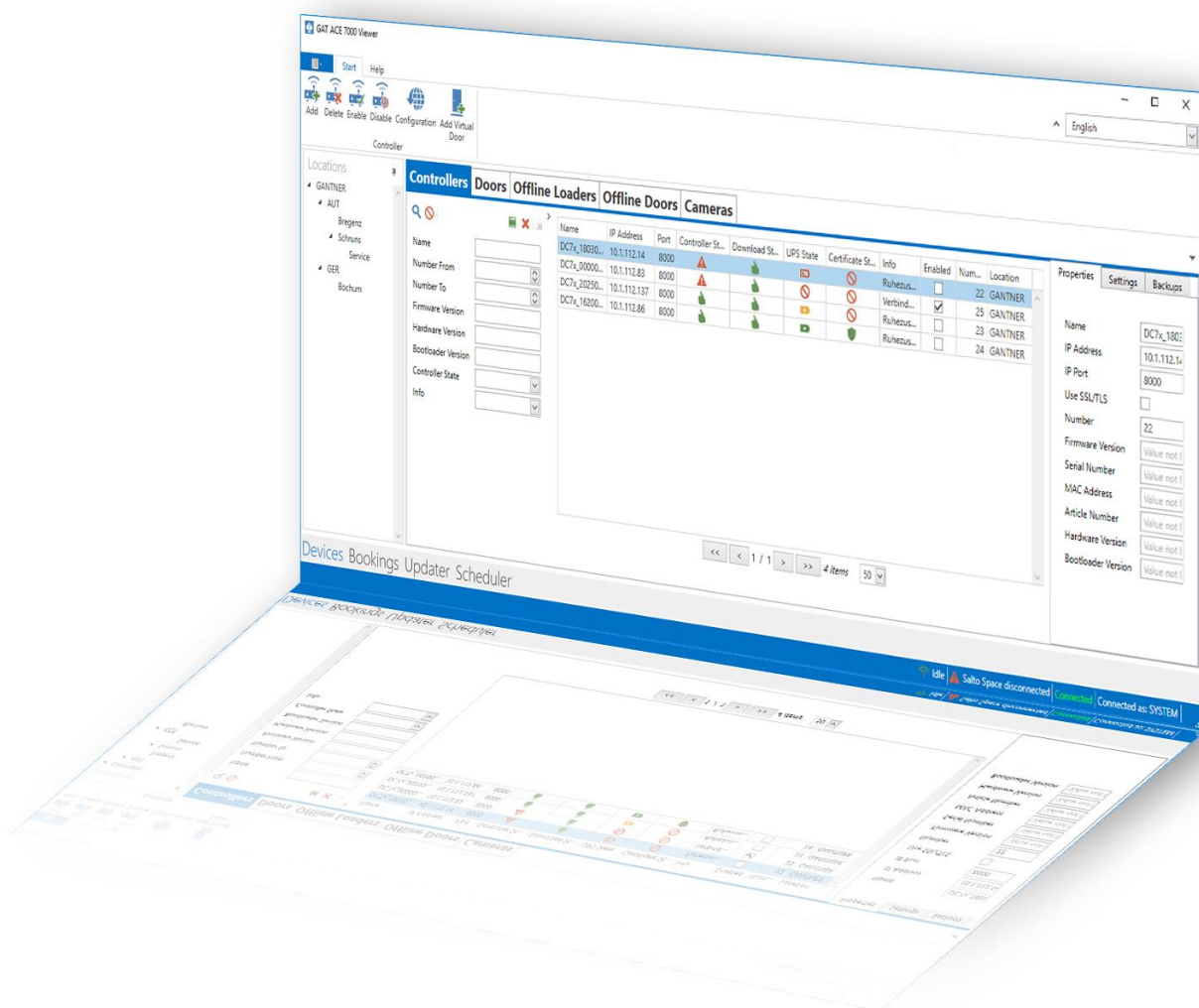


GAT ACE 7000

Middleware for Access Control by GANTNER Electronic GmbH



© Copyright 2023 GANTNER Electronic GmbH

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

Liability

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

Trademarks

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

Contact

The contact information for questions regarding GAT ACE 7000 or for general enquiries is listed below:

Contact address of manufacturer

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



General Warning and Safety Instructions

Dear Customer,

We congratulate you on selecting a product (appliance or software) from GANTNER Electronic GmbH. Our aim is to ensure 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:

1. 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 product documentation.
2. Before installing, commissioning, operating, or maintaining the product, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.
3. If there are 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.
4. Where not otherwise specifically documented, the appropriate installation, commissioning, operation and maintenance of the product is the customer's responsibility.
5. Directly on receipt of the goods, inspect both the packaging and the product itself for any signs of damage. In addition, check that the delivery is complete and includes all accessories, documentation, auxiliary devices, etc.
6. 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 resolve the problem as quickly as possible.
7. The installation, commissioning, and servicing of our products must be performed by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association (e.g., ÖVE [Austrian], VDE [Germany]).
8. Where not otherwise stated, installation and maintenance work on our products must be carried out when disconnected from the power supply. This particularly applies to appliances that are normally supplied by low-voltage current.
9. It is prohibited to alter the products or remove protective shields and covers.
10. Do not attempt to repair a product after a defect, failure, or damage is detected. In addition, do not put the product back into operation. In such cases, it is essential to contact your GANTNER representative or the GANTNER support hotline.
11. GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.
12. Although 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.
13. 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.
14. We especially look forward to hearing from you if you just want to tell us that everything is functioning perfectly.

We wish you a successful experience with our product and look forward to welcoming you again as a customer soon.

CONTENTS

1	INTRODUCTION	7
1.1	About this manual	7
1.2	Formatting	7
1.3	General information	8
1.4	Features of GAT ACE 7000	9
1.5	Supported devices	9
1.6	Terminology	9
2	INSTALLATION	13
2.1	Hardware requirements	13
2.1.1	Configuration example 1	13
2.1.2	Configuration example 2	13
2.2	Software requirements	14
2.2.1	Supported operating systems for GAT ACE 7000	14
2.2.2	Database server	15
2.2.3	Microsoft .NET Framework	15
2.3	Installation of GAT ACE 7000	16
2.3.1	Installation of SQL Server 2019 Express	16
2.3.2	Installation of GAT ACE 7000	19
2.3.3	Windows Services settings	22
2.3.4	License	23
2.3.5	TLS certificate configuration	23
2.3.6	Installing the TLS certificate	26
2.4	Updating GAT ACE 7000	30
3	STARTING GAT ACE 7000 VIEWER	31
3.1	Start-up	31
3.1.1	GAT ACE 7000 Service	31
3.1.2	Creating a database	32
3.1.3	Login window	33
4	SOFTWARE SETTINGS	35
4.1	Database settings	36
4.2	Application settings	37
4.3	Email notification settings	39
4.3.1	Editing automatic email notifications	40
4.4	"Space interface" settings	41
4.5	Roles and user management settings	42
5	OPERATION	43
5.1	Functional overview of GAT ACE 7000 Viewer	43
5.2	Configuring an access system	46
5.2.1	Structuring locations	46
5.2.2	Adding controllers	47
5.2.3	Configuring controllers	50
5.2.4	Copying the configuration of a controller	53
5.2.5	Backup and restore a controller configuration	54
5.2.6	Updating controllers and readers	55
5.2.7	Initializing a controller	55
5.2.8	Restarting a controller	56

5.2.9	Assigning virtual doors to controllers	56
5.2.10	Status display for online doors	57
5.2.11	Configuring offline loaders and offline doors	59
5.2.12	Synchronizing offline loaders and offline doors	66
5.2.13	Remote sync transfer of offline data	70
5.2.14	Updating firmware of the GAT DL 73xx offline controllers and GAT locker locks	75
5.2.15	Configuring cameras for license plate recognition systems	76
5.3	Bookings	79
5.4	Updating online controllers and readers	80
5.5	Scheduler	81
5.5.1	SQL database backup	82
5.5.2	Cleanup of the database table	83
5.5.3	Cleanup of the door controller backups	84
5.6	Help functions	85
5.6.1	Show Manual	85
5.6.2	Quick Support	85
5.6.3	Diagnostics	86
5.7	Troubleshooting	88
5.7.1	VPN Connection Problem	88
6	AUTORIZATION MANAGEMENT	89
6.1	Function blocks	89
6.2	Role management	90
6.3	User management	92
6.3.1	Active Directory	94
6.3.2	Default users	95
7	DATA PROTECTION	97
7.1	General Data Protection Regulation (GDPR)	97
7.1.1	Perform an inventory analysis	97
7.1.2	Create a processing directory	98
7.1.3	Data protection impact assessment	98
7.1.4	Comply with information requirements and declarations of consent	98

1 INTRODUCTION

1.1 About this manual

Chapter "1. INTRODUCTION" of this manual provides an overview of GAT ACE 7000 and describes its main features. Also defined in this section are the most important terms used throughout the manual.

Chapter "2. INSTALLATION" describes the system requirements for GAT ACE 7000 and how to configure the database. Also available here is an overview of the installation options. Following on from this is a detailed description of the installation process for GAT ACE 7000 and its additional components such as the .NET Framework and database.

Chapter "3. STARTING GAT ACE 7000 VIEWER" outlines the initial start-up process for GAT ACE 7000 including how to complete the one-off configuration requirements such as establishing the database connection.

Chapter "4. SOFTWARE SETTINGS" includes the general configuration settings for GAT ACE 7000 including the database settings, the settings for synchronising directories, and the role and user settings. These settings usually only need to be defined once after installing GAT ACE 7000, however, they can be viewed and changed at any time.

Chapter "5. OPERATION" describes the layout of the GAT ACE 7000 interface and how to use the main functions therein. In addition, the most important instructions required to configure an access control system are outlined here. This chapter also includes a detailed description of all the functions available in GAT ACE 7000.

In chapter "6. AUTORIZATION MANAGEMENT", information on the GAT ACE 7000 authorisation management system is available. Different users can be created within the application and each assigned various rights. For example, the facility operator can be assigned to the role of administrator, who can access all the settings and functions in GAT ACE 7000, and employees of the facility can be assigned to the role of "Daily User", who can access important functions in GAT ACE 7000 but cannot change the system configuration.

Chapter "7. DATA PROTECTION" informs you about the new EU General Data Protection Regulation and how GAT ACE 7000 supports compliance with the requirements.

1.2 Formatting

Important, function-critical information is displayed in this manual using the following formatting (with sample text). These instructions must be read and followed:

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.

Important, but not safety-critical, information and helpful tips are formatted as follows (with sample text):

i *The text next to this symbol contains interesting information relating to the current topic. The information will help you better understand the description in this section or provide interesting tips for using the software.*

Action steps, to be performed by the reader, and the results of these actions are formatted as follows.

- ▶ This symbol represents an action or instruction that you must follow.
 - This symbol represents the result after executing the previous action.

1.3 General information

GAT ACE 7000 is a middleware application for configuring access control systems that include controllers and other peripheral devices from GANTNER Electronic GmbH. It serves as an interface and controls all communication between the controllers and the higher-level software. GAT ACE 7000 runs on a Microsoft Windows® operating system (see "2.2.1 Supported operating systems for GAT ACE 7000").

The structure of the access control system is defined in GAT ACE 7000. This structure includes the settings, configurations, addresses, and communication parameters for each controller. In addition, GAT ACE 7000 also offers the possibility to evaluate the controller bookings and to view the communications log.

GAT ACE 7000 consists of a Windows® service, which operates in the background and manages the communication requirements, and a user interface ("GAT ACE 7000 Viewer"), which is used for system configuration and management of the service. As the user almost always interacts with the application via the graphical user interface, the term "GAT ACE 7000" is used in this manual to refer to the user interface component of GAT ACE 7000.

The assignment and management of access rights to individuals or data carriers is carried out by a higher-level access control application, which is a separate application to GAT ACE 7000. For this purpose, GANTNER provides GAT Matrix as the ideal partner to combine with GAT ACE 7000. In addition, building management and monitoring systems can also operate effectively with GAT ACE 7000.

GAT 7000 ACE manages GANTNER's latest 7000 series access controllers, e.g., the GAT DC 7200. Previous controller series, such as the GAT Terminal 3000 and GAT Terminal 3100, are managed by GAT ACE 3000 for which a separate manual is available. GAT ACE 3000 and GAT ACE 7000 can be installed and operated in parallel. For the user granting access authorizations in GAT Matrix, only minor differences exist between the two GAT ACE variants, e.g., GAT ACE 7000 can distinguish between and use different types of data carriers.

It is possible to install GAT ACE 7000 and GAT Matrix, GAT ACE 3000 and/or another access control application, on a single computer, or alternatively, to install GAT ACE 7000 on a central server thereby allowing multiple GAT Matrix installations (clients) to share the same GAT ACE 7000 database (see chapter 2.3.2. Installation of GAT ACE 7000).

1.4 Features of GAT ACE 7000

- Bi-lingual (English & German languages supported)
- Runs on all modern Windows operating systems (32- and 64-bit)
- Communication channels limited only by the hardware
- Communication via TCP/IP network
- A total of 999 GAT ST 210, GAT ST 22x and TAC per system
- A total of 4095 GAT DL 3xx, GAT DL 73xx and GANTNER locker locks per system
- Interface to GAT Matrix and other access management systems
- Interface to SALTO ProAccess SPACE software
- Rapid communication speeds with the controllers (parallelization) and management software
- Encrypted communication with GAT DC 7200 controllers via TLS/SSL possible
- UPS status display for the controller
- Service runs without requiring user login
- Direction of movement recognized
- Attack PIN code (i.e., duress code)
- Controller initialization
- Setting of controller addresses
- Memory allocation
- Supports both online and offline controllers
- Location-specific updating for offline devices
- Virtual doors for an advanced system configuration
- Display of access and time bookings
- Read/write CardNET data for time systems
- Direct control of controller via commands
- Logging of events and communication
- Scheduler for the automatic activation of system tasks

1.5 Supported devices

GAT ACE 7000 supports Series 7000 online access controllers from GANTNER Electronic GmbH. This currently includes the GAT DC 7200. In addition, the following offline devices are supported:

- | | | |
|--------------|------------------|--|
| - GAT DL 32x | - GAT ST 210 | - GAT DL 73xx |
| - GAT DL 34x | - GAT ST 220/225 | - GAT ECO.Side Lock 7000 NW BA CardNET |
| - GAT DL 350 | - TAC | - GAT ECO.Lock 7100 NW BA CardNET |
| - GAT DL 360 | | - GL7p.2300 CardNET, GL7p.330x CardNET |
| - GAT DL 370 | | |

The GANTNER device's support capability has been tested with the latest firmware version of the device. Devices with older firmware versions must be updated to ensure that communication between GAT ACE 7000 and the device is possible.

