayed by the terminal's screen depending on the function, are listed for each language. The languages are divided into blocks that can be opened and closed by clicking on the language name.

- ▶ The display texts are predefined in German and English by default. If one of these languages is deleted, you can insert it again by clicking on "Add language".
- ▶ To add a new language, click on "Add language" and select "Custom".



- A new text block is inserted underneath the last language.
- ▶ Enter the language code of the new language according to ISO 693-1, e.g., it, fr, etc.
- ▶ Enter a "language name". This name is shown on the display when selecting the language.
- ▶ The order of the language blocks can be changed using the arrows in the language headers.



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

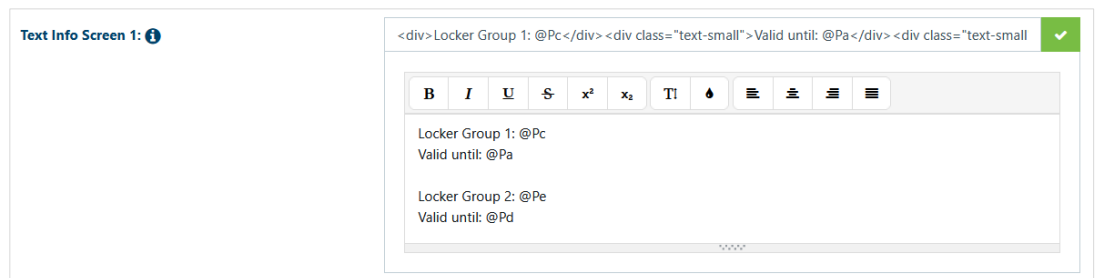


Figure 4.11 – Editing display texts

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

NOTE! Formatting must always be done within the editor; text cannot be edited directly.
- ▶ Via the delete icon  , a language including all text modules can be deleted.

