

GAT DC 7200

Door controller for electronic access control



© Copyright 2026 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 markings and registered trademarks used in this manual. All product and company names, which are mentioned in this manual, are only used for identification and explanation purposes. Some of these names may be trademarks or registered trademarks of the corresponding company.

Contact

The contact information for questions regarding 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

Important Information

Dear customer,

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

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

Notation of safety information and safety symbols

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

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

1. Safety messages for personal injury

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



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

Format of safety messages that apply to an entire section:

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

CAUTION



Electrical shock

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

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

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

2. Property damage messages

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

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

NOTICE

Risk of damage to the device and connected devices

Risk of malfunction

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

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

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

3. Definition of the signal words

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

4. Definition of the safety symbols

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

⚠ Important Safety Information ⚠



- The installation, commissioning, and servicing of our products must be performed only by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association.

→ Unqualified personnel may potentially perform actions that result in injury due to electrical shock.



- Where not otherwise stated, installation and maintenance work on our products must be carried out when disconnected from the power supply. This applies in particular to appliances that are normally supplied by low-voltage current.

→ If the appliance is not disconnected from power, touching terminals or other internal parts of the appliance may lead to injury due to electrical shock.



- It is prohibited to alter the products (devices, cabling, etc.).

→ Alterations to the products may subsequently result in personal injury, property damage, or damage to the products.

- Do not remove protective shields and covers.

→ Removing protective shields and covers may result in personal injury or property damage.

- Do not attempt to repair a product after a defect, failure, or damage is detected. In addition, do not put the product back into operation. In such cases, it is essential to contact your GANTNER representative or GANTNER Technical Support.



- The installation, commissioning, operation, and maintenance of the product must be carried out in accordance with the technical conditions of operation as described in the corresponding documentation. Therefore, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.

- If there are still some points that are not entirely clear, please do not take a chance. All queries can be clarified by your GANTNER representative or by ringing the GANTNER support hotline.

- Directly on receipt of the goods, inspect both the packaging and the product itself for any signs of damage. Also check that the delivery is complete and includes all accessories, documentation, auxiliary devices, etc.



- If the packaging or product has been damaged in transport, or should you suspect that it may have a fault, the product must not be put into service. Contact your GANTNER representative who will endeavor to resolve the problem as quickly as possible.

- GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.

Although great care is taken and we are continuously aiming for improvement, we cannot completely exclude the possibility of errors appearing in our documentation. GANTNER Electronic GmbH therefore accepts no responsibility for the completeness or the accuracy of this manual. The right is reserved to make alterations at any time without prior notice.

Should you discover any fault with the product or in its accompanying documentation, or you have any suggestions for improvement, you may confidently inform your GANTNER representative or GANTNER Electronic GmbH directly.

We especially look forward to hearing from you if you want to let us know that everything is functioning perfectly

The GAT DC 7200 was developed and fabricated under the quality management standard ISO 9001 and GANTNER Electronic GmbH is also certified according to standard ISO 14001.



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

- 2014/53/EU (Radio Equipment Directive)

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

http://www.gantner.com/en/products/downloads-GAT-DC-7200_o84nFQzc7D



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



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

CONTENTS

1	INTRODUCTION	11
1.1	About this manual	11
1.2	Chapter overview	11
1.3	Target group	12
1.4	Formatting	12
1.5	Contact & inquiries	12
2	GENERAL INFORMATION	13
2.1	Intended use	13
2.2	Functional description	13
2.3	Highlights	14
2.4	Device features	14
2.5	Terminology	16
2.6	RFID technology and data carriers	18
2.7	Mobile Credential	18
3	INSTALLATION	19
3.1	Target group	19
3.2	System overview	19
3.3	Installation instructions	20
4	ELECTRICAL CONNECTIONS	23
4.1	Target group	23
4.2	Network connection	23
4.2.1	Status display	24
4.3	Reader connection	25
4.3.1	Example connection: GR7.13xx to GAT DC 7200	27
4.3.2	Example connection: GR7.23xx / GR7b.23xx to GAT DC 7200	28
4.3.3	Example connection: GR7.13xx and GAT SR 7000 Wiegand to a door	30
4.3.4	Status display	31
4.3.5	Automatic reader identification (IDENT)	31
4.3.6	Manipulation alarm	32
4.3.7	Relay outputs and optocoupler inputs	32
4.4	Access point GAT DL 091	33
4.5	Peripheral devices	35
4.5.1	Expander GAT IO 7054 / GAT IO 7055 connection	35
4.5.2	Status display	36
4.6	Relay outputs and optocoupler inputs	37
4.7	Power supply	38
5	CONTROLS AND SIGNALIZATION	39
5.1	General	39
5.2	Target group	39
5.3	Restart	39
5.4	Reset configuration password and network settings	40
5.5	Restart and reset to default settings	40
5.6	Signaling overview	41
6	START-UP AND CONFIGURATION	43
6.1	Target group	43
6.2	Switching on the power supply	43

6.3	Startup	43
6.4	Configuration	44
6.4.1	Certificate configuration for TLS/SSL connection	45
6.4.2	Live status display and door control	51
6.4.3	UPS power supply	52
6.4.4	General information	53
6.4.5	Users	54
6.4.6	Language of the web interface	55
6.4.7	Door configuration	56
6.4.8	Reader configuration	63
6.4.9	Hardware extensions	78
6.4.10	Alarm system settings	81
6.4.11	Database settings	83
6.4.12	Power over RS-485	84
6.4.13	Security and user	84
6.4.14	Network settings	88
6.4.15	Date and time	90
6.5	Configuring Mobile Credential	91
6.5.1	Delete VCP from a reader	95
6.6	Bookings	97
6.7	Administration and maintenance	98
6.7.1	Maintenance	98
6.7.2	Inputs and outputs	100
6.7.3	Update controller	101
6.7.4	Update sub devices	101
6.7.5	License	102
7	AUTHORIZATION MANAGEMENT	105
8	STANDALONE MODE	107
8.1	Target group	107
8.2	Enabling standalone mode	107
8.3	Authorization management	108
8.3.1	Adding persons and authorizations	108
8.3.2	Adding time plans	111
8.3.3	Adding day plans	113
8.3.4	Adding special days	115
8.4	Limitations of standalone mode	116
9	FREQUENTLY ASKED QUESTIONS	117
9.1	Entry and exit	117
9.2	Transmitter	117
9.3	WiNET access points	117
9.4	Door licenses	117
9.5	Proxy credentials	117
9.6	Proxy reader	118
9.7	Elevator control	118
9.8	Anti-pass-back function	118
9.9	Long-range reader	118
9.10	Network security	118
9.11	Configuration saving	119
9.12	Configuration sharing	119
9.13	Extending the outputs	119
9.14	Extending the inputs	119
9.15	Video integration	120
9.16	Plug&Play PLUS	120

9.17	CardNET	120
9.18	GANTNER SVN	120
9.19	Short-circuit protected connections	120
9.20	Communication via the reader socket	121
9.21	Reset to default settings	121
9.22	Network connection	121
9.23	Using GAT SR 3xx series readers	121
9.24	MIFARE Classic	121
9.25	MIFARE DESFire	122
9.26	LEGIC prime and advant	122
9.27	HID iClass	122
9.28	Bookings	122
9.29	Data carrier types	122
9.30	Alarm system	123
9.31	Status of the inputs/outputs	123
9.32	Time server	123
9.33	Time zone	123
9.34	Daylight saving time switchover	123
9.35	Backup settings	123
9.36	Controller and reader updates	124
9.37	Installation	124
9.38	Reader ports	124
9.39	Power for locks	124
9.40	Identification and verification	124
9.41	Special authorizations	124
9.42	Multi-card handling	125
9.43	Reading range	125
9.44	ISO 15693 standard	125
9.45	ISO 14443 standard	125
9.46	Reader speed	125
9.47	Authorization changes	125
9.48	Inputs and outputs	126
9.49	Installation	126
9.50	WiNET	126
9.51	Test mode	126
9.52	Remote control of doors	127
9.53	GAT DIRECT.Connect interface	127
9.54	Mobile Credential	127
10	TECHNICAL DATA	129
10.1	Power supply	129
10.2	Server interface	129
10.3	Reader	129
10.4	"Sub" peripheral interface	130
10.5	Relay outputs	130
10.6	Optocoupler inputs	130
10.7	Memory and time management	130
10.8	Signaling elements	131
10.9	Housing	131
10.10	Ambient conditions	131
10.11	Dimensions	131

1 INTRODUCTION

1.1 About this manual

This manual contains all the necessary information required to install, configure, and operate the GAT DC 7200 door controller. You will also find the service instructions and disposal notes as well as the technical data of the GAT DC 7200.

The configuration of the GAT DC 7200 is also described, which is done via an Internet browser using the GAT DC 7200 web interface. The necessary information for configuration is available in this manual and is valid for controller firmware version 2.1.

1.2 Chapter overview

In chapter "2 GENERAL INFORMATION", you will find a functional description and overview of the GAT DC 7200 including the readers, peripherals, and RFID technologies supported by the device. In addition, a description of the main terms used in this manual is available in this chapter.

Chapter "3 INSTALLATION" includes the DIN rail mounting and wall mounting instructions for the GAT DC 7200. Here you will also find the measurements required for installation.

Chapter "4 ELECTRICAL CONNECTIONS" describes the connection of the external readers and I/O devices as well as the digital inputs and outputs. Also available in this chapter are the instructions for completing the network connection for communication as well as the voltage supply connection.

In chapter "5 CONTROLS AND SIGNALIZATION", you will find an explanation of the GAT DC 7200 operational processes and status signalization.

In chapter "6 START-UP AND CONFIGURATION", you will find a description of how to configure the GAT DC 7200 and commission for use. The configuration is performed via web interface in an Internet browser. Also described in this chapter are the main functions of the web interface and an overview of the possible configuration settings.

In chapter "7 AUTHORIZATION MANAGEMENT" you will find information on administering authorizations using access control software.

In chapter "8 STANDALONE MODE" you will find information on administering authorizations without access control software.

In chapter "9 FREQUENTLY ASKED QUESTIONS", you will find the answers and information for the most frequently asked questions about the GAT DC 7200.

Chapter "10 TECHNICAL DATA" contains all the technical information and measurement diagrams of the GAT DC 7200.

1.3 Target group

This manual contains information relevant for the various stages in the operating life of the GAT DC 7200. Information about the installation, electrical connection, commissioning, and service/maintenance of the GAT DC 7200 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, operation, configuration)
- Service technicians of the access control system (service and maintenance)
- End users of the GAT DC 7200 (user manual)

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

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

1.4 Formatting

The following formatting is used in this manual to indicate non safety-critical information that is relevant for the particular section.

i *Information text.*

Instructions that must be completed by the user, and the result of each instruction step, are formatted as follows.

- ▶ Instruction text.
 - Result of instruction.

NOTE! This signal word is used to indicate important information, relating to the current topic, which must be read and followed in order to complete a task.

1.5 Contact & inquiries

If you have any questions concerning the GAT DC 7200, 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 GAT DC 7200 door controller is designed for the electronic access control of interior and exterior doors in public buildings such as company, sales, and factory buildings. In addition to the GAT DC 7200, one or more external readers (available from GANTNER Electronic GmbH) as well as an electronic door lock are required. The identification of system users at the connected readers takes place using contactless RFID (Radio Frequency Identification) data carriers, biometrics, code input or mobile devices with Mobile Credentials.

The types of doors being controlled are independent of the GAT DC 7200. The appropriate electronic door lock must be used for the applicable door type.

2.2 Functional description

To gain access to an area of a building secured by the GAT DC 7200 door controller, the person uses their personal RFID data carrier for identification at the RFID reader or Mobile Credential, which is connected to the door controller. Several readers can also be used. The door controller then checks the identification data with the authorization data and timetables stored in the door controller. If access is permitted, the door controller controls the electronic door opener via the configured relay or unlocks the electronic door lock.

The door controller is installed in a secure area with communication between the door controller and the reader encrypted to prevent manipulation. Communication for configuring the door controller via the web interface is also encrypted for optimum security (TLS/SSL connection).

The GAT DC 7200 allows a flexible configuration for the control of doors. Depending on the application, several doors can be monitored and controlled by a door controller, and up to 4 readers (or 16 with expansion license) can also connect to a GAT DC 7200. This makes it possible to implement functions such as direction detection, e.g., one reader for access identification and one reader for exit identification. The GAT IO 7xxx devices can be connected to expand the digital inputs and outputs of the door controller.

The GAT DC 7200 door controller operates autonomously and connects to access control software via the Ethernet interface. GANTNER Electronic GmbH provides GAT ACE 7000 software for hardware communication and configuration and Matrix software for access authorization. GAT ACE 7000 provides the interface between Matrix and the door controller and is used to configure the door controllers, readers, and system. In Matrix, the timetables and access authorizations for persons, data carriers, etc., are defined before being uploaded to the door controller.

The GAT DC 7200 can also communicate with third-party software via the GAT DIRECT.Connect software and a suitable adapter. See "9.53. GAT DIRECT.Connect interface" for further information.

All permitted entries and access attempts are recorded by the GAT DC 7200 and can be displayed and evaluated via the network.

2.3 Highlights

- Access control for up to 4 doors (or up to 16 with expansion license).
- Up to 16 multi-technology readers for LEGIC, MIFARE®, ISO 15693, and HID iClass can be connected.
- Identification using smartphones or smartwatches
- Automatic reader recognition.
- Plug&Play installation.
- Ethernet connection via RJ45 plug.
- 6 relay outputs and digital inputs.
- Extension of relay outputs and digital inputs via connectable GAT IO 7xxx devices.
- Sub interface for peripherals.
- Configuration via clear, secure web interface (TLS/SSL connection).
- Integration with GAT ACE 7000 and Matrix access control software.
- Connection to third-party software via GAT DIRECT.Connect possible.
- Support of the SALTO SVN function.
- Internal clock (protected against power failure) with automatic switching for daylight-saving time.
- Simple DIN-rail mounting.

2.4 Device features

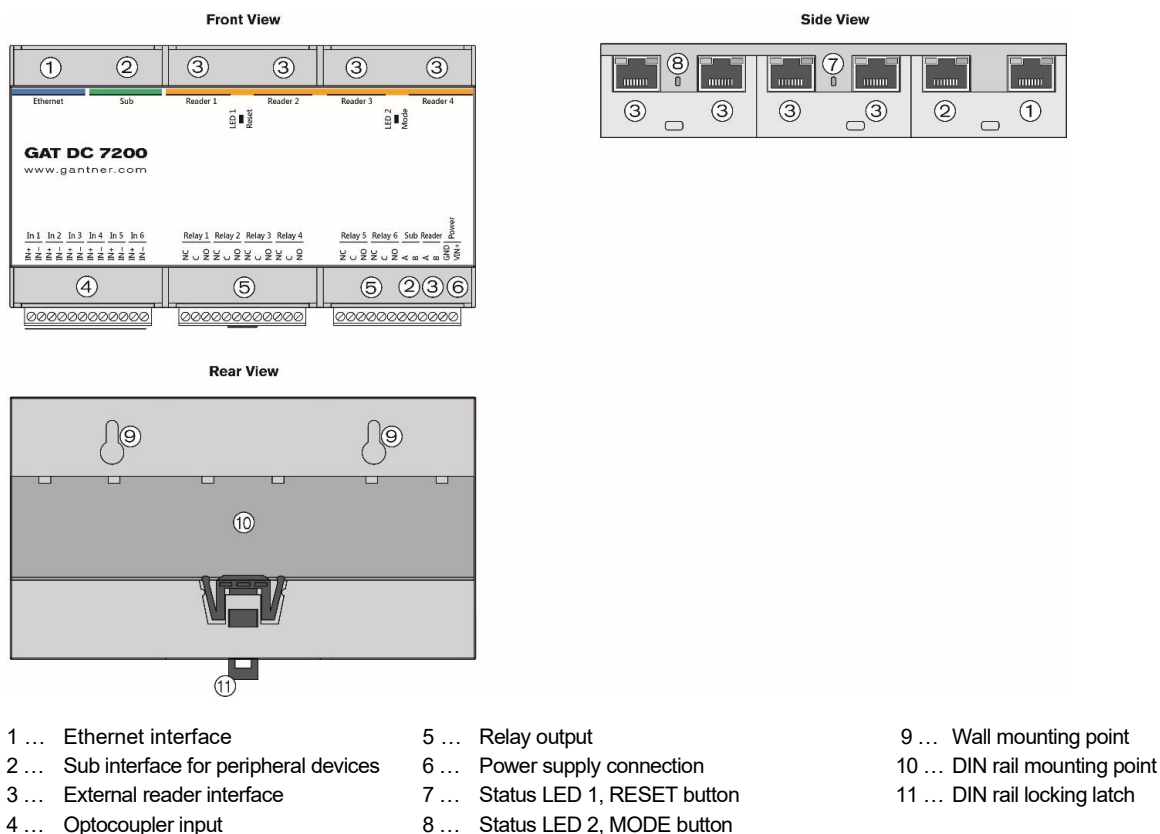


Figure 2.1 – Device features

Order Information	Part No.
GAT DC 7200 Door controller, 4 external readers per door, 6 digital inputs, 6 relay outputs, Ethernet interface, sub interface	532220

Expansion Licenses	Part No.
Note: The designation "email" enables the activation of the license via email	
GAT DC 7200 PLUS license	753023
GAT DC 7200 PLUS license email	732222
GAT DC 7200 expansion license from 4 to 16 doors	
GAT DC 7200 elevator license	794028
GAT DC 7200 elevator license email	793936
Expansion license for elevator and locker control	
GAT DC 7200 APB and online license	1100191
GAT DC 7200 APB and online license email	1100190
Expansion license for the Anti-Pass-Back function and Online Management (e.g., for GAT DIRECT.Connect)	
GAT DC 7200 Mobile Credential license	1117572
GAT DC 7200 Mobile Credential license email	1117571
Extension license for GAT DC 7200 for the use of "mobile devices as data carriers"	

Accessories	Part No.
GAT SP 070, 2.0A DIN-rail power supply. Output: DC 12 V, I = 2 A	759534
GAT SP 070, 7.1A DIN-rail power supply. Output: DC 12 V, I = 7.1 A	759433
GAT SP 070 UPS Online 30W DIN-rail power supply with integrated battery. Output: DC 12 V, I = 2.5 A	1104715
GAT SP 070 UPS Online 55W DIN-rail power supply with integrated battery. Output: DC 12 V, I = 4.6 A	1104716
GAT SP 074, 1.5A DIN-rail power supply. Output: DC 24 V, I = 1.5 A	759231
GAT SP 074, 3.8A DIN-rail power supply. Output: DC 24 V, I = 3.8 A	759332
GAT SP 074 10A DIN-rail power supply. Output: DC 24 V, I = 10 A	1102259
GAT SP 074 20A DIN-rail power supply. Output: DC 24 V, I = 20 A	1102258
GAT SP 074 UPS Online 30W DIN-rail power supply with integrated battery. Output: DC 24 V, I = 1.25 A	1104717
GAT SP 074 UPS Online 55W DIN-rail power supply with integrated battery. Output: DC 24 V, I = 2.3 A	1104718
GAT SP 07x Fuse Block GAT SP 07x fuses for DIN-rail mounting	803726
Installation Box 9118 Circuit breaker box with 1 DIN rail, IP 65, W:40 x H:33 x D:13 cm	803625

Installation Box 9236 Circuit breaker box with 2 DIN rails, IP 65, 40 x 48 x 13 c W:40 x H:48 x D:13 cm	803524
Installation Box 9354 Circuit breaker box with 2 DIN rails, IP 65, W:40 x H:63 x D:13 cm	1105526
GAT IO 7054 IO expansion unit with 4 outputs and 12 inputs, RS-485 interface	1105454
GAT IO 7054 NW IO expansion unit with 4 outputs and 12 inputs, RS-485 interface, wireless interface	1105455
GAT IO 7055 IO expansion unit with 8 outputs and 16 inputs, RS-485 interface	1105456
GAT IO 7055 NW IO expansion unit with 8 outputs and 16 inputs, RS-485 interface, wireless interface	1105457

2.5 Terminology

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

User / Person

These terms refer to the persons who wish to gain access to a door controlled by a GAT DC 7200 using their data carrier or fingerprint for identification at the connected reader.

Facility

Refers to the building where access to specific areas is controlled by the GAT DC 7200.

Computer / PC

These terms refer to all desktop and laptop computers running a Microsoft® Windows® operating system used, e.g., to configure the GAT DC 7200.

Controller / Door controller

General term for access control devices used for door control.

Lock

This term refers to the electronic door lock that is controlled by a GAT DC 7200.

Door

This term refers to the entry point being controlled by the GAT DC 7200. This is usually a door that is restricting access to a room or area in a building. However, gates, turnstiles, and other similar devices can also be controlled and monitored. A GAT DC 7200 can monitor up to 4 doors (or up to 16 with additional expansion license).

Reader

Readers are devices that connect to a GAT DC 7200 via serial RS-485 interface and used to read/transmit data carrier information to the controller. Different types of readers can be used in the system.

Data carrier

A data carrier is a form of identification media with electronic memory and ID number that is used by staff and visitors in a facility for identification at the readers connected to the door controllers. Data carriers are available in a variety of different forms (e.g., chip cards and key tags) and for different identification systems (LEGIC, MIFARE®, ISO 15693).

RFID (Radio-Frequency Identification)

Identification over a short distance using radio frequency. An RFID data carrier is used to identify individual users in GANTNER systems.

FID (Company ID) and Site Key

The FID and Site Key are unique numbers assigned to every facility installation. LEGIC systems use the FID number while MIFARE® systems use the Site Key, which is a combination of the FID and the read and write keys. The FID / Site Key is encoded in every data carrier and device in the facility to ensure that data carriers from one installation are not used in other installations.

Web interface

To configure the GAT DC 7200, it is possible to access the GAT DC 7200 directly using a web browser via the IP address or the device name. The configuration interface is displayed directly in the browser after a valid login. The term web interface is used in this manual to refer to this configuration connection and display.

TLS / SSL

Encryption protocol for secure data transmission, e.g., when configuring the GAT DC 7200 via the web interface. In this manual, the new designation TLS (Transport Layer Security) is used. The previous designation of this technology is SSL (Secure Sockets Layer), which is synonymous with TLS.

GAT DIRECT.Connect

Software for integrating devices such as the GAT DC 7200 into various software packages with the appropriate software adapter.

Mobile Credential

Identification of users via their mobile devices (e.g., smartphone or smartwatch). An authorization badge is stored on the mobile device (e.g., in Google Wallet or Apple Wallet). Certain requirements must be met for this application (see "2.7. Mobile Credential").

2.6 RFID technology and data carriers

For identification at a GAT DC 7200 via contactless data carriers, various radio frequency identification (RFID) readers and technologies are available from GANTNER Electronic GmbH.

As the GAT DC 7200 does not have an integrated reader and communication with the connected external readers occurs via RS-485 and the corresponding protocol, it does not matter which RFID technology is used with the GAT DC 7200.

The information in this manual is therefore generally applicable for RFID technologies that are supported by the GAT DC 7200 and the connected RFID readers. These are essentially the following technologies:

- LEGIC prime
- LEGIC advant
- MIFARE DESFire EV1®, EV2® and EV3®
- ISO 14443A
- ISO 14443B
- ISO 15693
- Sony Felicia
- Inside Contactless (HID iClass)

In addition to the RFID technologies mentioned, numerous other technologies (e.g., 125 kHz, UHF long-range, etc.) can be used with the GAT SR 7000 Wiegand interface.

2.7 Mobile Credential

Starting with version 3.7, the GAT DC 7200 offers the option, with a suitable license and configuration, to use mobile credentials (identity in Google or Apple Wallet) stored on mobile devices such as smartphones and smartwatches for user identification. Certain prerequisites are necessary for this.

Prerequisites for the use of Mobile Credential:

- GAT DC 7200 firmware: V3.7 or newer
 - Reader firmware: V03.06 or newer
 - LEGIC Chip OS in the readers: V5.3.1 or newer
 - Supported readers: GR7.13xx, GR7.23xx, GR7.73xx, GAT SR 73xx, GAT SLR 73xx
 - GAT DC 7200 Mobile Credential license must be installed
 - A valid configuration (VCP) must be loaded in the reader
 - The appropriate ECP frame must be entered in the GAT DC 7200
 - The settings for Google Wallet or Apple Wallet must be configured in the data carrier settings.
 - The mobile device must support Mobile Credentials and NFC.
 - The system must be operated in countries where Apple and Google Wallet support is available.
- Current information for Apple Wallet can be found on Apple Support. Information for Google Wallet is available on Google Support.

Link to Apple Wallet information:



<https://support.apple.com/en-mk/102775>

Link to Google Wallet information:



<https://support.google.com/wallet/answer/12060037?hl=en#zippy=%2Cuse-google-wallet-for-payments-and-storing-passes>

In chapter "6.5. Configuring Mobile Credential" you will find detailed instructions for activating and configuring Mobile Credential.

3 INSTALLATION

This chapter describes the process required to install the GAT DC 7200. This includes the possible installation locations and what to consider during installation.

NOTICE

Risk of damage or failure to the GAT DC 7200

- Read the information in this section carefully before installing the GAT DC 7200.
- Install the GAT DC 7200 in a dry place, protected from rain and dripping water.
- Carefully observe the installation diagrams.
- Use the correct tools to install the GAT DC 7200.

3.1 Target group

This chapter provides information for technicians who install the GAT DC 7200 door controller. Experience in mechanical work and basic electrical knowledge is required. Previous knowledge of the GAT DC 7200 or GANTNER access systems is not required.

3.2 System overview

The GAT DC 7200 can control one or more doors, and one or more readers can be connected. In addition, the GAT DC 7200 must be connected to an Ethernet network and requires a power supply for operation. Additional devices such as electronic door openers and door contacts can also be connected. These connections and the cabling required must be considered when selecting the installation location.

The following figure shows an example installation.

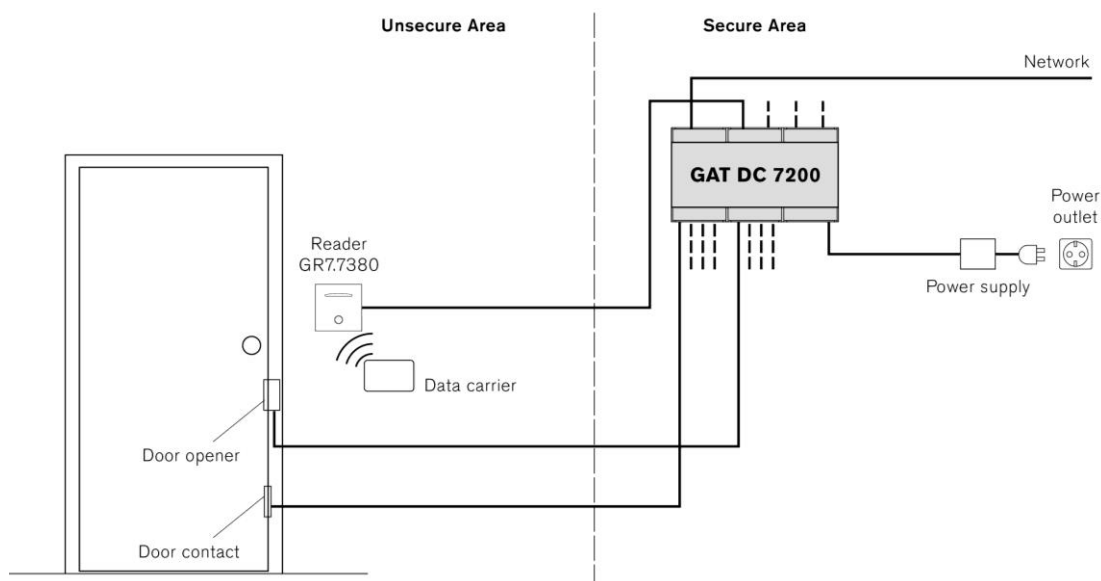


Figure 3.1 – System overview

3.3 Installation instructions

The GAT DC 7200 is designed to mount onto a DIN rail (top hat type) e.g., in a server cabinet. The GAT DC 7200 attaches to the DIN rail as shown in the following diagram.

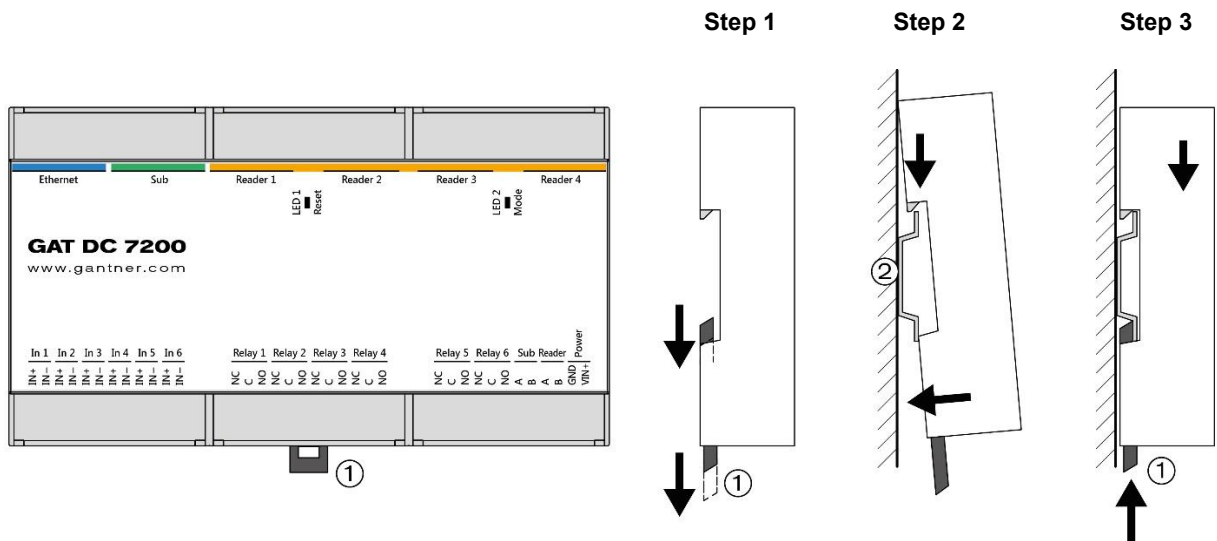


Figure 3.2 – DIN rail mounting

- ▶ Pull the DIN rail locking lever (1) down and hold it in this position.
- ▶ Attach the top of the GAT DC 7200 onto the DIN rail (2) then swing the bottom of the unit forwards.
- ▶ Push the DIN rail locking latch (1) upwards until the tab of the latch engages in the DIN rail.
 - The tab of the locking latch locks into the DIN rail.
- ▶ Ensure that the GAT DC 7200 is held securely.

Alternatively, it is possible to mount the GAT DC 7200 onto a wall using two screws.

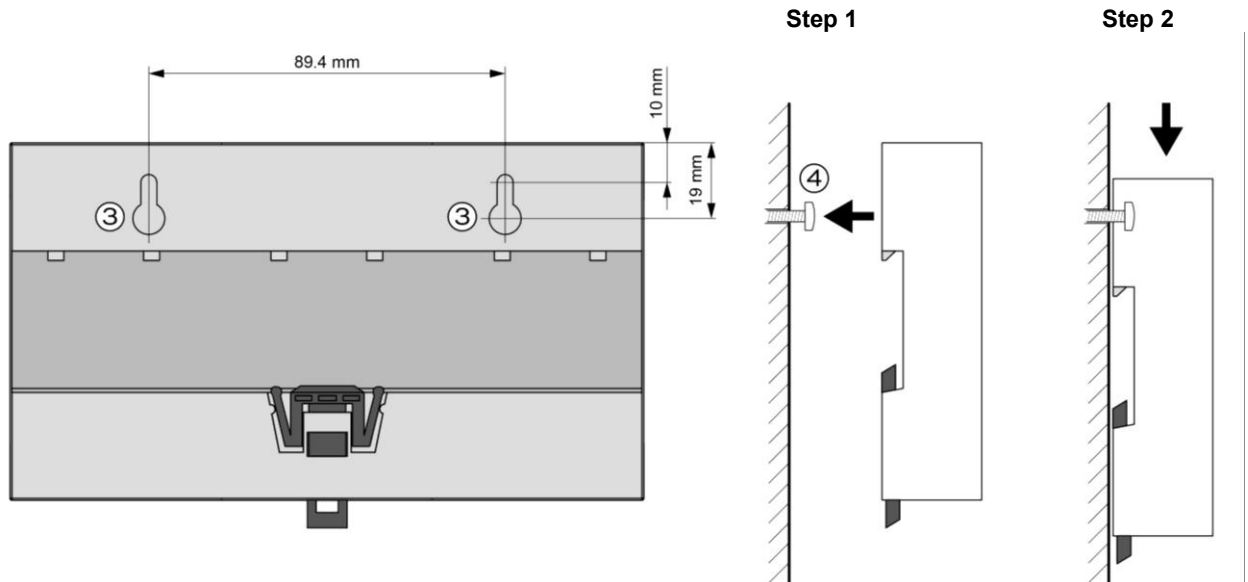


Figure 3.3 – Wall mounting with two screws

- ▶ Mark the two mounting holes (3) onto the wall (horizontal orientation, 89.4 mm apart).
- ▶ Drill the mounting holes to the correct depth.
NOTE! Depending on the wall material, use a suitable drill as well as screws and dowels (if necessary) so that the GAT DC 7200 is held securely. The GAT DC 7200 weighs approximately 210 g.
- ▶ Fasten the screws until approximately 5 mm protrudes from the wall.
- ▶ Attach the GAT DC 7200 onto the screws then push down so that the screw heads lock into the top of the mounting holes.
- ▶ Ensure that the GAT DC 7200 is held securely.

4 ELECTRICAL CONNECTIONS

This chapter describes how to complete the network, power supply, reader, and peripheral device cabling connections.

⚠ CAUTION



Electric Shock

- ➔ *Touching the power cables may result in electrical shock.*
 - *Electrical connections may only be performed by the specified target group.*
 - *Always follow the instructions described in this chapter.*
-

NOTICE

Damage to or malfunction of the GAT DC 7200

- *Read the information in this chapter carefully before connecting the GAT DC 7200.*
 - *Complete the cabling connection in the order and at the terminals/connectors described.*
-

4.1 Target group

This chapter contains information for personnel completing the GAT DC 7200 electrical connections. Observe the legal requirements for electrical installations where the GAT DC 7200 is being installed, e.g., electrical connection only by suitably trained electrician, material specifications, and tools used. Also observe the spatial and climatic operating conditions of the GAT DC 7200.

4.2 Network connection

An Ethernet connection is necessary for configuration and communication with the higher-level access control system. The GAT DC 7200 provides a 10/100 MBit interface via an RJ45 socket.

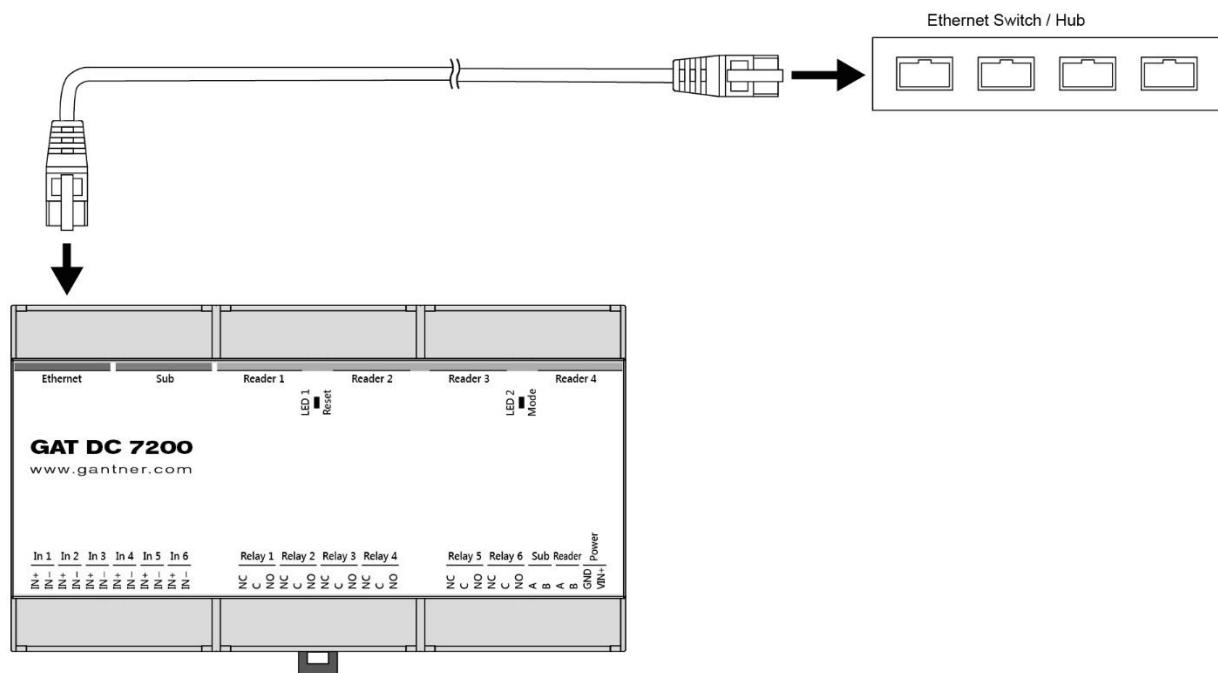


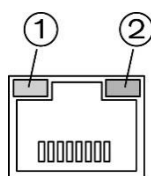
Figure 4.1 – GAT DC 7200 Ethernet connection

Observe the following important points for the Ethernet connection.