Transferring data to offline devices is done using one of the following devices.

- | | | |
|--------------|--------------|---------------|
| - GAT DL 092 | - GAT MT 010 | - Remote Sync |
|--------------|--------------|---------------|

1.6 Terminology

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

Access control software

This term describes software of a higher level than GAT ACE 7000, e.g., the GAT Matrix software package from GANTNER Electronic GmbH, which is used for the granting and administration of user authorisations.

User

The term “user” describes the person operating GAT ACE 7000. Multiple users can be created in the system, each with a personal username and unique password.

Person

In this manual, “person” refers to the end user of the access system, which is normally a company employee. For every person who should have access, an individual data set is created in the access control system, e.g., GAT Matrix, and a data carrier with unique number assigned for identification. The data set includes data such as the staff card number, data carrier number (also called card number), PIN code, and assignment to a group or fingerprint data.

Data carrier

Data carriers are used for identification at readers connected to a controller. Depending on the device, various types of data carriers can be used with the reader, e.g., contactless RFID cards, or magnetic and infrared cards. The contactless data carriers are available in various shapes and sizes including cards, key tags, and wristbands, and for different kinds of identification systems (LEGIC prime, PROXY, MIFARE®, ISO 15693, ISO 14443A, ISO 14443B).

Controller / terminal

The terms “controller” and “terminal” are synonymous in this manual and refer to the devices used to read the data carriers of persons at doors, check access authorisations, and electronically lock and unlock the doors accordingly. With a built-in RFID reader, the controllers can directly read data carriers or, as with the GAT DC 7200 controller, use one or several remote reading devices for reading the user data carriers.

The controllers are managed in GAT ACE 7000. A web interface allows access to the controllers in order to edit their configuration data.

A distinction is made between online and offline controllers. Online controllers are equipped with a network interface that allows them to connect to a local network (Ethernet). Online controllers allow a direct connection, thus enabling a direct configuration and a real-time status display. Offline controllers are not equipped with a network interface. The configuration of and the communication with these controllers is performed on-site, using a programming device, via corresponding data carriers, or over radio frequency.

Inputs / outputs

Most controllers are equipped with one or more digital optocoupler inputs to identify the door status and relay outputs to control equipment, e.g., the unlocking relay of a door. The functionality of these inputs and outputs can be set precisely during the configuration of the controller.

Door

In this manual, the term “door” refers generally to the access point being monitored and controlled. In most cases, this is a door that restricts access to a room within a facility. It is also possible to control and monitor a turnstile or a driveway with an access gate. The principle of access control, i.e., the configuration process in GAT ACE 7000, is identical in each of these cases.

However, it is important to clearly distinguish between door and controller as a single controller can control several doors, depending on the type of controller.

Reader

One or several readers are connected to each controller or are installed on a permanent basis. Identification is performed at the readers using data carriers with read data transmitted to the controller where the evaluation is performed. Depending on the reader model, data can also be written onto the data carrier by the reader.

There are various reader models, e.g., separate reader units connected to the controller via RS-485 interface. There is a further distinction made between close-range readers and long-range readers, the latter enabling an identification at a distance of several meters.

CardNET

This term describes a type of operating mode for offline controllers and offline locker locks. It is important here to distinguish between CardNET G1 and CardNET G2.

CardNET means that for the configuration of the controllers on-site, a programming device is used. The authorizations of the persons are then stored on the data carriers.

The authorization data of the persons for offline controllers and locker locks is sent by the access control software (e.g., GAT Matrix) to specific, specially designated, online controllers in the access system. At these online controllers, the authorization data is written directly onto the data carriers. These special online controllers must support the read/write function (read/ write or CardNET function) and the readers must be enabled (authorized) with an authorization card for writing to LEGIC and DESFire data carriers. The data carriers must therefore be valid and configured for this use.

CardNET G1 supports LEGIC prime and LEGIC advant data carriers only and can store max. 10 doors and 30 door groups on the data carrier.

CardNET G2 supports LEGIC advant and MIFARE DESFire and is not limited to the 10 doors and 30 door groups storage. CardNET G2 is supported by the following devices:

- Offline controllers GAT DL 32x and GAT DL 34x
- Readers GAT SR 73xx and GAT SLR 73xx
- Readers GR7.xxxx
- Door controllers GAT DC 7200
- Locker locks GAT ECO.Lock 7100 NW BA CardNET, GAT ECO.Side Lock 7000 NW BA CardNET, GL7p.xxxx CardNET
- Time & Attendance terminals GAT ST 38x/39x EVO PoE

Older devices with the FLEX protocol (e.g., GAT Terminal 3100, 3000, 2500, GAT SR 3xx and GAT SLR 3xx, and the GAT ST 38x/39x) only support CardNET G1.

It is also possible to use combi data carriers that combine CardNET G1 and G2 on a single data carrier. This allows different authorizations for different doors on one data carrier to be realised. Not all variants of G1 and G2 are possible with a combi data carrier:

- G1 LEGIC prime and G2 LEGIC advant = It is possible.
- G1 LEGIC prime and G1 LEGIC advant = It is possible.
- G1 LEGIC advant and G2 LEGIC advant = It is not possible.

WiNET

This term describes a type of operating mode for offline controllers. WiNET means that the offline terminals are equipped with a radio connection that allows them to communicate with an online controller. The configuration and authorisations are administrated via the radio network.

SPACE / ProAccess Space

This is a SALTO software solution used to manage users, data carriers and SALTO access control readers in a facility. GAT ACE 7000 provides an interface to SALTO Space to allow common management of SALTO doors and users in GAT Matrix.

SALTO Virtual Network (SVN)

The SALTO SVN is a 'Data on Card System' with patented read and write functionality and encrypted data transfer. In the SVN, the authorizations are stored on the data carrier.

Schedule

A schedule defines access authorisations and controller functionalities and can be established for a controller (Generally Open Schedule or Door Schedule) or for persons (Staff Schedule).

Generally open schedule / Door schedule

A "generally open schedule" can be assigned to a controller and determines which controller functionalities should be active at a point in time. With a generally open schedule, it is possible to unlock a door for a certain period, activate a special relay schedule, or disable alarms without requiring identification.

Personnel schedule

A personnel schedule defines access authorisations for each day of the week, as well as for 10 types of special days. Personnel schedules are assigned to persons and controllers in the access control software thereby defining the type of access authorisation granted at each controller.

Special rights

Special rights can be assigned to any person, for single or multiple doors, provided the controllers that control these doors are also configured for the special rights option. Different types of special rights are possible (see full description in the GAT Matrix manual) and some examples include:

- Following identification, the controller's "special rights" relay output is activated in addition to the normal unlocking operation. This can be used, e.g., to control a second parking barrier.
- The activation or deactivation of an alarm system at a controller equipped with a control relay.
- Special verification functionality, e.g., the use of a PIN code instead of a fingerprint.
- Activate or deactivate the anti-pass-back blocking function or only show infringements of this function.
- Activate or deactivate the double-booking blocking function or only show infringements of this function.
- Activate or deactivate the pool management blocking function or only show infringements of this function

Threat PIN code

Depending on the configuration and staff data, a PIN code can also be configured for access authorization in addition to identification via data carrier. In this case, it is also possible to define a threat PIN code for additional security. The threat code is combined with the respective PIN code to trigger a covert threat alarm when an unauthorized door opening is obtained by force.

Bookings

Whenever an event, e.g., identification of a person, alarm messages, etc., occurs at a controller, a booking is generated and recorded in an internal log. These bookings can be saved and evaluated in GAT ACE 7000.

GAT locker lock

A battery-powered lock that is used for the electronic locking of lockers, e.g., in office applications. The users are identified at the lock by means of contactless RFID data carriers. GAT ACE supports different types of locks (GAT ECO.Lock 7100 NW BA CardNET, GAT ECO.Side Lock 7000 NW BA CardNET, GL7p.xxxx CardNET). In this manual and in GAT ACE 7000, the shortened term "GAT Locker Lock" is used for these locks.

GAT DL 73xx

Offline controller for the autonomous control of doors (without network connection). The GAT DL 73xx is mounted next to the door being controlled and reads contactless RFID data carriers that the users use for identification. Note: The GAT DL 73xx is a GAT SR 73xx or GR7 reader with special firmware.

UPS

An abbreviation of uninterruptible power supply, this is an emergency power supply with battery to ensure that power is supplied to the controller even in the event of a power failure. For example, the GAT SP 074 UPS Online 30W (Part No. 1104717) from GANTNER can be used. The charge status is shown on the controller display in GAT ACE.

2 INSTALLATION

2.1 Hardware requirements

Depending on the type of configuration required for the PCs/servers, different installation requirements must be considered for GAT ACE 7000 and the accompanying access control software, e.g., GAT Matrix.

2.1.1 Configuration example 1

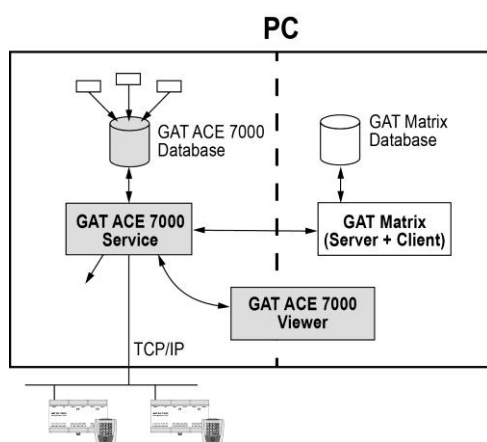


Figure 2.1 - Installation of GAT ACE 7000 and GAT Matrix on the same PC

2.1.2 Configuration example 2

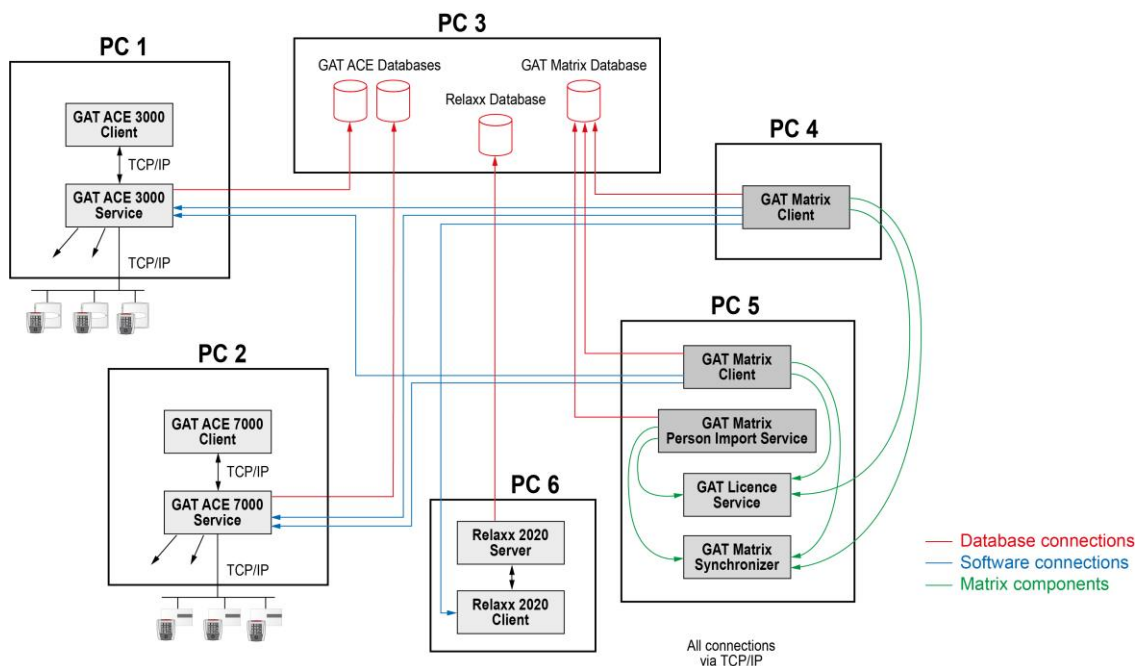


Figure 2.2 – GAT Matrix and GAT ACE 3000/7000 installation on different PCs, GAT Matrix and GAT ACE databases on own PC

Hardware recommendations for PCs:

- IBM compatible PC, e.g., Core i5, 3 GHz or equivalent CPU
- Network card (TCP/IP)
- PC interfaces: Ethernet (TCP/IP) and USB
- Internet access for updates
- Monitor (1024 x 768 min. resolution)
- Internet browser - Internet Explorer 7.0 or later version

Computer hard drive and RAM requirements for each application:

- Free RAM: Approx. 1 GB for GAT ACE 7000
 Approx. 2 GB additionally for Microsoft SQL Server 2014 Express
- Free hard drive: 20 GB (for protocol and configuration data)

Depending on how many applications are installed on each PC, the total minimum requirement for the PC must be calculated.