4.7 Emergency mode

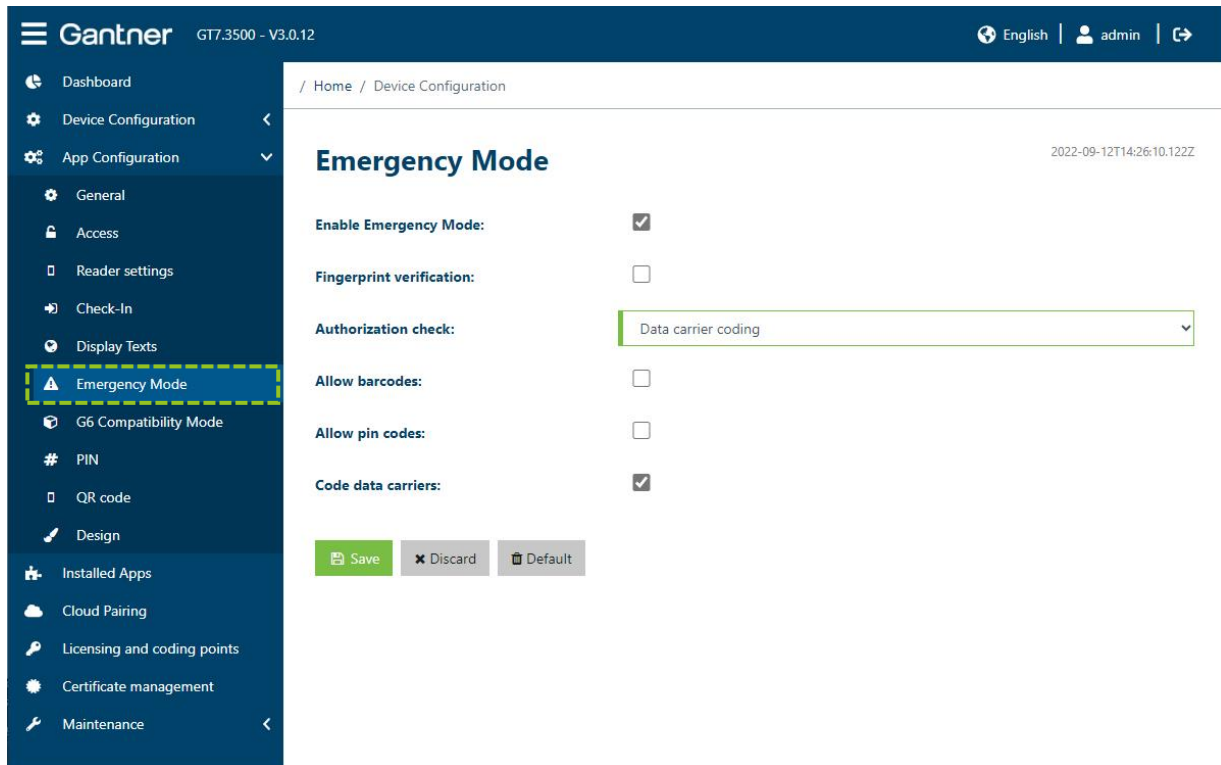


Figure 4.12 – G7 Access Apps – Emergency mode

If communication between the GT7 terminal or GC7 controller and the server is interrupted, operation of the GT7 or GC7 is not possible if emergency mode is disabled. In this case, the GT7 will display the default text "Out of Order" or for the GC7, the LED on a connected GR7 reader will turn red.

By enabling emergency mode, operation of the G7 Access Apps with the current configuration is possible even if communication is interrupted. In this case, the bookings recorded in emergency mode are stored in the device and can be retrieved by the management software when communication is restored. The GT7 terminal and GC7 controller can store up to 10,000 bookings and delete the oldest bookings when the limit is reached.

- Enable Emergency Mode: Select this option to activate emergency mode for the GT7 or GC7. Emergency mode is deactivated by default.
- Fingerprint verification: If a fingerprint reader (e.g., GT7b.2000) is connected to the GT7 terminal, this option can be enabled to request additional verification by fingerprint during emergency mode.
- Authorization check: Here you can select the type of authorization check that the GT7 or GC7 performs during emergency mode.
 - Data carrier coding: When reading the data carrier, the GT7 or GC7 checks whether the FID number of the data carrier matches that of the GT7/GC7, i.e., whether the data carrier belongs to the same facility in which the device is operating. If the FID number is identical, operation can continue.

- Authorization list: The GT7/GC7 checks the data carrier UID against the internal authorization list. If the data carrier UID is included in this list, operation can continue.

NOTE! The authorization list must be loaded from a management software into the GT7 or GC7 via the G7 API.

- Remember authorization: During online operation, the GT7/GC7 stores the authorization of a UID. If the GT7/GC7 switches to emergency mode, the terminal or controller checks whether the read UID read is contained in the authorization list stored in the device.

- Authorization valid for: This option is displayed if the "Remember authorization" option has been selected for the "Authorization check". The number of hours entered here is the time that the UID number of a data carrier has been stored in the watch list in the GT7/GC7 since the last time the UID was read out in online mode.
- Allow barcodes: This option is displayed if "Data carrier coding" has been selected for the "Authorization check". If a barcode reader (e.g., ATR 110 barcode scanner) is connected to the GT7 terminal, this option can be enabled to allow barcodes to operate the terminal in emergency mode.
- Allow pin codes: If this option is enabled and the PIN code input is activated (see "4.9. PIN"), access via PIN code input (and without data carrier) is possible. Otherwise, if this option is not enabled but the PIN code input is activated, a PIN code can be entered but access will be denied.
- Code data carriers: If a license for encoding data carriers is available in the GT7/GC7 device (see the GT7 or GC7 manual) and encoding is also enabled in the data carrier settings, data carriers can also be encoded in emergency mode. To do this, the "Enable Emergency Mode" option must be enabled and then also the "Code data carriers" option.