- Cable type: min. CAT 5 (STP)
- Cable length: max. 100 m (according to Ethernet standard)
- Cable connector: RJ45
- Connects to network hub or switch

4.2.1 Status display

There are two LEDs on the RJ45 socket of the Ethernet interface that signal the following information.



LED	Status	Meaning
orange (1)	on	100 MBit
	off	10 MBit
green (2)	flashing	Connection (link) and communication active
	off	Connection and communication not active

Table 4.1 – LED signaling – Ethernet interface

4.3 Reader connection

The following latest generation of GANTNER RFID readers and devices can connect to the GAT DC 7200:

- GR7.1300
- GR7.1310
- GR7.2300
- GR7.2310
- GR7b.2300
- GR7b.2310
- GR7.7380
- GAT DL 091 and WiNET components

GANTNER's previous generation of RFID readers can also connect to the GAT DC 7200:

- GAT SR 73xx
- GAT SLR 73xx
- GAT SR 3xx
- GAT SLR 3xx

NOTE! The GAT S(L)R 3xx readers do not support the CardNET function (see chapter "9.17 CardNET").



Only the connections for the latest generation of devices are contained in this manual. Please refer to the respective documentation for instructions on connecting the GAT S(L)R 73xx readers to the GAT DC 7200.

Communication with the readers occurs via a serial RS-485 interface.

The readers connect to the connectors labelled "Reader". Depending on the type of reader cable, connection to the four RJ45 sockets labelled "Reader 1" ... "Reader 4" or the "Reader" screw terminal is possible.

NOTE! The GAT DL 091 can also be connected to the "Sub" interface. This is the preferred connection type for the GAT DL 091. Read section "4.4. Access point GAT DL 091" for more information.

Connecting to the RJ45 sockets has the advantage of the Plug&Play PLUS function. The controller automatically recognizes the connected readers and assigns the "Reader 1" reader to door 1, the "Reader 2" reader to door 2, etc. This function allows a reader to be exchanged without needing to change the configuration.

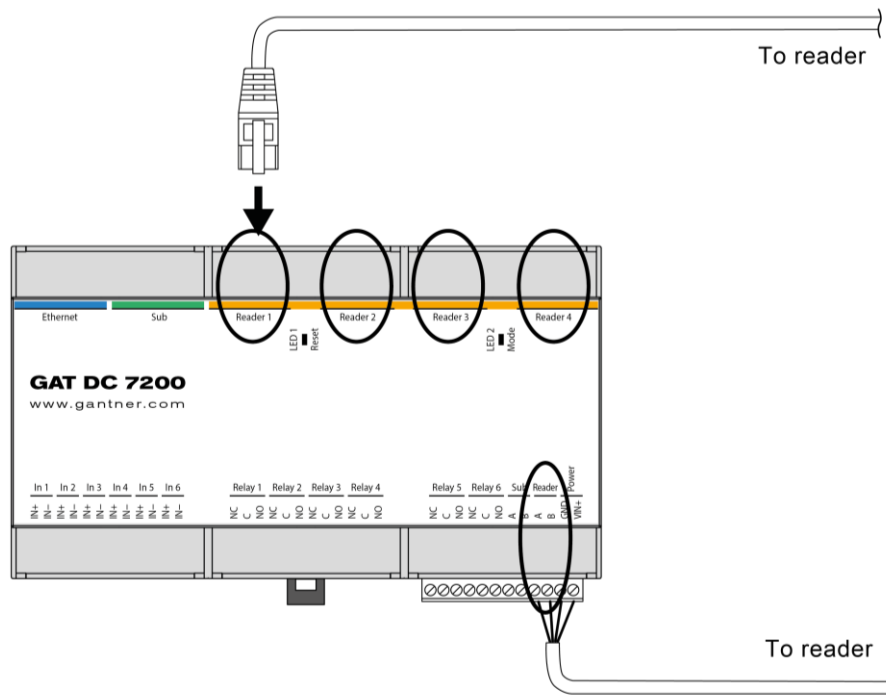


Figure 4.2 – Reader connection

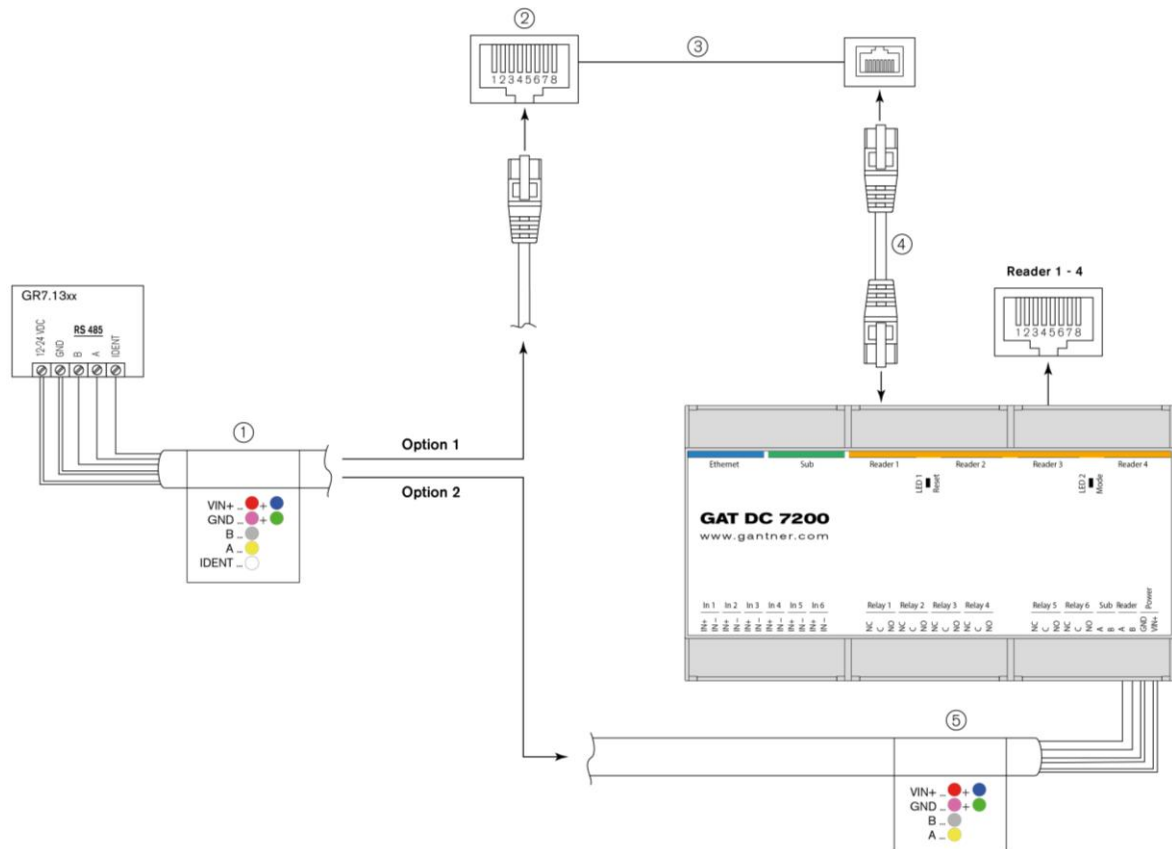
A total of 4 readers, or max. 16 with an additional expansion license, can connect to one GAT DC 7200. It is possible to use, e.g., a Y adapter to connect multiple readers to one socket.

Power is supplied to the readers by the GAT DC 7200, or alternatively, by a separate power supply. For the RJ45 sockets, voltage is supplied at the socket. The voltage can be switched individually at each socket and the sockets are individually protected against overload and short circuiting. Note that the total current per RJ45 socket must not exceed 1 A. In addition, the total power drawn from all RJ45 sockets of the GAT DC 7200 must not exceed 40 VA.

When connecting to the "Reader" screw terminal, you can draw power from the GAT DC 7200 to supply the reader or supply power via a separate power supply. The following chapters show how to connect the GR7 readers to the RJ45 sockets and screw terminals.

i Please note that when a reader is connected to the screw terminals, the IDENT line of the reader cannot be used thereby making the Plug&Play function unavailable.

4.3.1 Example connection: GR7.13xx to GAT DC 7200



1...Supplied connection cable (Part No. 1104997). PIN assignment and wire colors:

PIN	Wire color	Signal
1	white	IDENT
2	-	-
3	green	GND
4	yellow	A
5	gray	B
6	pink	GND
7	blue	+VIN (DC 12-24 V)
8	red	+VIN (DC 12-24 V)

NOTE!

- Cut the brown wire off.
- The GR7.1xxx Cable Set 3 m (Part No. 1106193) is available as an option.

Connection option 1

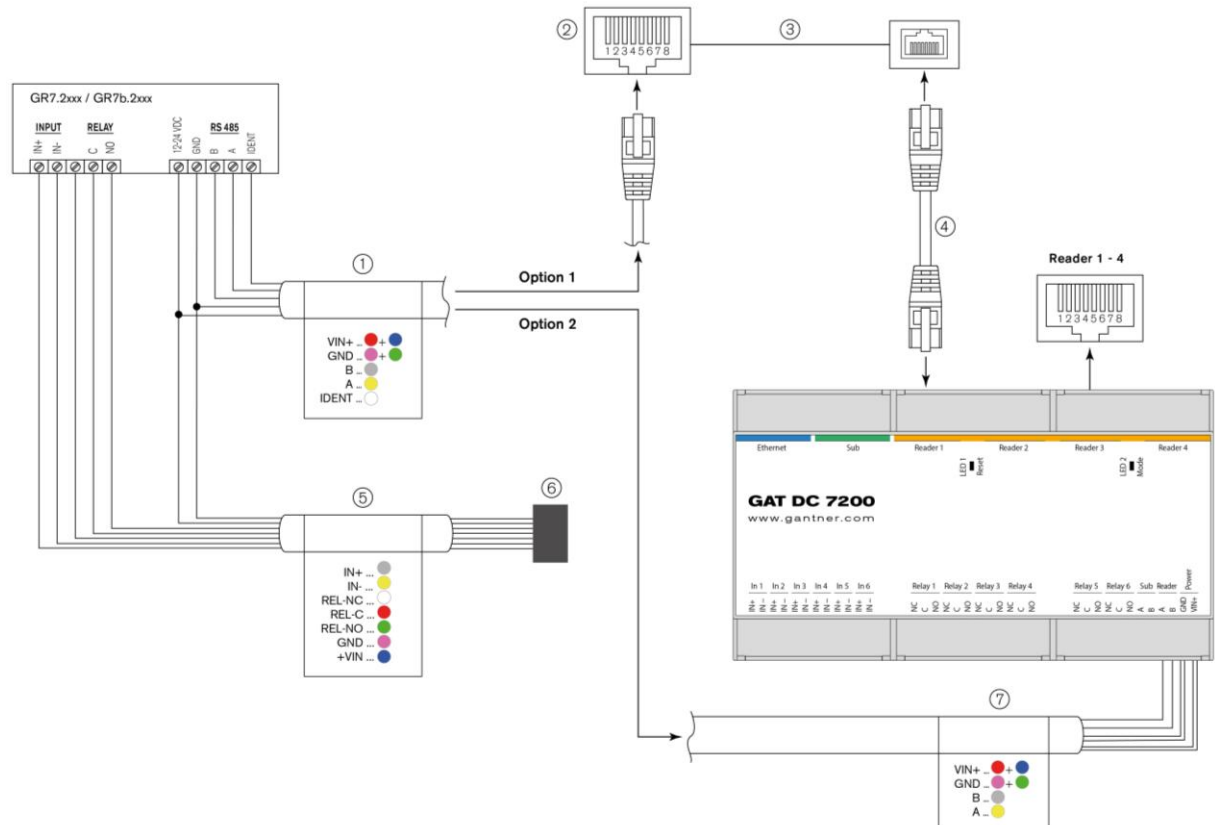
- 2...RJ45 plug
- 3...Structured cabling
- 4...Patch cable

Connection option 2

- 5...Connection via terminals. For this option, the IDENT wire is not used.

Figure 4.3 – Connection of a GR7.13xx to a GAT DC 7200

4.3.2 Example connection: GR7.23xx / GR7b.23xx to GAT DC 7200



1...Supplied connection cable (Part No. 1104994). PIN assignment and wire colors:

PIN	Wire color	Signal
1	white	IDENT
2	-	-
3	green	GND
4	yellow	A
5	gray	B
6	pink	GND
7	blue	+VIN (DC 12-24 V)
8	red	+VIN (DC 12-24 V)

NOTE!

- Cut the brown wire off.
- The GR7.2xxx Cable Set 3 m (Part No. 1106194) is available as an option.

Connection option 1

2...RJ45 plug

3...Structured cabling

4...Patch cable

5...Supplied connection cable (Part No. 1104995). PIN assignment and wire colors:

PIN	Wire color	Signal
1	gray	IN +
2	yellow	IN -
3	white	REL NC
4	red	REL C
5	green	REL NO
6	pink	GND
7	blue	+VIN (DC 12-24 V)
8	-	-

NOTE!

Cut the brown wire off.

6...Connector **NOTE!** A second connector (type F) and a joiner between the two connectors are included in the installation material to enable easy cabling.

Connection option 2

7...Connection via terminals. For this option, the IDENT wire is not used.

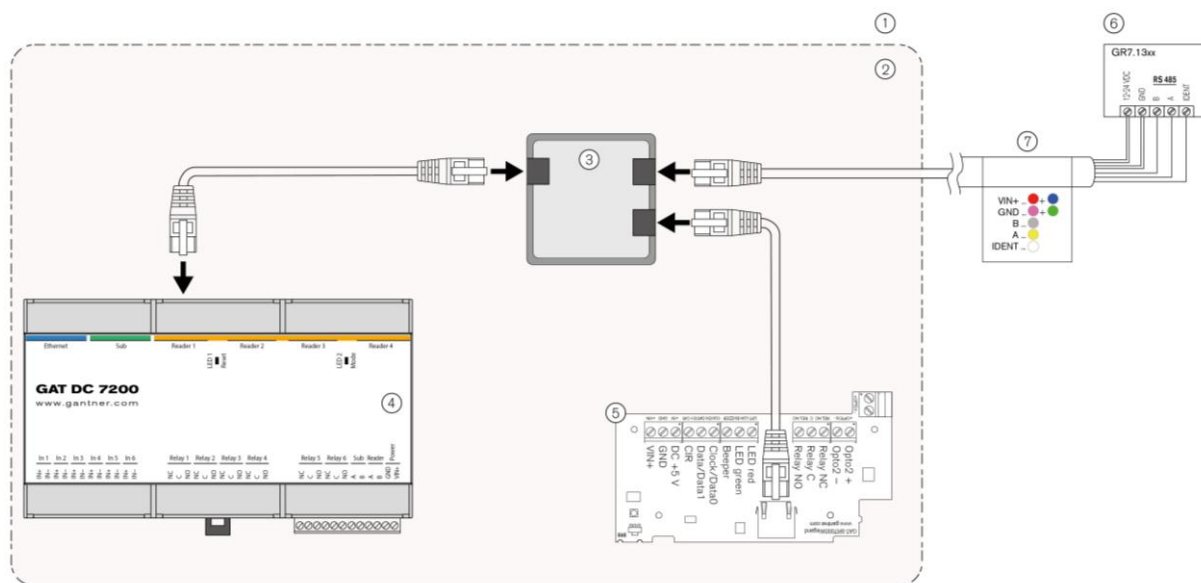
Figure 4.4 – Connection of a GR7.23xx / GR7b.23xx to a GAT DC 7200

NOTE! GR7.x3xx readers may only be connected to the RJ45 sockets labelled “Reader 1” to “Reader 4” or the “Reader” screw terminals as described. Never use the connections labelled “Sub” or “Ethernet”.

4.3.3 Example connection: GR7.13xx and GAT SR 7000 Wiegand to a door

Especially for existing RS-485 cabling, it can be advantageous for systems converting to the GAT DC 7200 that an RS-485 interface is used from the door to the controller with no additional cabling required for controller control signals. In such a case, an RJ45 splitter can be used near the door.

Both the RFID reader (GR7.13xx) and the I/O module (GAT SR 7000 Wiegand), which is mounted indoors, are connected to this splitter as shown in the figure below. The door control and monitoring then takes place from the secured indoor area and only the RFID reader is in the unprotected outdoor area.



1. .. Secure area
2. .. Unsecure area
3. .. RJ45 splitter
4. .. GAT DC 7200
5. .. GAT SR 7000 Wiegand
6. .. GR7.13xx
7. .. Supplied connection cable (Part No. 1104997). PIN assignment and wire colors:

PIN	Wire color	Signal
1	white	IDENT
2	-	-
3	green	GND
4	yellow	A
5	gray	B
6	pink	GND
7	blue	+VIN (DC 12-24 V)
8	red	+VIN (DC 12-24 V)

NOTE!

- Cut the brown wire off.
- The GR7.1xxx Cable Set 3 m (Part No. 1106193) is available as an option.

Figure 4.5 – RJ45 splitter for RFID reader and I/O module connection

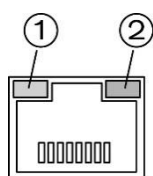
NOTE! For this type of installation, it is important that the following requirements are met:

- In the GAT DC 7200 web interface, the "automatic reader assignment" function (found via "Configuration" > "Readers" > "Auto assign reader ID to reader port number") must be deactivated for the general reader configuration.
- In GAT Matrix, two door licenses are required (one for the GR7.x3xx and one for the GAT SR 7000 Wiegand). Two doors are also required in the GAT DC 7200 for the components.

If structured cabling cannot be used, the RS-485 line can also be connected to the GAT DC 7200 via the "Reader A and B" screw terminals. An RJ45 plug must be terminated on the cable end that connects to the GAT SR 7000 Wiegand. The pin assignment for the RJ45 plug is as shown in chapter "4.3.1 Example connection: GR7.13xx to GAT DC 7200".

4.3.4 Status display

There are 2 LEDs on the RJ45 socket of the reader interface that signal the following information.



LED	Status	Meaning
orange (1)	on	Power supply for connected reader OK
	off	Power supply disabled or fault
green (2)	flashing	Communication to the connected reader OK (only with connected IDENT cable and devices that support Plug&Play PLUS)
	off	No communication (or IDENT line is not connected, or Plug&Play PLUS is not supported by the connected device)

Table 4.2 – LED signaling – Reader interface

4.3.5 Automatic reader identification (IDENT)

The GR7 series readers have an IDENT line for Plug&Play PLUS commissioning, which provides automatic reader allocation for readers connected to the RJ45 sockets of the GAT DC 7200. The connected readers are automatically identified and assigned to the doors with the same number as the reader connection (reader 1 at door 1, reader 2 at door 2, etc.).

Alternatively, an automatic reader search can be performed for GR7 readers or when more than 4 readers are used with a GAT DC 7200. The readers can be assigned manually to doors 1 to 16. Readers found during the search are inserted with the correct type in the configuration settings. A detailed description of configuring readers with the GAT DC 7200 is available in the GAT ACE configuration software manual.

NOTE! GAT SR 3xx and GAT SLR 3xx series readers do not support the Plug&Play PLUS function and must be manually configured.

4.3.6 Manipulation alarm

The GAT DC 7200 automatically detects when a reader is disconnected during operation and triggers a manipulation alarm for the relevant door (reader) when this occurs. Possible causes can include the severing of the cable or a communication interruption. The manipulation alarm is recorded internally as a booking and, when a relay of the GAT DC 7200 is configured for the manipulation alarm, the relay is activated.

4.3.7 Relay outputs and optocoupler inputs

Some readers (e.g., GR7.23xx) have a relay output and a potential-free optocoupler input. The function and timing of these inputs and outputs can be freely configured when connected to the GAT DC 7200.

NOTE! Unprotected inputs/outputs. Please note that the relay output and optocoupler input of these readers are unprotected when the housing is opened without authorization. Therefore, do not connect any security-critical elements to these terminals. For example, you can use the relay output to control a closing grid or lighting element that can be switched on/off via timing or identification operation.



A detailed description of all possible functions is available in the operating manual of the GAT ACE configuration software from GANTNER Electronic GmbH. Please also observe the information in the GR7.x3xx datasheet.

4.4 Access point GAT DL 091

The GAT DL 091 WiNET Access Point can be connected to the “Sub” or “Reader” ports. Connecting the GAT DL 091 to either of these ports allows the cable length or communication to be optimized.

i Up to four GAT DL 091 WiNET Access Points can be connected to a GAT DC 7200.

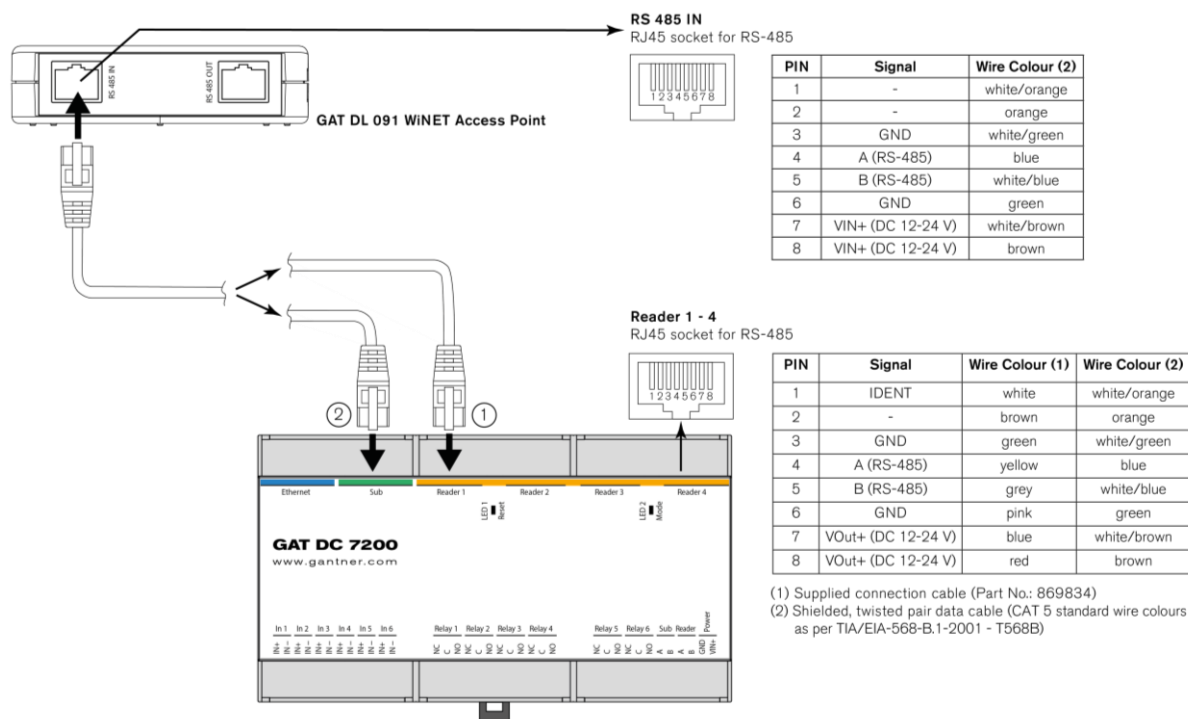


Figure 4.6 – GAT DL 091 Access Point connection to the GAT DC 7200

As an alternative, the GAT DL 091 can also be connected to the “A” and “B” screw terminals of the “Sub” or “Reader” terminals. As an example, the connection to the “Reader” terminal is shown below.

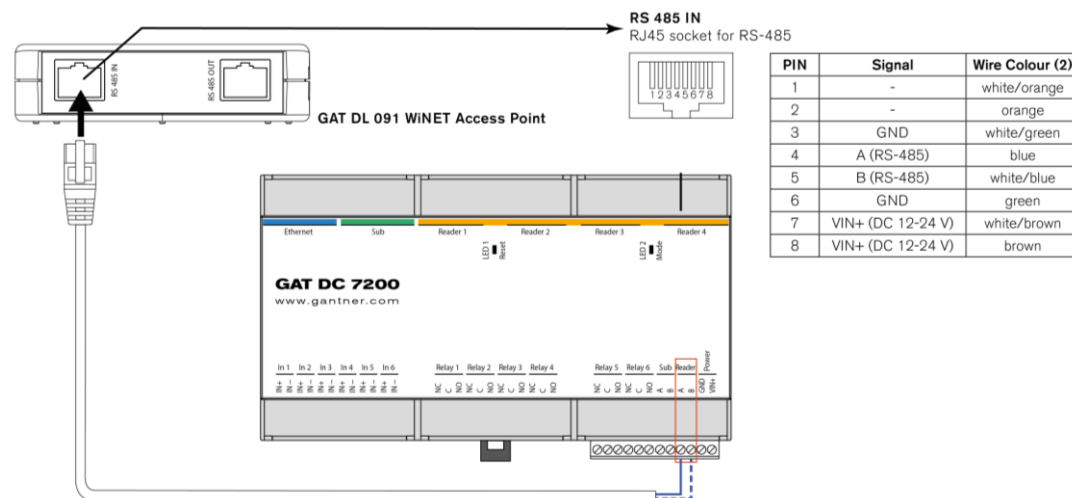


Figure 4.7 – GAT DL 091 Access Point alternative connection to the GAT DC 7200

Communication interruptions can occur if the GAT DL 091 Access Point is used with an RS-485 cable length >100 m. As a solution, a terminating resistor (220 Ohm), which is included with the device, is connected to the DC 7200.

- To check whether the resistor is required, go to "Maintenance" > "Inputs/Outputs" in the GAT DC 7200 web interface.

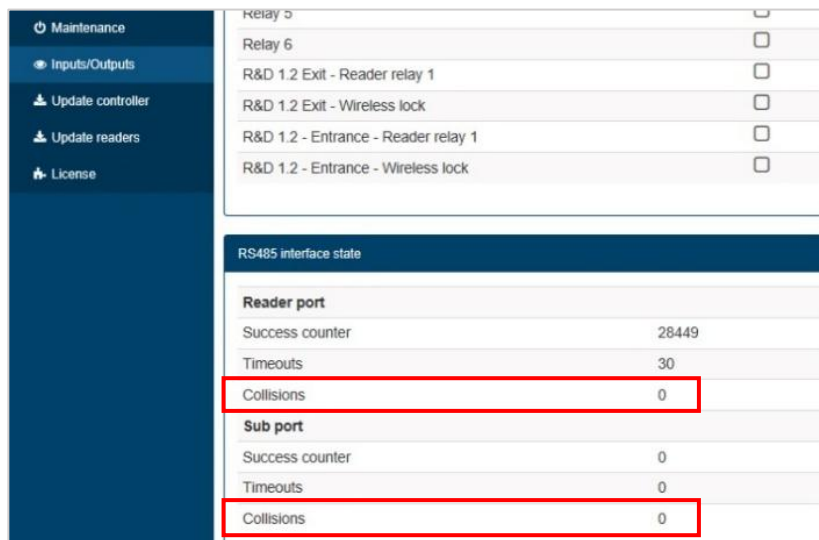


Figure 4.8 – Indication of RS-485 interface state

- The value in the "Collisions" column of the port where the GAT DL 091 is connected should be 0. If not 0, connect the resistor (1) to the screw terminals "A" and "B" of the same interface type ("Sub" or "Reader") to which the GAT DL 091 is connected. The following example shows the connection to the "Sub" interface. **NOTE!** Even if multiple GAT DL 091 access points are used (up to four are supported), only one resistor may be used.

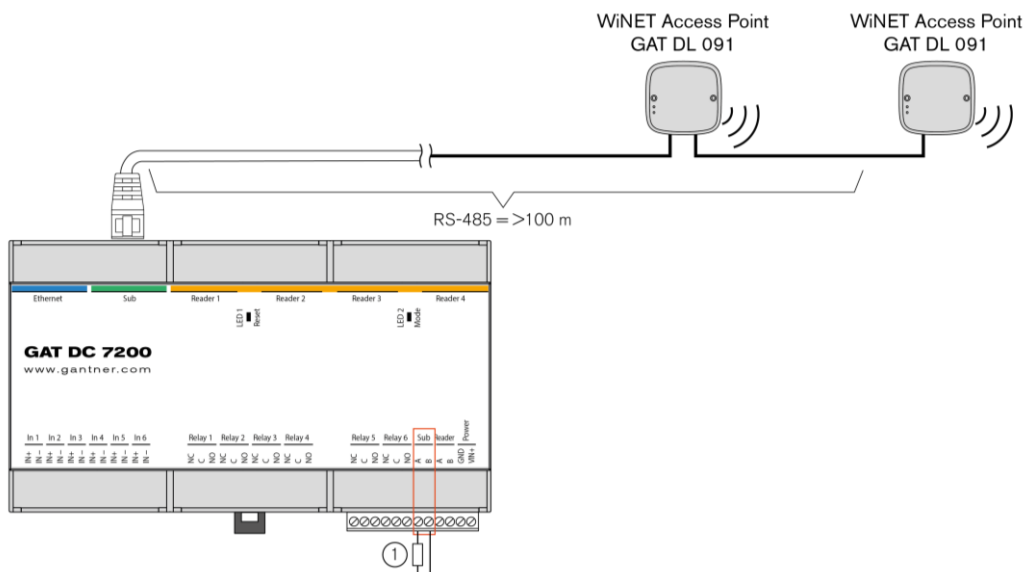


Figure 4.9 – Resistor connection on the GAT DL 091 to improve signal (example shows the usage of the "Sub" interface).

4.5 Peripheral devices

The connection of peripheral devices for the expansion of controller functionality is done at the "Sub" interface. For example, relay expanders could be connected here to increase the number of signal inputs and relay outputs and thus implement lift controls.

Peripheral devices can connect either via the RJ45 socket or the screw terminals. The current drawn from the RJ45 "Sub" socket must not exceed 1 A. In addition, the total power drawn from all RJ45 sockets of the GAT DC 7200 must not exceed 40 VA.



GAT DIRECT. Connect can only use peripheral devices if they are used as inputs and outputs for standard door functions. Use as an elevator or locker controller is not supported.

4.5.1 Expander GAT IO 7054 / GAT IO 7055 connection

With a GAT IO 7054 and GAT IO 7055, the number of status inputs and outputs of a GAT DC 7200 can be extended. This makes it possible to control more than six outputs with one door controller, e.g., for the selective activation of individual floors in lift control systems, and also to receive and process more than six status signals.

Up to eight GAT IO 705x can be connected to a GAT DC 7200. The mixed operation of GAT IO 7054 and 7055 expanders is possible.



For the GAT IO 7054 and GAT IO 7055 connection, only the most important instructions for connection to the GAT DC 7200 are provided here. Please also read the documentation of these devices.

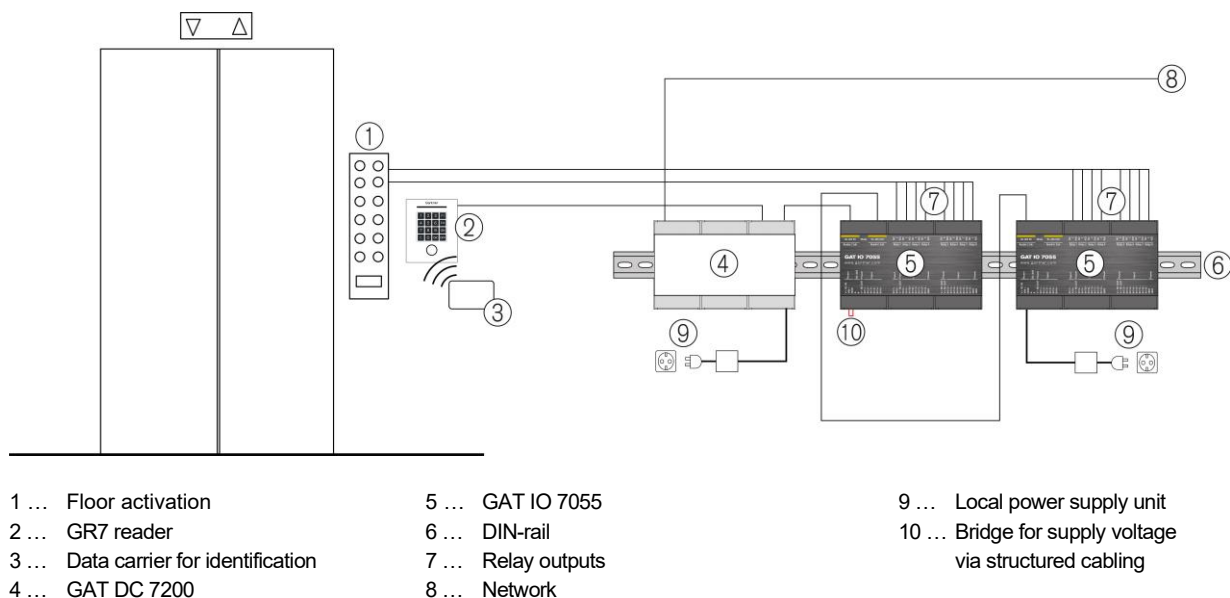
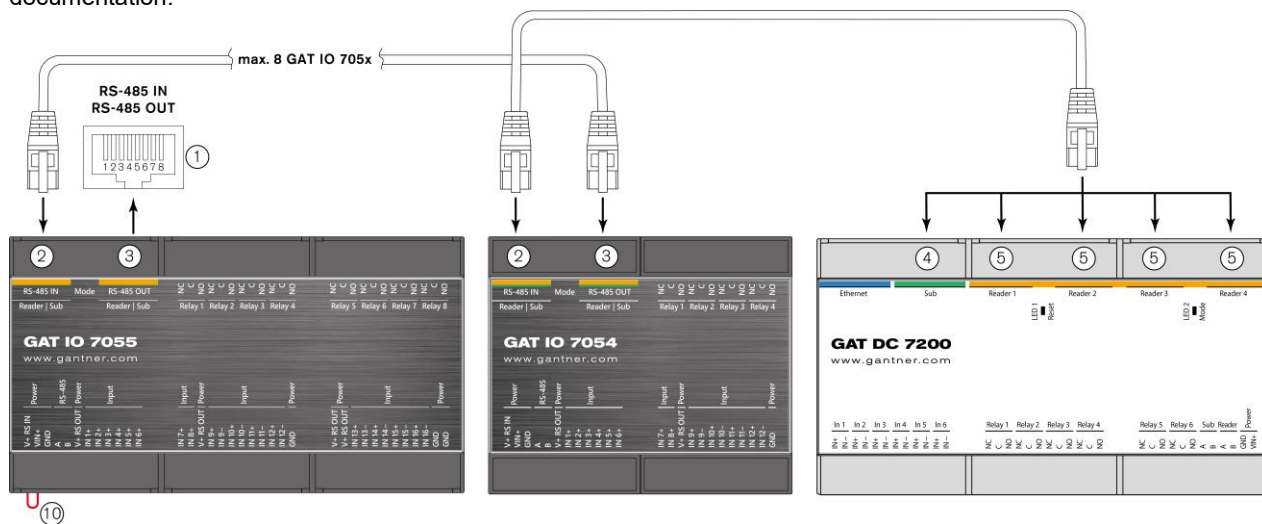


Figure 4.10 – Application example

A GAT IO 705x is connected to a GAT DC 7200 via RS-485 interface. Power can be supplied via the structured cabling (RS-485 interface) or via a separate power supply unit. If power is supplied via structured cabling, the wire bridge (10) must be inserted. It is recommended to use min. CAT. 5 cabling with supply via two wire pairs.

The following figure shows the connection of the GAT IO 705x. Also read the instructions in the GAT IO 705x documentation.



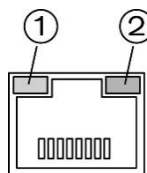
- 1 ... RJ45 socket of the RS-485 interface
- 2 ... GAT IO 705x: RS-485 IN
- 3 ... GAT IO 705x: RS-485 OUT
- 4 ... GAT DC 7200: "Sub" socket
- 5 ... GAT DC 7200: "Reader x" socket
- 10 ... Bridge for supply voltage via structured cabling

Figure 4.11 – Connecting a GAT IO 7054 and 7055 to the GAT DC 7200

The relay output and optocoupler input connections for the GAT IO 705x expanders is completed in a similar way to the GAT DC 7200 connections (see "4.6 Relay outputs and optocoupler inputs").