2.2 Software requirements

2.2.1 Supported operating systems for GAT ACE 7000

- Microsoft Windows® 10 (Pro, Enterprise), 64-bit
- Microsoft Windows Server® 2008 R2, 64-bit
- Microsoft Windows Server® 2012, 64-bit
- Microsoft Windows Server® 2012 R2, 64-bit
- Microsoft Windows Server® 2016 (Essentials, Standard, Datacenter), 64-bit
- Microsoft Windows Server® 2019 (Essentials, Standard, Datacenter), 64-bit

The Server Core installation option of Windows Server® 2008, Windows Server® 2008 R2, or Windows Server 2012 is not supported by GAT ACE. In addition, RT, Starter, Home, Small Business, and Web editions are not supported.

NOTE! Please note that GANTNER Electronic GmbH can only provide support assistance when GAT ACE 7000 is installed on a German or English version of Windows.

NOTE! The customer must provide the required licenses, e.g., for the operating system or database.

2.2.2 Database server

Supported databases:

- Microsoft® SQL Server® 2008 R2 Express
- Microsoft® SQL Server® 2008 R2
- Microsoft® SQL Server® 2012
- Microsoft® SQL Server® 2012 Express
- Microsoft® SQL Server® 2014
- Microsoft® SQL Server® 2014 Express
- Microsoft® SQL Server® 2016
- Microsoft® SQL Server® 2017
- Microsoft® SQL Server® 2019

NOTE! The updated system requirements for Microsoft® SQL Server® can be found via the following link:

<https://technet.microsoft.com/de-de/library/ms143506.aspx>

NOTE! Please note that the GAT ACE installation package does not contain a database server; however, the Microsoft® SQL Server® Express database is freely available. If a full version of the SQL database is required, this must be provided by the IT system administrator.

It is recommended to also install Microsoft SQL Server Management Studio Express. This application is included in the GAT ACE 7000 installation package.

NOTE! When using the Express version of Microsoft® SQL Server®, ensure the database maintenance function is enabled to keep the database size to a minimum.

For the folder where the database is located, the following points must be observed:

- Antivirus software is not allowed to scan the folder. Refer to Microsoft's recommendations: (<https://technet.microsoft.com/de-de/library/ms144228.aspx>).
- Automatic backups of the folder are not permitted.

2.2.3 Microsoft .NET Framework

For the operation of GAT ACE 7000, the .NET Framework 4.7.2 must be preinstalled.

2.3 Installation of GAT ACE 7000

This section describes the GAT ACE 7000 installation process and is valid for computers that do not already have an older access control system from GANTNER Electronic GmbH installed.

- ▶ Start the installation of GAT ACE 7000 by double-clicking on the "Setup.exe" file in the installation package.

2.3.1 Installation of SQL Server 2019 Express

A database is required for GAT ACE 7000. This section can be skipped if a database server is already installed. Otherwise, install a database server now. Microsoft® SQL Server® 2019 Express is available to download from the GANTNER Partner website and can be used for a database.

NOTE! Microsoft SQL Server Management Studio is also included in the installation package. It is recommended to also install this application to ensure the optimal environment for the maintenance and service of GAT ACE 7000.

NOTE! This section describes the most important points for installing Microsoft SQL Server 2019 Express. Database servers have many more configuration settings. To define these, MS SQL Server Management Studio Express is included in the GAT ACE 7000 installation package. Contact your database administrator for advice on configuring advanced settings.

- ▶ To install the Microsoft SQL Server 2019 Express database server, open the SQL Server directory in the installation package and double-click on the "Setup" file.
 - The database installation wizard starts.
- ▶ Click on "Continue >>".
 - The installation wizard guides you through the installation of Microsoft SQL Server 2019 Express.
- ▶ Confirm the license conditions.
 - The "Setup Support Files" are installed, and the following dialog opens. The individual installation steps are shown to the left and the installation settings are configured in the middle.

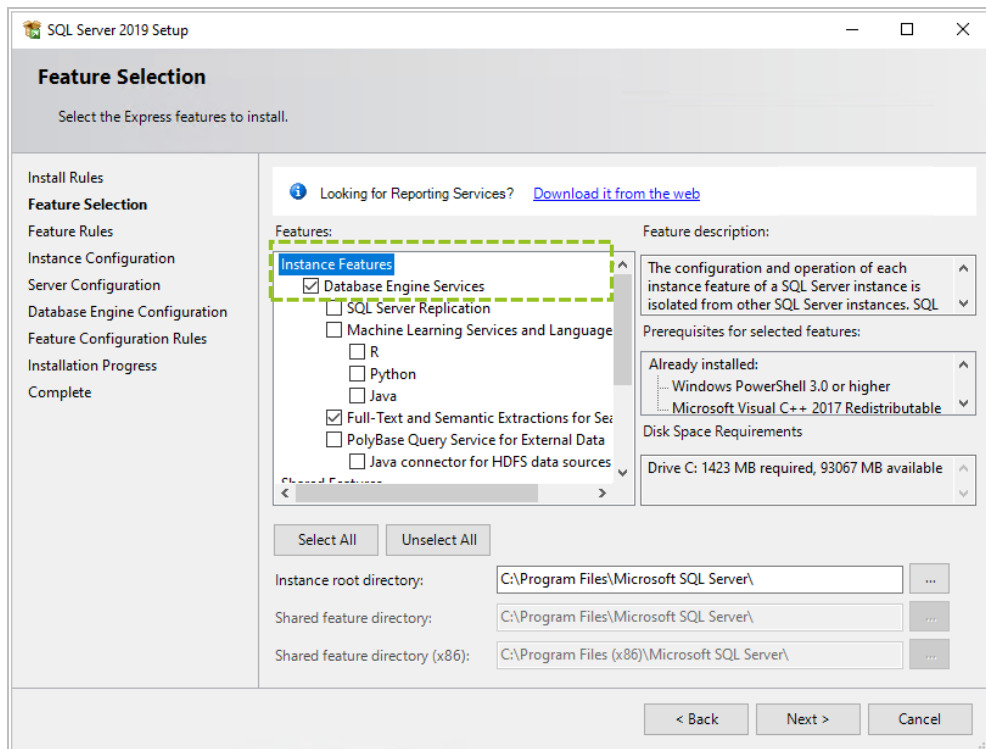


Figure 2.3 - Microsoft SQL Server 2019 Express - option configuration

- It is important to select the “Database Engine Services” option. This ensures that the SQL Server is installed as a Windows Service.
- Click on “Next >” until the “Server Configuration” window is displayed.

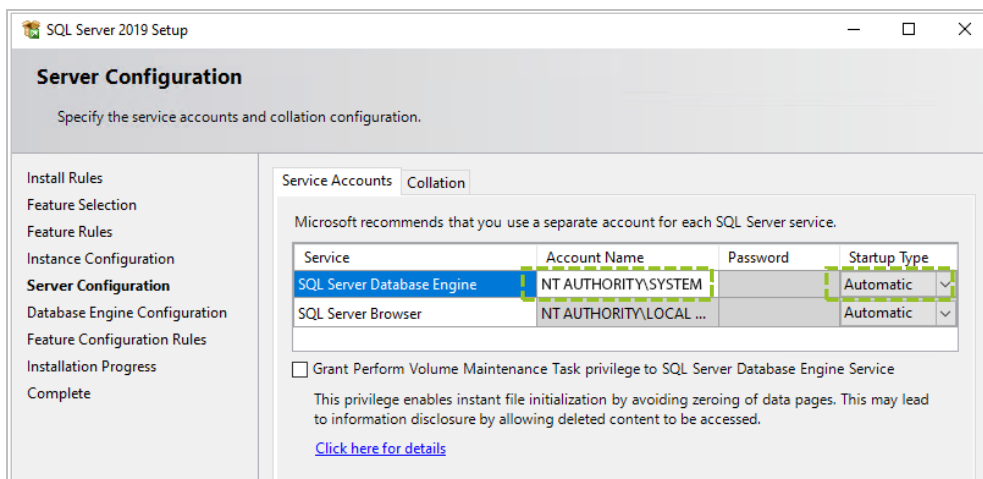


Figure 2.4 - Microsoft SQL Server 2019 Express – Server configuration

- In this window, define the user account under which the SQL Server will operate. If you have created a dedicated user account specifically for the SQL Server, enter the details here. Otherwise, the 'NT AUTHORITY\SYSTEM' account should be used.
- The “Startup Type” should always be set to "Automatic". This ensures that the services start automatically during Windows start-up.

- Click on "Next >" to continue to the "Database Engine Configuration" window.
 - Here the login method and the administrators for the SQL server are defined.

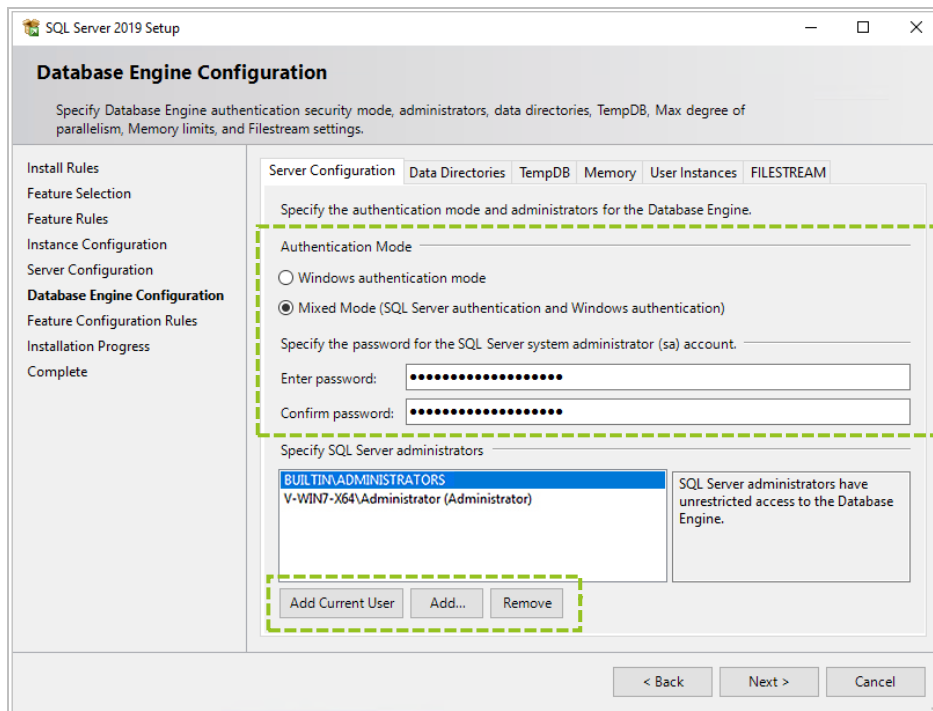


Figure 2.5 - Microsoft SQL Server 2019 Express – database configuration

- For local installations, e.g., one where GAT ACE 7000 and GAT Matrix are installed on the same PC/server, select the “Mixed Mode” option. The password that is later used in GAT ACE 7000 for the user “sa” is predefined by GANTNER. You can change this to your own, customer-specific password during installation. If you require the password specified by GANTNER, please contact GANTNER Support.

NOTE! When using your own password, use a strong password. The password should be at least 7 characters long and contain at least one uppercase letter, one lowercase letter and one number. Please follow the IT guidelines that apply to you.
- An alternative to Mixed Mode is the “Windows authentication mode”. This option uses the current Windows user login data for database login.
- For “Mixed Mode”, you can define Windows user accounts that will have administrator rights for the server. This is done using the “Add Current User” and “Add” buttons.
- Finally, keep clicking on “Next >” until the installation is complete.

2.3.2 Installation of GAT ACE 7000

Once all the previously described components are installed (Windows Installer 4.5, .NET Framework Version 4.5, SQL Server database), the installation of GAT ACE 7000 proceeds as follows.

NOTE! GAT ACE 7000 must be installed by an administrator with full user rights.

- ▶ Open the folder with the installation package of GAT ACE 7000.
- ▶ Double-click on the “setup.exe” file.
 - The installation wizard opens.



Figure 2.6 - GAT ACE 7000 installation - step 1

- ▶ Click on “Next”.

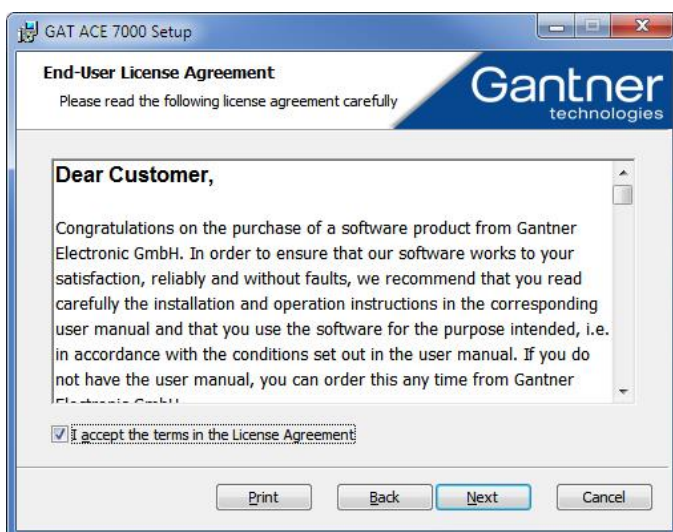


Figure 2.7 - GAT ACE 7000 installation - step 2

- ▶ Read the license agreement information and click on the “I accept the terms in the License Agreement” option to accept the licensing terms.
- ▶ Click on “Next”.