4.8 G6 compatibility mode

The screenshot shows the Gantner G7.3500 - V2.12.0 App Configuration interface. The left sidebar contains a menu with options: Dashboard, Device Configuration, App Configuration, General, Access, Reader settings, Check-In, Display Texts, Emergency Mode, G6 Compatibility Mode (highlighted), PIN, Design, Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, and Maintenance. The main area is titled 'G6 Compatibility Mode' and contains the following settings:

- Enable G6 Adapter:** ☒
- Management software timeout:** 10 s
- Language Characterset:** 1252_WesternEurope
- Fingerprint mode:** Online controlled
- Lockercheckin before CardIdent:** ☐
- Deny if Check-In failed:** ☒
- Extended barcode mode:** ☐
- Send Lockgroup 1:** ☐
- Send Lockgroup 2:** ☐
- Send custom segment data:** ☐
- Send Fitness member data:** ☐
- Button event:** Disabled

At the bottom of the main area are three buttons: Save, Discard, and Default.

Figure 4.13 – G7 Access Apps – G6 Compatibility Mode

The settings on the “App Configuration” -> “G6 Compatibility Mode” page are used to communicate with the GT7 terminal / GC7 controller in the same way as the GAT Access 6xxx, one of GANTNER's previous generation 6 devices.

After the “Enable G6 Adapter” option has been selected, the GT7 / GC7 with G7 Access and G7 Advanced Access app uses the same protocols as the generation 6 device, e.g., a GAT Access 6100 or GAT Access 6200, and will operate with the management software in the same way as these devices. The G6 compatibility mode thus allows the GT7 / GC7 to replace a G6 device without major changes in the management software.

After activating the mode via the "Enable G6 Adapter" option, you can define the following options:

- Management software timeout: This can be used to define how long (in seconds) to wait for a request or response to the higher-level management software before a timeout is triggered.
- Language character set: Set the character set that applies to the communication here so that the characters are transmitted correctly. For Latin characters for languages in Western Europe or similar, use "1252_WesternEurope".
- Fingerprint mode: Defines when verification via fingerprint should occur.
 - Online controlled: The management software can individually control for each user whether verification via fingerprint is required.

- Always before Card Ident: Fingerprint verification occurs after reading a data carrier and before a Card Ident command is sent to the management software.
- Always after Card Ident: Fingerprint verification occurs after the data carrier has been read.
- Locker check-in before CardIdent: If this option is enabled, the locker check-in is completed immediately after reading the data carrier information and before a request has been sent to the management software. For more information on the locker check-in function, see chapter "4.5. Check-in".
- Deny if Check-In failed: If the locker check-in cannot be completed successfully and this option is enabled, access will be denied.
For more details on locker check-in, see chapter "4.5. Check-in".
- Extended barcode mode: If this option is enabled, the GT7 or GC7 will send the barcode data in extended format.
- Send lock group 1 / 2: This option is used to specify whether the locker information should be transmitted from the data carrier.
- Send custom segment data: Data carriers may contain data (segments) other than the GANTNER data in the GANTNER segment. If this option is enabled, the data from the foreign segment will also be transmitted.
- Custom segment type Id: An ID number for the foreign segment can be entered here if this is enabled (see previous option).
- Send fitness member data: If this option is enabled, the fitness master data (user segment) for LEGIC prime data carriers will be read and transmitted.
- Button event: If this option is enabled, a "Button Event" command is sent if the confirmation of the user is completed via a button.

4.9 PIN

On the "PIN" settings page of the "App Configuration" menu, the G7 Access Apps can be configured to allow users to gain access by entering a PIN code. For GC7 controllers, which usually do not have a display, an external display can be connected.