4.5.2 Status display

The two LEDs on the RJ45 socket of the "Sub" interface indicate the following information.



LED	Status	Meaning
orange (1)	on	Power supply for connected device OK
	off	Power supply disabled or fault
green (2)	flashing	Communication to the connected device OK (only with connected IDENT cable and devices that support Plug&Play PLUS)
	off	No communication (or IDENT line is not connected, or Plug&Play PLUS is not supported by the connected device)

Table 4.3 – LED signaling – Sub interface

4.6 Relay outputs and optocoupler inputs

The GAT DC 7200 is equipped with six relay outputs and six potential-free optocoupler inputs. The function and timing of these inputs and outputs can be freely configured.

A common application of the relay outputs is the activation of the unlocking relay of a monitored door. Following valid identification and access authorization, the applicable relay is activated for the configured time thereby unlocking the electronic door lock.

The optocoupler inputs serve as digital status inputs, e.g., to detect door states or to enable a button release. The function and timing of these digital inputs can also be individually configured.

i A detailed description of all possible functions is available in the operating manual of GANTNER's GAT ACE 7000 configuration software.

The following figure shows the connection of an electronic door opener and a door feedback input.

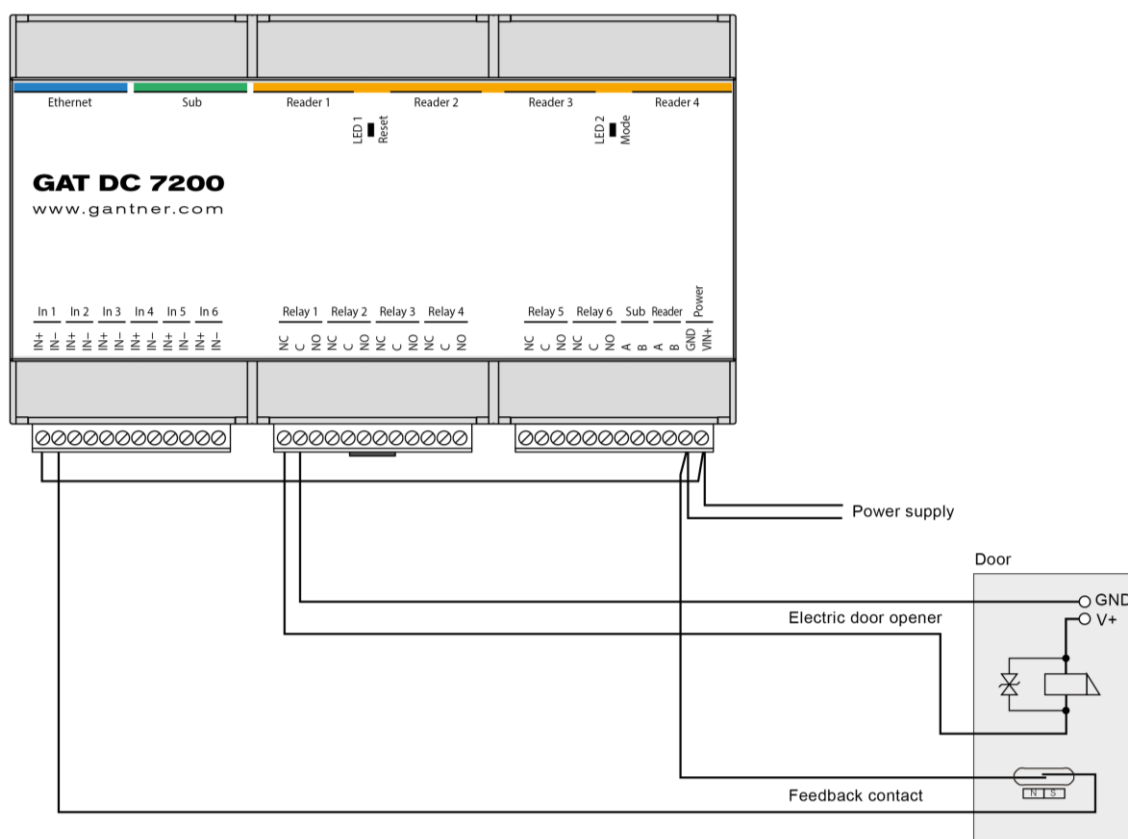


Figure 4.12 – Connection of the relay outputs and optocoupler inputs

The voltage for the optocoupler inputs can, e.g., be supplied by the GAT DC 7200 door controller or by an external source. Observe the permitted voltage and current values (see "10 TECHNICAL DATA"). The voltage for the relay outputs must be supplied by an external source.

4.7 Power supply

⚠ WARNING! Electrical Shock. Never touch mains voltage and always use an LPS (Limited Power Source) power supply with the appropriate specifications (see "10 TECHNICAL DATA").

The GAT DC 7200 requires a DC power supply. The permissible voltage range is 10 - 28 V and the nominal voltage 12 and 24 V. Only use one LPS (Limited Power Source) power supply unit for the voltage supply of the GAT DC 7200.

The power consumption of the GAT DC 7200 without connected devices is less than 5 VA. For dimensioning of the voltage supply, all connected devices must be considered. The applicable data for these devices can be found in the respective datasheets.

- Connect the supply lines to the VIN+ and GND screw terminals of the GAT DC 7200 "Power" terminal.

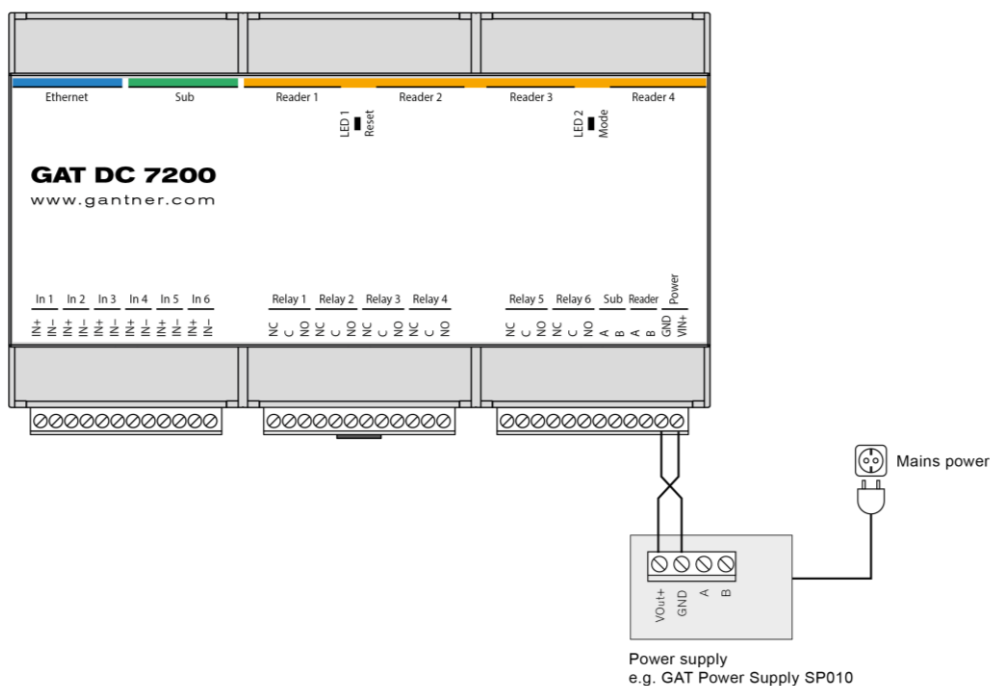


Figure 4.13 – Connection of the power supply

- Ensure that all additional cabling (Ethernet, reader, peripheral, etc.) is connected to the GAT DC 7200.
- Plug the mains cable of the power supply into the power outlet.
 - If mains power is switched on, the GAT DC 7200 starts up. Depending on the configuration, the start-up process takes about 10 to 20 seconds until the door controller and the readers are ready for use.

5 CONTROLS AND SIGNALIZATION

5.1 General

The GAT DC 7200 door controller operates with the predefined configuration and authorization data and waits for an identification request at a connected reader or signal from a digital input. For the selection of functions or the input of PIN codes, readers with a keypad can be connected.

Status information is displayed by the GAT DC 7200 via acoustic signals and LEDs. If required, the GAT DC 7200 can be restarted, the password and network settings can be reset, or the GAT DC 7200 can be reset to the default settings via a button.

5.2 Target group

This chapter provides information for service technicians responsible for maintaining the GAT DC 7200 system. This information is not intended for users of the access system.

5.3 Restart

This function can help if the GAT DC 7200 is not responding. When restarting, the GAT DC 7200 is idle for approximately 20 seconds until it restarts. All data and settings in the GAT DC 7200 are retained during the restart.

The reset button is located on the RJ45 socket side of the housing.

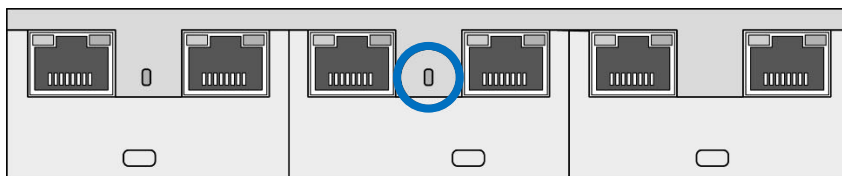


Figure 5.1 – Button for restarting the GAT DC 7200

- ▶ Insert a thin (not sharp) object into the hole shown in the figure above.
- ▶ Press the button in briefly and then release.
 - The GAT DC 7200 emits a short tone and restarts. This process takes approximately 10 to 20 seconds before the GAT DC 7200 is ready for use again.

5.4 Reset configuration password and network settings

If the password used for configuring the GAT DC 7200 via the web interface is forgotten, or if the network settings are incorrect, this information can be reset to the default settings. No other data apart from the network settings and password will be deleted from the GAT DC 7200.

The reset button is located on the RJ45 socket side of the housing.

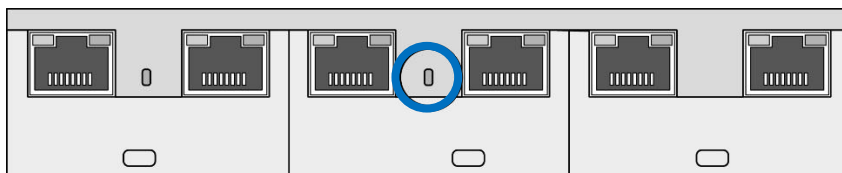


Figure 5.2 – Button for resetting the password and network settings

- ▶ Insert a thin, but not sharp, object into the hole shown in the figure above.
- ▶ Press the button in for 5 seconds until 2 beeps are heard.
- ▶ Release the button then briefly press it again to confirm.
 - The password and network settings are reset and the GAT DC 7200 restarts.
 - If this process has not worked, one low beep is emitted.

5.5 Restart and reset to default settings

This function can help if the GAT DC 7200 is unresponsive or not configured correctly. When resetting to the default settings, all the configuration data, bookings, schedules, etc., are deleted from the GAT DC 7200 and set to the values at the time of delivery. The configuration and authorization data must be recreated or uploaded after the reset.

NOTE! Save all required bookings and data before resetting the GAT DC 7200 to the default settings.

The reset button is located on the RJ45 socket side of the housing.

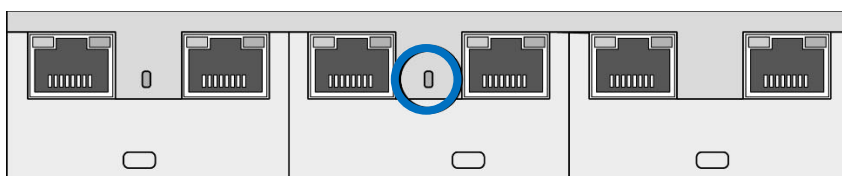


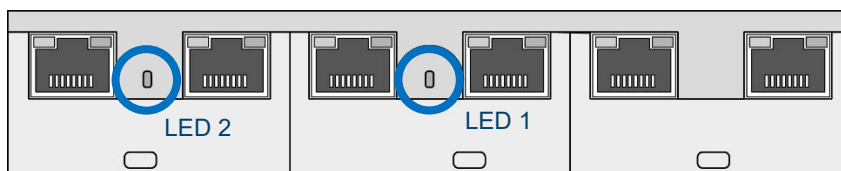
Figure 5.3 – Button for resetting the GAT DC 7200 to the default settings

- ▶ Insert a thin, but not sharp, object into the hole shown in the figure above.
- ▶ Press the button in for 10 seconds until three beeps are heard.
- ▶ Release the button then briefly press it again to confirm.
 - The data in the GAT DC 7200 is deleted and the controller restarts with the default settings.
 - If this process has not worked, one low beep is emitted.

5.6 Signaling overview

The GAT DC 7200 has two LEDs for displaying status information and operating states. The following table shows the meaning of the signaling.

General

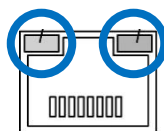


LED	Signal		Meaning
LED 1	green		Connect to host software OK
	red		No connection to host software
	flashing red/green		Bootloader mode
LED 2	blue		Reserved for future use

Table 5.1 - Overview of general LED signaling

RS-485 interface (RJ45 socket) for readers and peripherals

LED orange LED green

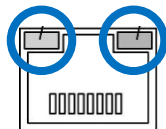


LED	Signal		Meaning
LED Orange	orange		Power supply for connected device OK
	off		Power supply disabled or fault
LED Green	flashing green		Communication to the connected device OK (only with devices that support Plug&Play PLUS)
	off		No communication or Plug&Play PLUS not supported by the connected device

Table 5.2 - LED signaling on the RJ45 sockets of the reader and peripheral interfaces

Ethernet interface (RJ45 socket)

LED orange LED green



LED	Signal		Meaning
LED Orange	orange		100 MBit connection
	off		10 MBit connection
LED Green	flashing green		Link and communication active

Table 5.3 - LED signaling on the RJ45 socket of the Ethernet interface

6 START-UP AND CONFIGURATION

In order to commission the GAT DC 7200 after installation, the device settings must be configured over the network via the web interface. The information required to configure the GAT DC 7200 is provided in this chapter.

The configuration contains the functional settings of the door controller. This includes, e.g., the delay settings for unlocking, max. allowed openings, the functional settings for the digital inputs and outputs, the settings for the connected readers (type, RFID technology, data format, etc.), and the alarm system and threat PIN code settings.

The authorization of system users for online-mode is not part of the configuration process as this is defined in the access control software, e.g., Matrix. The permission configuration for standalone mode can be found in chapter "8. STANDALONE MODE".

6.1 Target group

This chapter provides information for technicians who configure the GAT DC 7200 and put the device into operation. A base knowledge of electronics is assumed. It is also recommended to participate in a GANTNER training course on the access control system.

6.2 Switching on the power supply

- ▶ Ensure that all the required cabling (Ethernet, reader, peripheral, etc.) is correctly connected to the GAT DC 7200 as described in chapter "4 ELECTRICAL CONNECTIONS".
- ▶ Plug the mains cable of the power supply into the power outlet.
 - If mains power is switched on, the GAT DC 7200 starts up. Depending on the configuration, the startup process takes about 10 to 20 seconds until the door controller is ready for use.

6.3 Startup

When the GAT DC 7200 is first switched on after delivery, the door controller is preconfigured with the default settings. This means:

- The connected readers and GAT IO 705x are detected and activated automatically. The Plug&Play PLUS function ensures that readers connected to the RJ45 sockets are automatically assigned to doors 1 to 4 according to their socket connection number (Reader 1 to Reader 4).
- The readers are configured to read the unique numbers of data carriers. Only the authorization data of persons must be defined in the access control software, allocated to the corresponding data carriers, and uploaded to the controller.
- For readers of the GAT SR/SLR 73xx and GR7 series, the RFID technologies LEGIC prime, LEGIC advant, ISO 14443A, and ISO 15693 are enabled.

- Relay output 1 is pre-defined as an unlocking relay for door 1 and optocoupler input 1 pre-defined as door feedback for door 1. This default setting also applies to doors 2, 3, and 4 with relay and optocoupler 2, 3, and 4 respectively.
- The time zone is set to UTC +01:00 and the switchover for European daylight-saving time is activated.
- DHCP is activated to automatically obtain an IP address on the network. The network name of the GAT DC 7200 is set to the following:
DC7x_nnnnnnnnnn
where nnnnnnnnnn is the serial number of the device. The serial number is found on the back of the GAT DC 7200 or on the packaging. This means that every device in the network can be addressed uniquely.
- The default port for communication with GAT ACE 7000 is port 8000 (this port can be parameterized in GAT DC 7200 and in GAT ACE 7000).
- The default ports for FTP are 20 and 21. From version 2.0 of the GAT ACE 7000 software onwards, FTP is no longer required.
- As of version 3.0 of the GAT DC 7200 firmware, the default web server port for accessing the GAT DC 7200 configuration page is port 443 (encrypted connection via TLS/SSL). For older versions without TLS/SSL, port 80 is used.
- The NTP port for time synchronization is 123 (UDP) outgoing.
- The default port for communication with GAT DIRECT.Connect is port 8239.

6.4 Configuration

Configuration of the GAT DC 7200 is done via an internet browser and web interface. Any current browser can be used on a computer as well as the mobile variant on, e.g., a smartphone or tablet. GANTNER Electronic GmbH recommends using the latest version of the Firefox or Chrome web browser for configuration.

i The configuration with the GAT ACE 7000 software is also done via the same web interface.

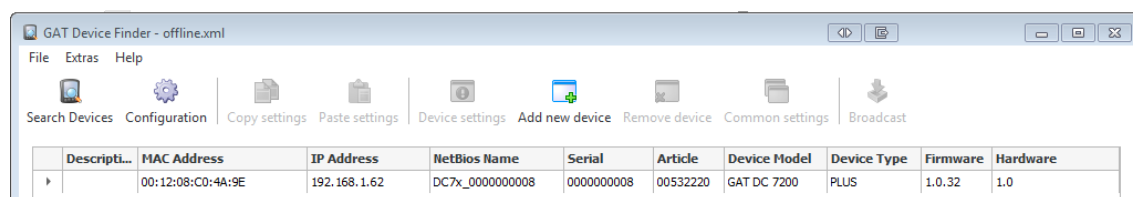
- Enter one of the following addresses into the web browser to open the web interface for configuring the GAT DC 7200. As of version 3.0 of the GAT DC 7200 firmware, the connection is encrypted via TLS/SSL by default (see the following section "6.4.1 Certificate configuration for TLS/SSL connection"):

`https://DC7x_nnnnnnnnnn` (where nnnnnnnnnn is the device serial number) or

`https://<IP-Address>` (where <IP-Address> is the IPv4 address of the GAT DC 7200 in the network)

Note: As of firmware version 3.0, a message is displayed in the browser when the page is called stating that it is not a secure connection if the certificate for the https connection has not yet been installed. You can skip this message to access the configuration page and install the certificate. For more information see "6.4.1 Certificate configuration for TLS/SSL connection".

i The GAT DC 7200 uses DHCP to automatically obtain an IP address from the network during startup. The IP address of the GAT DC 7200 can be found, e.g., using GANTNER's GAT Device Finder software.



Descripti...	MAC Address	IP Address	NetBios Name	Serial	Article	Device Model	Device Type	Firmware	Hardware
▶	00:12:08:C0:4A:9E	192.168.1.62	DC7x_0000000008	0000000008	00532220	GAT DC 7200	PLUS	1.0.32	1.0

- A login window opens.

- Enter your username and password into the login window to log into the GAT DC 7200.

NOTE! The default username and password are "admin" and "GAT" respectively. For security reasons, you must change the password to a secret password after the initial login (see "6.4.5 Users"). Ensure to store the password in a secure place (e.g., password manager).

- Click on "OK".
 - The main window with live view of the doors opens in the web interface (see Figure 6.11). Other web interface functions can be accessed via the menu.

NOTE! If there is no activity in the web interface for 15 minutes, the current user is automatically logged out to maintain security.

6.4.1 Certificate configuration for TLS/SSL connection

From version 3.0 of the GAT DC 7200, connecting to the GAT DC 7200 via the web interface is completed using TLS encryption by default. This encryption is also used for the communication with GAT ACE 7000 from version 2.0.0. Prior to this version, GAT ACE 7000 did not use TLS for communication with GAT DC 7200.

When the GAT DC 7200 configuration page is accessed on a PC for the first time, a message is displayed notifying that the page is unsecure.

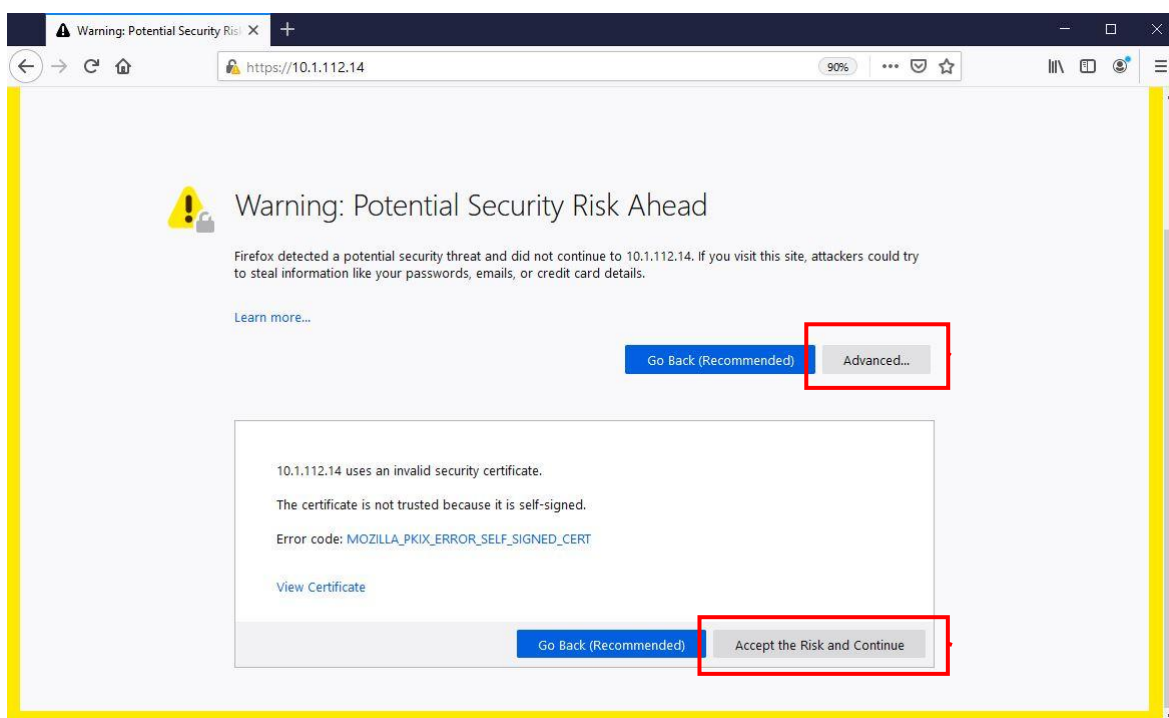


Figure 6.1 – SSL/TLS connection message

This message is displayed (Firefox browser shown) because no certificate has been installed yet on the PC to confirm the security of the configuration page. It is possible to issue a certificate yourself with the GAT DC 7200, which can be installed on the PC. Complete the following steps.

- ▶ If you are certain that the Internet address of the GAT DC 7200 has been entered correctly, select "Advanced ..." for this security message.
- ▶ Now select "Accept the Risk and Continue".
 - The connection to the GAT DC 7200 can be established. The login window is displayed.
- ▶ Log in with username and password (see previous page).
 - The configuration page of the GAT DC 7200 is displayed. You will see in the address bar that the connection is using https but is marked as insecure.
- ▶ In the menu to the left, switch to "Configuration" -> "Security and user".
- ▶ In the "General" tab, the "Use secure connection (SSL /TLS)" option under "Host interface settings" must be enabled for secure configuration via SSL.
- ▶ Open the "Certificates" tab.

Figure 6.2 – Create certificate

- ▶ Check whether the correct IP address and NetBIOS name are displayed for the certificate used (icon "Subject alternative names"). If not, click on "Create new self-signed certificate".

NOTE! Windows 8.0 or earlier Windows versions do not support "Alternative Names".

NOTE! The Firefox browser uses its own certificate store.

- ▶ Click on "Restart controller".
 - Wait approx. 30 seconds until the door controller has restarted. The connection is automatically re-established.
- ▶ You must now load the created certificate from the GAT DC 7200 to the PC. You have two options for this:

Option 1 – Load certificate via web interface

(Recommended - Firefox, Chrome, Edge)

- ▶ Click on "Download server certificate".
 - A file window opens where you can select the location and name of the certificate file. The certificate is saved in the format "server_Name.cer".

Option 2 – Download the certificate using the browser function

If the browser does not support direct download via web interface (e.g., Microsoft Edge), an error message will be displayed after clicking on "Download server certificate". You can also download the certificate using the browser function. This depends on the browser and can be completed for the Edge browser as follows for example.

- ▶ Click "Not secure" and then select "Your connection to this site isn't secure".
- ▶ In the message box that appears, click the icon at the top right.

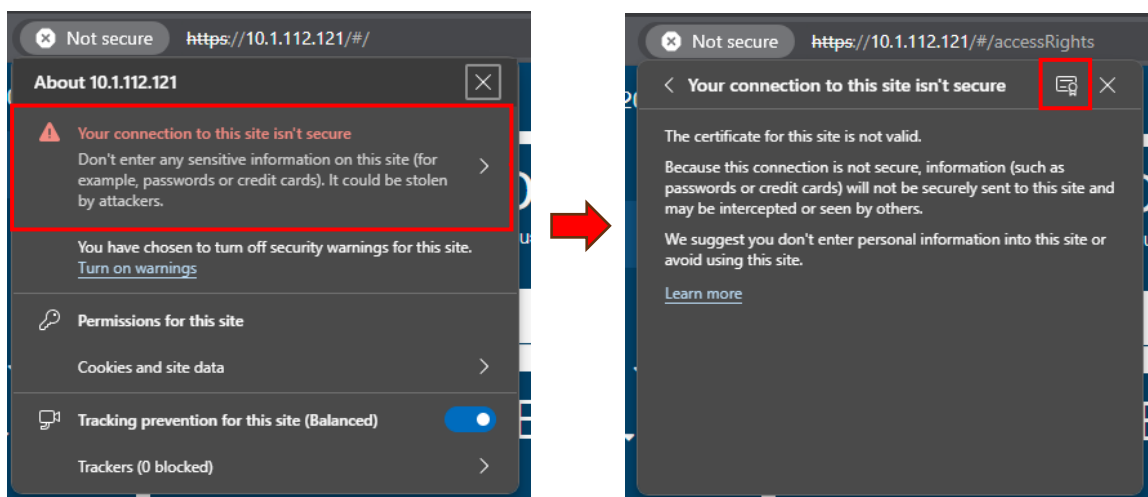


Figure 6.3 – Open certificate

- The certificate generated by the GAT DC 7200 is displayed in the "Certificate" window.

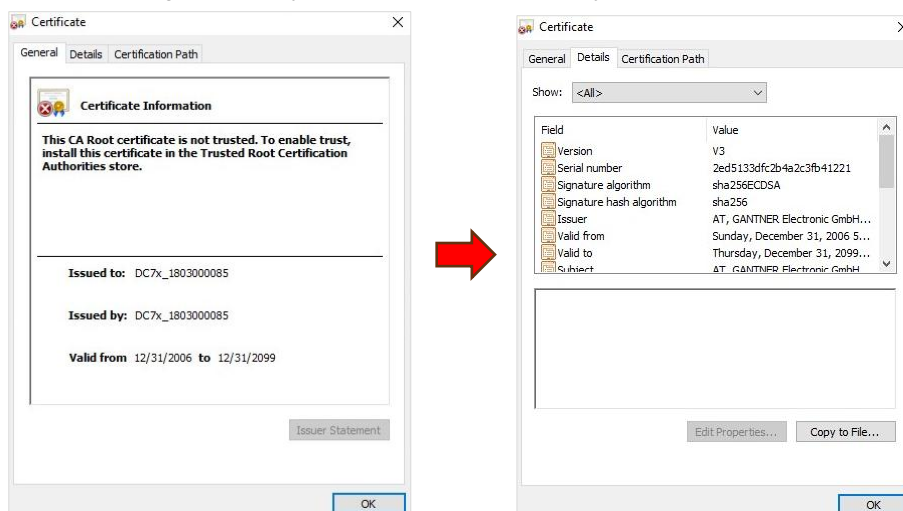


Figure 6.4 – Display certificate

- ▶ Switch to the "Details" tab.
- ▶ Select "Copy to file ...".
 - The certificate export wizard window is displayed.
- ▶ Click "Next" and then select the "DER encoded binary X.509 (.CER)" option.

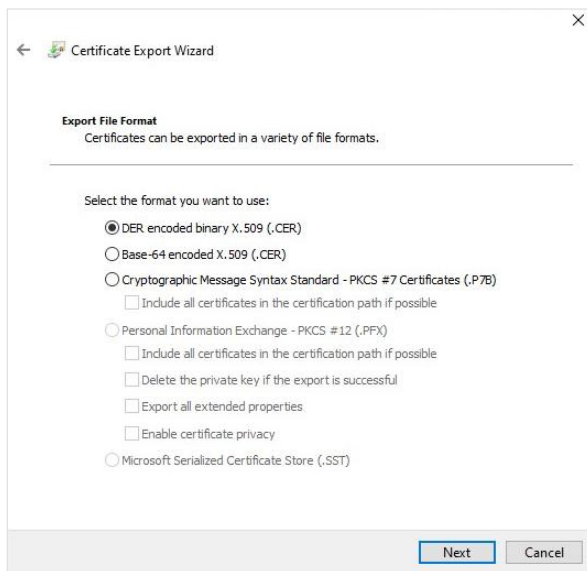


Figure 6.5 – Export certificate

- ▶ Click "Next" to select a file name and save the certificate file on the PC.

Install certificate on PC

After copying the certificate file (.cer) from the GAT DC 7200 to the PC, install it in Windows as follows.

- ▶ Double-click on the certificate (file with extension .cer).
 - The "Certificate" window is displayed.

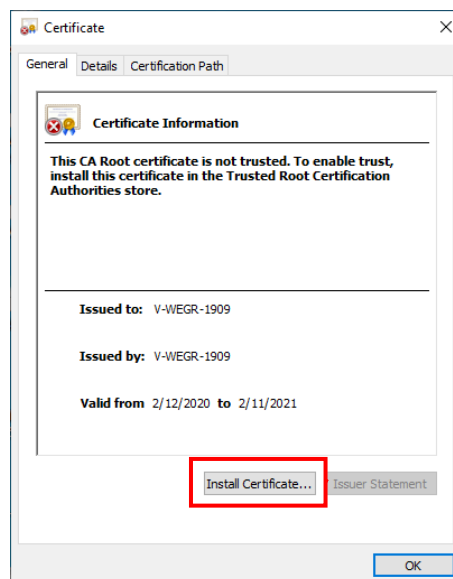


Figure 6.6 – "Certificate" window

- ▶ Click "Install Certificate".
 - The "Certificate Import Wizard" window opens.

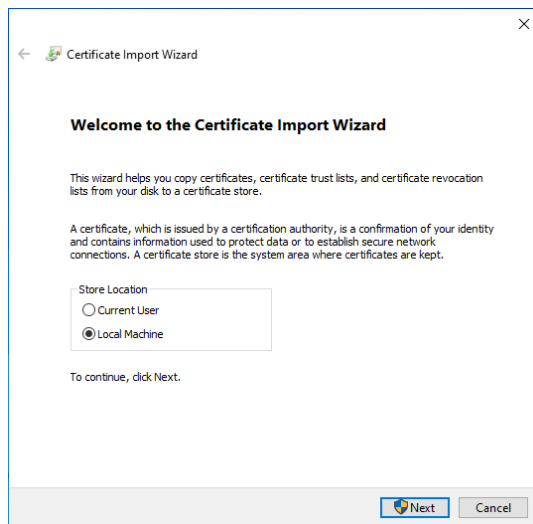


Figure 6.7 – "Certificate Import Wizard" – Step 1

- ▶ Select which certificate store to use ("Current user" or "Local computer") and click "Next".
NOTE! On the PC where you only want to access GAT ACE 7000 using Viewer or where you configure GAT DC 7200 using a web browser, please select "Local Computer". On the PC where the GAT ACE 7000 service is running, please select "Current user" and also install the certificate with "Local computer" if the GAT ACE 7000 viewer is to be used.

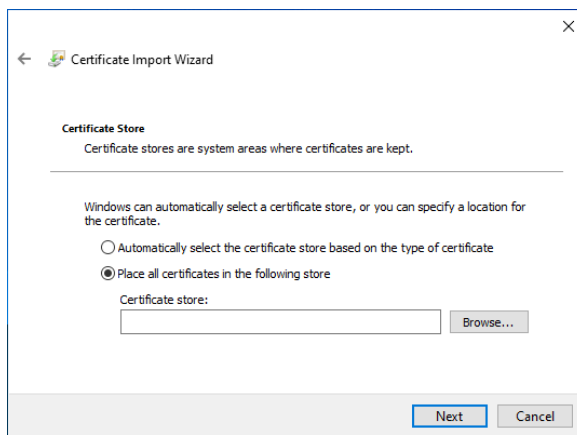


Figure 6.8 – "Certificate Import Wizard" – Step 2

- ▶ Select "Place all certificates in the following store" and click "Browse...".
- ▶ In the "Select Certificate Store" window, select "Trusted Root Certification Authorities" and click "OK".

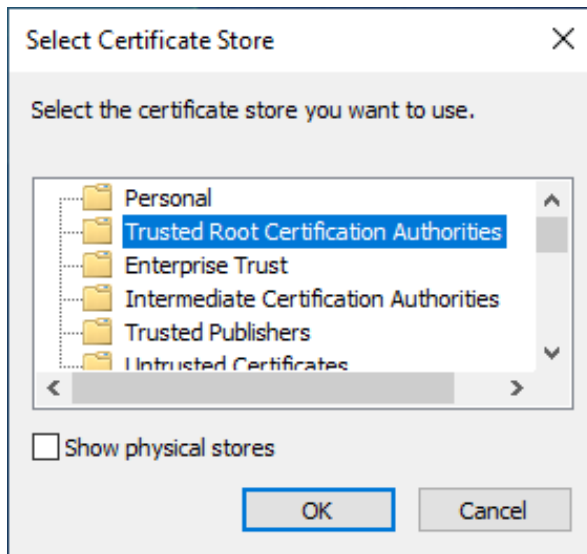


Figure 6.9 – "Certificate Import Wizard" – Step 3

- Click on "Finish" and confirm the subsequent message window by clicking on "Next".

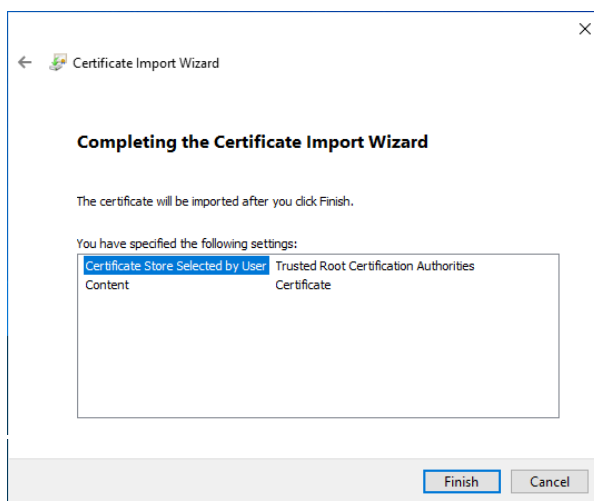


Figure 6.10 – "Certificate Import Wizard" – Step 4

6.4.2 Live status display and door control

If doors have already been configured, the status of the defined doors and the security status are displayed in the "Live view".