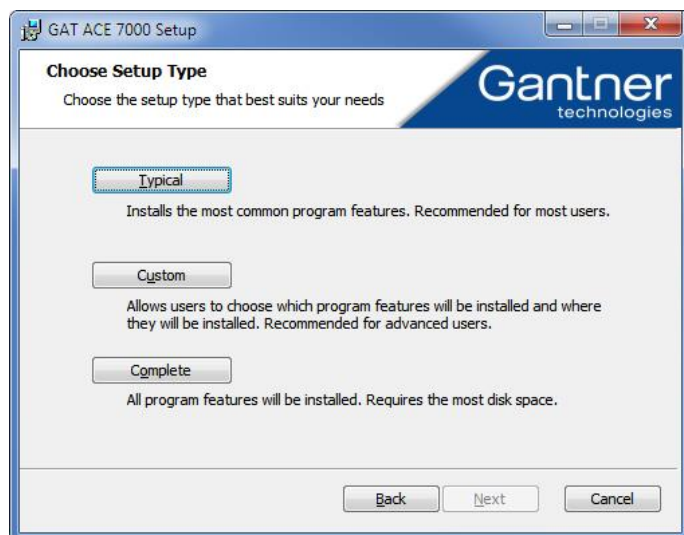


Figure 2.8 - GAT ACE 7000 installation - step 3

- ▶ Select the type of installation (standard = "Typical"):
 - Typical: Installs GAT ACE 7000 (service and client) and the most important components of the application. This is the default option for most users.
 - Custom: Allows you to select the installation location and the individual components to be installed by GAT ACE 7000. The following window appears when this type of installation is chosen. Here, "GAT ACE 7000 Viewer" represents the graphical user interface and "GAT ACE 7000 Service" represents the windows service.

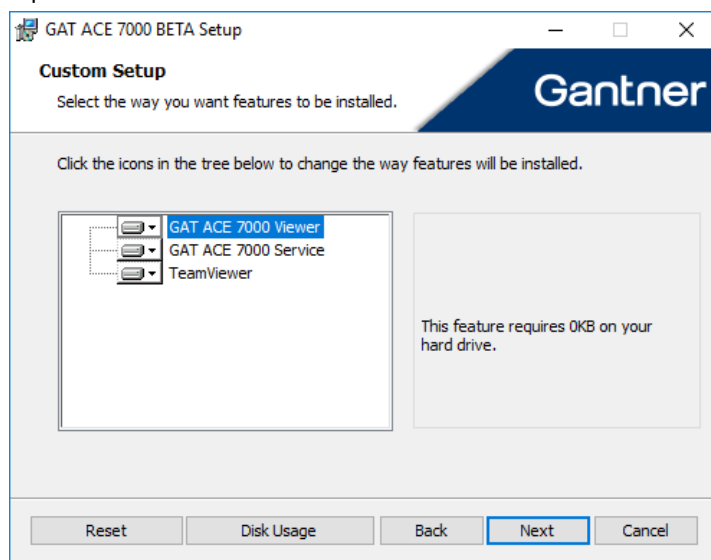
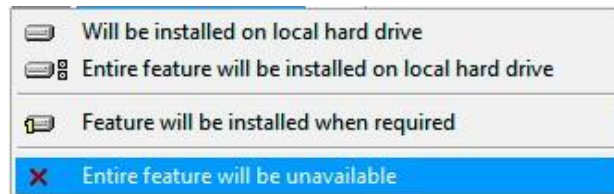


Figure 2.9 - GAT ACE 7000 installation - Custom Setup

- ▶ Select the components you want to install.
 - A white symbol in front of a component indicates that it is selected for installation.
- ▶ To change the installation status of a component, click on the icon in front of the component and select the desired action. For example, if the GAT ACE 7000 server is already installed on another server/PC and you only want to install the client, select “Entire feature will be unavailable” for the server.



- ▶ Now select the directory where you want to install GAT ACE 7000. If you do not want to use the default directory, click on “Browse” to select a different directory.
- ▶ Finally, click on “Next”.

- Complete: This type of installation installs all the components of GAT ACE 7000 and requires the most disk space.

After selecting the type of installation, the following window opens.

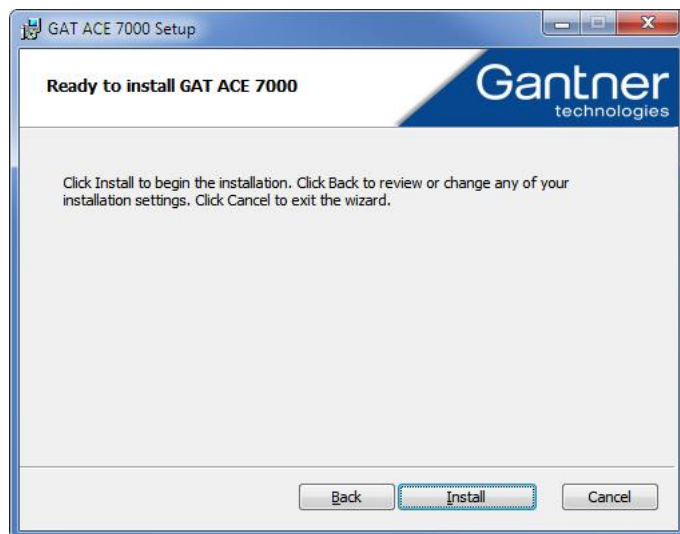


Figure 2.10 - GAT ACE 7000 installation - step 4

- ▶ Click on “Install” and confirm the following authorization request with “OK “.
 - The installation process begins. A green bar indicates the progress of the installation.
- ▶ After installation is complete, click on “Finish” to exit the installation wizard.
 - GAT ACE 7000 is now installed and ready for use.

NOTE! Antivirus Software

In regards to anti-virus software, it is vital to pay attention to the following points:

- Exclude the installation directories of GAT ACE 7000 Service and GAT ACE 7000 Viewer from all anti-virus scans. This includes scheduled real-time or live scans. For standard installations, this relates to the following directories:
 - For 32-bit Windows versions:
 - "C:\Program Files\GAT\GAT ACE 7000"
 - "C:\Program Files\GAT\GAT ACE 7000 Viewer"
 - For 64-bit Windows versions:
 - "C:\Program Files (x86)\GAT\GAT ACE 7000"
 - "C:\Program Files (x86)\GAT\GAT ACE 7000 Viewer"
- The components for the GAT ACE 7000 software must be excluded from a live scan of a virus software in order to prevent the triggering of false virus alarms.

2.3.3 Windows Services settings

When the GAT ACE 7000 Windows service and the SQL database are installed on the same PC, it is possible that the GAT ACE 7000 service starts before the SQL database. In this situation, GAT ACE 7000 cannot connect to the database and subsequently fails to start.

For Windows 7 and Windows Server 2008, this issue is easily solved.

- Open the Windows "Run" dialog via the "Windows" + "R" keyboard shortcut.
- Type "services.msc" into the field then click on "OK".
 - The Windows Services window opens.
- Search for "GAT ACE 7000" in the service list.

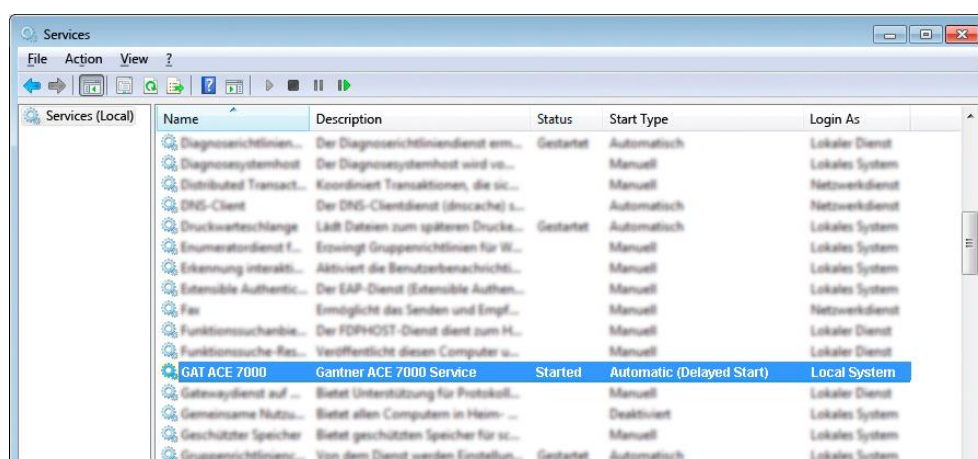


Figure 2.11 - Windows services

- Here, the "Start Type" must be set to "Automatic (Delayed Start)". Right-click on the GAT ACE 7000 service and select "Properties" from the pop-up menu.
 - The Properties window of the GAT ACE 7000 service opens.

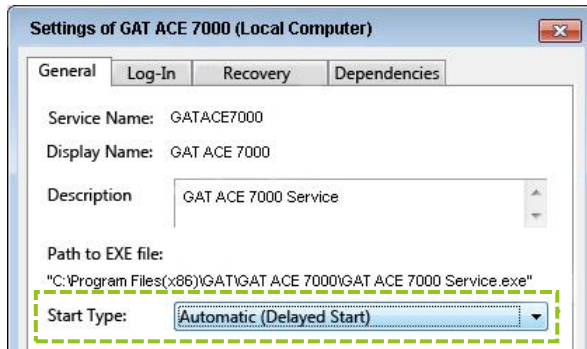


Figure 2.12 – GAT ACE 7000 service settings

- ▶ In the “Start Type” field, select “Automatic (Delayed Start)”.
- ▶ Click on “OK”.
 - This setting ensures that the GAT ACE 7000 service still starts automatically, but the start-up process is delayed.

2.3.4 License

GAT ACE 7000 operates in combination with GAT Matrix and uses the GAT Matrix license for operation. Therefore, the input of a license into GAT ACE 7000 is not required for standard operation. License data must be entered only when additional extensions are being used or if GAT ACE 7000 is used in combination with a third-party application, e.g., building management software or an external interface.

2.3.5 TLS certificate configuration

The communication between the GAT ACE 7000 server (Windows service) and the GAT ACE 7000 client, Matrix client, Building Management Software, Access Management Software, and a GAT DC 7200 (from Version 3.0) can be optionally encrypted using the TLS protocol. The GAT ACE 7000 server can use a certificate provided by the customer or create a self-signed certificate by itself. The first option is strongly recommended.

To configure the TLS encryption, complete the following steps:

- ▶ Optional but recommended: Provide a certificate that can be used by the GAT ACE 7000 service for identification with the client or GAT DC 7200.
 - a) The certificate for communication with the Matrix client or an access management software, etc., must be provided by the IT system administrator and can be inserted in the Windows certificate store (see section “2.3.6 Installing the TLS certificate”).
 - b) For encrypted communication with a GAT DC 7200, it is recommended to use the certificate created by the GAT DC 7200 for GAT ACE 7000. Information regarding certificate creation and the necessary GAT DC 7200 configuration settings is provided in the GAT DC 7200 manual. The following is an overview of the necessary steps.
 1. In the GAT DC 7200 web interface, create a certificate via the “Configuration” menu -> “Security and Users” -> “Certificates” tab -> “Create new self-signed certificate” button and restart the GAT DC 7200.
 2. Download the certificate as a file (default name = “servercert.cer”).

- Import the file into the Windows certificate store (see section “2.3.6 Installing the TLS certificate”).
- In the GAT DC 7200 web interface under the “Security and Users” section of the “Configuration” menu, open the “General” tab and enable the “Use secure connection (SSL/TLS)” option.

CAUTION! After the certificate has been installed on the server, an insecure certificate is still displayed in GAT ACE 7000 (🔴). The GAT DC 7200 must be deactivated and activated to use the installed certificate and display the corresponding icon (🟢) (see also “5.2.2 Adding controllers”). This can be done manually or automatically by GAT ACE 7000, which re-establishes the connection automatically after 1 minute.

- In the configuration files of the GAT ACE 7000 software, set the TLS function to “True” in order to use TLS for communication. The configuration files can be found in the following locations (for a standard installation):

ACE 7000 component	Default file path
Client (User Interface)	%appdata%\GAT\GAT ACE7\GATAce7.cfg
Server (Windows Service)	c:\Program Files (x86)\GAT\GAT ACE 7000\GATAce7000.cfg

Table 2.13 – Default file paths for TLS configuration of the GAT ACE 7000 components

- When TLS is to be used, set the “isslactive” parameter in those two configuration files to “True” (otherwise, set this parameter to “False”).

```
<isslactive TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">True</isslactive>
```

- In the file “GATAce7.cfg”, the parameter is included twice. Set both to “True”.
- In the file “GATAce7000.cfg”, the parameter can be set for different interfaces individually. The first section “Ace7Interface” (1) determines the communication between the service and the client UI.