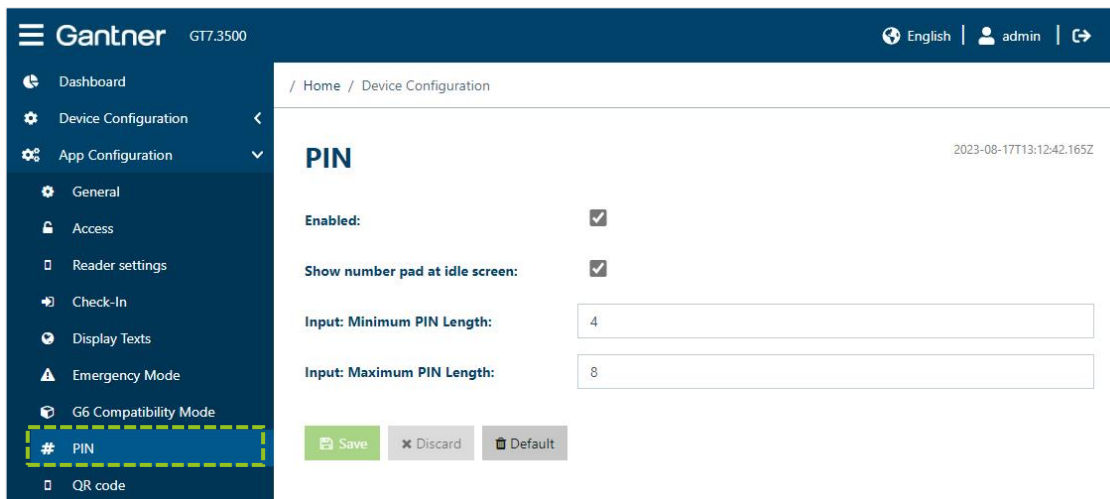


Figure 4.14 – G7 Access Apps – PIN settings

- Enabled:

With this option, the G7 Access Apps can be used without RFID data carriers, only by entering a PIN code. The user enters their PIN on the touchscreen for identification. After enabling this option, a keypad symbol is displayed on the touchscreen, which must be pressed to display the PIN keypad:



The following PIN settings are available after this option is enabled.

Note: The option "Allow pin codes" must be enabled (see "4.7. Emergency mode") to also allow access via PIN code in emergency mode.

- Show number pad at idle screen:

When this option is enabled, the option for identification using a data carrier is not displayed after the touchscreen is pressed. Instead, the user is prompted to enter their PIN to start using the app:



- Input: Minimum PIN length:

Define the minimum length of the PIN here.

- Input: Maximum PIN length:

Define the maximum length of the PIN here.

4.10 QR code

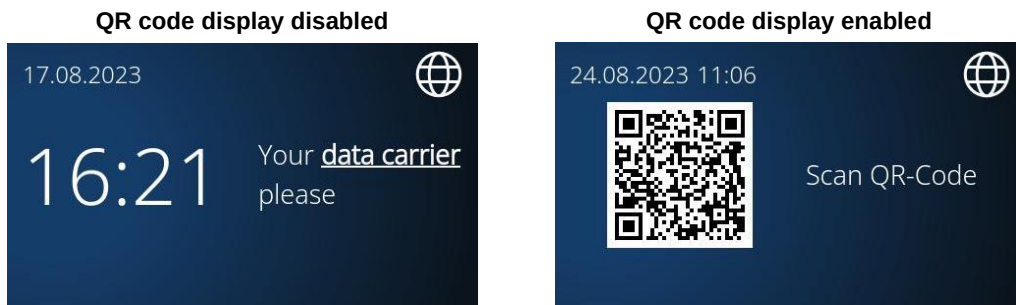
The settings on the "QR code" page of the "App Configuration" menu allow you to define a QR code that will be shown on the display of the GT7 device. The content of the QR code can be a static, manually defined text or the QR code can also be sent from a third-party software, which allows the identification of users via mobile apps for example.