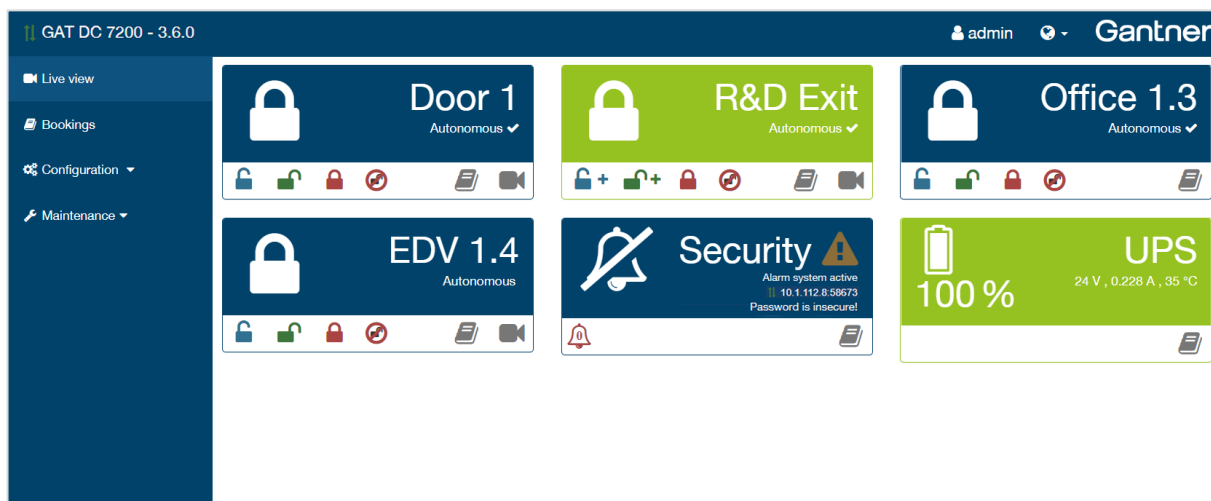


Figure 6.11 – GAT DC 7200 configuration - Web interface main window

The following information and controls are displayed for each door:



Buttons for the direct control of the door and acknowledgment of alarms are provided here.

- = Unlocks the door once. The door can be opened once without a data carrier and then it is locked again. Clicking on the "+" symbol additionally controls the special relay (output must be configured as special relay).
- = Unlocks the door permanently. The door can be opened and closed indefinitely. Clicking on the "+" symbol additionally controls the special relay (output must be configured as special relay).
- = Locks the door permanently. Access is not possible even after identification with a valid data carrier.
- = Suppress general open. Used to temporarily pause the general open function so that the door is locked, and access is only possible after identification with a valid data carrier.
- = Enable "Autonomous" mode, i.e., the door will be controlled according to the defined authorization data.
- = An alarm (e.g., door too long open), indicated by a red background color, can be reset with this button.

If door feedback is configured, the door state (open, closed) can also be displayed. In the event that an alarm is triggered at a door, this is also displayed here. Furthermore, the live view shows whether the door decides autonomously regarding access authorization and whether the connected reader is communicating or not.

The security display shows whether the intruder detection system is activated or deactivated, and whether it is ready for activation.

The  symbol indicates that the connection between the PC and GAT DC 7200 is secure. For more information, see the following chapters on configuring the system.

If a  symbol is displayed here instead, not all security settings are set optimally, e.g., the default password has not been changed.

As soon as a connection to the PC is established, the IP address of the host computer is displayed next to the  symbol.



6.4.3 UPS power supply

If a UPS (uninterruptible power supply) is connected to the GAT DC 7200, the charge status of the UPS is shown in the Live Status Display. The UPS is detected automatically during start-up of the controller when the UPS is connected to the “Sub” interface.

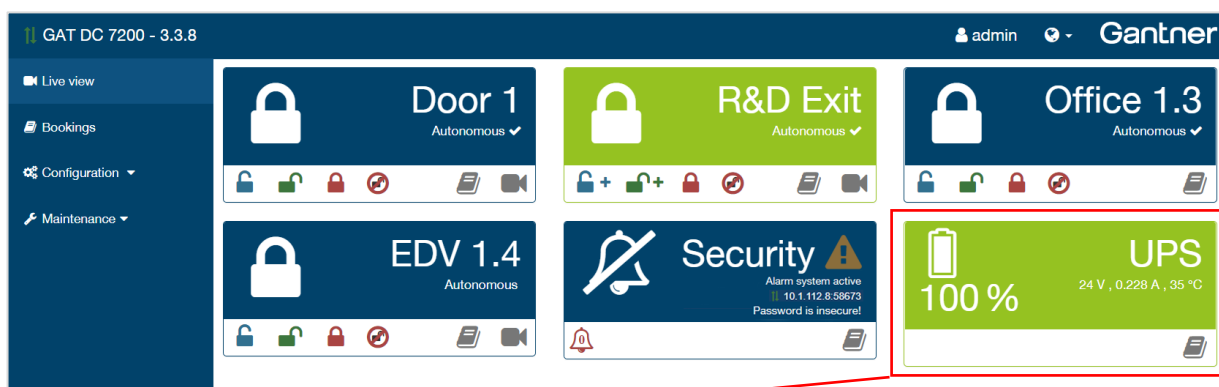


Figure 6.12 – Web Interface – UPS charging indicator in the Live Status Display

NOTE! Connecting the UPS together with other components to the same Sub interface is not permitted!

6.4.4 General information

Numerous settings can be changed during configuration of the GAT DC 7200. The settings must be saved in the GAT DC 7200 so that they can be activated. The function for saving always refers to individual settings groups that are related. If a value within a settings group is changed, the “Save” button becomes green and the corresponding menu is highlighted in red to indicate that a change has been made. As soon as the values are saved, the “Save” button returns to white and the menu indication disappears.

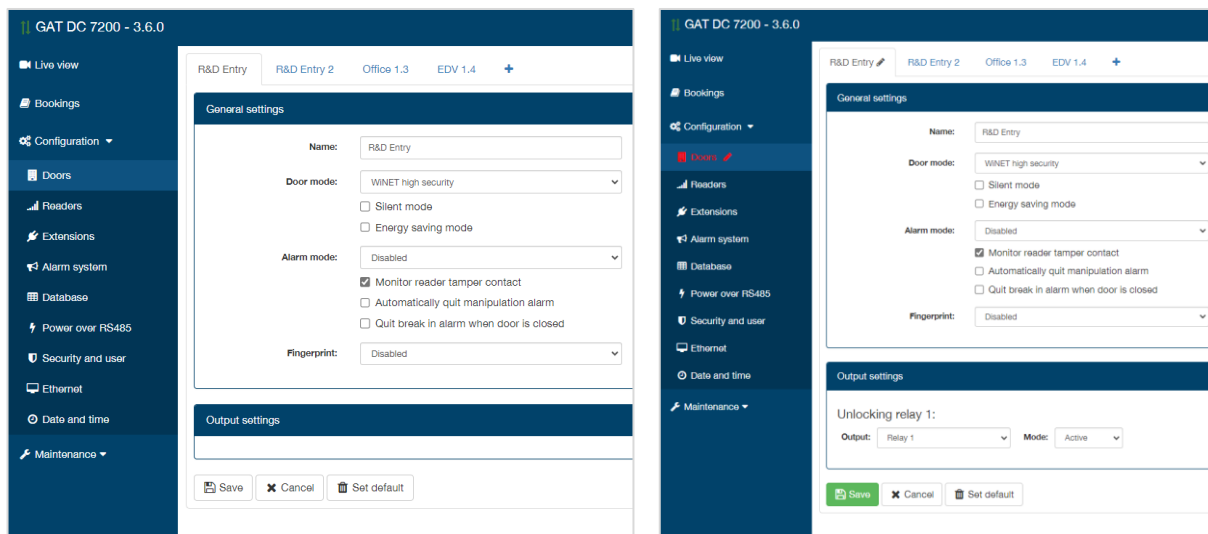


Figure 6.13 – Web Interface - Indication of unsaved changes (right side)

A warning is displayed when you attempt to leave the configuration interface of the GAT DC 7200 with changes that have not been saved yet.

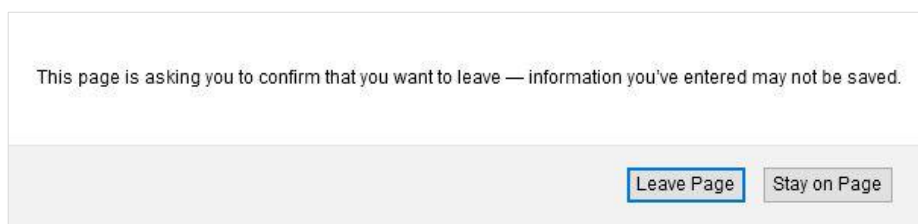


Figure 6.14 – Web Interface – Warning message for unsaved changes

- ▶ If you do not want to lose the changes, select “Stay on Page” and save the changes.
- ▶ If you press the "Leave Page" button, the changes will not be saved!

6.4.5 Users

The logged-in user is displayed next to the GANTNER logo.



Figure 6.15 – Web Interface – Username of current user

- You can change the user's password by clicking on the username.

Figure 6.16 – Web Interface – Change user password window

NOTE! After logging into the GAT DC 7200 for the first time, the yellow message (see image) is displayed in the password window. As of firmware version 3.6 it is mandatory to change the default password to a new, secret password after the initial login. The message is no longer displayed after the first password change.

- Enter the current password into the “Old password” field.
- Enter a new, secure password into the “New password” and “Confirm password” fields. The new password must be at least 8 characters long and contain at least one upper case letter, one lower case letter, and one number.

The “Change user” button allows you to log in as a different user with restricted permissions. To do this, users must first be defined in the configuration settings.

6.4.6 Language of the web interface

To change the display language of the GAT DC 7200 web interface, click on the globe symbol at the top of the window.

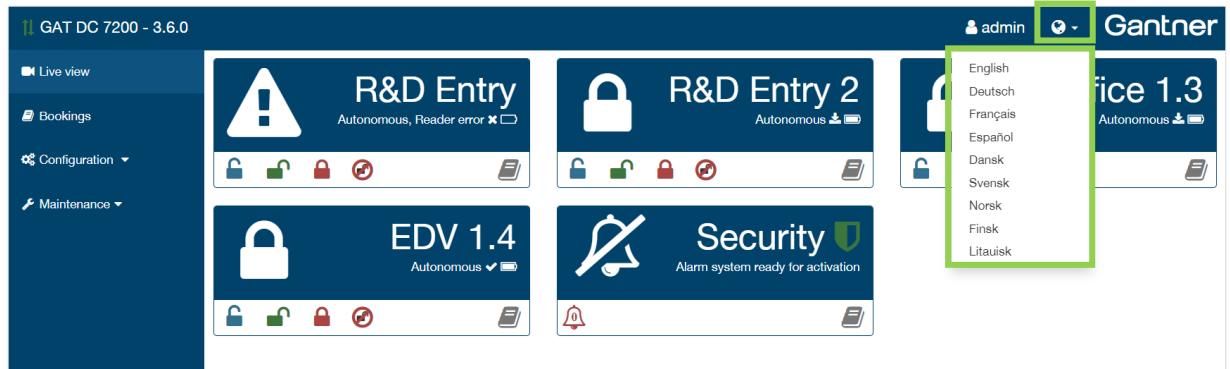


Figure 6.17 – Web interface – Changing the display language

- After selecting the desired display language, the language is changed immediately. Manually entered designations such as the door names remain in the original language.

6.4.7 Door configuration

Upon delivery of the GAT DC 7200, 4 doors (Door 1 to Door 4) are set by default. These are available under "Configuration" -> "Doors" and can be configured to your own requirements.

- For "Door 1", select a parameter suitable for your purpose.
- Rename the door to the usage accordingly, e.g., Main entrance.

Figure 6.18 – Web interface – Door settings

General settings

- Door mode: Each door can be set to operate in one of the following modes:
 - Disabled: The door will not be used when this mode is selected.
 - Access control with wired reader: Set the door to this mode if you are using a wired reader, e.g., GAT SR 73xx, GAT SLR 73xx, GAT SR 7xxx or GR7, or a wireless lock such as the GDL7m.
 - WiNET high security: With this setting for wireless networked locks with WiNET function, the GAT DC 7200 controller makes the access decision when the data carrier is presented at the door. This is the most secure version of WiNET; however, a stable wireless connection is needed.
 - WiNET comfort: The access rights are stored in the wireless networked locks with WiNET function after the first use. For subsequent access requests, a permanent, stable wireless connection is not needed. Updates to the access rights are sent to the locks at intervals of 10 minutes.
 - Locker control: For the control of a locker system (electronic locker locks), set the door mode to "Locker Control". An additional license is required for this mode (see ordering instructions).
With locker control, an authorized person can be assigned authorizations for one or more lockers. After identification, the desired locker can be opened by entering a locker number.

As of firmware V3.5.0, optimized operation is possible in which the locker is opened immediately after identification if authorization is only available for one locker. If several authorizations are available, the locker number must be entered after identification as before.

- Presence monitoring: Set the door to this mode to open a door (or activate the relays) when a valid data carrier is presented at the reader and to keep it open while the data carrier remains in front of the reader. This mode can be used, e.g., to activate the power in a hotel room or to control a machine when the user is at the machine.
- "GAT SMART.Lock": The modes "Access control (GAT SMART.Lock)" and "Locker control (GAT SMART.Lock)" are analogous to the identically named modes described above, with the exception that GAT SMART.Lock locks are controlled. For these door modes, the unlocking time is set automatically to the correct values for the GAT SMART.Lock. To ensure that the GAT SMART.Lock is not damaged, general open functions are not possible.
- Silent mode: If this option is enabled, the beeper of the respective reader is deactivated. For readers that do not support this function, the beeper is still heard in silent mode.
- Energy saving mode: This option sets the door to low-power mode during periods of inactivity in order to minimize power consumption. The LEDs on the reader are switched off after a period of inactivity (1 minute). The reader itself remains active. The LEDs are powered on again when an action occurs at the reader or the status of the reader changes (e.g., remote opening).
- Write CardNET/SVN data: If this option is enabled, CardNET data and/or SVN data (Salto Virtual Network) are written to (and read from) the data carriers by this door controller. This means that when a data carrier is read at a connected reader, the door controller automatically writes the relevant CardNET or SVN data sent by the access control software for the data carrier to it. When not enabled, no CardNET or SVN data is written by the door controller.
NOTE! The CardNET/SVN function must be enabled for the door controller, otherwise this option is not displayed (see "6.4.8 Reader configuration").
- Alarm mode: This setting allows you to activate or deactivate an intrusion detection system (IDS) for the respective door. Up to 4 different alarm system areas can be controlled by the GAT DC 7200 and each can be activated/deactivated via the "Alarm System" menu in the GAT DC 7200 web interface. If the IDS setting is enabled, access is prevented as soon as the IDS is activated to prevent an alarm from being triggered if the door is opened with a valid identification. It is also possible to select whether to display the IDS state at the reader point. The color is selected via the "Alarm System" menu in the web interface (see "6.4.10. Alarm system settings").
- Monitor reader tamper contact:
The reader tamper contact senses when unauthorized activity such as manipulation or tampering occurs. Select this option if you want to monitor the readers for manipulation or tampering.
NOTE! The tamper contact is not available with all types of readers.
- Automatically quit manipulation alarm:
If this option is enabled, a manipulation alarm that has been triggered (e.g., door opened for too long or opened without authorization) is automatically deactivated again as soon as the reason for triggering the alarm no longer exists (e.g., when the door is closed again after being opened for too long).

If the option is not enabled, the alarm remains active until it is manually acknowledged by an authorized person. In the latter case, multiple occurrences of manipulation would not be individually transmitted, e.g., to a control station, because the previous alarm has not been processed.

- Quit break in alarm when door is closed:

A break-in alarm is triggered, e.g., when the door is opened or broken into without authorization. When the option is selected, a break-in alarm can be acknowledged by simply closing the door again. However, the alarm is still recorded in the bookings.

- Fingerprint:

This setting determines whether fingerprints are to be used for verification, identification, or to not use these additional verification options at the door.

- Unlocking time:

This time determines how long the lock is unlocked for following valid identification. Select "Use full unlocking time" to unlock the lock for the entire unlocking time. Otherwise, the unlocking time ends as soon as the door is detected as being open.

- Enable permanent unlocking by button:

This option allows the door to be permanently opened by an external signal, e.g., push button. If this function is not enabled, the opening of the door via this signal only occurs for the unlocking time. For a new release, the signal must first expire before a new release is possible.

- Max. door open time:

This time determines the maximum time a door can be held open until a signal is triggered. The signal can be realized via a relay output or notification in the building control system. The signal is then enabled for the period defined in the "Door open warning time" field and if the door is not closed within this time, a "Door too long open alarm" is triggered.

- Quit door too long open alarm when door is closed:

When this option is selected, a generated "door too long open alarm" can be acknowledged by simply closing the door. Otherwise, this alarm will continue after the door is closed and it must be acknowledged manually in the live view or via the building control center.

- Direction:

Here, you can select whether the door is an entry or exit door. This information is displayed in the bookings.

- Office function:

If the office function is enabled for a door in GAT Matrix (see the GAT Matrix manual for instructions), the door can be permanently unlocked by reading a valid data carrier. The process can then be repeated to deactivate the office function for the door. Select from the menu how the office function will be activated: activation via short identification (default setting) or activation via long identification.

For long identification, the function is activated by keeping your data carrier held in front of the reader for approx. 4 seconds after identification. The LEDs of the GR7 reader will illuminate in succession and an ascending pitch acoustic signal is emitted to signal that you are activating the office function. Repeating the process deactivates the function with the signalization in reverse.

You can also combine the short or long identification with activation for persons with special authorization (also known as "special rights"), so that not all persons are able to activate the office function. The special rights must be activated for the respective persons in GAT Matrix (via the option "Office function special right") for each door. See the GAT Matrix manual for further information.

Output settings / Input settings

The settings in these areas are used to convert logic signals and states to electrical signals.

The GAT DC 7200 has 6 digital optocoupler inputs and 6 relay outputs, which can be configured to perform different functions (see table below). For the door settings, each door can be assigned an optocoupler input or a relay output with each of these functions if desired. This allows the GAT DC 7200 to be tailored to individual applications.

The use of the same relay or optocoupler with different doors is possible. For example, a collective alarm (manipulation alarm from all doors issued via a relay contact) or a collective control (one signal used to unlock multiple doors) can be easily implemented. However, it is important to realize that some functions are mutually exclusive or not applicable for certain applications. Such configurations are to be avoided.

Output settings

Unlocking relay 1:

Output: Relay 1 [Door 1,R&D Exit] Mode: Active

Unlocking relay 2:

Output: Disabled Mode: Active Delay: 0 s

Unlocking relay 3:

Output: Disabled Mode: Active Delay: 0 s

Unlock impulse:

Output: Disabled Mode: Active Time: 1 s

Lock impulse:

Output: Disabled Mode: Active Time: 1 s

Special relay:

Output: Disabled Mode: Active Time: 5 s

Not authorized:

Output: Disabled Mode: Active Time: 5 s

Break in alarm:

Output: Disabled Mode: Active Time: 5 s

Suppress break in alarm relay:

Output: Disabled Mode: Active Delay: 2 s

Manipulation alarm:

Output: Disabled Mode: Active Time: 5 s

Threat alarm:

Output: Disabled Mode: Active Time: 5 s

Door too long open warning:

Output: Disabled Mode: Active Time: 5 s

Door too long open alarm:

Output: Disabled Mode: Active Time: 5 s

Input settings

Door contact:

Input: Disabled Mode: Active

Unlock 1:

Input: Disabled Mode: Active

Unlock 2:

Input: Disabled Mode: Active

Lock permanent:

Input: Disabled Mode: Active

Tamper contact:

Input: Disabled Mode: Active

Suppress general open:

Input: Disabled Mode: Active

Figure 6.19 – Web interface – Input and output settings

Functions of the relay outputs

"Active" or "Passive" mode can be selected for the functions described below. The execution of the functions of the respective relay circuit can thus be adapted. Active means that the relay is activated (energized) when the function is active (e.g., in the case of the unlocking relay if a valid identification has been made and the door is to be unlocked). Passive means that the relay is activated (energized) in the idle state, and if the relevant function is active, the relay is deenergized.

Setting in the GAT DC 7200	Description
Unlocking relay X	This relay is used for door unlocking. When a person has made an identification and the authorization to open the door is available, the function is activated. The period and the expiry date, etc., are also considered in the authorization check. This function is also activated when a door schedule is active, or an opening is carried out via a button release, or an opening command is sent from the PC. If two or more unlocking relays are defined, a delay time in seconds can be entered for the relays in order to activate the relays with a time delay. If "0" is entered, the relay is activated at the same time as the first unlocking relay.
Unlock impulse / Lock impulse	These functions are used to send a short pulse from the relay to lock or unlock a lock. The relays are intended for locks that require such a short pulse to be sent, e.g., to an input of the control unit for unlocking and a pulse to be sent to another input of the control unit for the end of unlocking. The "Time" setting determines the duration of the activation.
Special relay	When a special authorization is defined for a person at the door, this function is activated following valid identification. The special relay is also controlled in parallel to the unlocking relay. The "Time" setting determines the duration of the activation.
Not authorized	This function is activated when an identification has been made but the person or the data carrier is not authorized for access. The "Time" setting determines the duration of the activation.
Break in alarm	This function is activated when the door is opened without authorization. To do this, the door status must be monitored using the optocoupler input. The "Time" setting determines how long the alarm remains active. If the value is greater than 0, the output is activated for the time entered. A value of "0" means that the alarm remains active until it is acknowledged or reset.
Suppress break in alarm relay	This relay is used, e.g., to bridge the magnetic contact of an alarm loop if the alarm system is armed but no alarm is to be triggered when access is authorized. The output is controlled together with the unlocking relay. The "Delay" setting determines how long the alarm suppression relay is activated. It remains activated for as long as the door is open + the time specified in the field (so as not to trigger an alarm by bouncing the magnetic contact).
Manipulation alarm	This function is activated if the housing of a connected reader is opened without authorization or the connection between a reader and the GAT DC 7200 is broken. The "Time" setting determines how long the output remains activated. If the value is greater than 0, the alarm is activated for the time entered. A value of "0" means that the alarm remains active until it is acknowledged/reset.

Threat alarm	This function can be activated by the user if they are under threat or duress during identification, e.g., while entering the building. Depending on the configuration, the user can trigger the threat alarm either by entering a threat PIN code during access rather than the personal PIN code, or by identifying themselves using their defined threat fingerprint, or by pressing the F1 key on the GR7.2310 reader before identification. See chapter "6.4.10 Alarm system settings" for information. The "Time" setting determines how long the output remains activated. If the value is greater than 0, the alarm is activated for the time entered. A value of "0" means that the alarm remains active until it is acknowledged/reset.
Door too long open warning	If an optocoupler input is set as for door feedback ("door contact"), the opening time of the door is measured when access is valid. If the door is open longer than the defined "Max. door open time", the function is activated. The "Time" setting determines how long the warning is displayed. If the door is still not closed after this time, a "door too long open alarm" is triggered.
Door too long open alarm	This function is activated, i.e., a "Door too long open alarm" is triggered, when the door after a valid opening remains open for longer than the defined max. door opening time + the "Door too long open warning" (if used; see previous point) remains open. The "Time" setting determines how long the output remains activated. If the value is greater than 0, the alarm is activated for the time entered. A value of "0" means that the alarm remains active until it is acknowledged/reset.

Table 6.1 – Functions of the digital outputs of the GAT DC 7200

Functions of the optocoupler inputs

"Active" or "Passive" mode can be selected for the functions described below. This means that the internal processing of the functions can be adapted to the respective wiring of the inputs. Active means that the respective function is active when the input is energized. Passive means that the function is active when there is no current at the input and passive when the function is energized.

Setting in the GAT DC 7200	Description
Door contact	This input signals to the controller whether the door is open. The function is usually implemented via a door contact that is connected to this input. The unlocking relay drops out as soon as the door status is signaled as open. If there is neither an identification nor a button opening or remote control by command and a door opening is still reported via the input, an intrusion alarm is triggered (unless suppressed in the door schedule). With a normal door opening, the "Max. door open time" is monitored (if not suppressed in the door schedule) and a "Door too long open warning" and/or a "Door too long open alarm" is triggered if the door is held open too long.
Unlock x	If this function is activated, e.g., by pressing a button or handle, or via intercom, a door opening is triggered, and this process is logged as a booking. The entry/exit direction of this booking is opposite to the direction defined for the door. If the "Enable permanent unlocking by button" option is not activated in the general door settings, the unlocking time consists of the duration of the signal at this input plus the set unlocking time. If the option is activated, the unlocking time is for as long as the signal is present at the input, e.g., for as long as the button on the input remains pressed.

Lock permanent	If this function is active, entry or exit is not possible even with a valid identification. The unlocking button also has no function. This can be used, e.g., in locks to lock a door so long as the opposite door is open. A permanent locking can also be done by the alarm system using the block lock function (see "6.4.10 Alarm system settings").
Tamper contact	For this input, an external tamper contact, e.g., a GR7.23xx reader mounted in a GR7m.2001 installation box, can be connected for manipulation/break-in monitoring. The tamper contact must be connected according to the active or passive mode setting so that the tamper function is activated correctly when the power supply is switched on or off.
Suppress general open	When this function is active, the currently active general open plan is deactivated so that the regular access authorization applies. A valid identification is then required for access.

Table 6.2 – Functions of the digital inputs of the GAT DC 7200

Special settings (delay times)

Use the "Special settings" tab in the top-right corner of the window to open additional time settings for the doors. The settings defined here apply to all doors created for the GAT DC 7200.

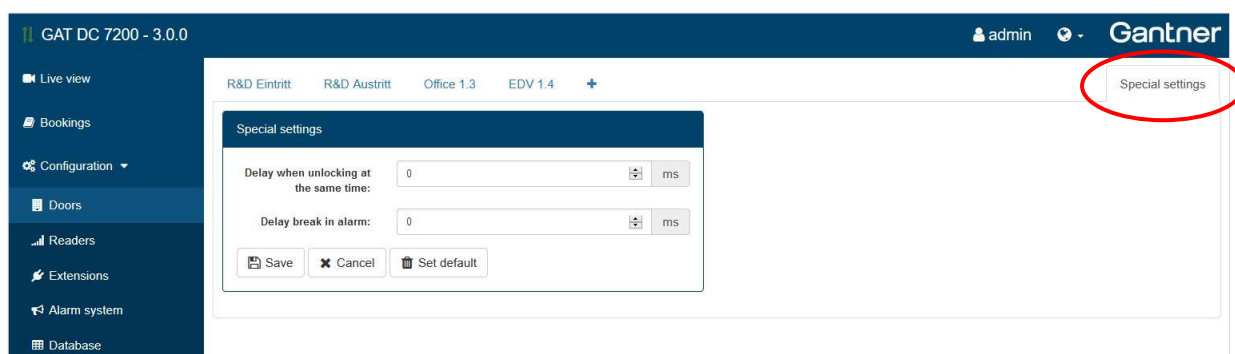


Figure 6.20 – Web interface - Special settings for the doors

- Delay when unlocking at the same time: When a time is entered here (value in milliseconds) and several doors are unlocked, i.e., when several relays are activated, the doors are activated when this delay time expires. A value of "0" here means that activation occurs simultaneously.
- Delay break in alarm: Enter a time here (value in milliseconds) to delay the triggering of an alarm if the locker door is forced open (break-in). A value of "0" here means that the alarm is triggered without delay.

6.4.8 Reader configuration

The configuration of readers is universal, which allows various types of data carriers and readers to use the GAT DC 7200. However, the simplest configuration is when GR7 series readers and data carriers with GANTNER coding are used. The reader settings are organized into different tabs at the top of the page, which are described in the following pages.

"General" tab

The following information can be defined in the "General" tab.

Figure 6.21 – Web interface – General reader settings

- Default company ID: Enter your system number in this field. You would have received this number together with delivery of the data carriers.
- Auto assign reader id to reader port number: This setting activates the Plug&Play PLUS function, which enables the automatic recognition of readers. If readers are used that do not support this function, or if several readers are connected to a reader socket, this function must be deactivated, and the assignment completed manually.

- WiNET:
 - Enable RFID wake up: When this setting is enabled, the WiNET lock regularly checks whether there is a data carrier in the reading field. Otherwise, the lock must first be woken up so that the reading field is activated, which is done in different ways depending on the lock (e.g., with the GAT DL 320 by turning the knob). Enabling this setting reduces the battery life as more energy is required.
 - GFSK modulation: This function is possible with WiNET locks with firmware version 4.0 onwards. This setting enables compatibility with the RED (Radio Equipment Directive), which has been required for new installations since 2017. For systems that were installed before the RED came into effect, the earlier standard, where the GFSK setting is deactivated, can also be used.
- RFID standards: In this area, select the identification technologies or ISO standards that apply for your data carriers. This selection/deselection of RFID standards is only possible for readers that support this function.
- ECP frame: This setting is required for the "Mobile Credential" function. The field is only displayed if the Mobile Credential license is activated. Enter the corresponding ECP frame number here. The number must be entered in hexadecimal format. You will receive this number from your wallet credential provider.
 The ECP frame can also be used to determine, among other things, whether verification (face, fingerprint or PIN code) is required to use the Mobile Credential or whether the Mobile Credential can also be used without verification ("Express Mode").
NOTE: Information on the necessary configuration steps for Mobile Credential can be found in chapter "6.5. Configuring Mobile Credential".
- Manipulation barrier: Here, you can define the number of incorrect entries of the PIN code or verifications with fingerprint that are allowed. If the limit is exceeded, you can define the length of time for which the person is blocked before further access attempts are allowed.
 First, if the number of incorrect PIN entries or fingerprint verifications exceed the values entered in the "Level 1" section, the person is blocked from all doors controlled by the controller for the time set for level 1.
 After this blocking time has elapsed, further failed attempts are calculated in relation to the "Level 2" values. These values may differ from level 1. If this number of failed attempts is also reached, the person is blocked from all doors controlled by the controller for the time set for level 2. After this time has elapsed, the person can re-attempt identification via verification provided that the person has not been blocked via the "Block person permanently" function (see below). All incorrect verifications by users are displayed in the bookings. In the example shown below, the user "Schlachter K." first activated level 1 with two incorrect attempts, then after 1 minute level 2 was activated with another incorrect verification (3).

GAT DC 7200 - 3.6.0

admin Gantner

Live view

Bookings

Configuration

Doors

Readers

Extensions

Alarm system

Database

Power over RS485

Security and user

Ethernet

Date and time

Maintenance

Time stamp	Booking	Door	Person	Card	Type	Info
2024-08-19 16:57:32	1233: Manipulation barrier	R&D Entry	7: Schlacher K.	36417865262111236	1	Level 2
2024-08-19 16:57:25	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	3
2024-08-19 15:51:55	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	2
2024-08-19 15:51:35	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	1
2024-08-19 15:49:40	1100: Access/Exit after identification	R&D Entry	7: Schlacher K.	36417865262111236	1	No door contact
2024-08-19 15:49:40	1000: Unlocked by identification	R&D Entry	7: Schlacher K.	36417865262111236	1	-
2024-08-19 15:36:31	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	2
2024-08-19 15:36:26	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	1
2024-08-19 15:33:46	1233: Manipulation barrier	R&D Entry	7: Schlacher K.	36417865262111236	1	Level 2
2024-08-19 15:30:46	1233: Manipulation barrier	R&D Entry	7: Schlacher K.	36417865262111236	1	Level 2
2024-08-19 15:30:31	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	3
2024-08-19 15:29:14	1233: Manipulation barrier	R&D Entry	7: Schlacher K.	36417865262111236	1	Level 1
2024-08-19 15:29:10	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	2
2024-08-19 15:29:04	1222: Invalid pin code	R&D Entry	7: Schlacher K.	36417865262111236	1	1

Users that have carried out incorrect verifications are displayed in the “block list”. The level that the user is currently on is also displayed here.

Manipulation barrier:

Level 1: Attempts PIN code verification: 2 Attempts fingerprint verification: 5 Block person for: 1 min

Level 2: Attempts PIN code verification: 1 Attempts fingerprint verification: 2 Block person for: 10 min

☐ Trigger manipulation alarm ☐ Block person permanent

Block list:	Person	Level
	2:Haudum K.	2
	7:Schlachter K.	1

By clicking on “Clear block list”, the blocked users can be released before the set blocking time for level 2 has elapsed.

Additional functions can be enabled via the two options “Trigger manipulation alarm” and “Block person permanent”.

- Trigger manipulation alarm: After exceeding the permitted values of level 2, a signal is sent to a relay set for a manipulation alarm (see “6.4.7 Door configuration”). This option can be used, e.g., for on-site signaling.
- Block person permanent: If this option is enabled, a person is permanently blocked from further access once the number of permitted values set for level 2 has been exceeded. This block applies to the current controller and the doors it is controlling. The person is not blocked in the entire access system, i.e., access can still be attempted at other controllers.

NOTE! The verification function can be enabled and set for users in the day plans. If standalone mode is being used, this is done directly in the GAT DC 7200 settings via the “Access rights” menu (see “8.3 Authorization management”).

Day plan 3

00:00 | 04:00 | 08:00 | 12:00 | 16:00 | 20:00

From: 07:00 To: 19:00 Verification: Pin code ☐ Identification code allowed

+ Add time span

- Third party reader bus delay: The default value of this setting is 0 ms, which is valid when only Gantner readers are used. If readers from other manufacturers are connected, the appropriate delay value (e.g., 10 ms) for communication must be set here according to the reader manufacturer's specifications.

"Data carrier" tab

The following data carrier settings can be defined in the "Data carrier" tab.

Figure 6.22 – Web interface – Data carrier settings

For standard data carrier coding, simple settings are available with simple defaults suggested automatically. Only change these settings if you understand the meaning. Otherwise, please contact your local supplier or GANTNER Technical Support.

Customer-specific data carrier coding can also be used in many cases when the coding information is available. In this instance, it is necessary to assess the data carriers for usability during the project planning process.

A simple method is to use the unique number of data carriers. You can set this by selecting "Unique number" or "Custom unique number". It should be noted that the security level of these data carriers is not as high as with coded data carriers.

To use mobile credentials, you must also enter your ID information for the data format "LEGIC Connect: Apple Wallet" and/or "LEGIC Connect: Google Wallet". The "Settings" must be configured appropriately for your system. You will receive this information from your sales partner.

i Note: If the VCP file is deleted from the readers (see next section about the "Reader" tab), the settings here will remain (for possible later reuse), however, the "Data format" field will be deleted, so this data carrier format can no longer be used.

“Reader” tab

This tab displays the readers that were identified and assigned automatically via Plug&Play PLUS. Please note that GAT SR 380 type readers cannot be used with the GAT DC 7200.

NOTE! Please pay attention, that the GAT Authorization Tag 400 BA is required for GANTNER SVN.

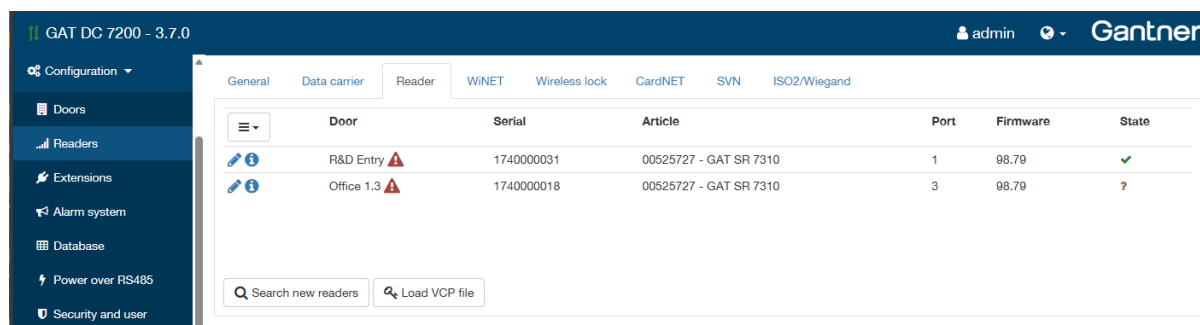


Figure 6.23 – Web interface – Reader settings

- If Plug&Play PLUS is not activated, you can search for readers manually via the “Search new readers” button and then assign them to the doors.

Initialize reader for CardNET function:

Readers that are being used for the CardNET function must be initialized (“launched”) once. This is necessary, so that the access rights can be written onto the data carriers.

- To initialize a reader, hold the authorization data carrier for your system (GAT Authorization Tag 400 B or BA) next to the reader until the initialization process is finished (approx. 15 seconds).
 - During initialization, the LEDs flash red and green alternately.
- Initializing readers with a GAT Authorization Tag 400 BA is also necessary for MIFARE DESFire systems and for GANTNER SVN.
- To determine whether a reader has been initialized, click on the “i” symbol next to the reader.
 - The following window opens.