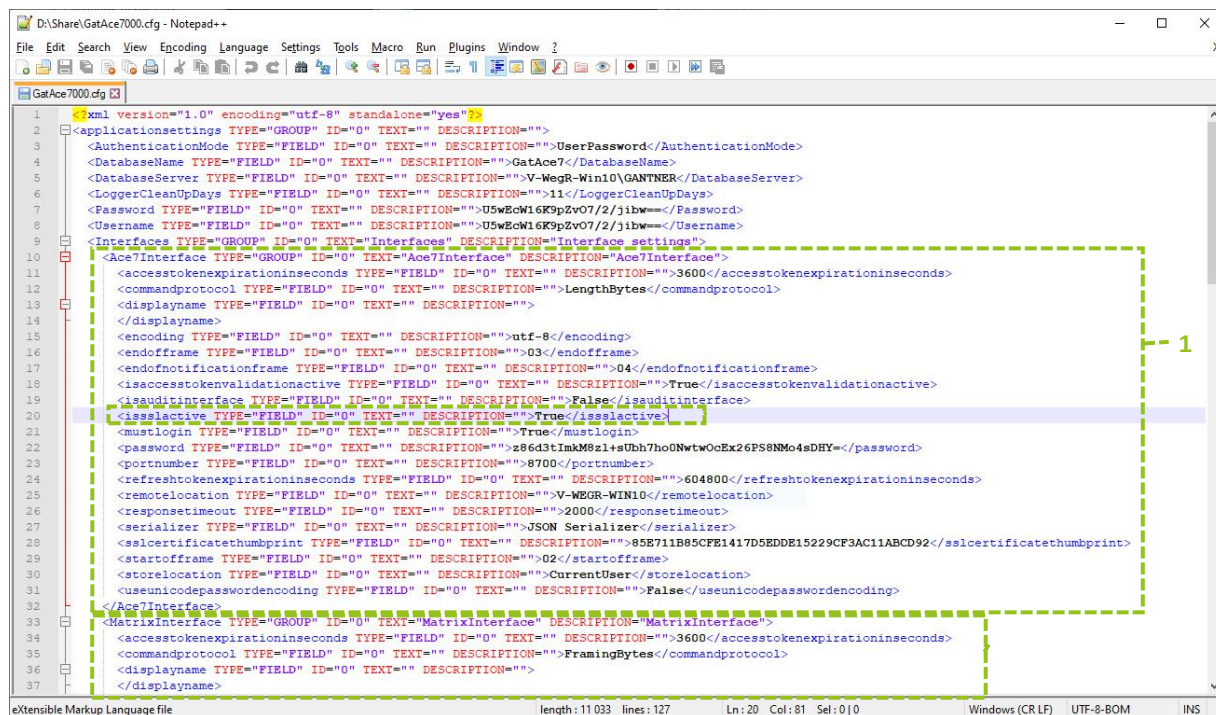


Figure 2.14 – Set parameter <isslactive> to “True”

- Define the parameter "UseUnicodePasswordEncoding". This parameter determines how the interface password, which is used for the authentication handshake, is internally encoded. For GAT ACE 7000, set this parameter to "False" (i.e., ASCII coding is used). When using a third-party software, the value of this parameter can be changed. Example:

```
<useunicodepasswordencoding TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">False
</useunicodepasswordencoding>
```

- Set the parameter "IsAccessTokenValidationActive" to "True". The parameter determines whether the authentication with JWT token is activated, which should always be the case when using TLS. Example:

```
<isaccesstokenvalidationactive TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">True
</isaccesstokenvalidationactive>
```

- In case the certificate has been provided by the customer, set the used certificate in the same config file by inserting the thumbprint in the parameter "sslcertificatethumbprint". Example:

```
<sslcertificatethumbprint TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">3C6011A9F
3D9C6C8DF3DA60B160B80AD66D7465C</sslcertificatethumbprint>
```

1. Open the certification store with "Manage computer certificates" in the Windows start menu.
2. Select the desired certificate by double clicking on it.
3. Open the "Details" tab.
4. In the "Field" list, go to "Thumbprint" and copy this value.

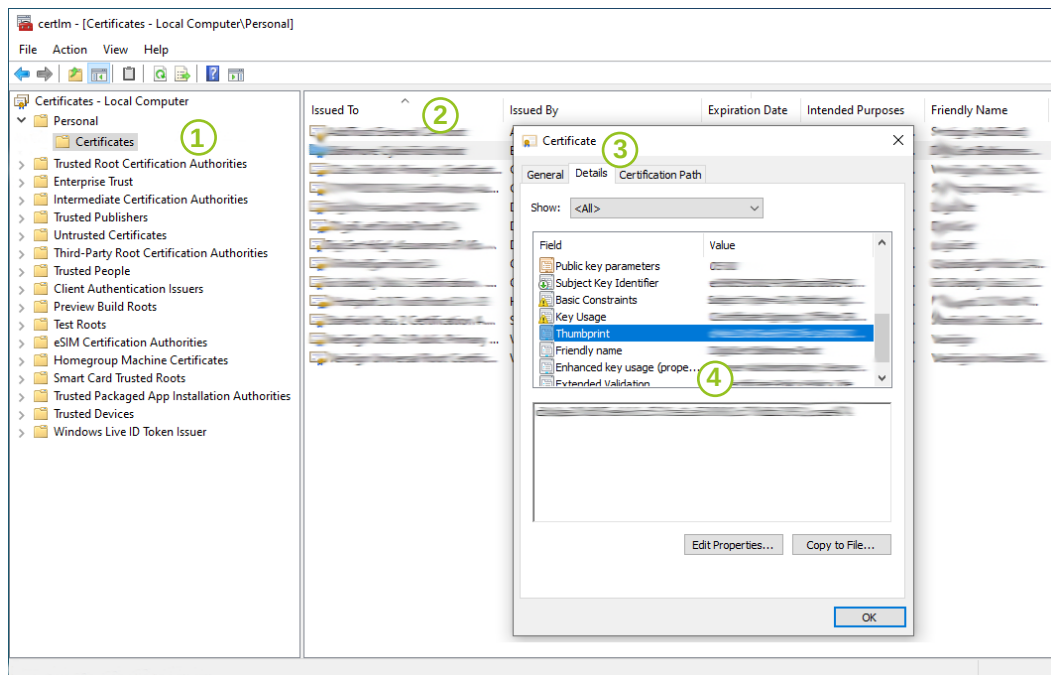


Figure 2.15 –Inserting a certificate provided by customer

5. Open both .cfg files of GAT ACE 7000 (see Table 2.13).
6. In the "Ace7Interface" section, find the "sslcertificatethumbprint" key and insert the thumbprint value.
7. In the sections of the interface that you want to configure, find the "sslcertificatethumbprint" key and insert the thumbprint value.

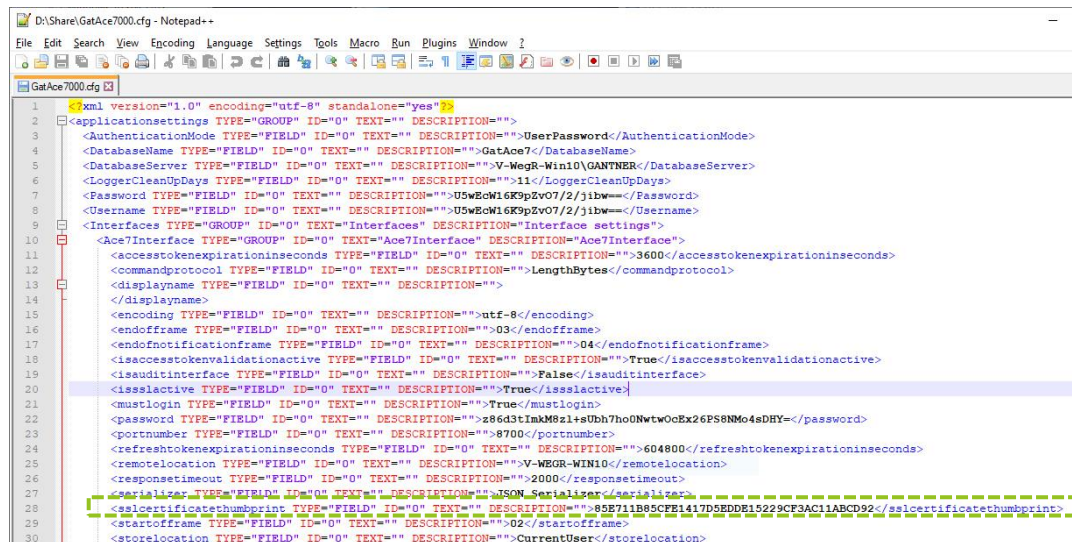


Figure 2.16 – Inserting a certificate provided by customer

- If no certificate has been provided or if the provided certificate is not valid anymore, the GAT ACE 7000 server will automatically create a self-signed certificate that is valid for one year. In this case, GAT ACE 7000 users must install the certificate once as “Trusted Root Certification Authorities” on the computer where the GAT ACE 7000 client is running.

After starting GAT ACE 7000 and successfully connecting to the GAT ACE 7000 service and database, the “Certificate” window is displayed. Here, you can generate and add a TLS certificate via which GAT ACE 7000 will operate. The process is described in the following chapter “2.3.6 Installing the TLS certificate”.

2.3.6 Installing the TLS certificate

To install a certificate for TLS/SSL communication with GAT ACE 7000, complete the following steps on the computer where the GAT ACE 7000 server (Windows service) is installed and also on those computers where the clients are installed if using GAT ACE 7000 clients.

NOTE! The following information is valid for the installation of a TLS/SSL certificate for the connection between GAT ACE 7000 server and software such as GAT ACE 7000 client, GAT Matrix, or building software as well as for the installation of a TLS/SSL certificate for the connection between GAT ACE 7000 server and a GAT DC 7200 (see “2.3.5 TLS certificate configuration” for information on activating TLS/SSL on a GAT DC 7200).

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

i If you want to use a certificate self-signed by GAT ACE 7000, this window will open automatically after the corresponding TLS configuration (see previous chapter) when GAT ACE 7000 starts.

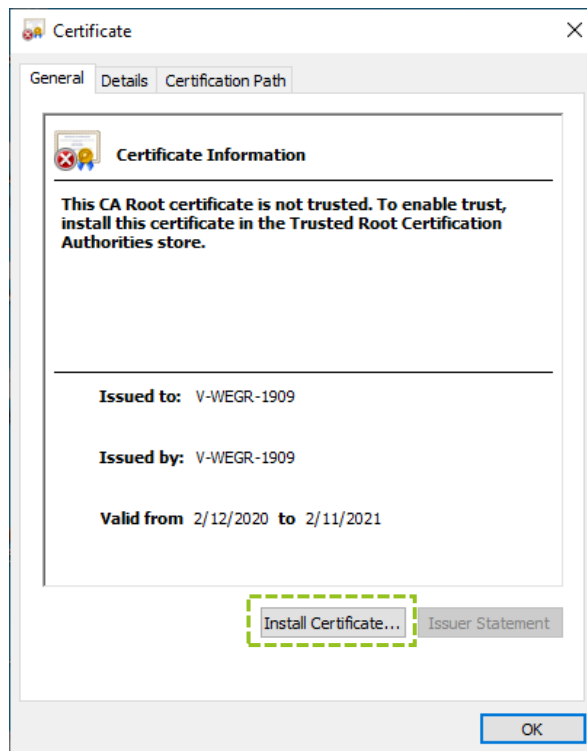


Figure 2.17 – “Certificate” window

- ▶ Click “Install Certificate”.
 - The “Certificate Import Assistant” opens.

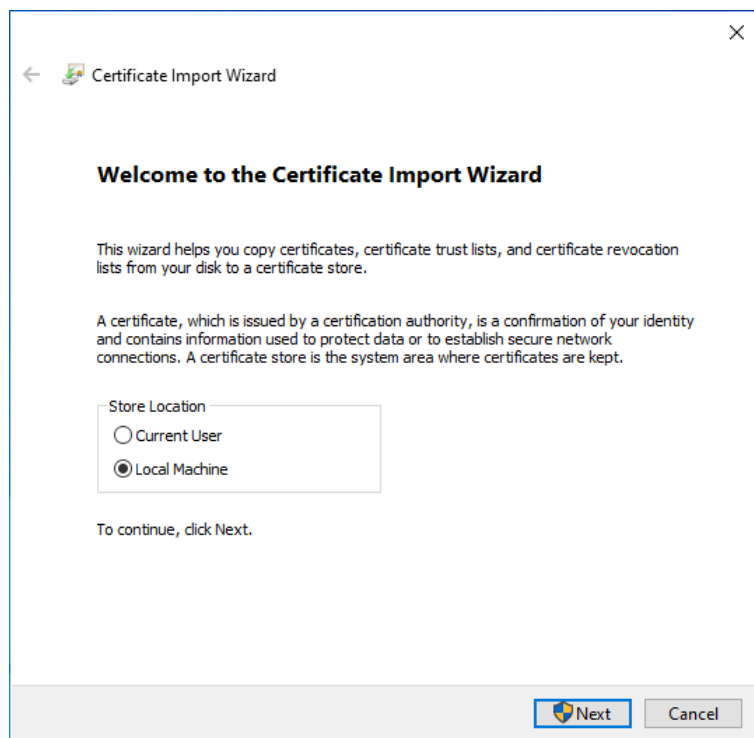


Figure 2.18 – “Certificate Import Assistant” – Step 1

- Select which Certificate Store (“Current User” or “Local Machine”) to use, and then click “Next”.

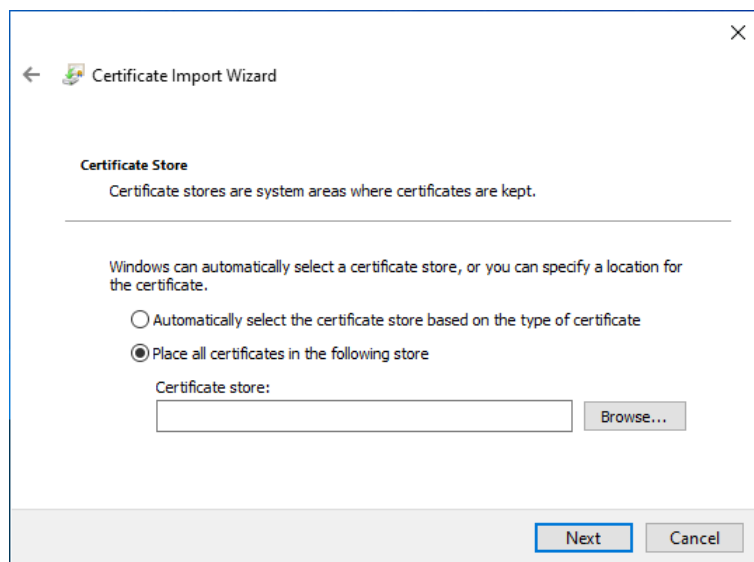


Figure 2.19 – “Certificate Import Assistant” – Step 2

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

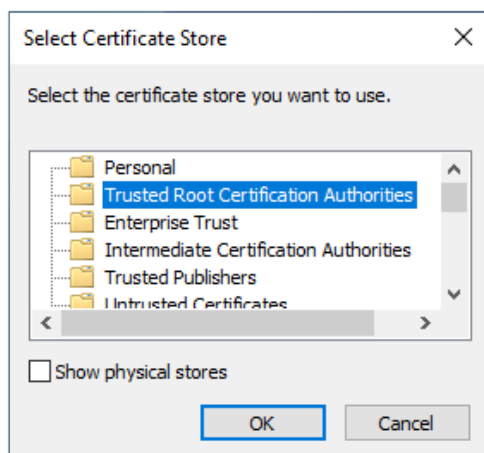


Figure 2.20 – “Certificate Import Assistant” – Step 3

- Finally, click on “Finish” and then accept the security warning in the following window by clicking on “Next”.