Figure 4.15 - G7 Access Apps - QR code settings

- Mode:
 - Disabled: The QR code generation is disabled and will not be shown on the display.
 - API: Via this setting, the data that is shown as a QR code on the display is sent by a third-party software via the interface to the GT7 device. For more information about the API interface, please contact interfaces@gantner.com.
 - Template: In this mode, a text can be entered in the "Template" field. This text is encoded into the QR code and shown on the display. It is possible to use placeholders (starting with @) as shown in the example image above.
 - @Device: This placeholder displays the name of the device. The name is defined under "Device Configuration" -> "Network" -> "Device name".
 - @Timestamp: This is the current date and time in the format "yyyy-mm-ddThh:mm:ssZ". The timestamp is updated every 30 seconds and a new QR code is shown on the display. For example: 2023-08-17T13:10:55Z
 - @Challenge: This is a random 8-digit number that is regenerated every 30 seconds, which means a new QR code is shown on the display every 30 seconds (see also @Timestamp)
- QR code size: The size of the QR code in pixels (square size). The default is 140 pixels. A QR code of this default size is shown in the following examples.

- **Encrypt data:** When this option is enabled, the QR code data is encrypted using 128-bit AES. The password for the encryption must be entered into the "Password" field by clicking on the edit button . Letters and numbers can be used in the password.

The following images provide an example of the display with and without a QR code.



4.11 Design

On the “App Configuration” -> “Design” page, basic settings for the appearance and layout of the GT7 display or the external display of a GC7 controller (if used) and the LED display (only relevant for the GT7 terminal) can be configured.

The screenshot shows the Gantner GT7.3500 Design settings page. The left sidebar contains a navigation menu with options like Dashboard, Device Configuration, App Configuration, General, Access, Reader settings, Check-in, Display Texts, Emergency Mode, G6 Compatibility Mode, PIN, QR code, Design (selected), Installed Apps, Cloud Pairing, Licensing and coding points, Certificate management, Maintenance, Device, Update Firmware, Addon Bus, Log Viewer, Device State, and Legal infos. The main content area is titled 'Design' and includes the following settings:

- Idle led circle color:** A color selection box currently showing blue.
- Message design:** A dropdown menu set to 'Icon middle'.
- Icon size:** A dropdown menu set to '8x'.
- Unlock icon:** A dropdown menu set to 'check'.
- Deny icon:** A dropdown menu set to 'times'.
- Locked icon:** A dropdown menu set to 'times'.
- Use default theme backgrounds and colors:** An unchecked checkbox.
- Backgrounds:** A section with a dropdown menu set to 'Background'.
 - Screen:** A dropdown menu set to 'default'.
 - Uri:** A text input field containing '@Theme/background.jpg'.
 - Refresh interval:** A text input field set to '0' with a unit dropdown set to 'ms'.
 - Design color:** A color selection box.
 - Style:** A text input field containing 'text-shadow: black 0px 0px 5px;'.

At the bottom of the page, there are three buttons: 'Save', 'Discard', and 'Default'.

Figure 4.16 – G7 Access Apps – Design settings

- **Idle led circle color:** The color of the LED circle near the RFID reader on the GT7, which is displayed in the idle state, can be changed via the color selection. This is blue by default but can be changed to a different color, e.g., to match a company color scheme, by clicking on the color box.
This setting is not relevant for a GC7 controller.
- **Message design:** This setting is used to specify whether the icon should be displayed on the left of a message, e.g., for a booking creation, and the output text on the right ("Icon left") or whether the icon should be centered and the text below it ("Icon middle").
- **Icon size:** This setting is used to define how large the icon should be displayed when creating a booking.
- **Unlock icon:** This setting is used to define the icon for when a valid access check and successful booking creation have been completed. Different icons are available for selection.
- **Deny icon:** This setting is used to define the icon for when access is denied. Different icons are available for selection.
- **Locked icon:** Here you can select the type of icon to display for when access is generally blocked. Different icons are available for selection.

- Use default theme backgrounds and colors:

If this option is enabled (default setting), the background images and colors from the design template (theme) are used (see also "Installed apps" -> "Theme").