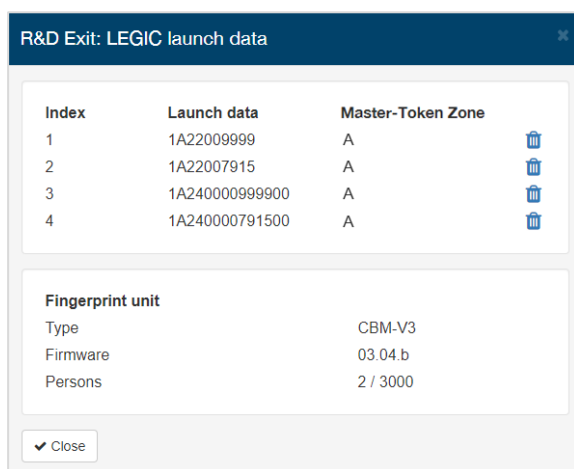


Figure 6.24 – Web interface – Reader information

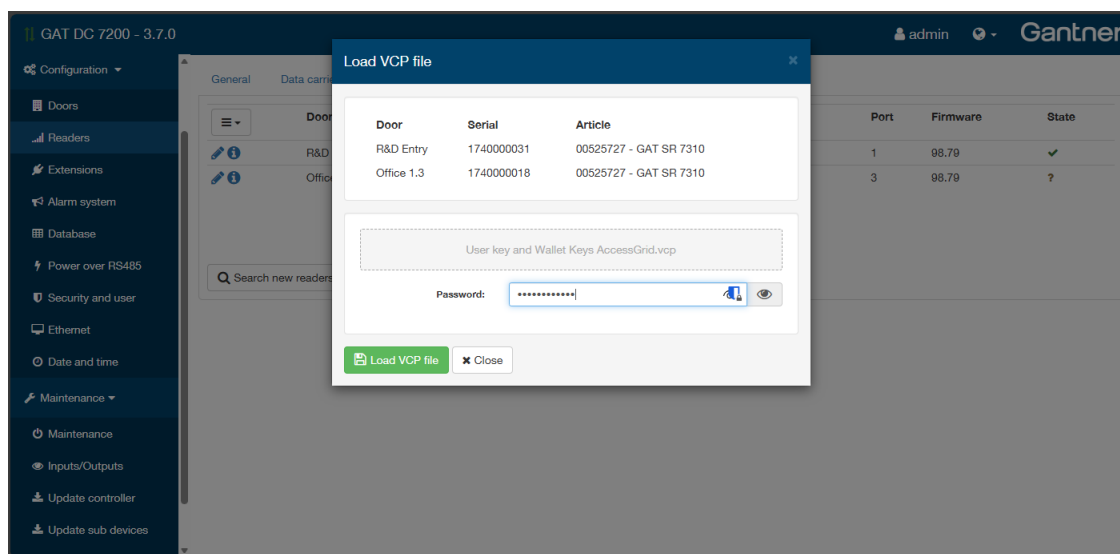
- If the reader is initialized, the initialization data is shown in the "Launch data" column.
- The information displayed in the "Master-Token Zone" column is relevant for installations that use the LEGIC Master-Token System. The different zones are set according to the media in use, which contributes to the long-term use of the access control system (see the LEGIC website for more information).
- ▶ If required, the initialization data (Launch data) can be deleted by clicking on the  symbol.
 - The "Fingerprint unit" section is only shown when a fingerprint reader is used with the reader. Shown here are the type of fingerprint reader, the firmware version installed, and the number of stored and max. possible persons (fingerprints).

Loading the VCP file (for Mobile Credentials):

For the Mobile Credentials function, it is necessary to load a VCP file onto the connected readers. This file contains specific LEGIC configuration parameters, enabling the use of Mobile Credentials on these readers. See also "6.5. Configuring Mobile Credential". You can obtain the VCP file from your wallet credentials provider. For the GR7 and S(L)R 73xx readers, VCPs for SM-4xxx chips are required.

For security reasons, a password is required to load and activate the VCP file.

- ▶ Click on the button "Load VCP file".
 - A pop-up window appears.



- ▶ Drag and drop the VCP file (file extension .vcp) in the field marked here.
- ▶ Enter the corresponding password into the field "Password".
- ▶ Click on "Load VCP file".
 - The file is loaded and activated in the displayed readers. If the file was successfully activated, you will see a green checkmark icon next to the corresponding reader.

Load VCP file

Door	Serial	Article
✓ R&D Entry	1740000031	00525727 - GAT SR 7310
📁 Office 1.3	1740000018	00525727 - GAT SR 7310

User key and Wallet Keys AccessGrid.vcp

Password:

••••••••

🔑

👁

📁 Load VCP file

✕ Close

NOTE: To remove a loaded VCP from a reader, a "Remove VCP" must be loaded. This is also done on this page. For more information, see "6.5.1. Delete VCP from a reader".

“WiNET” tab

When using battery-powered locks operating in WiNET mode, the detected access points (e.g., GAT DL 091 RS485) and the locks that are within range of the access points are displayed. These locks can be assigned to doors using their serial numbers. The following information is displayed in the "WiNET" tab.

GAT DC 7200 - 3.6.0

Live view

Access rights

Bookings

Configuration

Doors

Readers

Extensions

Alarm system

Database

Power over RS485

Security and user

Ethernet

Date and time

Maintenance

admin

Gantner

General

Data carrier

Reader

WINET

Wireless lock

ISO2/Wiegand

Door

Serial

Article

Firmware

Access point

RSSI

Last contact

Battery

R&D Entry

201535 / 0x3133F

00297535 - GAT DL 32x

9.9

1

-54 dBm / -65 dBm / -79 dBm / -95 dBm

⚠ 654 s / - / -

R&D Entry 2

682205 / 0xA68DD

00776133 - GAT DL 320

4.3

2

-74 dBm / -53 dBm / -77 dBm / -91 dBm

⚠ 861575 s / - / -

Office 1.3

525776 / 0x805D0

00803928 - GAT DL 34x

9.9

3

-80 dBm / -72 dBm / -69 dBm / -87 dBm

⚠ 861707 s / - / -

EDV 1.4

562099 / 0x893B3

00803928 - GAT DL 34x

9.9

4

-83 dBm / -85 dBm / -79 dBm / -94 dBm

⚠ 861674 s / - / -

Door 5

678777 / 0xA5B79

00803928 - GAT DL 34x

4.9

4

-81 dBm / -91 dBm / -73 dBm / -67 dBm

- / - / -

Door 6

582723 / 0x8E443

00803928 - GAT DL 34x

4.0

1

-56 dBm / -48 dBm / -70 dBm / -77 dBm

- / - / -

Clear unassigned devices

Search new access points

Access point

Serial

Article

Firmware

State

1

1732000040

00253123 - GAT DL 091 RS485

04.00

✓

2

1932000011

00253123 - GAT DL 091 RS485

04.01

⚠

3

1216000073

00253123 - GAT DL 091 RS485

04.00

⚠

4

1216000035

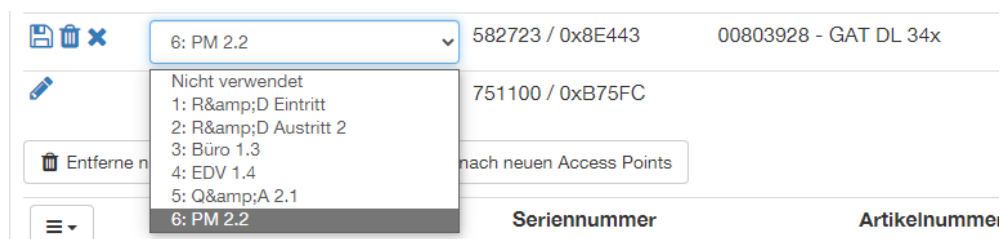
00253123 - GAT DL 091 RS485

04.00

⚠

Figure 6.25 – Web interface – WiNET settings

- Doors, locks: If access points are connected, the recognized locks are displayed in the upper list with the serial / article number and model name. To assign a lock to a door configured in the GAT DC 7200 (see previous chapter), click on the Edit icon  of the respective lock, select the desired door from the list, and click on the Save icon .



NOTE! If an exclamation icon is displayed next to a lock name (e.g., Office 1.3 ) , it is possible that another reader may be assigned to the door that the lock is assigned to ("Reader" tab).

NOTE! It is possible that the signal strength of an access point to which a lock is connected is weaker than the signal of another access point. In this case, the system automatically switches to the access point with the strongest signal while editing and saving the lock.

In the following example, the lock with serial number 582723 is connected to access point 1, but the signal from access point 4 is stronger (-78 dBm for AP1 and -63 dBm for AP4) ...

Door	Serial	Article	Firmware	Access point	RSSI
PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	1	-76 dBm / -77 dBm / -71 dBm / -63 dBm

... after editing and saving ...

PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	1	-76 dBm / -77 dBm / -71 dBm / -63 dBm
--------	------------------	-----------------------	-----	---	---------------------------------------

... the lock is assigned to Access Point 4 with a signal strength of -63 dBm.

PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	4	-76 dBm / -77 dBm / -71 dBm / -63 dBm
--------	------------------	-----------------------	-----	---	---------------------------------------

This manual configuration is only required if two access points have a connection to the lock and the switch to the stronger signal is not completed automatically.

- RSSI:

The values in the "RSSI" column (green - orange - red) indicate the strength of the wireless connection during the last connection between the lock and the access points. This enables the appropriate positioning of the access points to be optimized during commissioning.

Please note that the lock sends a "ready for operation" status approximately every 15 minutes if it is not activated. As there is no data carrier or person in front of the lock, stronger RSSI values are displayed here. If there is a person and data carrier in front of the lock, the RSSI values are weaker, so this must be considered during project planning.



= Good wireless connection.



= Intermittent wireless connection. Reposition the access point if possible.



= Poor wireless connection. The access point must be repositioned.

If multiple access points are connected, their values are displayed consecutively separated by a slash "/" (from left to right Access Point 1, 2, 3, etc.).

RSSI				
-54 dBm	-65 dBm	-79 dBm	-95 dBm	
-74 dBm	-53 dBm	-77 dBm	-91 dBm	
↑	↑	↑	↑	
AP 1	AP 2	AP 3	AP 4	

- Last contact: This column indicates the time elapsed since the lock last communicated with the GAT DC 7200.
- Battery: The condition of the battery is displayed in this column.
 -  = Battery condition weak. It is recommended to replace the battery now.
 -  = Battery empty; replace immediately.
- Further information in the door list:

Click on the symbol  to display additional door information:

 - Hardware: Displays the hardware version of the door lock.
 - LQI: The LQI value indicates the transmission quality of a wireless lock in values from 0 (poor) to 255 (very good).
 - Client RSSI: Analogous to the "RSSI" values, these indicate the signal strength between the access point and the wireless locks. The client value indicates the reception strength of the access point from the perspective of the wireless lock.
 - Client LQI: Analogous to the "LQI" values, these indicate the transmission quality of the data packets from 0 to 255. However, the client value indicates the access point value from the perspective of the wireless locks.
- Access point: A maximum of four GAT DL 091 RS485 access points can be connected to the GAT DC 7200. These are displayed in the list below.

Click on "Search new access points" to find newly connected access points. All detected access points are displayed in the list with consecutive numbering. These numbers are then displayed in the "Access point" column in the door list and show which access point a door is connected to or communicating with.

In addition to the number, the list also shows the serial number, the model name / article number, the firmware version, and the online status of each access point.
- Further information in the access point list:

The  symbol can be used to display further information on the access points:

 - Address: The network address of the access point.
 - Hardware: The hardware version of the access point.

ATTENTION! If an access point is expanded or a defective access point is replaced by a new one, the WiNET connection must be disconnected and reconnected for all connected locks after the replacement / expansion. When the WiNET connection is established, the previously configured access points are transferred to the locks once.

“Wireless lock” tab

Information on the wireless locks, e.g., GDL7m, which have been paired with readers is displayed here.

Door	State	Lock firmware	Lock serial number	RSSI
Door 1 (GDL7m)		99.0.15	D593F820EFCA	-46 dBm

Figure 6.26 – Web interface – Wireless lock settings

- Edit Icon: The edit icon in the first column allows you to disable the pairing between the wireless lock and the reader. Click on the edit icon and then the red link icon to disable the pairing.
NOTE! Only press the disable pairing button if absolutely necessary. For more information, see the manual of the respective wireless lock.
- Door: This field shows the name of the door to which the wireless lock is assigned.
- State: The following possible states for the wireless lock are shown here:
 - The first arrow icon is green, which indicates that communication between the lock and the reader is active. The second link icon is green indicating that the lock is paired with the reader.
 - The first warning symbol indicates that communication between the lock and the reader is inactive (possibly not within range). The green link icon indicates that the lock is still paired with the reader.
 - A red link icon indicates that pairing and communication between the lock and reader is inactive.
- Lock firmware: The current firmware version of the wireless lock is shown here.
- Lock serial number: The serial number of the wireless lock is shown here.
- RSSI: The value in the "RSSI" column indicates the strength of the wireless connection between the lock and the reader. A value less than -90 dBm (e.g., -100 dBm) indicates weak signal strength and possible communication problems. When the reader is installed within the recommended 2 m range of the wireless lock, the signal strength should be adequate.

“CardNET” tab

In this tab, the CardNET system can be enabled in the GAT DC 7200, which allows authorizations to be written onto data carriers that can then be used with battery-powered locks for authorization checks.

Figure 6.27 – Web interface – CardNET settings

The following settings can be defined here.

- Mode: This setting defines an operating mode for the CardNET system. Select one of the following options:
 - Industry: Select this setting for CardNET G2 data carriers or for CardNET G1 data carriers that have been coded with a segment labeled “Offline 1 (0A)”, which is the standard for most data carriers.
 - Hotel: Select this setting when the CardNET G1 data carriers have been coded with a segment labeled “Hotel (0C)”. The “Hotel” setting is only available for data carriers coded as CardNET G1.
 - Disabled: Select this option when CardNET G1 is not in use.
- Handling: This setting determines how the CardNET data is written to the data carriers.
 - Automatic: The CardNET data is written automatically when a data carrier is read. The prerequisite is that writing is enabled for the door (see “6.4.7 Door configuration”) and that the data should also be written/replaced according to the time settings (see setting below).
 - Manual: To write CardNET data to a data carrier, first press the “Coming” button on the reader and then hold the data carrier near the reading field. By pressing the “Leaving” button on the reader, the CardNET data can be deleted from the data carrier again.
 - Automatic and manual: The CardNET data is written automatically when a data carrier is read. The CardNET data can be deleted from the data carrier again by pressing the “Leaving” button.
- Handle battery segment: Select this option to read the battery condition of doors and forward this data to higher-level software.
- Write multi-tag data carriers: Select this option to allow data carriers with multiple technologies to be written.

NOTE! Do not use this setting if you have several types of data carriers in use but they are not combined onto one single card or key tag.
- Renewing for / Renewing before end: The periods for how long the authorizations are created and when they can be renewed are defined in these fields.

"SVN" tab

SALTO products use the Salto Virtual Network (SVN) technology to transport access authorizations. In combination with GANTNER coded data carriers, the "GANTNER SVN" technology is created, which is comparable to the existing CardNET technology. This function allows data carriers and locks from SALTO and GANTNER to be used together in a mixed system. The GANTNER SVN function can be enabled in the GAT DC 7200 on the "SVN" tab and applies globally to all readers connected to the GAT DC 7200.

i Certain requirements must be met to be able to use the GANTNER SVN function:

- SALTO ProAccess SPACE min. version 6.8
- GAT ACE 7000 min. version 2.2
- Firmware of the connected readers min. version 3.4.0
- Data carriers must be coded accordingly

For more information on this function, see also chapter "7. AUTHORIZATION".

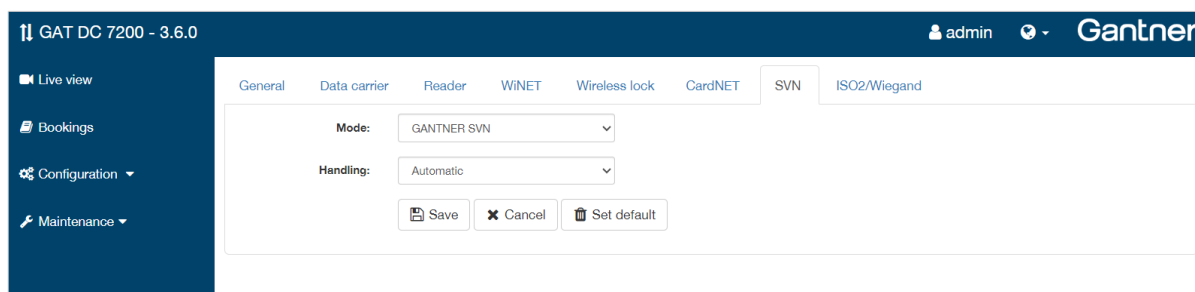
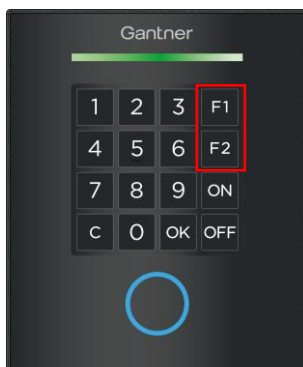


Figure 6.28 – Web interface – SVN settings

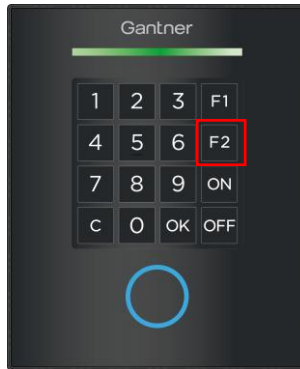
The following settings are configurable.

- Mode: Here you can enable the SVN function:
 - Disabled: Select this mode if you do not want to use the SVN function.
 - GANTNER SVN: Select this mode to enable SVN. This will allow the readers connected to the GAT DC 7200 to read and write SVN data.
- Handling: This setting determines how the reading and writing of SVN data to the data carriers will be carried out.
 - Automatic: The SVN data are automatically written to the detected data carriers and the bookings are read from the data carriers. A requirement for this is that the write function is enabled for the door (see "6.4.7. Door configuration").
 - Manual *: To write the SVN data to a data carrier, first press the "F1" key on the reader and then hold the data carrier before the reading field. The SVN data can be deleted from the data carrier by pressing the "F2" key on the reader.



- Automatic and manual *:

The SVN data are written automatically when reading a data carrier. The SVN data can be deleted from the data carrier by pressing the "F2" key on the reader.



* **NOTE!** For the two "manual" settings, please note that the "F1 + Identification" function must NOT be selected for the "Trigger threat alert" option in the alarm system settings (see "6.4.10 Alarm system settings"). This can lead to overlapping with the SVN function, which means that it is not executed correctly.

“ISO2/Wiegand” tab

In the “ISO2/Wiegand” tab, the settings for long-range readers, readers with other RFID technologies (e.g., PROXY 125 kHz readers), and user-defined formats, e.g., for vehicle recognition, can be defined.

Figure 6.29 – Web interface – ISO2/Wiegand settings

Various data formats and configuration options are available here for Wiegand or Omron readers that are connected via the “SUB” interface (see “4.3.3 Example connection: GR7.13xx and GAT SR 7000 Wiegand to a door”). Select one of the following data formats:

- ISO2 (Omron): For readers that connect via the Omron interface.
- Wiegand 26 bit / 37 bit (with system code): For readers that use the Wiegand interface (26 bit or 37 bit). A system-dependent code is also considered with the additional “Site code” entries. This can be entered into the displayed field.
- Custom format: This protocol allows you to define your own data format for the reader interface, e.g., when connecting a Wiegand reader with a special data format. Enter the offsets and lengths of the individual data fields according to the communication settings specified by the reader.

Site code:

Protocol:	Custom format	▼
Data length:	0	Bit
Site code offset:	0	Bit
Site code length:	0	Bit
Site code:	0	
Number offset:	0	Bit
Number length:	0	Bit
Data carrier type:	1	

- GAT Reader 550: Select this option for the GANTNER reader GAT Reader 550. In the "Assign channel x to" fields, you can select one of the doors defined in the GAT DC 7200 and assign it to the corresponding channel of the GAT Reader 550.

Protocol:	GAT Reader 550
Data carrier type:	1
	☐ Ignore unknown data carriers
Assign channel 1 to:	1: R&D Entry
Assign channel 2 to:	2: R&D Entry 2
Assign channel 3 to:	3: Office 1.3
Assign channel 4 to:	4: EDV 1.4

- GAT Reader 405 AP / 500 UP: Select this option for the GANTNER readers GAT Reader 405 AP or 500 UP.
- GAT Reader 86x / 900: This data format is intended for the long-range readers from GANTNER.
- Data carrier type: This option is available for all data formats and allows different types of data carriers that differ in technology (LEGIC prime, LEGIC advant, etc.) or in the CardNET generation or in their use with Salto ProAccess SPACE to be used together in one system. Here you can select which defined data carrier type should be assigned to the respective data format. More information about the data carrier types is provided in the GAT Matrix manual.
- Ignore unknown data carriers: If this option is enabled, bookings for all unknown data carriers that are sent via the Wiegand protocol are not saved in the GAT DC 7200. Enabling this option is recommended, e.g., for vehicle license plate recognition. Only the valid or known license plates are then recorded and unnecessary bookings, e.g., for visitor or guest license plates, are not saved. However, these unknown data carriers can still be processed by connected third-party software. Only the logging in the GAT DC 7200 is prevented.

6.4.9 Hardware extensions

The “Extensions” settings are used to manage hardware extensions such as lift controllers, locker control systems, images from video cameras, or online access management and the anti-pass-back function for doors.

“Relay expander” tab

The relays of the relay expanders connected to the GAT DC 7200 are displayed here. Up to two GAT IO 055 or up to 8 GAT IO 7054 or GAT IO 7055 can be used.

NOTE! Combined operation with GAT IO 055 and GAT IO 705x is possible; however, the total number of 64 relay outputs must not be exceeded.

Name	Relays	Inputs	Serial	Article	Firmware	Hardware	Port
Expander 1	1 - 8	1 - 16	2106000004	01105457 - GAT IO 7055 NW	99.22	02.00	2
Expander 2	9 - 16	17 - 32	2106000003	01105457 - GAT IO 7055 NW	99.22	02.00	2
Expander 3	17 - 24	33 - 48	2106000013	01105457 - GAT IO 7055 NW	99.22	02.00	2
Expander 4	25 - 32	49 - 64	2106000006	01105457 - GAT IO 7055 NW	99.22	02.00	2

Expander relay	Name	Used for	Locker number
Relay 1	Ext. Relay 1	General purpose	1
Relay 2	Ext. Relay 2	General purpose	2
Relay 3	Ext. Relay 3	General purpose	3
Relay 4	Ext. Relay 4	General purpose	4
Relay 5	Ext. Relay 5	General purpose	5
Relay 6	Ext. Relay 6	General purpose	6

Figure 6.30 – Web interface – Relay expander settings

- To detect the relay expanders connected to the GAT DC 7200, click on "Search new devices".
 - The found expanders are listed in the upper area of the window (e.g., in the example above, 4 GAT IO 7055 NW relay expanders are used).
- You can edit the name as well as the relay and optocoupler ID numbers. To do this, click on the edit icon (✎) next to a relay expander.
 - The following window opens.

Expander 1

Name:

Relay start id:

Input start id:

Figure 6.31 – Relay expander details

- ▶ You can define a new name for the relay expander here or use the default name.
- ▶ The numbers in the "Relay start ID" and "Input start ID" fields define the start numbers of the relay outputs and status inputs.
 - Depending on the number of inputs and outputs, the remaining inputs/outputs are then numbered in ascending order.

All relays of the connected relay expanders are displayed in a list. In the column "Expander Relay" you can see the ID numbers of the relays according to the automatic numbering starting with the set ID start number.

- ▶ In the "Name" column, you can enter a designation for each relay, e.g., its use. This name is then also displayed in GAT Matrix when defining the relay plans.
- ▶ In the "Used for" column, select the desired relay function:
 - "General purpose": Sets the relay(s) for general purposes. Any relay with this setting can be selected for door configuration or when configuring the alarm system.
 - "Door Name": Assigns the relay(s) to a door. The relay will then not be available for selection at another door.
- ▶ When an elevator license has been installed on the GAT DC 7200, the relays can also be used for elevator controllers or locker control systems.
- ▶ The process for configuring locker control is the same as for elevator control, however, select "Locker control" instead of "Normal" in the "Door mode" field.

"Security camera" tab

In the "Security camera" tab, a video camera can be configured for each door. The image from this video camera can then be displayed in the "Live view" of the doors.

Door	URL
1: R&D Entry	http://192.168.8.123/livcam1/hksjdthfknck
2: R&D Entry 2	http://192.168.8.124/livcam2/hksjdthfknck
3: Office 1.3	http://192.168.8.125/livcam3/hksjdthfknck
4: EDV 1.4	http://192.168.8.126/livcam4/hksjdthfknck

Save Cancel Delete

Figure 6.32 – Web interface – Security camera settings

- ▶ Enter the URL for the video stream of the video camera you are using into the field "URL". You will find this information in the manual of the video camera.

If a camera is configured for livestream, the "Live view" is reproduced. If only one frame is configured, the current image can be displayed in the browser by pressing F5 (update).

“Online access management and APB” tab

In the “Online access management” tab, two options for each configured door are available that allow you to set the door for use with online access management and the Anti-Pass-Back (APB) function.

Door	Online access management	Anti-pass-back
1. Main entrance	☒	☒
2. Server room 1	☐	☐
3. Engineering	☐	☐
4. Printer room	☐	☐

Server timeout: s

Save Cancel Set default

Figure 6.33 – Web interface – Online access management and APB settings

Online access management is only applicable for persons that are not known in the GAT DC 7200. When these persons identify themselves at a door, their data is sent to the GAT ACE 7000 online management interface and a server software must decide whether the person is allowed access or not. The server software can be a visitor management, a ticketing solution, or any other organization software that is connected to the online management interface.

Anti-Pass-Back is used to control repeated entries with the same data carrier. An exit is only allowed if the previous action was an entrance and vice versa. The APB check is only possible if persons are known in the GAT DC 7200, the GAT ACE 7000 APB is installed and configured, and all controllers of an access zone are online.

NOTE! If the APB function is used, it is not possible to anonymize the bookings as the GAT ACE 7000 APB would only receive anonymous bookings and therefore cannot make any access decisions.

Booking configuration

Number of system bookings:

Number of person bookings:

☐ Anonymize person bookings

☐ Create bookings at database import

Save Cancel Set default Delete all bookings

Figure 6.34 – Person bookings cannot be anonymized when the APB is used

If the bookings are anonymized, online management is possible as only unknown persons are sent via the online management interface. These persons are unknown to the GAT DC 7200 (anonymous) and the software that makes the online management decision may, if necessary, anonymize the bookings itself.

6.4.10 Alarm system settings

The settings for the handling of an alarm system in the facility are valid for the GAT DC 7200 generally and do not refer to a specific door but to the entire controller. In the door configuration, it is possible to define which doors are influenced by the alarm system or which doors can influence it.

The screenshot displays the 'Alarm system' configuration page in the GAT DC 7200 web interface. The left sidebar contains a navigation menu with options: Live view, Bookings, Configuration, Doors, Readers, Extensions, Alarm system (selected), Database, Power over RS485, Security and user, Ethernet, Date and time, and Maintenance. The main content area is titled 'GAT DC 7200 - 3.3.4' and shows the 'Alarm system' settings. The 'General settings' section includes: 'Enable alarm system area' with checkboxes for Area 0 (checked), Area 1, Area 2, and Area 3; 'Alarmed status LED' set to 'Green'; 'Turn on verification' set to 'No verification'; 'Turn off verification' set to 'Pin code'; 'Turn off automatically if authorized' (checked); 'Allow identification with PIN code' (checked); 'Threat pin mask' (empty field); and 'Trigger threat alert' set to 'Identification + threat PIN code'. Below this are two sections for 'Area 0: Output settings' and 'Area 0: Input settings'. The 'Area 0: Output settings' section includes 'Turn on relay' and 'Turn off relay' with 'Output' set to 'Disabled', 'Mode' set to 'Active', and 'Time' set to '1 s'. The 'Area 0: Input settings' section includes 'Alarm system ready for activation' and 'Alarm system active' with 'Input' set to 'Disabled' and 'Mode' set to 'Active'. At the bottom of the main content area are buttons for 'Save', 'Cancel', and 'Set default'.

Figure 6.35 – Web interface – Alarm system settings

The following settings can be defined in the “Alarm system” menu:

- Enable alarm system area: Here you can enable or disable the alarm system for the different areas.
- Alarmed status LED: The color of the LED that indicates an activated alarm system is defined here.
- Turn on/off verification: Select whether verification at the GAT DC 7200 is required for switching on/off the alarm system, and if so, how the verification is carried out.
 "Turn off automatically if authorized": When this option is enabled, an active alarm is automatically disarmed by a valid identification, e.g., for an access.
 "Allow identification with PIN code": When this option is enabled, an alarm can be disarmed by a valid identification using a PIN code.
- Threat pin mask: Here, a threat PIN code can be defined for the controller that can be used by all valid persons to trigger a silent alarm in the event of a threat or an attack. The input of the threat code must be 8 characters long. The characters "x" or "*" can be used as placeholders. Only a few digits of the threat code are defined with the remaining digits represented by a placeholder.

Example:

Personal PIN code	-	-	-	-	1	2	3	4
Threat PIN code	x	x	x	9	x	x	x	9
PIN code to trigger the threat alarm	-	-	-	9	1	2	3	9

To trigger the threat alarm, the user must enter the corresponding digit of their personal PIN code instead of the placeholder. Leading zeros do not have to be entered.

NOTE!

- Ensure that a person's personal PIN code is not identical to the threat PIN code, as this would trigger an alarm each time the personal PIN code is entered.
- The threat PIN code can only be entered when PIN code entry is enabled for regular access.

- Trigger threat alert:

Select here how the user can trigger the silent treat alarm. Two options are available:

Identification + threat PIN code: Default option. To trigger the threat alarm, the user must enter their threat PIN code as defined in the previous "Threat pin mask" setting.

F1 + identification: To trigger the threat alarm, the user must press the F1 key on the GR7.2310 keypad before identification is completed. This option can be used when the PIN code input setting is not permanently enabled.

NOTE! F1 + identification

1. This option is only available for GR7.2310 readers connected to the GAT DC 7200.
2. On the "Configuration -> Readers" -> "CardNET" page, "Automatic" must be set for the "Handling" setting. If not, a corresponding message is displayed when the "F1 + identification" option is being used.

- Output settings:

The "Turn on relay" and "Turn off relay" outputs of the GAT DC 7200 or the connected readers can be assigned to the applicable functions for switching the alarm system on and off. Either use two separate outputs or the same output for arming and disarming the alarm system.

The "Attempt to turn on when not ready" output can be used to log an attempted arming of the alarm system when the alarm system is not ready. If this occurs, a signal is sent to the alarm system where the arming attempt is logged, which can be used as evidence in cases that involve the police and insurance companies. The same relay can also be defined for this output as for the "Turn on relay" output, which means that only one contact must be wired to the alarm system.

NOTE! The input "Alarm system ready for activation" should still be used so that the user is informed whether the alarm system is ready or not.

For all relay outputs, the time can be set to enable and/or disable, e.g., to only send a pulse with the entered time or to output a continuous signal when entering "0" (e.g., output activated if the alarm system is armed). "Active" mode means that the output is activated when the function is active. "Passive" means the output is activated when the function is not active.

- Input settings: The optocoupler inputs of the GAT DC 7200 or the connected readers can be assigned to the applicable functions for the status detection of the alarm system. With the "Alarm system ready for activation" function, the activation of the alarm system can be performed depending on the state of this input signal. This can prevent the alarm system from being armed in certain cases (i.e., provided the function is not activated). The alarm system can be activated via a signal with the "Alarm system active" input. "Active" mode means that the respective function is only active when a signal is applied. With "Passive" mode, the function is only active when no signal is applied.

6.4.11 Database settings

In the "Database" menu, you can specify the memory size for system events and person/door-related bookings. Both types of memory are cyclical memories where the oldest event is overwritten when the memory is full.

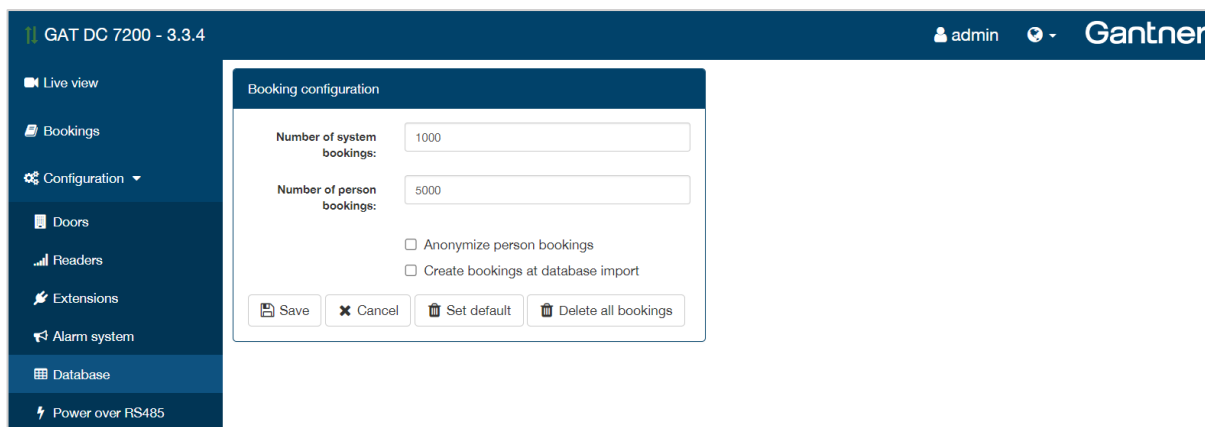


Figure 6.36 – Web interface – Database settings

Regardless of these settings, only the last 1000 bookings are displayed in the GAT DC 7200 booking display. More bookings can only be made via the interface.

The "Anonymize person bookings" option can be used to ensure that no names or personnel information are displayed for person-related bookings. If this function is deactivated again, the information in the bookings is displayed again. Please read the notes for the Anti-Pass-Back function provided in the section "Online access management and APB" tab.

If the "Create bookings at database import" option is enabled, a booking is generated to document that the controller has been loaded with new data. The database import booking is displayed on the "Bookings" page (see chapter "6.6 Bookings").

6.4.12 Power over RS-485

This function allows you to switch the power supplied from the “Reader” and “Sub” ports on and off. In this way, a reader or connected device can be depowered, e.g., to switch off a GAT IO 705x relay expander.

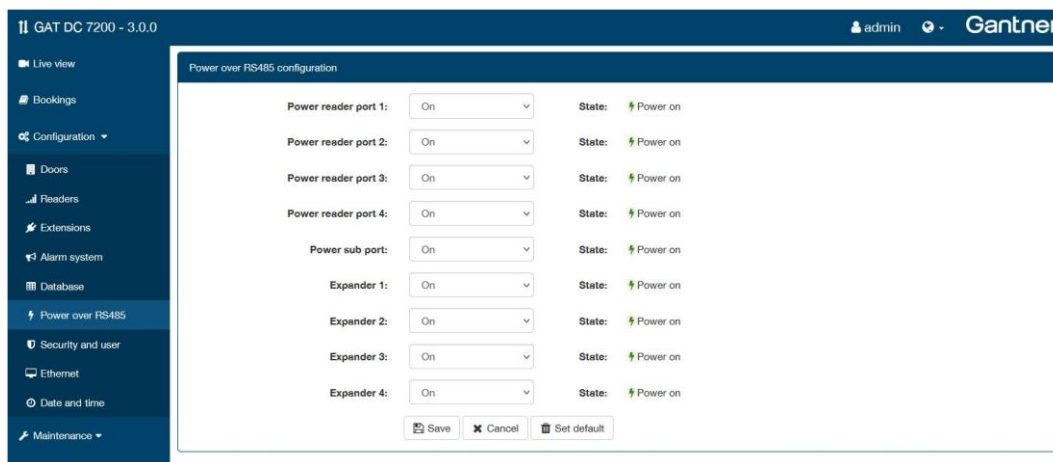


Figure 6.37 – Web interface – Power over RS-485 settings

In the event of a short circuit or an overload on the connection, the power supply is automatically switched off to protect the GAT DC 7200 and the connected devices. The power status is displayed.

6.4.13 Security and user

In the “Security and user” menu, various security settings can be configured in the “Security options” area, and additional users created in the “User configuration” area.