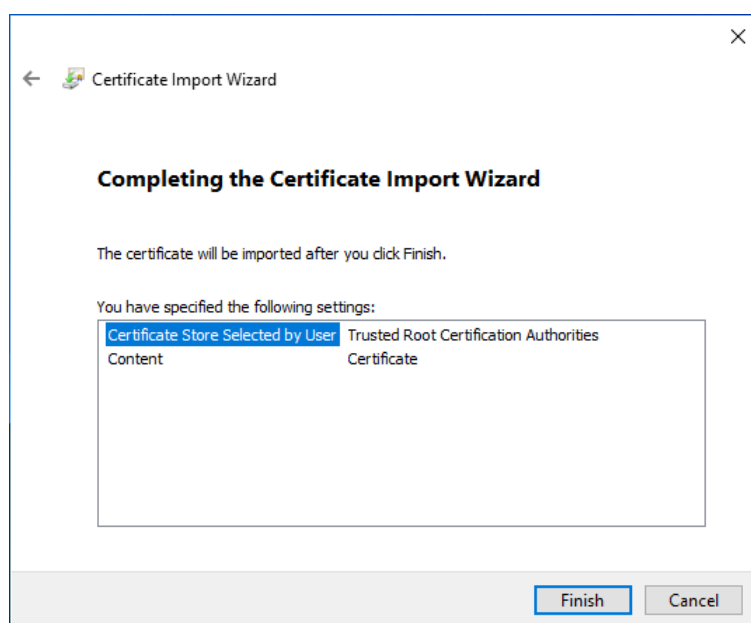


Figure 2.21 – “Certificate Import Assistant” – Step 4

2.4 Updating GAT ACE 7000

When a software update is available for GAT ACE 7000, you can manually install the update over the existing GAT ACE 7000 version without needing to delete the existing version first (depending on the type of update).

NOTE! After installing the update, ensure that the rights for GAT ACE 7000 users are configured correctly.

Once the update is complete, the same license that was used before the update can still be used. It is possible that new functions (e.g., the anti-passback function) are included with the update. These cannot be used with the existing licence and the appropriate extension licence must be purchased to activate their use.

Following the update, the database must also be updated as new database fields are added during the update. The existing data is not changed or deleted during the database update.

NOTE! It is recommended to always create a backup before updating the database. For more information about how to backup the SQL database, refer to chapter “5.5.1 SQL database backup”. Also refer to Microsoft’s documentation available via:

<https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server>

3 STARTING GAT ACE 7000 VIEWER

For the initial start-up of GAT ACE 7000 following installation, further configuration processes such as establishing the database connection must be completed. For each subsequent start-up of the application, you are directed to the login screen.

3.1 Start-up

- Start GAT ACE 7000 by selecting “GAT ACE 7000 Viewer” from the Windows Start menu.

NOTE! After installing GAT ACE 7000, a program entry for the application is installed in the Windows Start menu in the following location: Start -> All Programs -> GANTNER Electronic GmbH -> ACE 7000 Viewer.

- The GAT ACE 7000 start-up process begins.

During start-up, GAT ACE 7000 checks the connection to the GAT ACE 7000 service and database. If the service is not running or the connection is not configured correctly, a notification is displayed on the screen. A similar notification is also displayed if the database does not exist or a connection cannot be established.

3.1.1 GAT ACE 7000 Service

The GAT ACE 7000 service is a Windows service that runs in the background and manages the communication and data processing requirements between the database and the configured devices for one or several GAT ACE clients. The service must therefore always be operating in order to use GAT ACE 7000 Viewer. Upon start-up, GAT ACE 7000 checks the connection to the GAT ACE 7000 service. If the server with an installed service is found, but the service has not started yet, an error message is displayed where you can select to start the service. When the service is not running and cannot be found, the following window opens.



Figure 3.1 – Server configuration for the GAT ACE 7000 service

- If the GAT ACE service is installed on another server/PC, enter the address of the server and port number then click "Save".

NOTE! If the service is installed on the local PC where GAT ACE is operating, enter "localhost" in the "Remote Location" field then press "Save".

3.1.2 Creating a database

Once GAT ACE 7000 is installed, a database for GAT ACE 7000 must be created and a connection to the database established. GAT ACE 7000 recognizes automatically upon start-up if a connection to the database exists or if one must be configured first.

To create the database and configure the connection to the database, complete the following steps:

- The following window opens during start-up when the database connection settings are not configured correctly.

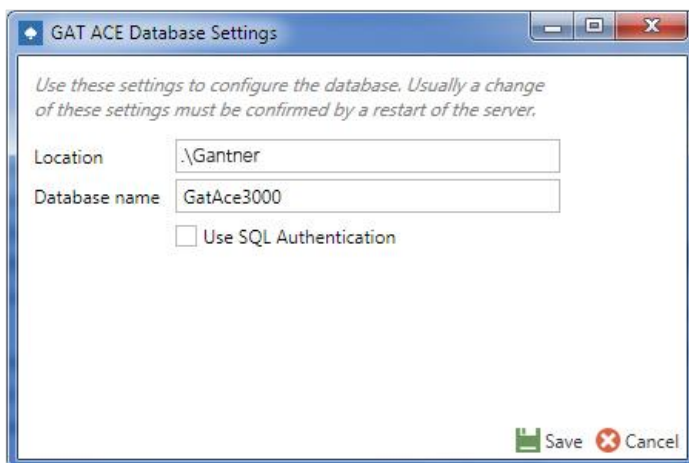


Figure 3.2 - Database connection settings

- In the "Location" field, enter the location of the database server. The server location indicates exactly where the database is installed. Enter the network name or IP address of the PC/server followed by the name of the SQL server instance. When the database is installed on the same PC as GAT ACE 7000, "." can be used for the network name. After a default installation with local database, the name ".\Gantner" is predefined.
- Enter the name of the database in the "Database name" field (Standard = "GatAce7000").
- The "Use SQL authentication" option allows you to select which login settings GAT ACE 7000 uses to log in to the database. It is possible to use the Windows authentication settings of the current user account or the SQL authentication with username and password. GANTNER recommends to using SQL authentication so select this option to do so.
 - When the option for SQL authentication is activated, enter a username and password into the respective fields to use for database login.
 - If this option is not activated, the Windows authentication is used.

NOTE! Be aware that a database can only be generated based on the default settings when an SQL Server instance named “SQLEXPRESS” is installed on the computer and configured for Windows authentication. This is the case when you install SQL Server Express together with GAT ACE 7000.

NOTE! The GAT ACE 7000 database settings can be accessed at any time in GAT ACE 7000 via the program settings (click on the  icon and select “Database Settings”).

- ▶ Save the configuration by clicking on “Save”.
 - GAT ACE 7000 restarts and attempts to connect to the database. As yet, a database bearing the configured name has not been created and you are asked whether the database should be created now.

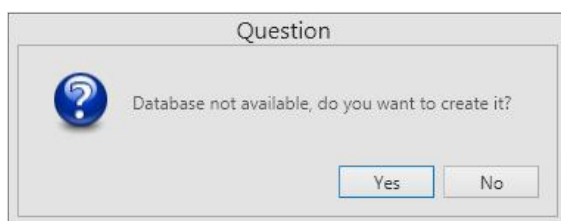


Figure 3.3 - Establishing a new database

- ▶ Click on “Yes” to create the database and continue.

3.1.3 Login window

After GAT ACE 7000 has successfully connected to the GAT ACE 7000 service and established the database connection, the login window appears after a brief pause. The user must enter their login details including username and password to gain access to the main application window of GAT ACE 7000.

NOTE! You can create different users with different privileges in GAT ACE 7000. See chapter “6 AUTHORIZATION MANAGEMENT” for more information.



Figure 3.4 - Login window for GAT ACE 7000 Viewer

- ▶ Enter your username in the “Username” field.
- ▶ Enter your password in the “Password” field. Ensure to enter your password in the correct case.
- ▶ Confirm your details then click on “Login”.
 - When valid login details are entered, the main screen of GAT ACE 7000 Viewer opens (see “5.1. Functional overview of GAT ACE 7000 Viewer”). Otherwise, you have the option of entering the username and password again.

NOTE! Change the default passwords immediately after installing GAT ACE 7000.

After installing GAT ACE 7000, the “SYSTEM” and “Administrator” users are preconfigured with default passwords. It is very important that you change the default passwords of these users to secure and secret new passwords and keep them saved in a secure place, protected against unauthorized use. See chapter “6 AUTORIZATION MANAGEMENT” for more information.

4 SOFTWARE SETTINGS

The basic functionality of GAT ACE 7000 is configured via the software settings. The settings are organized into three areas: the database settings, the application settings, and the role/user management settings. The software settings are described in the following chapters and can be accessed as follows.

- Click on the  icon above the main menu bar.

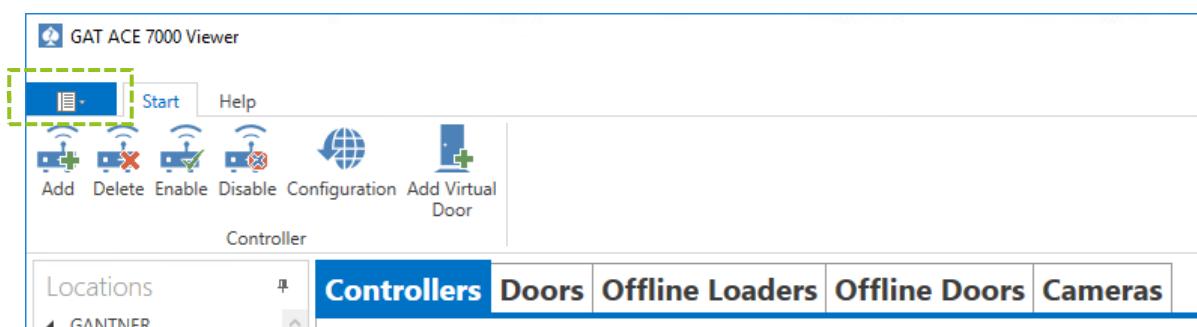


Figure 4.1 – Icon for accessing the software settings

- The software settings list is displayed.

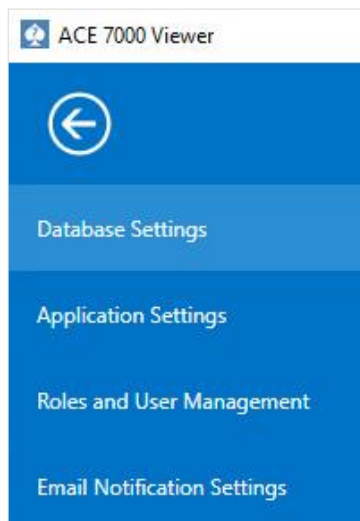


Figure 4.2 – Software settings list

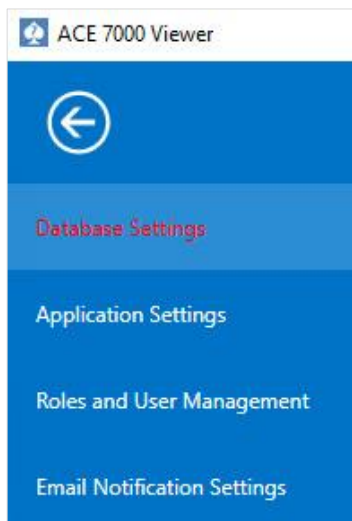


Figure 4.3 – Software settings area with unsaved changes

- Select the desired software settings from the list.
 - The settings are displayed to the right of the list.

NOTE! Changes made to the software settings must be saved using the “Save” button, which becomes available after a change has been made. Software settings with amended but unsaved settings are marked in red (see Figure 4.3).

4.1 Database settings

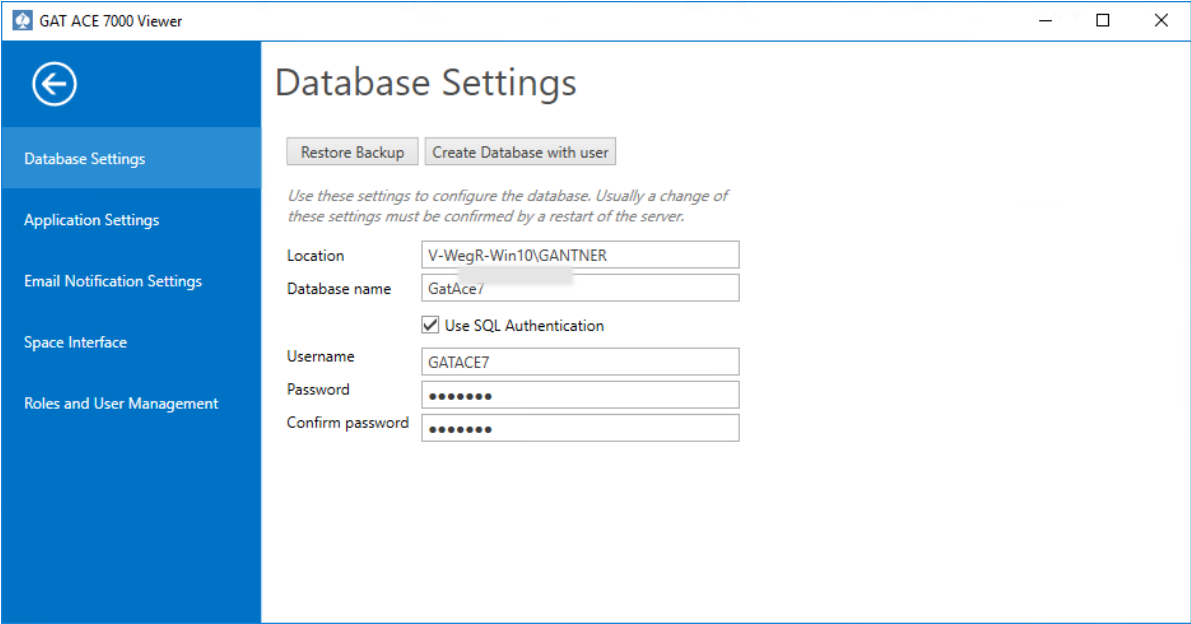


Figure 4.4 – Database Settings

On this settings page, the connection settings for the GAT ACE 7000 database are available.