If individual images or colors are to be used for devices, these can be specified in the app configuration. The "Use default theme backgrounds and colors" option must be disabled in this case. The "Backgrounds" section is displayed.

In this case, you can insert a new configuration block for each defined screen by clicking on "Backgrounds" and configuring the following settings:

- In the "Screen" field, select the screen for which the configured image is to be used. All available screens of the G7 Access app as well as result displays are available for selection.
- Specify the source of the display in the "URL" field. Images that are available in the theme or that have been uploaded to the device via FTP can be used as the source. Alternatively, images that are stored online by a server can also be displayed. The syntax for the different sources is:

Images from the theme:

@Theme/filename.jpg

Example: @Theme/background.jpg

Images uploaded to the device via FTP:

/ftp/filename.jpg

Example: /ftp/mybackground.jpg

Images stored on an FTP server:

ftp://username:password@ip-address/filename.jpg

Example: ftp://admin:admin@10.1.1.100/test.jpg

Images provided, e.g., from a webcam:

http://username:password@ip-address/api/scene//live?t=@Random

Example: http://admin:admin@10.1.1.100/api/scene/live?t=@Random

To use images provided online, contact GANTNER support for further information.

- By specifying a time in the "Refresh interval" field, it is also possible to continuously update an image provided by the server. In this way, screenshots from webcams for example can also be displayed on the screen.
- Design color: The font color that is used to display information on the display.
- Style: Here you can define a different style of HTML formatting for the text. For example: "text-shadow: black 5px 5px 10px" will display a black shadow with 5 pixels distance and 10 pixels size. Other settings include, for example:
 - background-color: rgba(0,0,0,0.8) - color overlay of background.
 - text-transform: uppercase – text is shown in capital letters.
 - text-align: right - text is aligned to the right side of the screen.
 - line-height: 1 – adjusts the line height of text.

5 OPERATION

5.1 Target group

This chapter is intended for the system administrator, personnel, and end users of the facility where the GT7 terminal / GC7 controller with G7 Access App is operating.

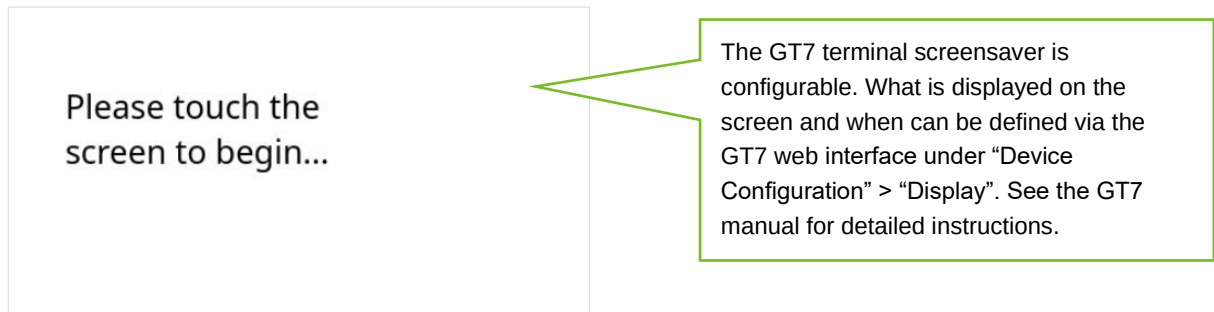
5.2 Operation of the G7 Access Apps

The operation of the G7 Access App and G7 Advanced Access App is intuitive, as the user is guided through the various options via the GT7 display or, in the case of a GC7 controller with a connected reader, the user only needs to hold the data carrier up to the reader.

This section provides an overview of the operation of the apps and the sequence can be adapted to different requirements via the settings (see "4 APP CONFIGURATION").

5.2.1 Operation with display

- To start operation, touch the display.