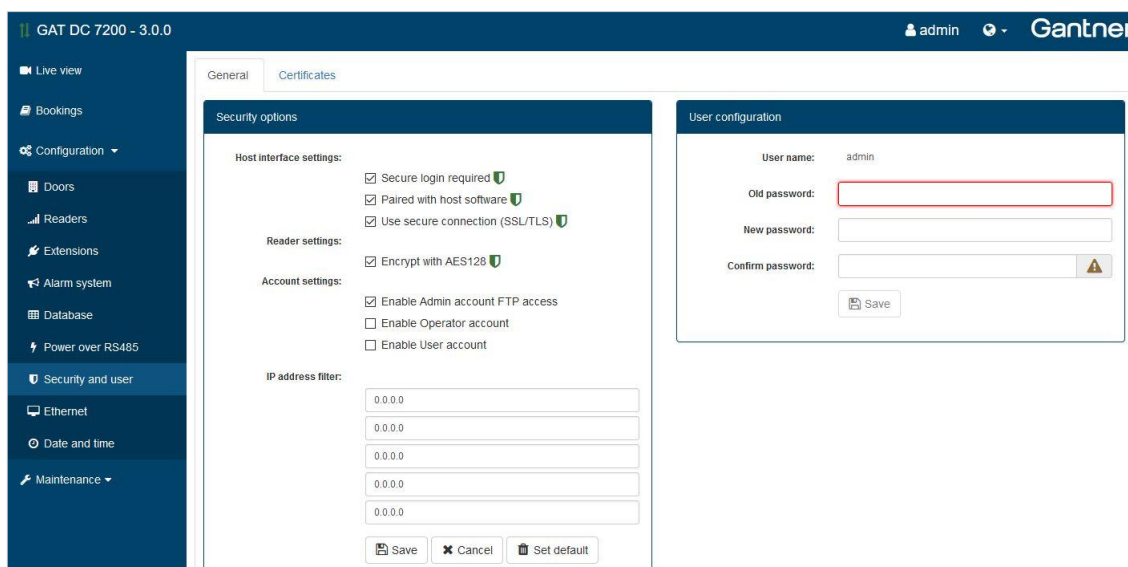


Figure 6.38 – Web interface – Security and user settings

“General” tab -> “Security options” area

- Secure login required: This function requires a secure connection to GAT Matrix and a multi-level authentication method. It is strongly recommended to enable this function and only disable it in instances where the accessibility software is not supported.
- Paired with host software: This function indicates that the access software has changed the password for host communication. If the access software is modified, the deactivation of this function allows the password for host communication to be reset to the default so that reconnection is possible.
NOTE! This configuration is not available when the GAT DC 7200 is used in standalone mode.
- Use secure connection (SSL/TLS): The connection to the GAT ACE 7000 can be encrypted using a TLS connection to increase security against interception. Enable this option to do this. The valid certificate for the TLS connection (GAT ACE 7000 and configuration website) must be installed on the PC (see "6.4.1 Certificate configuration for TLS/SSL connection").
NOTE! GANTNER recommends enabling this option for security reasons.
- Encrypt with AES 128: This function provides encrypted communication between readers and the GAT DC 7200. This setting should only be disabled when readers that do not support encrypted communication are connected.
- Enable Admin account FTP access: This function determines whether the “Admin” user can access the GAT DC 7200 via FTP to exchange files in this way.
- Enable Operator/User account: These functions determine whether the “Operator” and “User” users are available or not. The “Operator” user can use the “Live view” and “Bookings” menus, and the “Access rights” menu in standalone mode but cannot perform any configuration or maintenance work. For the “User” user, only the “Live view” is available. The passwords must meet certain requirements (see next page).
- IP address filter: The settings in this area define whether the GAT DC 7200 can be accessed from any computer (all fields set to 0.0.0.0) or only from the computers (IP addresses) defined in these fields.
NOTE! If the IP address filters are used, ensure that the computer where the configuration is made and the computer via which the software communicates are included here.

"General" tab -> "User configuration" area

In the "User configuration" area, the password of the administrator and the users can be changed.

NOTE! As of firmware version 3.6 it is mandatory to change the default password to a secure password!

The default password for the "Operator" and "User" users is "GAT".

NOTE! It is also mandatory for these users to replace the default passwords with secure passwords. The "Administrator" user can override the passwords for these two users and replace them.

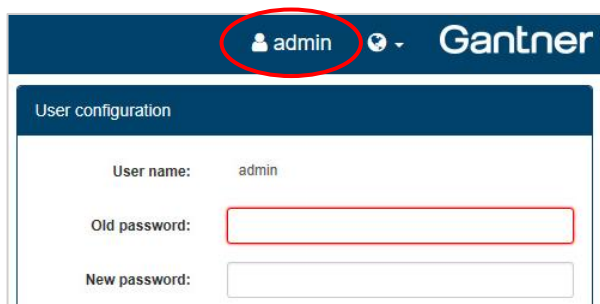


Figure 6.39 – Current user

- The logged-in user can also change their password by clicking on their username (top right near the logo) and entering a new password in the window.

NOTE! The password must be at least 8 characters long and contain at least 1 upper case letter, 1 lower case letter, and 1 number.

- With the "Change user" function in this window, the logged-in user can also be changed.

In the "Live view", the **Security**  symbol indicates that all the security settings are set optimally. If a security setting is not activated or the password of the "Admin" user is still set to the default, this is indicated by the **Security**  symbol.

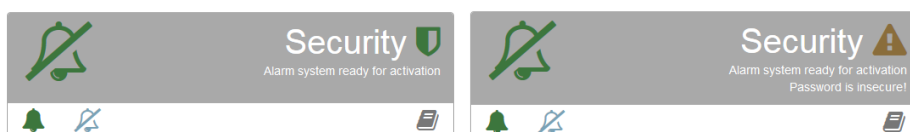


Figure 6.40 – Display of the strength of the security settings

"Certificates" tab

In this area a certificate can be created and downloaded from the GAT DC 7200. This is required to carry out the configuration and communication with GAT ACE via a secured TLS/SSL connection. Instructions for the necessary settings in GAT ACE can be found in the GAT ACE software manual.

NOTE! It is recommended to use a Firefox or Microsoft Edge browser. With other browsers, downloading may only be possible in a roundabout way (see "6.4.1 Certificate configuration for TLS/SSL connection").

There are generally two options for creating a certificate:

- The GAT DC 7200 can create a certificate, or
- A certificate request can be created, which then must be signed by a registered certification authority.

Figure 6.41 – Create certificate for TLS

a) Create a self-signed certificate

In the "Server certificate" field, the data that will be used for the certificate when the GAT DC 7200 creates the certificate is displayed.

- To have the GAT DC 7200 create the certificate, click "Create new self-signed certificate".
 - Click on "Download server certificate".
 - You can use this to download the created certificate to the computer as a .cer file. This file must then be installed on the PC. This is described in section "6.4.1 Certificate configuration for TLS/SSL connection" and in the GAT ACE manual for GAT ACE.
- NOTE!** On the PC where you only want to access GAT ACE 7000 via Viewer or where you configure GAT DC 7200 via web browser, please select "Local Computer". On the PC where the GAT ACE 7000 service is running, please select "Current User" and install the certificate with "Local Computer" if the GAT ACE 7000 viewer is to be used.

b) Create certificate request for certification authority

In the "Certificate signing request (CSR)" area, enter the data for the certificate.

- Enter the data for your company and the door controller here.
- In the "Alternative name" fields, you can enter the network name for example. If the IP address changes, the TLS connection can still be established via the network name.

NOTE! Windows 8.1 or earlier Windows versions do not support IP addresses in the alternative name fields.

- Click "Create CSR".
 - The request file will be saved to the PC as a CSR file.

- ▶ Specify the storage location in the file window.
- ▶ Send the file to the certification authority.
- ▶ On the PC, install the root certificate of the certification authority as described in “6.4.1 Certificate configuration for TLS/SSL connection”.
- ▶ Install the certificate received from the certification authority (in PEM or DER format) in the GAT DC 7200 by dragging the certificate file into the "Drag signed certificate here" field.
 - The certificate is installed in the GAT DC 7200 and the controller must be restarted.

The screenshot shows the 'Create certificate for TLS' interface. On the left, there's a box with 'Signed using: ECDSA with SHA256' and 'Key size: EC 256 bits'. Below it is a 'Download server certificate' button. At the bottom left are 'Restart controller' and 'Create new self signed certificate' buttons. On the right, there are input fields for 'Common name (domain name or IP): DC7x_Alex_T1', 'Alternative name: DC7x_Alex_T1', and 'Alternative name: 10.1.112.125'. Below these is a 'Create CSR' button. At the bottom right is a dashed box labeled 'Drag signed certificate here' with the text 'Import successful, reboot required'.

Figure 6.42 – Create certificate for TLS

- ▶ Click on “Restart controller”.
 - The controller restarts automatically, and the configuration interface is displayed again after approx. 30 seconds.

6.4.14 Network settings

In the “Ethernet” menu, the network settings of the GAT DC 7200 can be changed.

The screenshot shows the 'Ethernet configuration' page in the GAT DC 7200 web interface. The sidebar on the left has 'Ethernet' selected. The main area contains the 'Ethernet configuration' form with the following fields: DHCP (On), NetBIOS name (DC7x_1803000085), Static IP address (0.0.0.0), Static subnet mask (0.0.0.0), Static def. gateway (0.0.0.0), Static DNS1 (0.0.0.0), Static DNS2 (0.0.0.0), Port (8000), Maximum Transmission Unit (MTU) (1500), and Mode (Auto negotiate). At the bottom of the form are 'Save' and 'Cancel' buttons. To the right, a 'Current Ethernet settings' box shows: MAC (00:12:08:C0:F4:BD), IP address (10.1.112.14), Subnet mask (255.255.255.0), Def. Gateway (10.1.112.254), DNS1 (10.15.0.1), and DNS2 (10.1.14.1).

Figure 6.43 – Web interface – Ethernet settings

On the right side under "Current Ethernet settings", the network settings currently set for the GAT DC 7200 are displayed. On the left side under "Ethernet configuration", the settings for the controller can be defined:

- DHCP: By default, the DHCP function is activated (On) for the GAT DC 7200. You can activate or deactivate DHCP function here.
- NetBIOS name: The network name of the GAT DC 7200. By default, this is set to "DC7x_nnnnnnnnnn" where nnnnnnnnnn is the serial number of the controller. The serial number can be found on the device label or on the packaging.
For networks that use a DHCP server, you can use the following network name to access the controller and change the settings:
`http://DC7x_nnnnnnnnnn`
- IP address, subnet mask, gateway, DNS: Here you can define the IP addresses for the controller, the gateway, and the Domain Name Services and also define the subnet mask. These settings depend on your network configuration. When using a DHCP server, the server sets the IP address of the controller. For networks without a DHCP server, you can use the GAT Device Finder software to find the controller and change the network settings to the desired values.
- Port: Set the port number that is used for communication with GAT ACE 7000. The following default ports are used for communication:
 - GAT ACE 7000: 8000
 - FTP: 20 and 21 (as of GAT ACE 7000 version 3.0, FTP is no longer required)
 - Webserver (accessing the UI): as of GAT DC 7200 firmware version 3.0, port 443 (encrypted connection via TLS/SSL). Older versions still use port 80.
 - NTP port for time synchronization: 123 UDP outgoing.
 - GAT DIRECT.Connect: default 8239
- MTU In customer networks or with VPN connections, it is possible that communication with the GAT DC 7200 will not operate properly. This issue is caused by jumbo frames that are used in Gigabit networks or can be caused by the overhead of VPN connections.
The GAT DC 7200 communication is based on the IEEE 802.3 Ethernet Standard (10/100 MBit) where the maximum package size is 1472 bytes. Jumbo frames are Ethernet frames with more than 1500 bytes of payload and are not part of IEEE 802.3.
Reducing the server's maximum transmission unit (MTU) value so that the maximum packet size of the VPN is not exceeded can assist in solving the problem.
- Mode: Select the communication mode (speed and duplex). With the "Auto negotiate" setting, the mode is selected automatically.

6.4.15 Date and time

In the "Date and time" menu, the date and time of the GAT DC 7200 can be set and settings for automatic time synchronization can be defined.

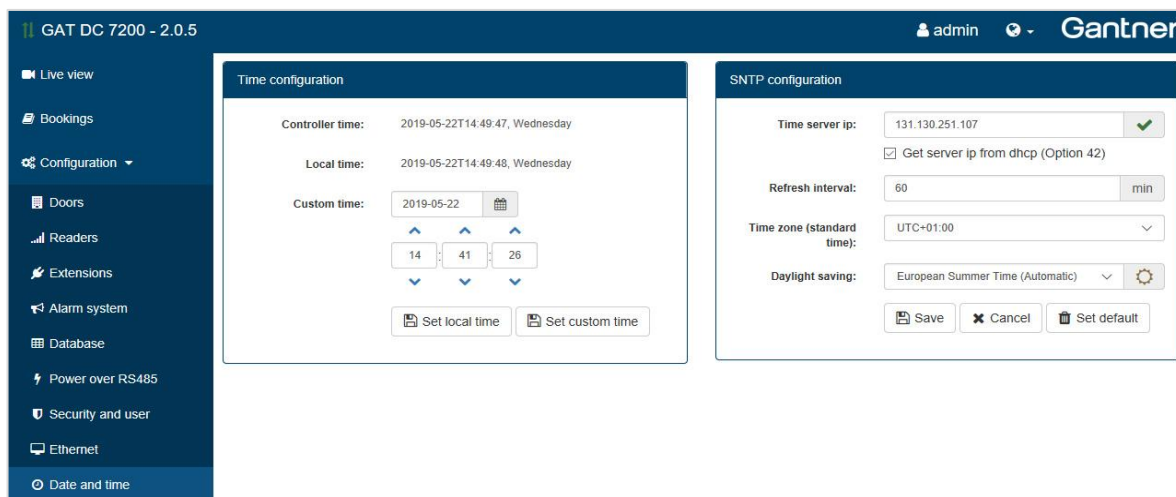


Figure 6.44 – Web interface – Ethernet settings

On the left side under "Time configuration" there are two possibilities to set the date and time of the controller.

- Set local time: This button sets the date and time of the controller to the values of the current computer (as shown next to "Local time").
- Set custom time: This button is used to set the date and time of the GAT DC 7200 manually. Therefore, enter the desired date and time into the "Custom time" fields.

The standard method for time management is to define a time server from which the time is retrieved at regular intervals (defined via "Refresh interval") or when the GAT DC 7200 restarts. This can be defined under "SNTP configuration" to the right.

- Time server ip: Enter the address of the time server in this field. Alternatively, the IP address can be set by a DHCP server (if a DHCP server is used and supports this functionality) by selecting the option "Get server ip from dhcp (Option 42)".
- Refresh interval: Time period in minutes defining how often the time will be synchronized.

Set the time zone and enable/disable the daylight-saving setting according to the controller's location.



To the right of the daylight-saving setting, a symbol indicates whether the controller is currently in winter- (snowflake) or summertime (sun).

6.5 Configuring Mobile Credential

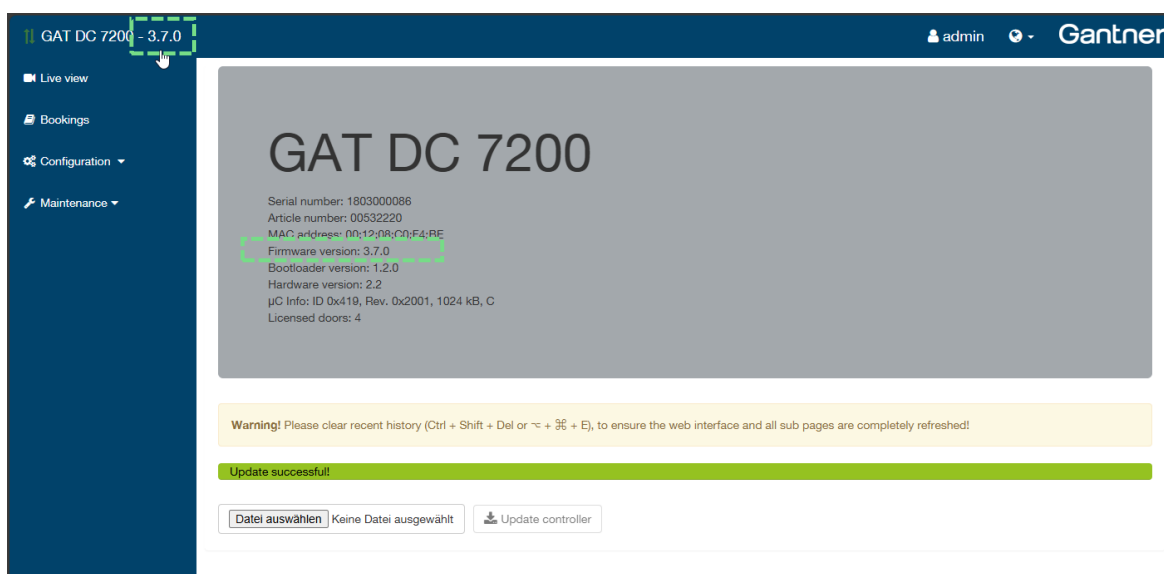
To use Mobile Credential with a GAT DC 7200 and a connected reader, the appropriate license and some configuration steps are required. Afterwards, users can identify themselves to the access control system using their mobile device, such as a smartphone or smartwatch with the stored access credentials.

This section describes the configuration steps necessary for using Mobile Credential. Please also note the prerequisites for Mobile Credential (see "2.7. Mobile Credential").

The following description assumes that the mobile credentials were created via LEGIC Connect. In this case, all necessary settings can be applied as described, and the required parameters can be generated and provided via LEGIC Connect.

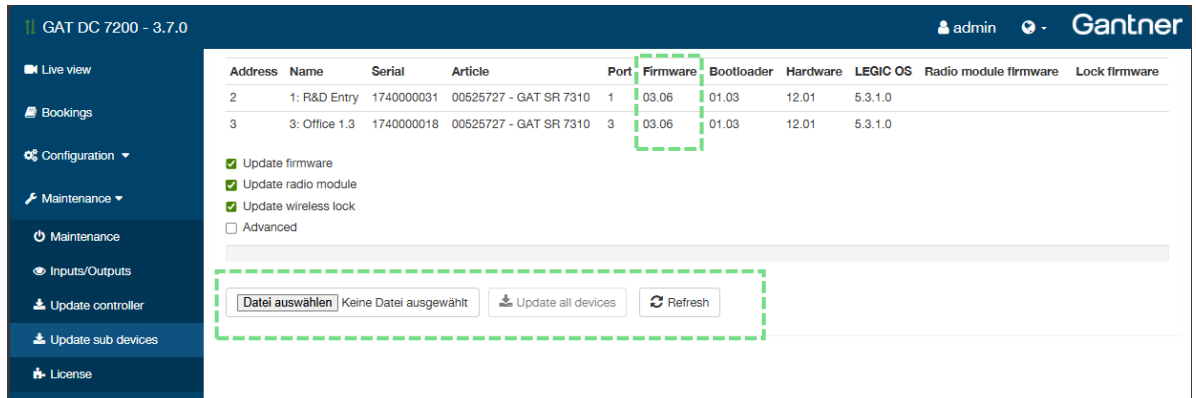
If mobile credentials created on other platforms are to be used, the parameters must be provided in a comparable manner via that platform. It is recommended to check the compatibility of the credentials during project planning.

- The controller firmware must be at least version 3.7. You can see the version number in the header of the web interface. You can update the firmware using the "Update Controller" menu in the "Maintenance" section. You will need the appropriate firmware file from the Gantner partner page.



After loading the file into the controller, it will restart and the new version number will be displayed. See "6.7.3. Update controller".

- Readers on which the Mobile Credential function is to be used must have at least firmware version 3.06. You can update the readers in the "Update sub devices" menu. The current firmware version of the readers is also displayed there.



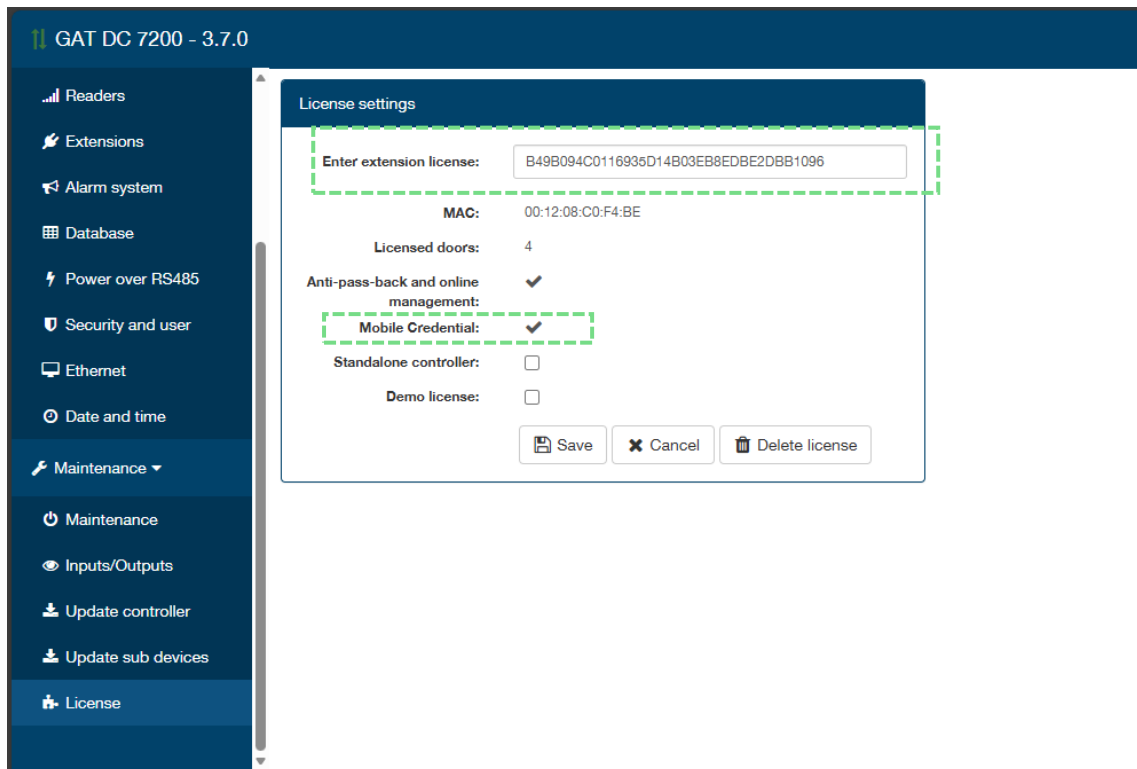
The list shows all connected readers. The "Firmware" column displays the firmware version of each reader.

To update the firmware of one or all readers, download the latest reader firmware from the Gantner Partner Page. Then select the file (extension ".enc") by clicking "Select File" and load the new firmware file onto the readers. Click "Update All" to complete the process. During the update, the LED indicators on the readers will flash in a colorful sequence. For more information, see "6.7.4. Update sub devices".

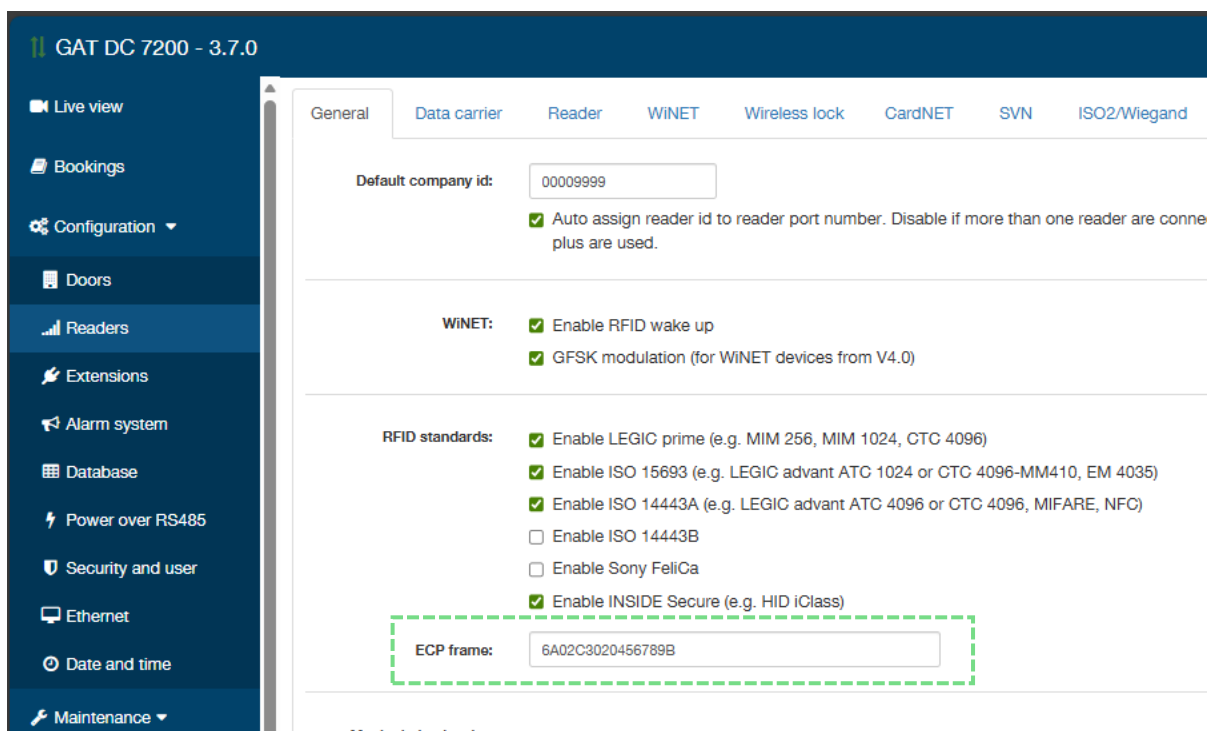
- The operating system (OS) of the LEGIC chip must be at least version 5.3.1. You can also find this version on the "Update sub devices" page in the "Maintenance" section, specifically in the "LEGIC OS" column. To update this OS version, you can load the appropriate update file (extension ".bin") into the readers, similar to a firmware update. During the update, an alternating red/green flashing light will be displayed on the readers.
- Now you need to activate the Mobile Credential license. To do this, go to the "License" page in the "Maintenance" section. In the "Enter extension license" field, enter the license code for the Mobile Credential license. Then click "Save".

When the Mobile Credential license is activated, the entry of the same name with a checkmark symbol is displayed, as shown in the following image. Otherwise, this line is hidden.

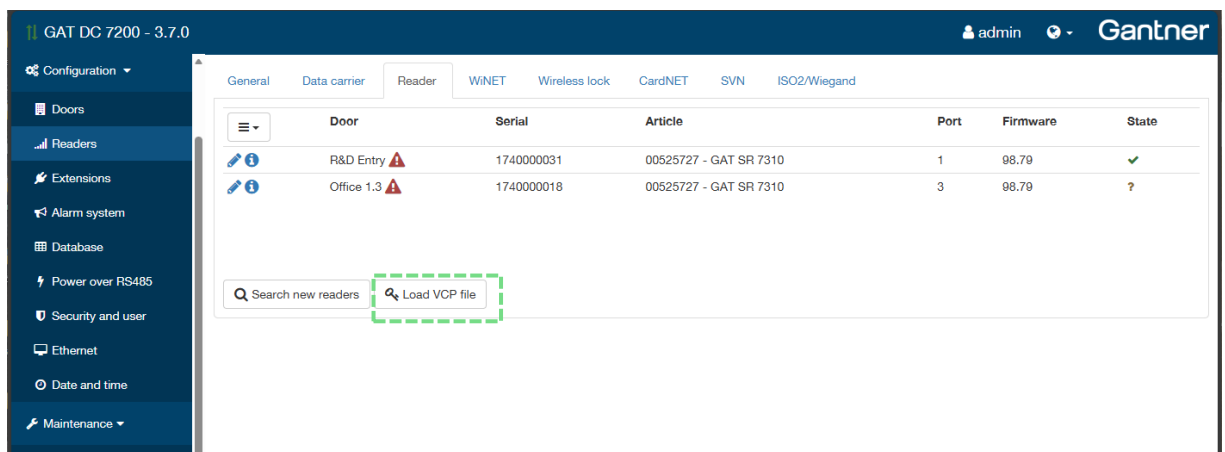
NOTE: Activating the demo license allows you to test whether mobile credentials not issued via LEGIC Connect can be used with the controller and readers. This unlocks the necessary settings for 4 days without having to purchase a mobile credential license.



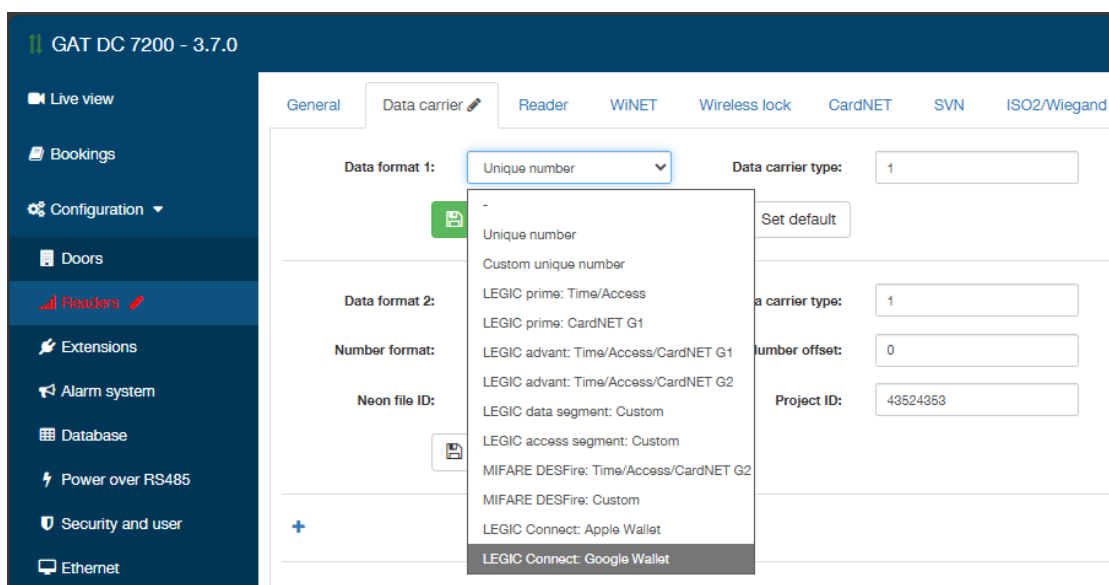
- After activating the Mobile Credential license, an additional field "ECP frame" will appear in the reader settings (page "Readers - General" in the "Configuration" section). Enter the number for the ECP frame (in hexadecimal format) there and confirm by clicking "Save". See also "6.4.8. Reader configuration".



- Now the VCP file must be loaded on the readers. This file contains the LEGIC configuration parameters for the readers. To do this, go to the "Configuration" section, "Readers" menu, "Reader" tab.".
Reading mobile credentials on the readers will only be possible after the VCP file has been loaded. For security reasons, a password must be entered to activate the VCP parameters on a reader.
Successful loading is indicated by a green checkmark next to the respective reader. For more details, see "6.4.8. Reader configuration".
NOTE: VCP files for SM-4xxx chips are required for GR7 and GAT S(L)R 73xx readers.



- As a next step, configure the settings for the Mobile Credential IDs so that the identification data from the Mobile Credentials is processed and read correctly. To do this, go to the "Configuration" section, "Readers" page, "Data carrier" tab.
A data format is required for each data carrier type and must be configured accordingly. For Mobile Credential, add a new data format (using the "+" button) and then select "LEGIC Connect: Apple Wallet" or "LEGIC Connect: Google Wallet". The settings for these data formats must be configured correctly. See example and "6.4.8. Reader configuration" – tab "Data carrier".



- ▶ With the steps described here, the GAT DC 7200 and readers are prepared for the use of mobile credentials.
- ▶ The credentials must still be stored in Apple or Google Wallet on the mobile device.
The correct procedure for creating and storing the wallet credentials on mobile phones must be clarified with the issuer of the wallet credentials.
Wallet credentials cannot currently be issued via Gantner platforms (e.g., Matrix). Only the assignment of issued wallet credentials to existing users can be done in Matrix or, in stand-alone mode, in the controller's web interface.

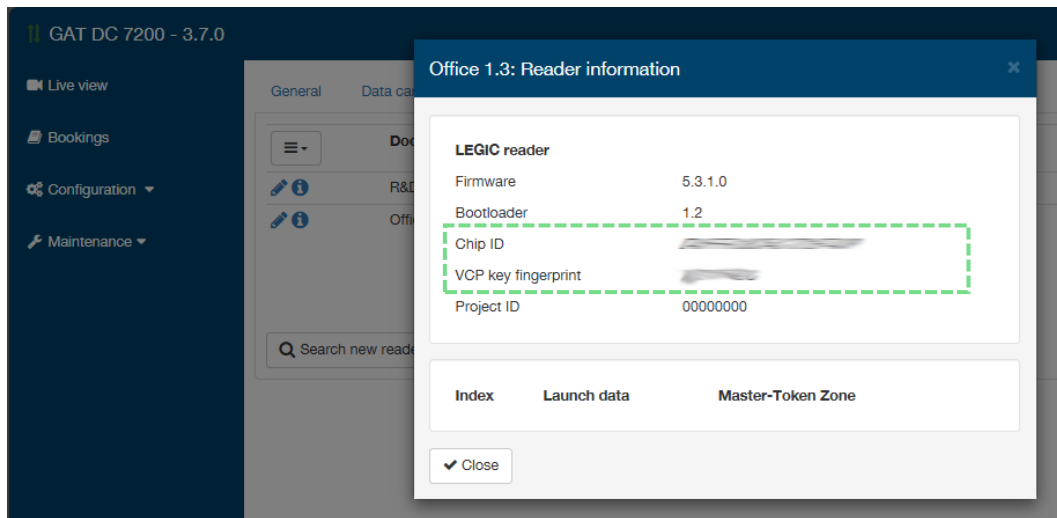
6.5.1 Delete VCP from a reader

To remove a loaded VCP from a reader, a "Remove VCP" file must be loaded. You can obtain this from your wallet credentials provider.

i Please note that if a reader is returned to Gantner, e.g. for repair or service purposes, the VCP must be deleted from the reader before it is returned, or a Remove VCP must be provided to Gantner for the corresponding chip ID and VCP password.

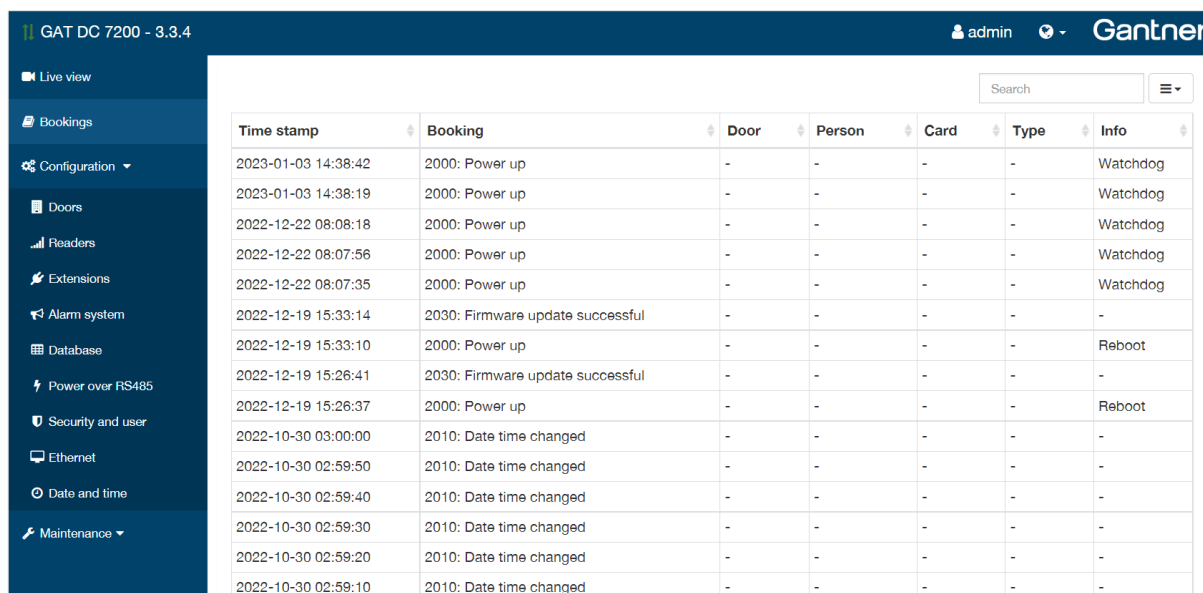
Each Remove VCP is bound to the chip ID of a reader chip and therefore must be created individually for each reader.

i To delete a VCP from a reader, in addition to the VCP password and the "Chip ID," the reader's "VCP Key Fingerprint" is also required. You can display this information by clicking on the icon  next to the relevant reader.



6.6 Bookings

In the “Bookings” area, the bookings for all doors as well as system-related bookings for the controller are displayed.



Time stamp	Booking	Door	Person	Card	Type	Info
2023-01-03 14:38:42	2000: Power up	-	-	-	-	Watchdog
2023-01-03 14:38:19	2000: Power up	-	-	-	-	Watchdog
2022-12-22 08:08:18	2000: Power up	-	-	-	-	Watchdog
2022-12-22 08:07:56	2000: Power up	-	-	-	-	Watchdog
2022-12-22 08:07:35	2000: Power up	-	-	-	-	Watchdog
2022-12-19 15:33:14	2030: Firmware update successful	-	-	-	-	-
2022-12-19 15:33:10	2000: Power up	-	-	-	-	Reboot
2022-12-19 15:26:41	2030: Firmware update successful	-	-	-	-	-
2022-12-19 15:26:37	2000: Power up	-	-	-	-	Reboot
2022-10-30 03:00:00	2010: Date time changed	-	-	-	-	-
2022-10-30 02:59:50	2010: Date time changed	-	-	-	-	-
2022-10-30 02:59:40	2010: Date time changed	-	-	-	-	-
2022-10-30 02:59:30	2010: Date time changed	-	-	-	-	-
2022-10-30 02:59:20	2010: Date time changed	-	-	-	-	-
2022-10-30 02:59:10	2010: Date time changed	-	-	-	-	-

Figure 6.45 – Web interface – Bookings display

Every action, permitted entry, and access attempt is recorded by the GAT DC 7200 and displayed here with the respective times and applicable person identified via their data carrier. A maximum of 1000 bookings can be displayed via the web interface. If you want to evaluate further bookings, you can do this using the GAT Matrix software.