- Restore Backup: Here you can restore a database backup file. Click on the “Restore Backup” button and locate the file via the “Open” window. Click on “Open” to restore the backup file. See chapter “5.5.1 SQL database backup” for information on how to schedule automatic database backups.
- Create Database with user: A new database can be created here. The following settings are displayed after clicking on the “Create Database with user” button:

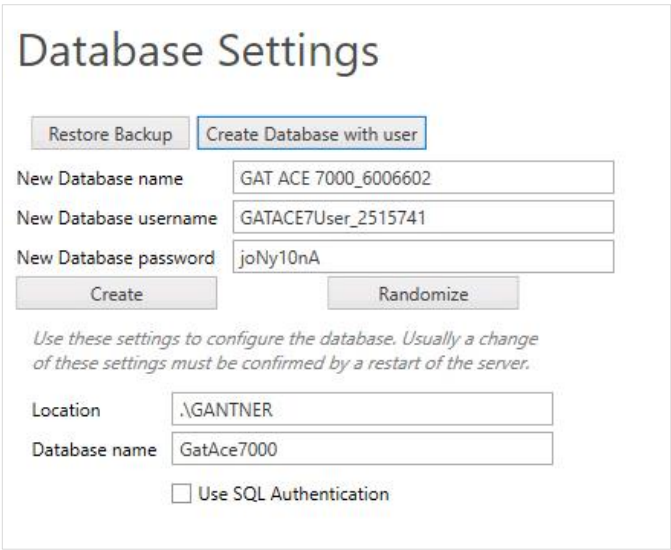


Figure 4.5 – Settings for creating a new database

To create a new database, enter the required information (name, username, and password) into the respective fields. Alternatively, you can use the default

- information as shown in the fields. Click on “Randomize” to change the default information if desired. Click on “Create” to save the new database settings.
- Location: Location (computer and database instance) where the GAT ACE 7000 database is installed. For local installations (GAT ACE 7000 Viewer and GAT ACE 7000 Service installed on the same PC), a "." can be entered for the location followed by the database name (e.g.: ".\Gantner").
 - Database name: The database name specified when creating the GAT ACE 7000 database.
 - Use SQL authentication: Select whether to use the user's Windows authentication or SQL authentication (username and password – SQL authentication recommended by GANTNER) to connect to the database.



A detailed description of the database settings is available in section “3.1.2 Creating a database”.

4.2 Application settings

Figure 4.6 - Application settings

In these settings, you can enable or disable the exchange of CardNET data with GAT SyncManager software and configure the cleaning settings for backups and bookings data. The following settings are available:

- GAT SyncManager CardNET Settings:

When "GAT SyncManager CardNET Enabled" is selected, authorization data is provided for offline controllers with CardNET functionality as well as for GAT SyncManager software.

If the function is active, enter the location of a folder to use for the exchange of offline data into the "GAT SyncManager CardNET Path" field.

NOTE! The folder must be accessible by GAT ACE 7000 and GAT SyncManager and the service, or the user under which the service is running, must have read/write authorization for these folders.

NOTE! Ensure that GAT ACE 7000 also has a booking file from GAT SyncManager named "accessbookings.exp". The name of the booking file can be freely selected in GAT SyncManager and must therefore be exactly defined.

- GAT ACE 3000 CardNET Settings:

When "GAT ACE 3000 CardNET Enabled" is selected, authorization data is provided for offline controllers with CardNET functionality as well as for GAT ACE 3000 software.

If the function is active, enter the location of a folder to use for the exchange of offline data into the "GAT ACE 3000 CardNET Path" field.

NOTE! The folder must be accessible by GAT ACE 7000 and GAT ACE 3000 and the service, or the user under which the service is running, must have read/write authorization for these folders.

NOTE! GAT ACE 3000 only supports CardNET G1.

- Remote Sync default configurations output path:

Path for generating the configuration file for remote sync (see "5.2.13. Remote sync transfer of offline data"). When no path is set here, a window is displayed where the user must select the directory to export the configuration file. When a path is entered, the configuration file is automatically saved in that directory.

- Remote Sync default information import path:

Enter the path where the import files for remote sync are stored (see "5.2.13. Remote sync transfer of offline data"). If this field is left empty when importing with remote sync, a window is displayed where the user must select the directory and file manually.

4.3 Email notification settings

Figure 4.7 - Settings for the automatic email notification function

With these settings you can set up automatic email notifications. GAT ACE 7000 offers the possibility to send an email to a specific recipient or group of recipients when certain events occur (e.g., alarms or connection interruptions). In the input fields, the settings of the email server that is used to send the messages are defined. The “Edit Email Notifications” button allows you to configure the messages and recipients. The following settings are available.

- | | |
|-------------------------------|---|
| - Enable email notifications: | For email notifications to be sent, this option must be checked. |
| - Email server: | Enter the address of the email server to be used as well as the send port into this field. |
| - Use SSL: | Select this option if you want to send notifications using SSL encryption. |
| - Sender: | Enter the email address that will be displayed as the sender address. |
| - Use default credentials: | If this option is selected, the Smtplib client will try to use the default system credentials to authenticate the mail server. Most mail servers require the Smtplib client to authenticate itself before an email is sent from it. |

- Username / Password: If the default credentials are not used to authenticate the mail server, enter the desired username and password here.
- Recipients of test email: Here you can enter an email address for testing purposes and send a test email to the address by pressing the “Test Email Settings” button.
- Edit email notifications: This button opens the window for configuring the email notifications (see following section).

4.3.1 Editing automatic email notifications

The following window for configuring the email notifications opens after pressing the “Edit Email Notifications” button.

Figure 4.8 - Create and edit automatic email notifications

Shown in the left column are the previously defined email notifications.

- Click on “Add” to define a new email notification, or to edit an existing notification, select it in the list.
- Enter the data for the selected notification in the area to the right. The following settings are available.
 - Notification Name: Define a relevant name for the notification here.

- Recipients: Enter the email address to which the message will be sent. It is also possible to enter several addresses here, which are separated by a line break (see example).
 - Events: Via the five settings fields, select the events for which the notification email will be sent when the event occurs. You can select multiple options here to respond to multiple events with one notification.
- Save the changes by clicking on “Save”.

4.4 “Space interface” settings

Figure 4.9 - Software settings for connection to ProAccess SPACE software

In this setting page, the interface to the ProAccess SPACE software from SALTO can be activated. This interface is used by GAT ACE 7000 to query SVN data, send it to the controllers (e.g. GAT DC 7200) and write it to the data carriers there. SVN (Salto Virtual Network) is a mode to store and manage user authorizations on their data carriers for offline access readers from SALTO (comparable to CardNET from GANTNER).

- Use Space interface: Check this option if the interface is to be used.
- Server: Enter the computer name or IP address of the computer on which the SALTO ProAccess SPACE software is installed. Here "localhost" can be used if Space is installed on the same computer as GAT ACE 7000.
- Port: Port number for communication with ProAccess SPACE Synchronizer. Default = 8100.
- Transport Protocol: Select the transport protocol here (default = http).

- Authentication: Here you can select the type of login to SALTO ProAccess SPACE. Default is "Basic". After selecting the authentication method, enter the other authentication data. If "Basic" is selected, the user name and password must be entered. With "Custom", the so-called "Ship Key" can be used.
NOTE: These settings must match the settings configured in the GAT Matrix (In GAT Matrix in the "Settings" -> "ProAccess Space Synchronizer" menu).
- The "Test Space Connection" button is used to perform a connection test to the ProAccess SPACE. If the connection works, the message "A connection to Salto Space could be established successfully" is displayed.

4.5 Roles and user management settings

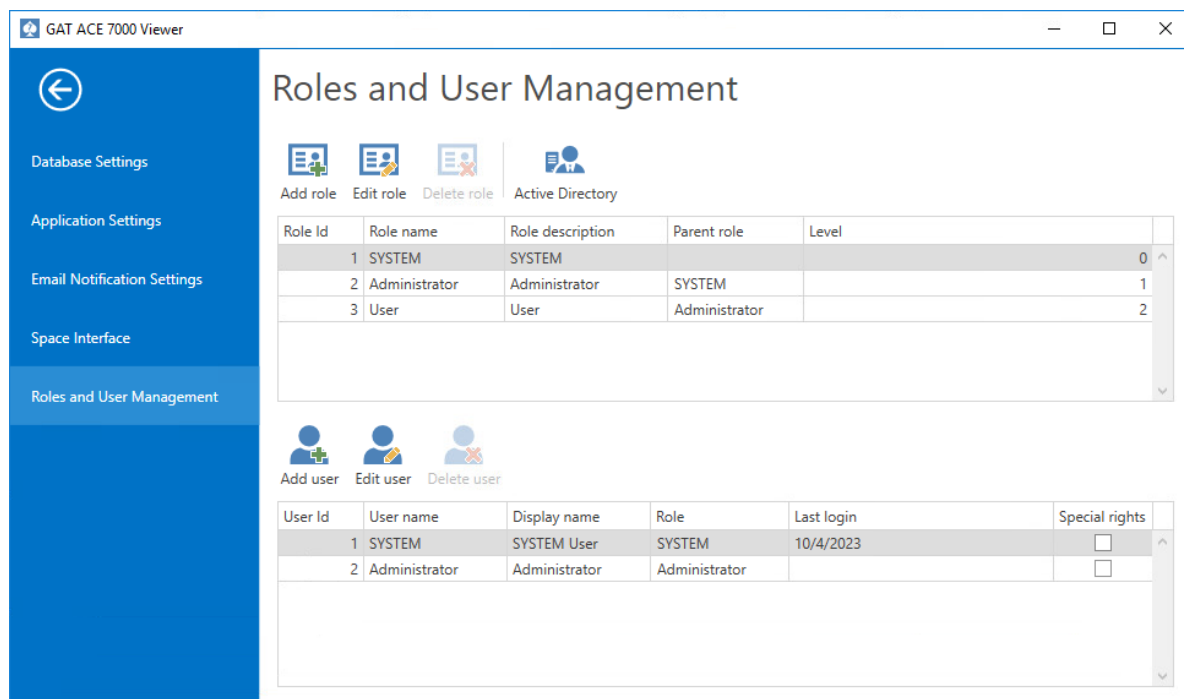


Figure 4.10 - Roles and user management settings

In order to work with GAT ACE 7000 Viewer, the user is required for security reasons to log in with a username and password. The user system has a hierarchical structure that allows each user to be assigned different permissions (rights). The user's rights in the system are defined by assigning roles, which are configured and saved in GAT ACE 7000.

On this settings page, the roles and users are created, and roles assigned to users. The roles and user management system is described in detail in chapter "6 AUTHORIZATION MANAGEMENT".

5 OPERATION

This chapter provides a functional overview and detailed description of the operation of GAT ACE 7000 Viewer.

5.1 Functional overview of GAT ACE 7000 Viewer

This section provides an overview of the main functions of GAT ACE 7000 Viewer.

After starting GAT ACE 7000 Viewer, the user is required to log in with a valid username and password (see “3.1.3. Login window”). GAT ACE 7000 is delivered with default users with specific passwords and user roles pre-defined (see “6.3.2. Default User”). The role assigned to a user determines the functions they can access and perform in GAT ACE 7000. This chapter describes the operation for the SYSTEM user who has access to all available software functions.

After successfully logging in using the SYSTEM username and password, the main screen of GAT ACE 7000 Viewer is displayed. The main screen is divided into the following areas.

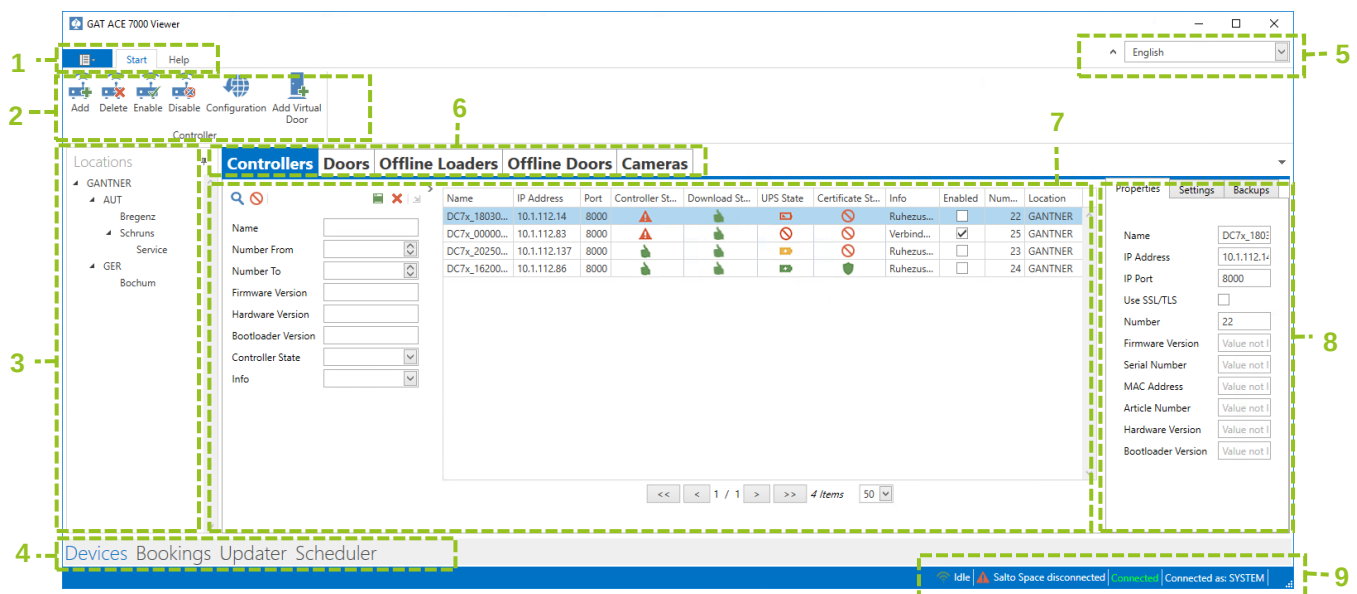


Figure 5.1 - GAT ACE 7000 Viewer – Main screen

- 1 Main menu: Available for selection in the main menu are:
 - The software settings via the icon (see “4 SOFTWARE SETTINGS”).
 - The main features of GAT ACE 7000 Viewer via “Start”.
 - Help functions including a diagnostics tool and the user manual via “Help”.
- 2 Taskbar: Available here are icons used for performing common tasks in the currently selected view (see item 6). The icons vary according to the currently selected view tab.
- 3 Locations: In this area you can organize the structure of controllers in a larger system and assign the controllers to different locations. This is particularly useful for offline controllers to transfer separate offline data, and for the selective handling of CardNET data.
- 4 Areas: These buttons allow you to switch between the “Devices” area, where controllers and doors are assigned, the “Bookings” area, where all activity recorded in the system is displayed, the “Updater” area, where the controller/reader software is updated, and the “Scheduler” area, where reoccurring system tasks are scheduled.