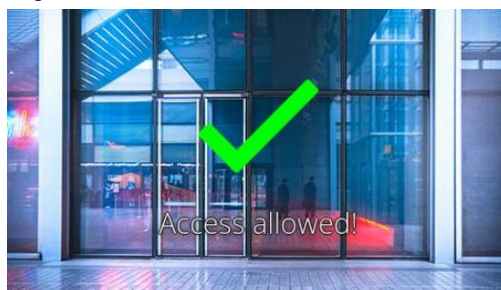
- The default display is shown.
 - a) By default, the display shows "Identification":



- b) If PIN entry keypad is enabled for the idle screen (menu "App configuration" -> "PIN"), the PIN code keypad is displayed as the default display.



- After identification via data carrier or PIN code entry, the access authorization is checked, and access is granted or denied.



i The length of the release of an access can be defined in the configuration ("unlocking time"). In addition, further outputs can be controlled or the release decision can be influenced using digital inputs (e.g., for entry/exit controls).

i If the locker check-in function is enabled, locker information is also written to the data carrier after a valid access using a data carrier occurs.

5.2.2 Operation with a GC7 Controller without display

- If a GC7 controller without display is being used with an external reader (e.g., GR7), the user must identify themselves at this reader using their data carrier or PIN code.
 - In the idle state, the reader's reading field LED is blue (1) and the LED bar is red (2), i.e., access is not permitted.



- ▶ Hold the data carrier in front of the reading field.
 - The data on the data carrier is read and transferred to the GC7.
- ▶ Depending on the configuration, it may also be necessary to enter a PIN code or scan a fingerprint.
Note: The GC7 can be configured to allow access using a PIN code only with no data carrier required. The fingerprint is only possible as additional verification, i.e., a data carrier is also always required.
 - This data is also transmitted to the GC7.
 - In emergency mode operation, the GC7 checks the authorization based on the stored configuration. In normal operation, the data is sent from the GC7 via the network interface to a higher-level PC software. This checks whether the data carrier is authorized to access the current door at the current time and sends the result to the GC7 controller.
 - For a valid authorization, the GC7 activates the relay(s) defined as the unlocking relay in the Access App. This activates the door or turnstile and enables access.
For an invalid authorization, access remains blocked.
 - The LED bar (2) and the reading field LED (1) use colors to indicate the status to the user (e.g., green = access permitted, red = access not permitted). In addition, acoustic signals are emitted via a beeper.
Note: LEDs and beepers can be used to signal a wide variety of information. A detailed description can be found in the manual of the respective reader.
- ▶ Following valid authorization, the user must open the door or turnstile within the set unlocking time.
 - The GC7.3000 then returns to the idle state, depending on the door feedback.

5.2.3 Checking the EU digital COVID certificate

Depending on the configuration settings, either only a user's COVID certificate or the COVID certificate in combination with the user's data carrier can be checked.

- ▶ For a COVID check without an additional data carrier, the user must hold their COVID certificate to the barcode scanner.
 - The GT7/GC7 then checks the authorization and then enables or disables access.
- ▶ For a COVID check in combination with a data carrier, the user's RFID data carrier must also be read by the reader after the process described above is completed.
 - Access is not permitted until both authorization checks are successful. If a check fails or a timeout occurs, access authorization is denied.

NOTE:

This manual is valid as of 24th August 2023. It is subject to change.
Amendments can be made without prior notice at any time!
Information in this manual refers to G7 Access App Version 2.7.7 and G7 Advanced Access App Version 1.5.1.



GANTNER is active in over 60 countries. **Please visit www.gantner.com**

Nüziders, Austria
info@gantner.com

Houten, the Netherlands
info@gantner.nl

Sydney, Australia
info-aus@gantner.com

London, United Kingdom
info-uk@gantner.com

Bochum, Germany
info-de@gantner.com

Los Angeles, USA
info-us@gantner.com

Ypern, Belgium
info@gantner.be

Dubai, UAE
info-me@gantner.com

Ahmedabad, India
info@gantnerticketing.com

Current contact information: www.gantner.com/locations

www.gantner.com