Click on the  button to show or hide additional columns of information.

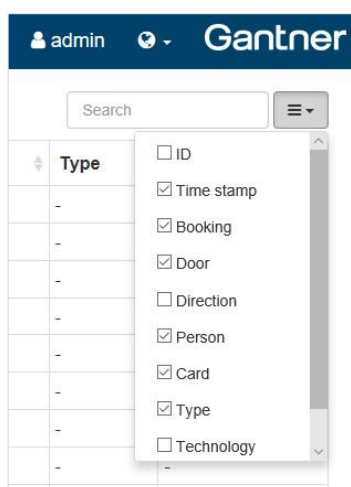


Figure 6.46 – Web interface – Show/hide additional information on the “Bookings” page

6.7 Administration and maintenance

Various administration and maintenance tasks can be performed via the "Maintenance" menu and the sub-menus therein.

6.7.1 Maintenance

"Controller" tab

In the "Maintenance" area under the "Controller" tab, various information on the GAT DC 7200 is available including the firmware and hardware version, serial number, part number, the number of licensed doors, and the memory usage.

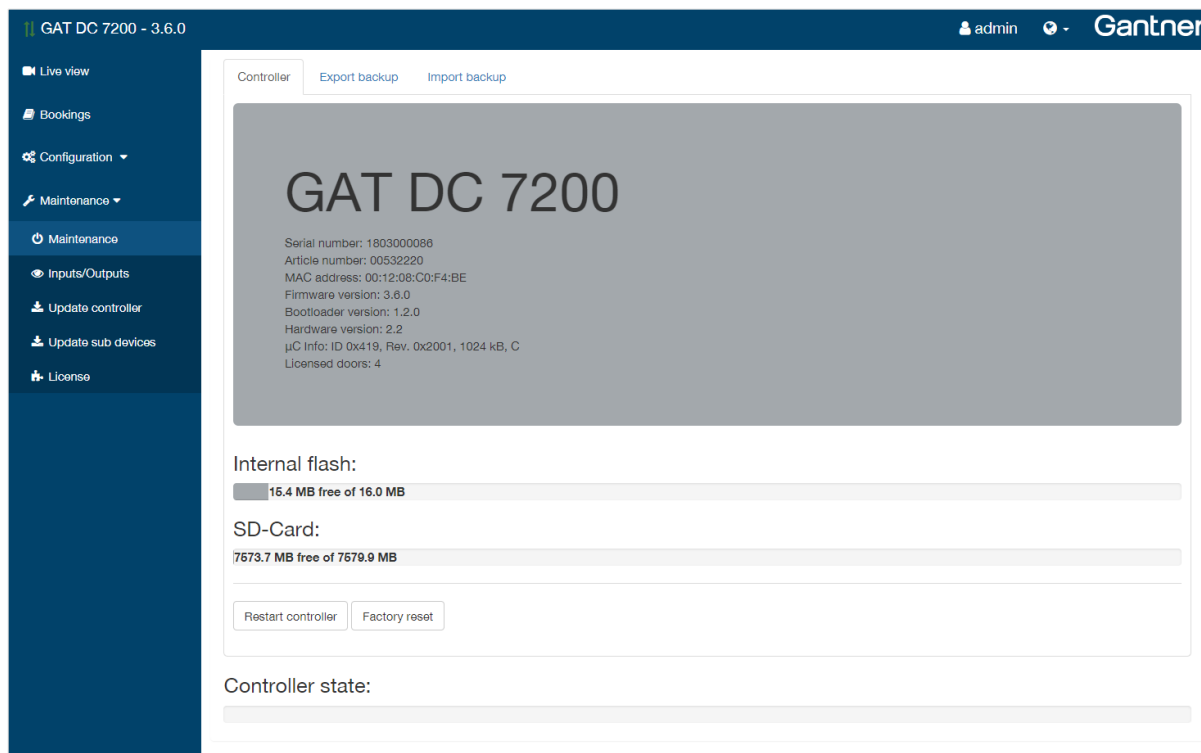


Figure 6.47 – Web interface – Maintenance – "Controller" tab

- Restart controller: Click on this button to restart the controller.
- Factory reset: Click on this button when you want to reset the GAT DC 7200 to the default settings. All changes made since the initial start-up will be deleted.

"Export backup" and "Import backup" tabs

In the "Maintenance" area under the "Export backup" tab, a backup file of all (or some) of the GAT DC 7200 settings can be created and exported. The file can be used as a backup or to document a certain state, e.g., when moving a system.



When using GAT Matrix or other access control solutions that work together with GAT ACE 7000, the backups for configuration changes in GAT ACE 7000 are created automatically.

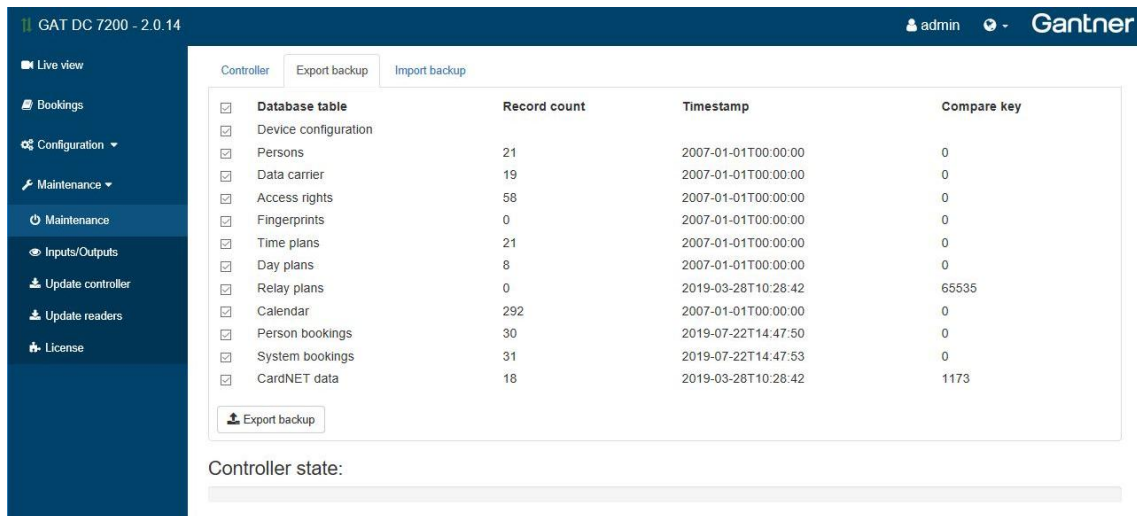
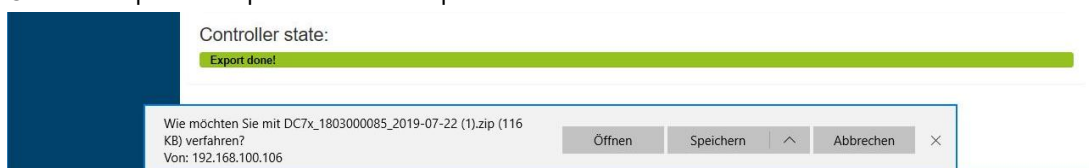


Figure 6.48 – Web interface – Maintenance – “Export backup” tab

- ▶ Open the “Export backup” tab.
- ▶ The default setting has all data categories selected for export to the backup file. The default settings can remain, or you can individually select the different data categories to be exported by marking the boxes as required.
- ▶ Click on “Export backup” to create the export file.



- A zip file is created that can be downloaded from the GAT DC 7200 and saved to the local PC or exported via USB stick, etc.
- ▶ Under the “Import backup” tab, the backup file can be reloaded into the GAT DC 7200.

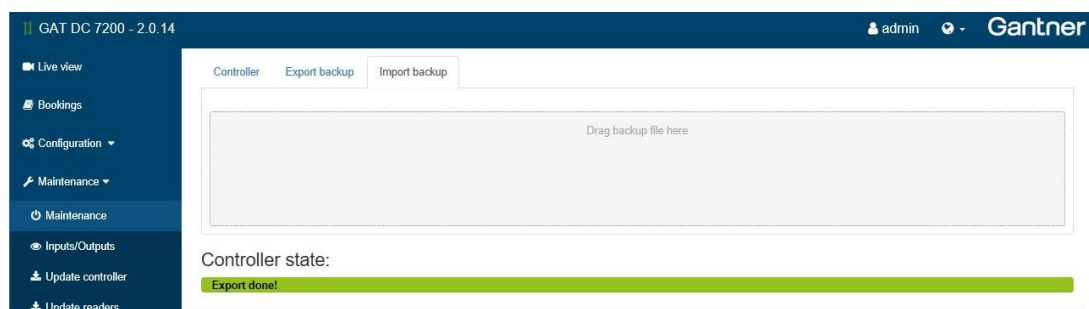


Figure 6.49 – Web interface – Maintenance – “Import backup” tab

- ▶ Drag and drop the backup file from its location on the PC to the marked area.
 - The overview of the data in the backup is shown again.
- ▶ Mark the data that is to be imported and click on "Import backup".
 - After successful importation, the "Import done" message is displayed, and the settings are restored.

6.7.2 Inputs and outputs

Under "Inputs/Outputs", you can see the states of the inputs and outputs of the GAT DC 7200 as well as the connected devices. A ticked box in the "State" column means that the relay is either currently activated or energized.

Output	State
Relay 1 [R&D 1.2 - Entrance, R&D 1.2 Exit]	☐
Relay 2	☐
Relay 3 [Office 1.3]	☐
Relay 4 [CAD 1.4]	☐
Relay 5	☐
Relay 6	☐
R&D 1.2 Exit - Reader relay 1	☐
R&D 1.2 Exit - Wireless lock	☐
R&D 1.2 - Entrance - Reader relay 1	☐
R&D 1.2 - Entrance - Wireless lock	☐

Input	State
Input 1 [R&D 1.2 - Entrance, R&D 1.2 Exit]	☐
Input 2 [R&D 1.2 - Entrance]	☐
Input 3 [R&D 1.2 Exit]	☐
Input 4	☐
Input 5	☐
Input 6	☐
R&D 1.2 Exit - Reader input 1	☐
R&D 1.2 - Entrance - Reader input 1	☐

RS485 interface state	
Reader port	
Success counter	28449
Timeouts	30
Collisions	0
Sub port	
Success counter	0
Timeouts	0
Collisions	0
<button>Reset counter</button>	

Figure 6.50 – Web interface – Inputs and outputs

For the inputs and outputs of the GAT DC 7200, the door for which the input or output is used is displayed in brackets. Multiple doors can be displayed here if the signal has been assigned to more than one door, e.g., for a collective alarm.

For external inputs and outputs, the door to which the reader has been assigned is displayed before the input/output number.

In the "RS485 interface state" area, communication information about the reader and sub interfaces is displayed. This information is useful for service technicians. With the "Reset counter" button, the calculated events and information can be reset to zero.

To test the RS-485 interface state, complete the following steps:

- ▶ Reset the counters via the "Reset counter" button.
- ▶ Complete a 10-minute trial period with all readers and access points configured and connected.
 - Timeouts should be <0.3% of the packet count.
 - Collisions should not occur. If the "Collisions" counter is not 0, a resistor must be connected to the GAT DC 7200 for the respective RS-485 line (see chapter "4.4 Access point GAT DL 091").

6.7.3 Update controller

On the “Update controller” page you can select a firmware update and upload it to the controller. The current firmware version is indicated in the “Maintenance” area or in the title line next to the product name.



It is recommended to create a backup before the update!

All authorization data is deleted when the controller is updated, and the data must be reloaded after the update. In standalone mode, the authorization data is retained during the update.

6.7.4 Update sub devices

In the “Update sub devices” menu, all connected readers and external devices such as relay expanders are listed, and the versions of the installed firmware are displayed.

Address	Name	Serial	Article	Port	Firmware	Bootloader	Hardware	LEGIC OS	Radio module firmware	Lock firmware
2	4: DC7x_Alex_T1 Türe 4	1807000017	00525727 - GAT SR 7310	2	98.40	01.02	12.01	3.1.1.0		
3	1: DC7x_Alex_T1 Türe 1	1812000024	00525727 - GAT SR 7310	2	98.40	01.02	13.00	3.1.1.0	QS9322: 1.1.0	
4	0: -	2106000003	01105457 - GAT IO 7055 NW	0				0.0.0.0		
5	0: -	2106000013	01105457 - GAT IO 7055 NW	0				0.0.0.0		
6	0: -	2106000004	01105457 - GAT IO 7055 NW	0				0.0.0.0		
7	0: -	2106000006	01105457 - GAT IO 7055 NW	0				0.0.0.0		
30	Expander 1	2106000004	01105457 - GAT IO 7055 NW	2	99.22	99.07	02.00			
31	Expander 2	2106000003	01105457 - GAT IO 7055 NW	2	99.22	99.07	02.00			
32	Expander 3	2106000013	01105457 - GAT IO 7055 NW	2	99.22	99.07	02.00			
33	Expander 4	2106000006	01105457 - GAT IO 7055 NW	2	99.22	99.07	02.00			

☒ Update firmware
☒ Update radio module
☒ Update wireless lock
☐ Advanced

Update successful!

Browse... No file selected. Update all devices Refresh

Figure 6.51 – Web interface – Updates for sub devices

- ▶ Click on “Browse” to select a new firmware (.zip file) for updating the sub devices.
- ▶ To update the firmware in a device, select the “Update firmware” check box.
- ▶ The firmware for the wireless modules and wireless locks can also be updated via the respective check boxes below the readers list. The firmware for these components is included in the GR7 firmware.
- ▶ Select the “Advanced” option to select individual readers by their address and only update these readers. You can then enter an address to only load the sub device with this address.
- ▶ If you do not select “Advanced”, all connected readers and sub devices are updated in succession.
- ▶ If different readers are connected that require different firmware versions, the update process must be repeated for each reader type in order to update all readers to the current software version.

6.7.5 License

In the "License" menu, additional software functions for the GAT DC 7200 can be activated. Figure 6.52 shows a GAT DC 7200 with all available expansion licenses activated.

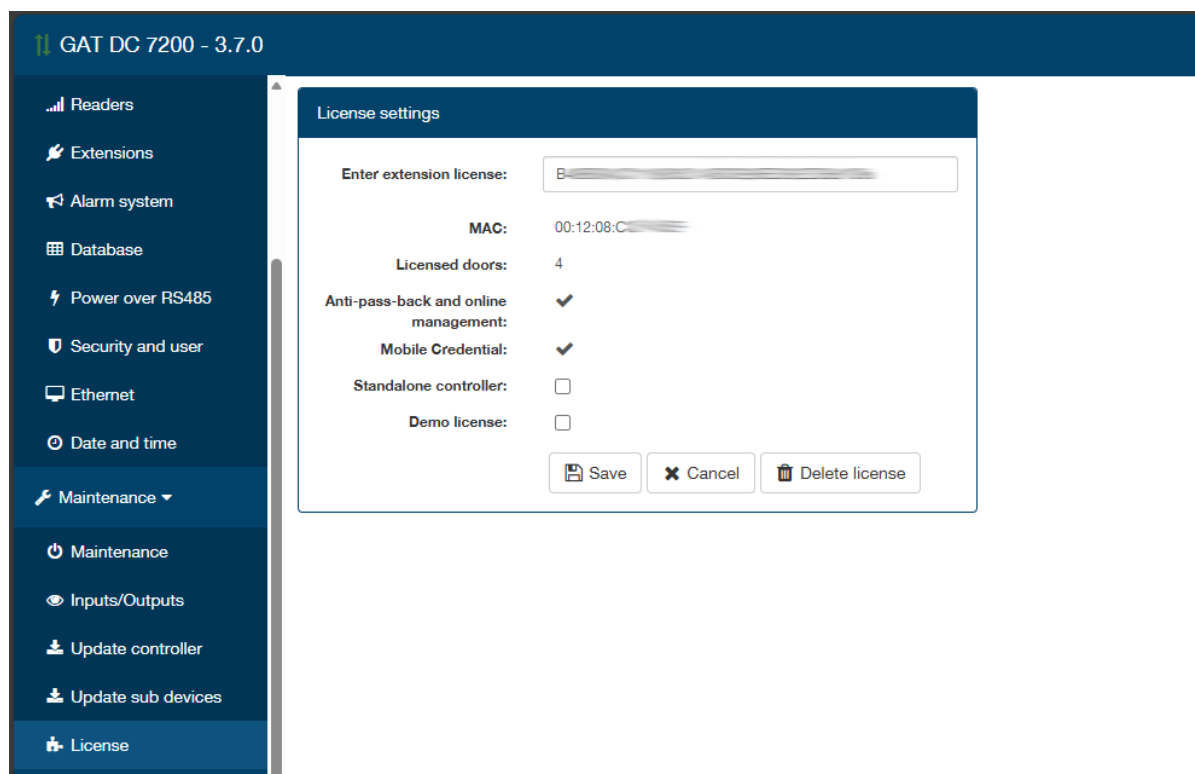


Figure 6.52 – Web interface – License settings

The following licenses are available:

- Standalone license: For operating the GAT DC 7200 in standalone mode. From V2.1, the standalone license is automatically available. The license can be activated or deactivated by selecting or deselecting the checkbox (see chapter "8 STANDALONE MODE").
- PLUS license: To extend the number of controllable doors from 4 to 16. The number of controllable doors can be found behind "Licensed Doors".
- APB license: To enable the anti-pass-back function, which prevents the shared use of data carriers for access. This license also includes the Online Management license. This is necessary when the GAT DC 7200 is to be used with a third-party software via GAT DIRECT.Connect.
- Elevator license: To enable the control of elevators and lockers. Please note that the control of elevator or locker systems is not possible in standalone mode.
- Mobile Credential: This function allows permissions (mobile credentials) on mobile devices such as smartphones or smartwatches to be used for identification at readers on the GAT DC 7200. See section "6.5. Configuring Mobile Credential".



The desired expansion license(s) can be ordered from GANTNER or your local GANTNER sales partner.

- ▶ Enter the license code you received for your controller via email or printed card into the appropriate field, then click on "Save".
 - The activated function is displayed below the MAC address.
- ▶ If you have multiple licenses that you want to enable for the controller, repeat the process for each license.
- ▶ To set GAT DC 7200 to standalone mode, enable "Standalone controller" option (see "8 STANDALONE MODE").
- ▶ With the "Demo license" option, you can temporarily activate all licenses and thus enable all functions, e.g., max. door count of 16 doors or the lift control. The demo license can be activated at any time but expires automatically after 4 days. The expiration date is displayed.

NOTE! The demo license is useful for testing purposes or if you want to configure and commission additional doors or a lift control outside of business hours. These can then be configured and commissioned in advance by activating the demo license and the necessary license can be requested from GANTNER later, e.g., the next day, and imported.



Ensure that the MAC address of the GAT DC 7200 matches the MAC address specified on the license.

7 AUTHORIZATION MANAGEMENT

The authorization data contains the access authorizations and timetables for the users of the access system. This data is usually defined in a separate application, e.g., GAT Matrix. In this application, you define, e.g., which doors the users are permitted to access and at what times. Many other functions and settings are also possible.



A detailed description of the authorization process is available in the Matrix user manual.



If the GAT DC 7200 is connected to a third-party software via GAT DIRECT.Connect, the authorization assignment and control of the door releases can also be carried out via the third-party software. Please see the documentation of this software. In the following section, the authorization assignment is described with regard to Matrix.

The authorization data is downloaded from the Matrix access control software to the GAT DC 7200 via GAT ACE 7000 software.

Standalone mode

For GAT DC 7200 controllers that are operating in standalone mode through the activation of an additional license, authorization assignment and communication with Matrix and GAT ACE 7000 are no longer possible. In this instance, authorization assignment is completed via the GAT DC 7200 web interface. Further information on this topic is available in chapter "8. STANDALONE MODE". To enable communication with these applications again, the standalone license must be deleted from the controller.

CardNET

In the CardNET system, the authorization data is created by an access control software such as Matrix and can be sent to the GAT DC 7200. If the write function for CardNET is enabled for the door controller (see "6.4.8 Reader configuration"), the CardNET authorization data for a data carrier is written to the data carrier when the data carrier is read at a connected reader. In addition, bookings and information such as battery warnings are also read from the CardNET data carriers and sent from the door controller to the authorization software.

Mobile Credential

Mobile Credential allows users to authenticate themselves at the access control system using their mobile device, such as a smartphone or smartwatch, and the stored access credential (in Google or Apple Wallet). To use Mobile Credential with a GAT DC 7200 and a connected reader, the appropriate license is required. See section "6.5. Configuring Mobile Credential" for more information.

GANTNER SVN

GANTNER SVN is a combination of Salto Virtual Network (SVN) technology and MIFARE DESFire data carriers with GANTNER coding.

When using GANTNER SVN (see also "6.4.8 Reader configuration"), access authorizations created in Matrix for SALTO products are written onto the GANTNER coded data carriers at online readers. The SALTO products check these authorizations and save the access events onto the data carriers. These events are read from the data carriers by the online readers and transferred back to Matrix.

A combination of GANTNER SVN and CardNET technology is technically possible thereby allowing mixed systems to operate.

Requirements:

- The following software versions are required to use the GANTNER SVN function:
 - SALTO ProAccess SPACE: min. version 6.8
 - GAT ACE 7000: min. version 2.2
 - Matrix: min. version 5.2
 - Reader firmware: min. version 3.4.0
- GAT Authorisation Tag 400 BA
- The settings required for Matrix and GAT ACE 7000 can be found in the respective software documentation.
- Only RFID data carriers of the type MIFARE DESFire may be used, and these must be coded with a GANTNER SVN file. This coding is used as the default coding for the data carriers in new systems. For existing systems, the data carriers can be additionally coded for new orders (please contact your access control system supplier for further information). The re-coding of existing data carriers is often possible using GT7 coding stations.
- To encode the GANTNER SVN data before writing to the data carriers, at least one dongle encoder is required for each ProAccess SPACE installation and the firmware version min. 01.12 must be installed on the dongle encoder. Further information about the settings required for ProAccess SPACE can be found in the Matrix manual.

8 STANDALONE MODE

To operate the GAT DC 7200 without a software installation on a PC, the controller can be set to operate in standalone mode. In this mode, the users and their authorizations, timetables, and daily schedules as well as the operating calendar can be managed via the GAT DC 7200 web interface.

i From version 2.1, the standalone license is available automatically in the GAT DC 7200. No additional license is required to activate the function.

8.1 Target group

This chapter provides information for administrators of access authorizations. This information is not intended for users of the access system.

8.2 Enabling standalone mode

To set the GAT DC 7200 to operate in standalone mode, ensure that the “Standalone controller” option is selected in the “Maintenance” menu under “License”, as shown below.

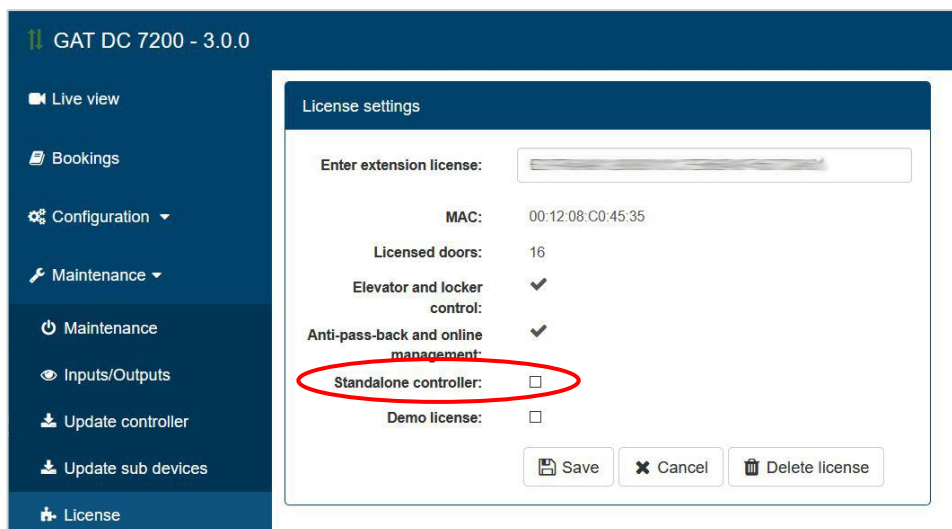


Figure 8.1 – Web interface – Option for standalone mode

i Standalone mode can be combined with the PLUS license to manage up to 16 doors.

By activating standalone mode, certain controller settings that are available when the controller is not operating in standalone mode become unavailable. Communication between GAT ACE 7000 and the GAT DC 7200 is also deactivated when the controller is operating in standalone mode.

8.3 Authorization management

You can create and manage user authorizations in the “Access rights” menu item. This includes configuring users with data carriers and fingerprints, timetables, daily schedules, and the operating calendar.

NOTE! If changes are made to these settings, they must be saved by clicking on the “Save changes” button before leaving the page. If you leave the page or close the browser, the changes are not saved.

A warning is displayed before you leave the configuration interface of the GAT DC 7200 before saving changes.

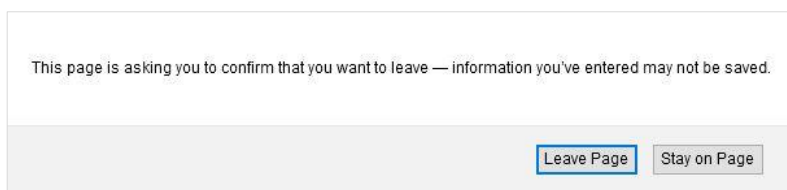


Figure 8.2 – Warning message for unsaved changes

- ▶ If you do not want to lose the changes, select “Stay on Page”, and save the changes.
- ▶ If you exit the page via the "Leave Page" button, the changes will not be saved!

8.3.1 Adding persons and authorizations

GAT DC 7200 - 2.0.5		admin Gantner			
- Live view - Access rights - Bookings - Configuration - Maintenance	Access rights	Time plans	Day plans	Calendar	
	Persons	R&D 1.2 - Entrance	R&D 1.2 Exit	Office 1.3	CAD 1.4
	1: Zwerger L.	3: MA2	3: MA2	-	3: MA2
	2: Haudum K.	1: IoP	1: IoP	-	-
	3: Kirchschläger A.	1: IoP	1: IoP	-	-
	4: Kickert B.	1: IoP	1: IoP	-	-
	6: Altmann F.	1: IoP	1: IoP	-	-
	7: Schlacher K.	1: IoP	1: IoP	-	-
	8: Peter P.	1: IoP	1: IoP	-	-
	9: Schumnig U.	1: IoP	1: IoP	-	-
	10: Wolf X.	1: IoP	1: IoP	-	-
	11: Woger H.	3: MA2	3: MA2	3: MA2	3: MA2
	12: Macierzynski V.	3: MA2	3: MA2	3: MA2	3: MA2
	13: Bader U.	3: MA2	3: MA2	3: MA2	3: MA2
	16: Müller R.	1: IoP	1: IoP	1: IoP	-
	17: Duller E.	1: IoP	1: IoP	1: IoP	-
	18: Ban T.	3: MA2	3: MA2	3: MA2	3: MA2

Figure 8.3 – Web interface – Access rights for the standalone function

- To add persons with access authorizations and to assign these authorizations, select “Add person” in the “Access rights” tab in the menu item “Access rights”.
 - The window for entering personal data opens.

Figure 8.4 – Web interface – Add person window

- Define the following personal and access authorization data.
 - Name: Enter the name of the person here.
 - Identification code: This code is a number that can be used for identification in addition to the data carrier or fingerprints. The function allows doors to operate in a simple ID code lock mode, whereby each person has their own code that can also be combined with a PIN code or fingerprint for verification. To use the identification code function, the setting must be enabled in the timetables and daily schedules.
 - Verification pin code: This is a secret PIN code that can be used for identification in addition to the data carrier to ensure that the holder of the data carrier is also the legitimate owner. The PIN code function can be activated in the timetables and daily schedules.
 - Alarm system: This setting is used to define whether the person is authorized to enable or disable the intrusion detection system (IDS).
 - Special relay: This setting determines whether the person has a special authorization and the type of special authorization relay to be activated during access. The special authorization function applies to all doors controlled by the GAT DC 7200.

- Office function: If you enable this option, the office function is activated for this person. If the office function is enabled, the door is generally unlocked after valid identification of the user at a door (= office function active) until further identification by the same user locks the door again (reset to autonomous mode). The door can then be opened again by an authorized user.
- Add data carrier: This button is used to assign any number of data carriers to the person. In addition to the data carrier number, the type of data carrier must also be entered. Data carrier types are defined in the menu "Configuration" -> "Readers" -> "Data Carrier". The data carrier number is often printed or can be determined by reading the data carrier with a reader and using the number and type information from the booking generated. Alternatively, the number can be read using a USB Desktop Reader (Part No. 863231).
- Add fingerprint template: With this button, up to two fingerprints per person can be recorded that can be used for identification or verification. The setting for defining whether the fingerprint data is used for identification or verification is available in the menu "Configuration" -> "Doors" -> "Fingerprint".
For fingerprint recording, the GAT FR 010 Scanner software is available, which uses a GAT FR 010 fingerprint reader to scan the fingerprints and save the data in the PC clipboard. The data can then be transferred from the clipboard to the "Fingerprint template" field. The software can be downloaded via the  button next to the field.

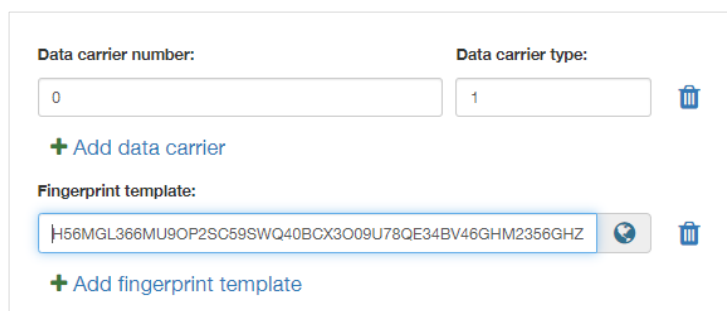


Figure 8.5 –Web interface – Fingerprint template window

After installing the software and connecting a fingerprint scanner to the PC, the fingerprints can be scanned. Place a finger three times onto the reader to record the data. The finger must then be scanned again for verification.

When the quality of the biometric features (minutiae) is sufficiently high, the fingerprint template is inserted as a text (hexadecimal string) into the clipboard. From there, it can be inserted into the capture field in the browser to store it in the controller. The software is ready to record the next finger immediately after verification.

- Access rights: Here the defined doors are listed. One time plan can be selected for each door. The "Always" time plan (always without PIN) is the default plan and can be used immediately. Additional time plans can be created in the "Time plans" tab.
- ▶ After entering all the data for the person, click on "Close" to save the data and exit the input window.
 - The changes are not implemented in the GAT DC 7200 until the data is saved via the "Save Changes" button.
- ▶ To make further changes to a person's data or authorizations, select the person from the list to open the window again.
- ▶ You can also delete the person from the controller via this window.

8.3.2 Adding time plans

In the “Time plans” tab, the existing time plans are listed.

There are personal time plans and door time plans. The top table shows the personal time plans, which can be assigned to the persons that use the access system. The default personal time plan is the “IoP” plan, which allows 24-hour access 7 days a week. Additional time plans can be created. The bottom table lists all doors and shows the time plans that can be assigned to each door.

The numbers in the tables show the numbers of the day plans, which are assigned to the persons and doors for every weekday and special day.

GAT DC 7200 - 2.0.5

admin

Gantner

Live view

Access rights

Bookings

Configuration

Maintenance

Access rights

Time plans

Day plans

Calendar

Person time plans

MO

TU

WE

TH

FR

SA

SU

S1

S2

S3

S4

S5

S6

S7

S8

S9

S10

1: IoP

1

1

1

1

1

1

1

1

1

1

1

1

1

1

1

1

1

2: MA1

2

2

2

2

2

-

-

-

-

-

-

-

-

-

-

-

-

3: MA2

3

3

3

3

3

-

-

-

-

-

-

-

-

-

-

-

-

4: REI

4

-

4

-

4

-

4

-

-

-

-

-

-

-

-

-

-

5: SER

5

5

5

5

5

5

-

-

-

-

-

-

-

-

-

-

-

+ Add person time plan

Door time plans

MO

TU

WE

TH

FR

SA

SU

S1

S2

S3

S4

S5

S6

S7

S8

S9

S10

R&D 1.2 - Entrance:

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

R&D 1.2 Exit:

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

Office 1.3:

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

CAD 1.4:

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

Save changes

Discard changes

Figure 8.6 – Web interface – Time plans for the standalone function

Person time plans

The person time plans are listed in the top table.

- Click onto a person time plan to edit the time plan or click on “Add person time plan” to create a new time plan.
 - For both options, the following window opens.

2: Employee plan 1

Name: Employee plan 1

Monday: 3

Tuesday: 3

Wednesday: 3

Thursday: 3

Friday: 3

Saturday: -

Sunday: -

Show special days: ☐

Close Delete

Figure 8.7 – Web interface – person time plan configuration

- ▶ In the field "Name" a name can be assigned to the plan.
- ▶ A day plan with time authorizations can be selected for each weekday and special day type. Day plans are created via the "Day plans" tab (see next section).
- ▶ Click on "Close" to exit the window.
 - The changes are not implemented in the GAT DC 7200 until the data is saved via the "Save Changes" button.

Door time plans

The door time plans are listed in the bottom table.

- ▶ Click onto a door row to edit the door time plan of this door.
 - The following window opens.

Figure 8.8 – Web interface – door time plan configuration

- ▶ In the "Name" field, a name can be assigned to the plan.
- ▶ A day plan with time authorizations can be selected for each weekday and special day type.
- ▶ Day plans are created via the "Day plans" tab (see next section).
- ▶ Click on "Close" to exit the window.
 - The changes are not implemented in the GAT DC 7200 until the data is saved via the "Save Changes" button.

8.3.3 Adding day plans

In the “Day plans” tab, the existing day plans are listed. The default day plan is 0 to 24 hours without a PIN. Additional day plans can be created.

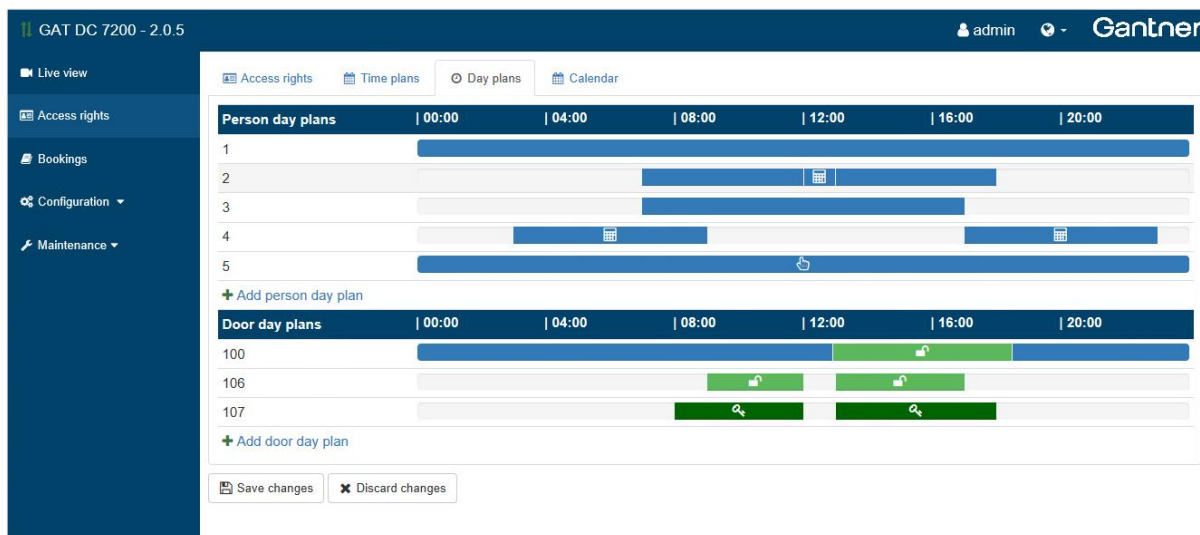


Figure 8.9 – Web interface – Day plans

Person day plans

The person day plans are listed in the top table.

- Click onto a person day plan to edit the day plan or click on “Add person day plan” to create a new day plan.
 - For both options, the following window opens.

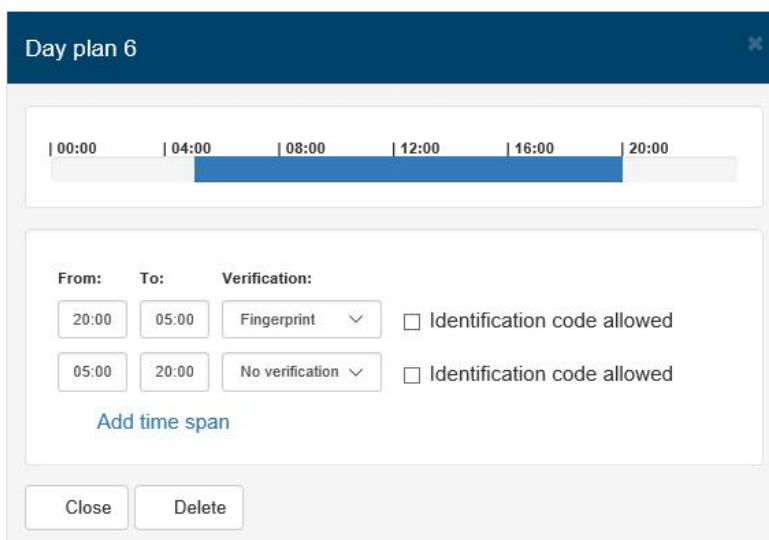


Figure 8.10 – Web interface – Person day plan configuration

- ▶ Up to ten time spans can be defined. For each time span, a certain type of verification can be selected. To add a time span, click on "Add time span". The following settings are possible for each time span.
 - From / To: Enter the start and end time of the time span.
 - Verification: You can define whether this is necessary and whether verification must be done using PIN code or fingerprint.
 - Identification code allowed: This setting is used to define whether access using an identification code is permitted during the time span or not.
- ▶ Individual time spans can be deleted via the  symbol.
- ▶ The entire day plan can be deleted by clicking on "Delete".
- ▶ Confirm the settings by clicking on "Close" and then "Save changes" in the daily schedule overview to apply the changes to the GAT DC 7200.

Door day plans

The door day plans are listed in the bottom table.

- ▶ Click onto a door day plan to edit the day plan or click on "Add door day plan" to create a new day plan.
 - For both options, the following window opens.

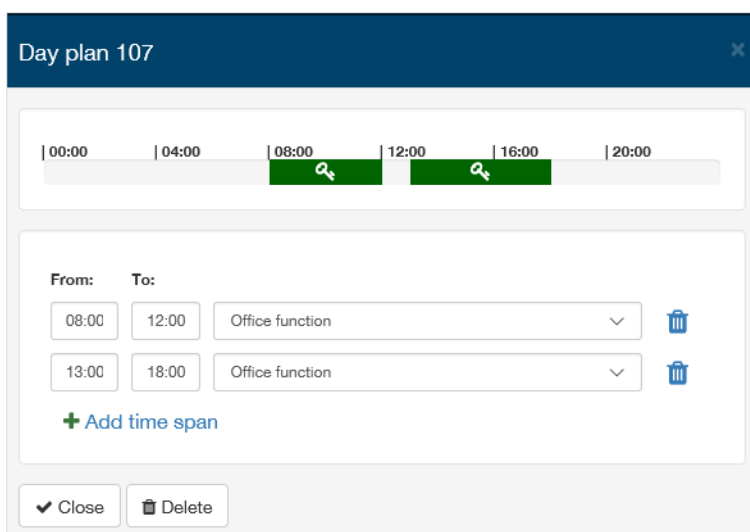


Figure 8.11 –Web interface – Door time plan configuration

- ▶ Up to ten time spans can be defined, and a certain type of door function can be selected for each time span. To add a time span, click on "Add time span". The following settings are possible for each time span.
 - From / To: Enter the start and end time of the time span.
 - Function: Select one of the following options:
 - General open: Door is unlocked and can be opened without identification.
 - General open after valid access: Same as previous function. Activation via a valid access.
 - Office function: With every valid identification, the mode switches between General Open and Autonomous (unlocking with valid identification).
 - Check company ID only: Only whether the data carrier belongs to the system is checked. This function can only be used for coded data carriers at wired readers.

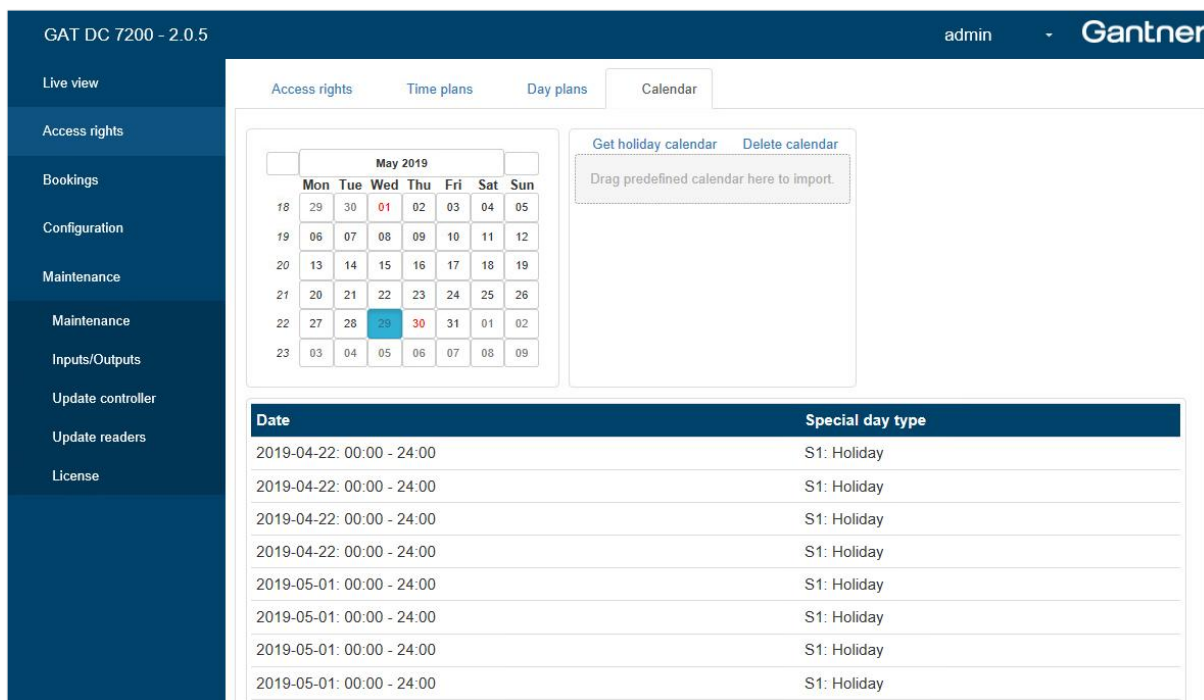
NOTE! Offline products (also with WiNET networking) do not support this function.

- ▶ Individual time spans can be deleted via the  symbol.
- ▶ The entire day plan can be deleted by clicking on "Delete".
- ▶ Confirm the settings by clicking on "Close" and then "Save changes" in the day plan overview to apply the changes to the GAT DC 7200.

8.3.4 Adding special days

Special days can be entered into the calendar of the GAT DC 7200. The time plans are used to specify that these special days are subject to different authorizations than on normal weekdays.

Up to ten different types of special days (S1 to S10) are possible. These can be assigned to any number of days in the calendar. The S1 special day type is for holidays and the S2 special day type intended for half-day holidays. The operator can use the remaining special day types as required.



The screenshot displays the GAT DC 7200 - 2.0.5 web interface. The top navigation bar shows 'admin' and the 'Gantner' logo. The left sidebar contains a menu with options: Live view, Access rights, Bookings, Configuration, Maintenance, Maintenance, Inputs/Outputs, Update controller, Update readers, and License. The main content area is titled 'Calendar' and features a calendar for May 2019. The calendar shows dates from 18 to 23, with specific days highlighted in red (01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31). Below the calendar is a table with the following data:

Date	Special day type
2019-04-22: 00:00 - 24:00	S1: Holiday
2019-04-22: 00:00 - 24:00	S1: Holiday
2019-04-22: 00:00 - 24:00	S1: Holiday
2019-04-22: 00:00 - 24:00	S1: Holiday
2019-05-01: 00:00 - 24:00	S1: Holiday
2019-05-01: 00:00 - 24:00	S1: Holiday
2019-05-01: 00:00 - 24:00	S1: Holiday
2019-05-01: 00:00 - 24:00	S1: Holiday

Figure 8.12 – Web interface – Calendar

- ▶ The "Get holiday calendar" function allows you to download prepared calendars from the GANTNER website. The calendars can be downloaded to the PC in file format and then dragged to the applicable field in the browser.
 - This imports the special days into the GAT DC 7200.
- ▶ The "Delete calendar" button deletes all existing special days.

- ▶ To add a special day, click on the day in the calendar.
 - An input window opens where you can select the type of the special day.

The screenshot shows a modal window titled "2019-05-29" with a close button (X) in the top right corner. Inside the window, there is a form with the following fields:

- "Special day type:" with a dropdown menu showing "S2: Half holiday".
- "From:" with a text input field containing "00:00".
- "To:" with a text input field containing "24:00".

At the bottom of the window, there are two buttons: "Close" and "Delete".

- ▶ The special days are valid for the whole day by default. By changing the "From" and "To" values, it is possible to activate these special rights for a specific period (e.g., during an event) with the standard access rights used before and after the period.
- ▶ Click on "Delete" to delete an individual special day.
- ▶ Click on "Close" to exit the window.
 - The changes are not implemented in the GAT DC 7200 until the data is saved with "Save Changes" on the page "Access Rights".

8.4 Limitations of standalone mode

Most of the GAT DC 7200's functions are available when the controller is operating in standalone mode; however, there are also some limitations.

- The special authorizations of persons cannot be as precisely controlled as is possible in the networked variant via software.
- Battery-powered locks can only be integrated with WiNET mode functionality. CardNET and Read Only modes are not supported in the standalone version.
- Control of elevator or locker systems is not possible in the standalone version.
- Communication with GAT Matrix and GAT ACE 7000 is also not possible in standalone mode. In this instance, the authorizations can only be managed via the GAT DC 7200.

9 FREQUENTLY ASKED QUESTIONS

9.1 Entry and exit

For door entry and exit control, two doors are used with the GAT DC 7200. This allows the authorization settings to be precisely configured including the necessary criteria for identification and verification. The authorizations for entry and exit can also be assigned differently.

Two doors that use the same inputs and outputs are automatically coupled in the controller. This ensures that the door signaling is displayed correctly and an alarm is not triggered when the door is opened in the other direction.

Please note that two door licenses for each door with entry and exit are required for the GAT DC 7200 and Matrix.

9.2 Transmitter

The GAT Active Tag 552 or GAT Active Tag 554 and the GAT Reader 550 AA can connect to the GAT DC 7200 using a GAT SR 7000 Wiegand.

Only one GAT Reader 550 AA can be used per controller.

9.3 WiNET access points

Up to four GAT DL 091 access points for a maximum of 16 doors can operate per GAT DC 7200.

9.4 Door licenses

The GAT DC 7200 is designed for the control of four doors. The purchase of a GAT DC 7200 PLUS License allows you to extend this functionality to sixteen doors. The license is sent to the customer via email after the controller's MAC address is provided (Part No. 732222) or in card form with the printed license data when Part No. 753023 is ordered.

The license is entered via the GAT DC 7200 web interface.

9.5 Proxy credentials

Proxy credentials are administered by the GAT DC 7200 without the previously used Proxy Customer Codes. Therefore, conversion of the data carrier numbers is required!

Until now, the typical Proxy Customer Codes were 001 = 0, 004 = 1, 015 = 2. This results in, e.g., an ID number of 12345678901 from the previous FLEX system being converted to 0042345678901 in the new system.

9.6 Proxy reader

Proxy readers such as the GAT Reader 405 AP and GAT Reader 500 UP can connect to the GAT DC 7200 using a GAT SR 7000 Wiegand.

The GAT SR 7000 Wiegand does not support direction differentiation via the Card-in-reader line or the sub-bridge.

Two GAT SR 7000 Wiegand devices must be used for entry and exit control. Up to 16 GAT SR 7000 Wiegand devices can operate per GAT DC 7200.

9.7 Elevator control

Lift or locker control can be realized on the GAT DC 7200 with relay expanders (with 1 or 2 GAT IO 055 or with up to 8 GAT IO 7054 and/or GAT IO 7055). This means that a different number of additional relay outputs and optocoupler inputs are available depending on the expander. The relays can be assigned to one or more doors. The relay expanders are connected to the "Sub" or "Reader" interface of the GAT DC 7200.

A GAT DC 7200 Elevator License is required for elevator or locker control. Without this license, the relays of the relay expanders can only be used as general outputs.

Elevator control is not possible with GAT DIRECT.Connect.

9.8 Anti-pass-back function

The anti-pass-back function is not included with version 1.0 of the GAT DC 7200. This function will be implemented at a later date. The first development stage will be a "local anti-pass-back" setting in the controller with a "controller-system anti-pass-back" function implemented at a later stage of development.

The anti-pass-back function requires the GAT DC 7200 Anti-Pass-Back License.

9.9 Long-range reader

Long-range readers such as the GAT SR 861 can connect to the controller using a GAT SR 7000 Wiegand.

9.10 Network security

The GAT DC 7200 offers the possibility to enable TLS (formerly SSL) for communication. This enables the connection via a secured HTTPS connection. The certificate for this connection can be created by a GAT DC 7200 itself or requested via a certificate signing request (CSR) from a certification authority for X.509 certificates (CA).

9.11 Configuration saving

When using the GAT DC 7200 with GAT ACE 7000 software, a change to the configuration of the controller is automatically noticed by GAT ACE 7000 and a backup created. Thus, the settings for each controller are saved in the GAT ACE 7000 database.

9.12 Configuration sharing

When using the GAT DC 7200 with GAT ACE 7000 software, system-wide settings, e.g., data carrier settings, can be made at a controller. These settings are copied from the controller via GAT ACE 7000 and sent to all other controllers.

The selection of the settings to be shared can be determined by the user in GAT ACE 7000.

9.13 Extending the outputs

The GAT DC 7200 provides six relay outputs, which can be used much more flexibly than in the previous system. The relays can be used as additional outputs for GR7 series readers.

If additional outputs are required in a secure area, one or more GAT SR 7000 Wiegand devices (1 output per device) can be connected. Each GAT SR 7000 Wiegand requires a door license for the controller.

It is also possible to connect IO expanders and thus extend the number of outputs. Up to 2 GAT IO 055 or up to 8 GAT IO 7054 and/or GAT IO 7055 can be connected per GAT DC 7200. The number of inputs and outputs is extended by the following values per expander:

- GAT IO 055: 32 additional outputs
- GAT IO 7054: 4 additional outputs
- GAT IO 7055: 8 additional outputs

9.14 Extending the inputs

The GAT DC 7200 offers six optocoupler inputs, which can be used much more flexibly than in the previous system. The optocouplers can also be used as additional inputs for GR7 series readers.

If additional inputs are required in a secure area, one or more GAT SR 7000 Wiegand devices (2 inputs per device) can be connected. Each GAT SR 7000 Wiegand requires a door license for the controller.

Furthermore, the number of inputs can also be extended by the following values via IO expanders:

- GAT IO 7054: 12 additional inputs
- GAT IO 7055: 16 additional inputs

9.15 Video integration

In the GAT DC 7200 Live View, a video signal for each door can be integrated thereby allowing video streams from different cameras to be displayed. The video signal must be delivered directly from the camera and displayed in a browser without any additional plug-ins so that they function with the GAT DC 7200.

9.16 Plug&Play PLUS

The GAT DC 7200 Plug&Play PLUS function allows connected devices that support the Plug&Play PLUS function to be automatically detected, configured, and assigned to a door.

The function is only available when one device is connected per reader port. If more than one device is connected to a reader port, the automatic door allocation function is not possible.

Devices that do not support Plug&Play PLUS, e.g., GAT SR 3xx or GAT SLR 3xx, must be manually located and configured.

9.17 CardNET

CardNET is only possible with the GAT DC 7200 using GR7 and GAT SR 73xx series readers. GAT SR 3xx series readers do not support the writing of CardNET data.

CardNET is available with any GAT DC 7200 (if configured) and can be enabled for all doors. In order for it to be active at the door, the reader used must be authorized accordingly.

CardNET is not available when the GAT DC 7200 is operating in standalone mode.

9.18 GANTNER SVN

GANTNER SVN is a combination of the Salto Virtual Network (SVN) technology and MIFARE DESFire data carriers with GANTNER coding.

See chapter "7. AUTHORIZATION MANAGEMENT" for further information about the requirements for GANTNER SVN.

9.19 Short-circuit protected connections

The reader sockets and the sub socket are protected against short-circuiting. If current of more than approx. 1 A is drawn from one of the sockets, the voltage at this socket is automatically switched off. The other sockets can still be used as normal.

Should the controller restart following a short circuit, the restart is caused by weak voltage in the controller power supply.

The voltage supplied by a reader socket can also be switched off in the configuration settings. The state of the power supply (on/off) is indicated by a yellow LED on the reader socket and via the web interface.

9.20 Communication via the reader socket

The green LED on the reader sockets indicates support for devices with Plug&Play PLUS functionality when active communication occurs with the connected device (or connected devices).

For devices without Plug&Play PLUS functionality, communication is not signaled via the reader socket.

9.21 Reset to default settings

The GAT DC 7200 can be reset to the default settings via a button. This is necessary, e.g., if the access data (see network security) has been changed and is no longer known. There are a few steps required to reset the GAT DC 7200 to the default settings (see "5.5 Restart and reset to default settings").

9.22 Network connection

For security reasons, only one network connection is possible per controller. The network connection is indicated by LED 1 (see "5 CONTROLS AND SIGNALIZATION").

9.23 Using GAT SR 3xx series readers

The GAT DC 7200 supports the GAT SR 3xx series readers, however, not the GAT SR 380. In addition, the Plug&Play PLUS and CardNET functions are not available with the supported readers. LEGIC prime and advant data carriers (ISO 14443 and ISO 15693) are supported by readers of this series.

9.24 MIFARE Classic

The unique number of MIFARE Classic or other ISO 14443A data carriers can be used with the GAT DC 7200. It is not relevant whether the unique number is 4 or 7 bytes.

Due to the unsecure technology, the GAT DC 7200 does not read ID numbers from sectors of MIFARE Classic data carriers.

9.25 MIFARE DESFire

In addition to reading the unique number of MIFARE DESFire data carriers, coded data can also be read and CardNET data written. For this purpose, a GANTNER application with data files is encoded with corresponding files.

DESFire EV1 and DESFire EV2 data carriers are supported.

Note: For the GANTNER SVN function, only data carriers of type MIFARE DESFire may be used.

9.26 LEGIC prime and advant

GANTNER specific segments, KGH segments, LEGIC advant Access Standard segments and numerous customer segments are supported by the GAT DC 7200.

9.27 HID iClass

The unique number of HID iClass data carriers can be used with the GAT DC 7200. However, the reading of data areas is not possible with these data carriers.

9.28 Bookings

The GAT DC 7200 has two independent ring memories for recording bookings. On one memory, personal bookings and access events are stored. On the other, system-related events are stored. The size of both ring memories can be freely configured, so as to differentiate the length of the evaluation period.

An anonymization can also be activated for person-related bookings so that access bookings are saved, but the identity of the person is hidden.

9.29 Data carrier types

The GAT DC 7200 can handle up to nine different types of data carriers simultaneously. These can be different technologies (e.g., LEGIC prime and advant) or different coding formats (e.g., segments or customer codes). The various types of data carriers can be managed in the access control software as one or several different types (if supported by the software).

If the unique number of a data carrier is to be used as a data carrier type, it must be considered that this can lead to undesirable effects. Please contact your supplier or the GANTNER Support Team for further information.

9.30 Alarm system

The GAT DC 7200 allows you to define and control up to four alarm system areas for a block lock function. The arming/disarming of an area is possible from several doors. The influence of the block lock function can be used for single or all doors.

Due to the range control for several doors, less cabling is required, and fewer inputs and outputs are needed at the controller.

You can define for each door whether the status of the alarm system is to be displayed on the reader or not.

For arming and disarming, it is possible to define per alarm system area whether verification is required for the operation or not and which type of verification to use (PIN or biometrics). The authorization is also managed by a special authorization for persons.

9.31 Status of the inputs/outputs

The status of the inputs and outputs can be conveniently displayed via the web interface. It is therefore no longer necessary to look for the installation location of the controller in order to test the signals.

9.32 Time server

Time synchronization for the GAT DC 7200 occurs via a freely adjustable time server (NTP server). The GAT DC 7200 retrieves the current time from this server at configurable intervals. The time server can be configured manually or via the DHCP server option (DHCP Option 42).

9.33 Time zone

The time zone in which the GAT DC 7200 operates can be freely configured.

9.34 Daylight saving time switchover

The switchover from standard time to daylight-saving time and back again is carried out independently by the controller.

9.35 Backup settings

The configurations settings of the GAT DC 7200 are automatically saved by GAT ACE 7000 in the form of a backup file. If GAT ACE 7000 is not already installed, a backup can also be created manually via the web interface.

9.36 Controller and reader updates

Updating the GAT DC 7200 and its connected peripherals is easily done via GAT ACE 7000. If GAT ACE 7000 is not yet installed, updates can also be done via the web interface.

The updating of peripheral devices is only possible when this is supported by the peripheral devices, e.g., the GAT DL 091 is currently not supported.

9.37 Installation

The GAT DC 7200 is designed for installation in distribution lockers and has a protection class of IP 30. If the controller is to be used in more demanding conditions, a corresponding housing (Installation Box 9118 or 9236) must be used.

9.38 Reader ports

The reader connections are RS-485 interfaces, which can also be split into several RJ45 connectors via suitable splitters. This makes simple cabling possible even if more than four readers are to be connected to a controller.

Observe the maximum cabling length of the system (max. 200 m per reader, max. 1000 m for all peripherals).

9.39 Power for locks

The GAT DC 7200 and the readers provide potential-free contacts for the control of locks or feedback contacts. Power for the locks must be supplied by a separate power supply with a suitable cable cross-section.

9.40 Identification and verification

The GAT DC 7200 allows the precise configuration of identification and verification settings. For example, user identification can be time-controlled via a number input or the criteria for verification can be changed depending on the time of day or day of the week, e.g., PIN during the day with fingerprint verification during off-hours.

9.41 Special authorizations

With the GAT DC 7200, special authorizations can be managed in more detail than before. For example, it is possible to allow different people to enable the alarm system but not to disable it, or to require certain persons to use fingerprint verification with PIN verification sufficient for others.

9.42 Multi-card handling

The GAT DC 7200 supports multi-card handling; a function that selects the data carrier required for access when multiple data carriers are read. Thus, the user's ID card can remain in their wallet with other ID cards or credit cards not affecting the identification process.

This function requires the data carriers to be coded accordingly. For further information, please contact your supplier or a GANTNER technical support specialist.

9.43 Reading range

GR7 readers as well as GAT SR 73xx and GAT SLR 73xx series readers have a significantly improved reading range with the reading center clearly indicated by the illuminated blue dot in the center of the reader symbol. The reading range declines significantly away from the reading center.

9.44 ISO 15693 standard

Data carriers conforming to the ISO 15693 standard can be used for identification at GR7, GAT SR 73xx, and GAT SLR 73xx series readers with the GAT DC 7200. For LEGIC advant data carriers, coded information can be used according to this standard. For other types, the unique number is used as an identification number.

9.45 ISO 14443 standard

Data carriers conforming to the ISO 14443 standard can be used for identification at GR7, GAT SR 73xx, and GAT SLR 73xx series readers with the GAT DC 7200. For LEGIC advant or MIFARE DESFire data carriers, coded information can be used according to these standards. For other types, the unique number is used as an identification number.

9.46 Reader speed

The GR7 series readers are faster than previous readers. This is noticeable in the handling of data carriers (depending on their technology and coding). A clear difference in speed is also noticeable in the processing and storing of fingerprint templates.

9.47 Authorization changes

Authorization changes can be sent many times faster to the GAT DC 7200 than previously possible with the FLEX system. All data is always sent to the controller when authorization changes occur, which eliminates data inconsistencies.

The GAT DC 7200 remains fully functional while receiving the data. After the data has been received, the active memory area is updated without a noticeable interruption and the new authorizations are active from this point on.

The transferal of data to the GAT DC 7200 via GAT DIRECT.Connect is not possible.

9.48 Inputs and outputs

With the GAT DC 7200, there is no fixed predefined assignment of inputs and outputs to doors. The default settings can be changed as required in the configuration. This provides significantly more flexibility than the previous system with more functionality available for implementation with the same number of inputs and outputs.

Regardless of this, the GAT DC 7200 has more inputs and outputs than the previous system.

9.49 Installation

The GAT DC 7200 can be quickly and easily installed in a server cabinet using a DIN rail for mounting. If wall mounting is required, the controller can be mounted without a DIN rail using two screws.

9.50 WiNET

The GAT DC 7200 includes all the prerequisites required for WiNET systems to be easily installed and put into operation. The display of signal strengths for individual locks allows the positioning of the WiNET access points to be optimized.

The WiNET functionality via GAT DIRECT.Connect is not supported.

9.51 Test mode

The GAT DC 7200 web interface makes it easy to test an installation when access control software has not been installed or no authorizations have been distributed.

The correct activation and feedback of the door can be checked by the remote-control option. If a lock is not yet connected to the GAT DC 7200, you can check the status of the inputs and outputs via the web interface or use the integrated beeper to "signal" a state.

Data carrier settings can also be evaluated based on the recorded bookings.

The integrated beeper is also useful for locating the GAT DC 7200 when the exact installation location is unknown.

9.52 Remote control of doors

In addition to door monitoring, doors can also be controlled remotely via the web interface. It is possible to unlock individual doors, permanently unlock doors, and also lock doors via remote control. These functions can also be implemented without an existing security control station.

9.53 GAT DIRECT.Connect interface

When using this interface, the Online Management license must be installed (included in 1100190 - GAT DC 7200 APB license email or 1100191 - GAT DC 7200 APB license). With this software and the corresponding adapter, it is possible to connect the GAT DC 7200 to an access control software without having to modify the software.

Up to 16 doors and different readers such as the GR7, GAT SR 7xxx, and GDL7m can be used, and it is possible to send control commands to the controller.

The following limitations must be considered with GAT DIRECT.Connect:

- WiNET devices are not supported by the GAT DC 7200.
- Elevator and locker controllers (e.g., GAT IO 705x) are not supported.
- Data transfers to the GAT DC 7200 are not possible.
- A parallel connection to GAT ACE or Matrix is not possible.

9.54 Mobile Credential

Mobile Credential allows you to use permissions stored on mobile devices such as smartphones or smartwatches to identify users at the readers connected to the GAT DC 7200. To use this feature, a Mobile Credential license must be activated on the GAT DC 7200. Certain prerequisites (including minimum firmware version 3.7) and configuration steps are also required. See section "6.5. Configuring Mobile Credential" for more information.

10 TECHNICAL DATA

10.1 Power supply

Nominal voltage:	DC 12 / 24 V
Permitted voltage range:	DC 10 - 28 V
Power supply:	Only with LPS (Limited Power Source) power supply
Max. current consumption:	4 A at 12 V 2 A at 24 V

10.2 Server interface

Interface type:	Ethernet 10/100 Mbit
Standard:	IEEE 802.3
Required ports:	- 20, 21 (for FTP, no longer required as of GAT ACE 7000 version 2.0) - 443 (for web interface via TLS/SSL), 80 without TLS/SSL (not recommended) - 8000 (default for communication with GAT ACE 7000, can also be changed) - 123 UDP (NTP, for time synchronization) - 8239 for GAT DIRECT.Connect

10.3 Reader

Interface type:	RS-485
Supported readers:	GANTNER Generation 7 readers: GAT SR 7300 / 7305 / 7307 GAT SR 7310 / 7315 / 7317 GAT SR 7340 / 7345 / 7347 GAT SR 7350 / 7355 / 7357 GAT SR 7380 GAT SLR 7300 / 7307 GAT SLR 7310 / 7317 GAT SR 7000 Wiegand GR7.1300 / 1310 / 2300 / 2310 / 7380 GANTNER Generation 3xx readers (with limitations): - GAT SR 300 / 305 - GAT SR 310 / 315 - GAT SR 340 / 345 / 347 - GAT SR 350 / 355 / 357 - GAT SLR 300 - GAT SLR 310 WiNET reader: - GAT DL 091

10.4 "Sub" peripheral interface

Interface type:	RS-485
Supported devices:	- GAT IO 055 Relay Expander - GAT IO 7054 / GAT IO 7055 - GAT DL 091 WiNET Access Point - GAT REX 118 RS485 - GAT SR 7000 Wiegand

Note: For the GAT DL 091 with firmware version prior to v4.1, the GAT DL 091 and GAT IO 055 or GAT REX 118 cannot be connected to the Sub interface at the same time.

10.5 Relay outputs

Quantity:	6
Function:	NO/NC (function and timing configurable)
Switching voltage:	Max. 30 VAC/DC
Limiting continuous current:	Max. 2 A
Switching power:	Max. 60 VA

10.6 Optocoupler inputs

Quantity:	6
Function:	Function configurable
Input voltage:	10 to 30 VDC
Input current:	4.5 mA

10.7 Memory and time management

Memory capacity:	- 16 MB Flash - 8 GB Mass storage
Memory allocation:	Dynamic memory allocation, e.g.: 50,000* persons + 100,000 data carriers + 100,000 authorizations + 100,000 bookings * ... For systems with more than 5,000 persons, please contact your supplier or GANTNER Support for advice on the best possible system configuration.
Internal clock:	- Quartz-controlled, real-time clock - Automatic daylight-saving time switching - Support for automatic time synchronization via SNTP server

10.8 Signaling elements

Visual signaling:	LEDs for Ethernet, RS-485 interfaces (reader, peripheral devices), host connection
Acoustic signaling:	Beeper

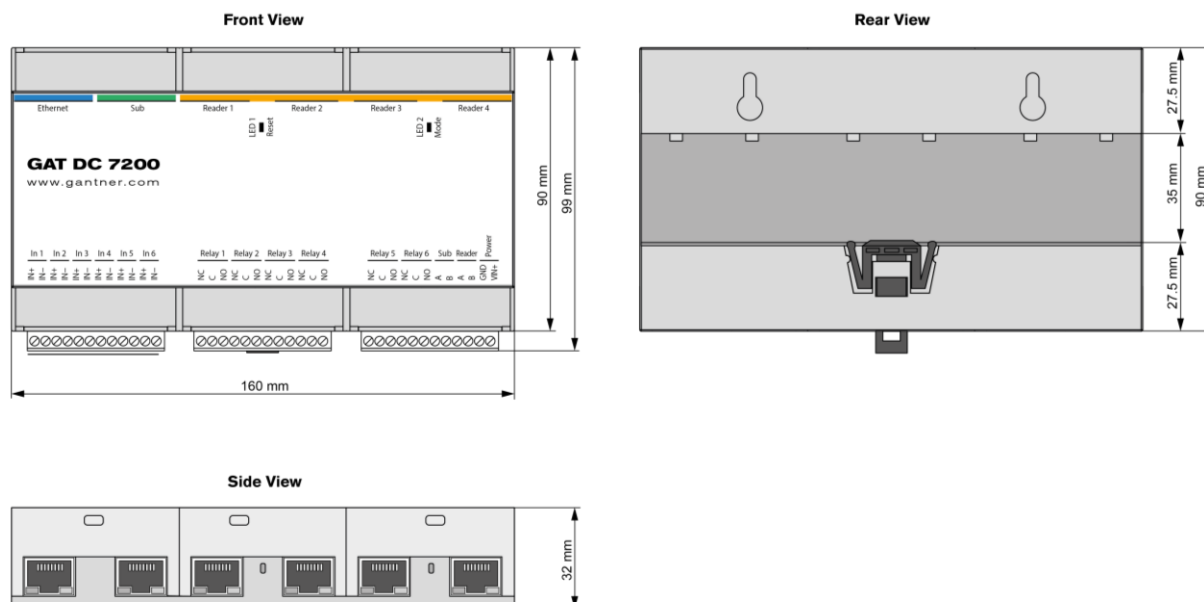
10.9 Housing

Housing material:	Impact-resistant, robust plastic housing
Dimensions:	160 mm x 90 mm x 32 mm
Weight:	approx. 210 g

10.10 Ambient conditions

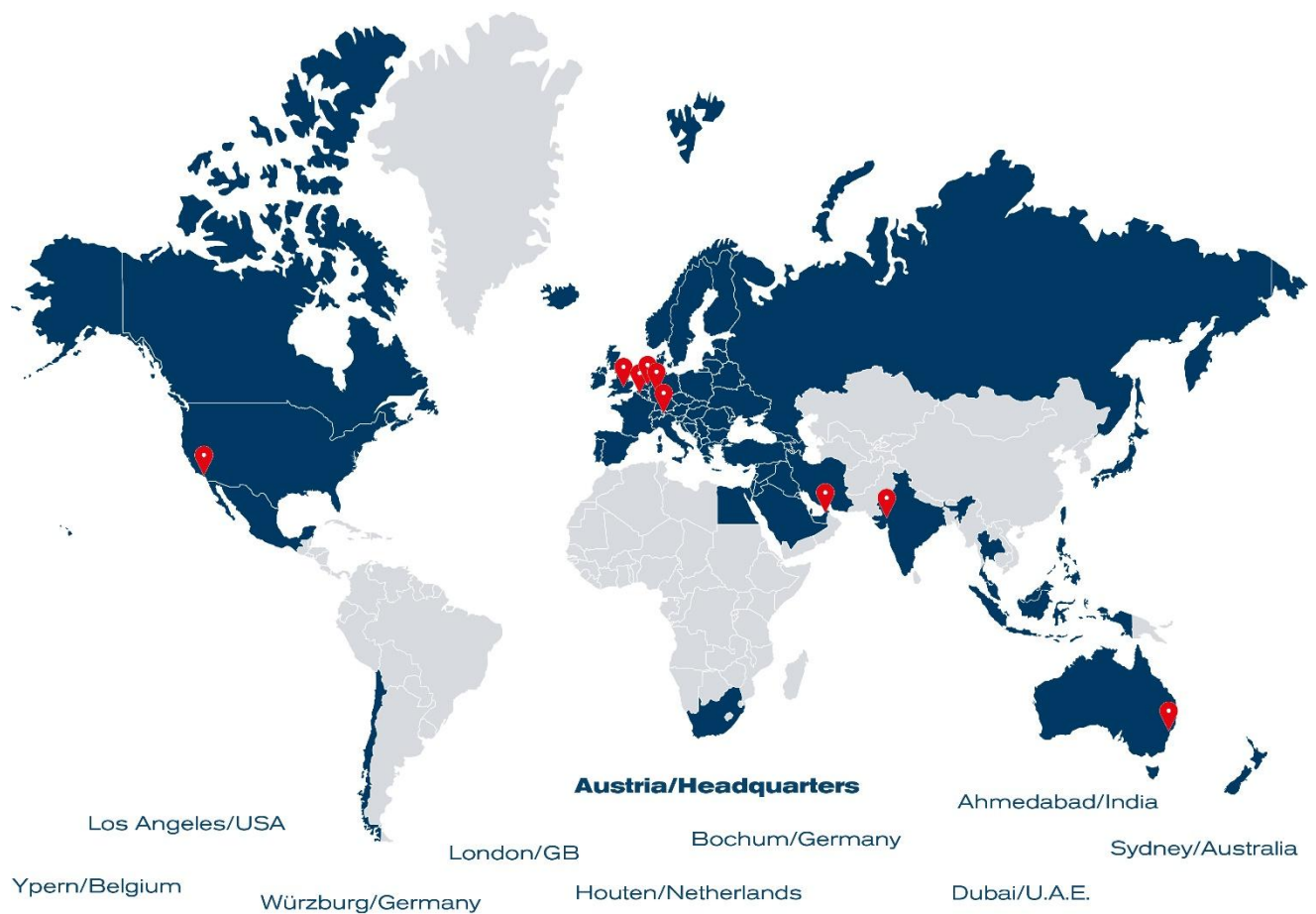
Permitted ambient temperature:	-10 °C to +55 °C
Permitted storage temperature:	-10 °C to +55 °C
Protection type:	IP 30
Environment class	II (conditions in indoor areas)
based on VdS 2110:	

10.11 Dimensions



Note:

This manual is valid as of March 6th, 2026. It is subject to change.
Amendments and changes can be made without prior notice at any time.



GANTNER operates in over 60 countries worldwide. **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