- 5 Language: Select between English and German for the language used to display GAT ACE 7000 Viewer.
- 6 View tabs: The view tabs are used to select a view for configuring controllers, online and offline doors, offline managers, and cameras for license plate recognition.
- 7 View: This is the main workspace in GAT ACE 7000 Viewer and used for configuring the system. Different information is displayed here depending on the selected view tab.
- 8 Information display: Detailed information for the currently selected view is displayed in this area. You can also copy the settings of a controller to other controllers or backup the configuration of a controller here.

- 9 Status bar:



The status bar shows additional information including whether GAT ACE 7000 Viewer is connected to the GAT ACE 7000 service. Communication with devices/controllers is only possible when the green “Connected” text is displayed here. The current user is also displayed in the “Connected as” field (here “SYSTEM”). In addition, if the allocated data memory is 90% or more occupied, a warning message is displayed in the status bar. Depending on the SQL database settings, the database is automatically managed or augmented by SQL Server. If you have questions, contact your IT administrator.

The view tabs can be repositioned within the software window by clicking onto a desired tab and dragging it away from the current position. After removing the tab, a positional locator is displayed in the middle of the window that is used to relocate the view to one side or to reposition on the bar again as shown in the following figures.

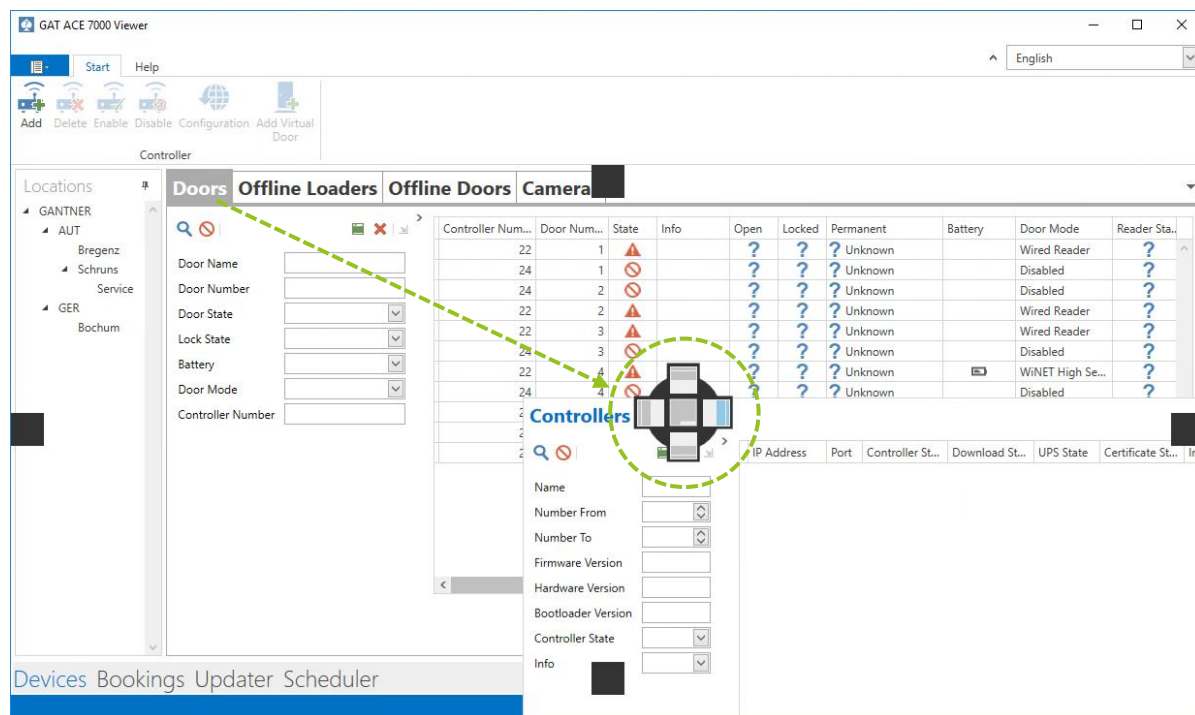


Figure 5.2 – Repositioning a view 1

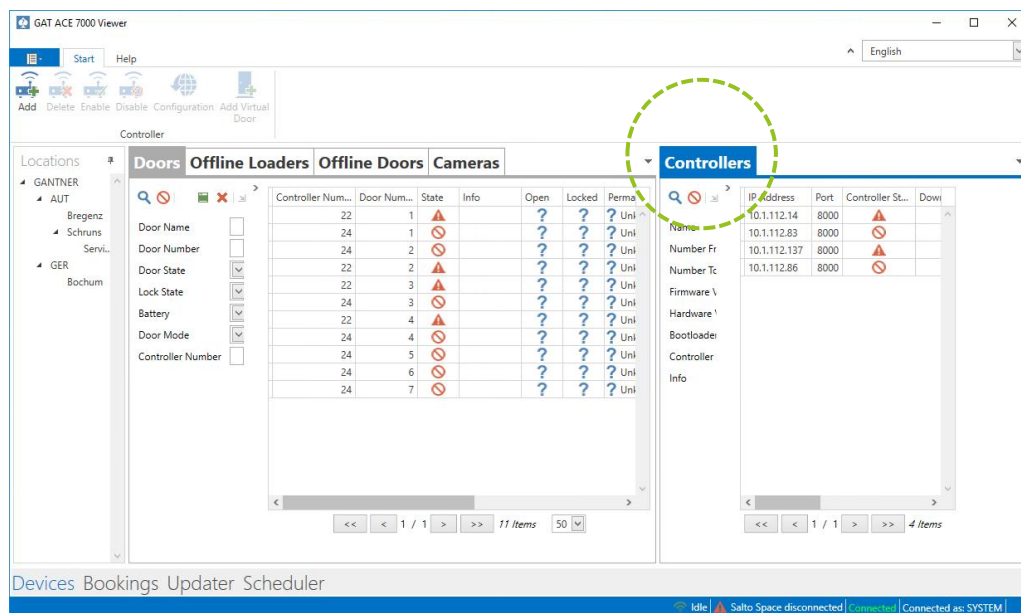


Figure 5.3 – Repositioning a view 2

5.2 Configuring an access system

This section describes the basic procedure for configuring an access control system with GAT ACE 7000 Viewer. Instructions are provided for the configuration process that must be performed normally once at each facility. Descriptions of further settings and functions can be found in the subsequent chapters.

5.2.1 Structuring locations

Structuring locations is not absolutely necessary to configure an access control system in GAT ACE 7000 Viewer. However, defining locations can be especially helpful for larger systems or different company sites to structure the controllers and access system clearly and logically. The locations are organized hierarchically.

For offline controllers, through the configuration of offline loaders and offline doors, it is possible to only transfer authorizations assigned to a location to a programming device, which greatly reduces the amount of data and loading time in larger systems and makes the update process easier to manage.

In addition, a value range for the CardNET comparison byte can be defined separately for each location. This can be used to ensure that the CardNET authorization data is always rewritten and not just extended when access is granted at a new location (with a different value range).

- ▶ In the locations list, select the desired location under which a new location is to be inserted.
- ▶ Click on “Add Child” in the taskbar.
 - A new location is added and highlighted for editing.
- ▶ Name the location.
- ▶ To delete a location, right-click onto the location and select “Delete” from the menu.

NOTE! A location with sub-locations assigned to it cannot be deleted.

NOTE! When a location with controllers assigned to it is deleted, the controllers are automatically assigned to the parent location.
- ▶ To rename a location, right-click onto the location and select “Rename” from the menu.
 - The name of the site is highlighted and ready for editing.
- ▶ To define the CardNET comparison byte range for a location (see info in text above), double-click on the desired location or right-click on the location and select “Edit” from the pop-up menu.
 - The “Location” window opens.

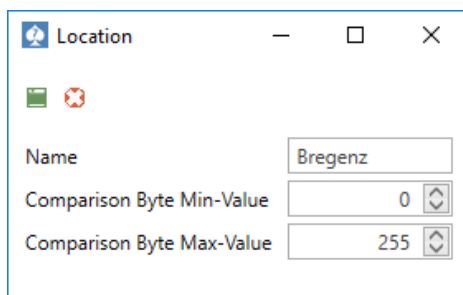


Figure 5.4 – Edit location window

- ▶ Enter the minimum and maximum values for the comparison byte range here. Ensure that the values for the desired location groups do not overlap.

5.2.2 Adding controllers

All access controllers in the system must be added to the controller list. GAT ACE 7000 only communicates with controllers that are defined in the controller list.

- In the “Devices” area, click on the “Controllers” tab.
 - The controllers view opens.
- In the location list, select the location where you want to insert a controller.

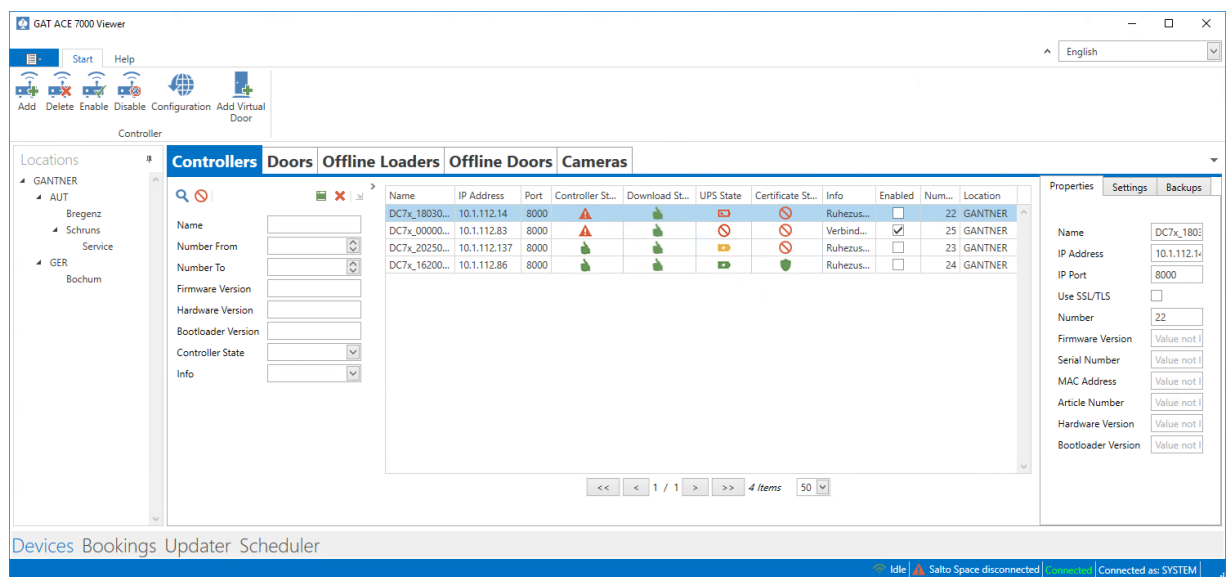


Figure 5.5 – “Controllers” view

- In the controller view, all defined controllers in the system for the selected location and any associated sub-locations are clearly listed. The most important data for each controller is also displayed.
 - In the “IP Address” and “Port” columns, the network address and port number (default = 8000) of the controller are displayed
 - In the “Controller State” column, the current status of each controller is displayed:
 - 🟢 The controller is connected to GAT ACE 7000 and communication is functioning.
 - 🔴 The controller is not connected to GAT ACE 7000.
 - ❓ The controller state is unknown.
 - 🚫 The controller is deactivated.
 - In the “Download” column, the communication status from GAT Matrix to the controllers is displayed:
 - 🟢 The previous changes in GAT Matrix have been successfully uploaded to the controller.
 - ❓ Connection to the controller is interrupted and the most recent data in GAT Matrix has not yet been uploaded to the controller. Attempts to upload the data are automatically performed every few minutes. If uploading is not possible for about 15 minutes, the following status is displayed.
 - 🔴 The previous configuration data has not yet been uploaded to the controller by GAT Matrix. You must upload the changes after re-establishing a connection to the controller.
 - 🔄 Data transmission to the controller was unsuccessful and GAT ACE 7000 retries every 2 minutes to load the data into the controller again.

- In the “UPS state” column, the battery status of an emergency power supply (UPS) is shown. The color indicates the charge status of the UPS battery (green = over 50%, orange = between 20% and 50%, red = under 20%). The type of symbol indicates whether the mains supply is active or whether the UPS is supplying power in the event of a mains failure:

 The mains supply is active. The UPS battery is being charged or not being used for supply.

 The mains supply has failed. The controller is supplied by the UPS battery.

 No UPS is being used.

- In the “Certificate State” column, the current status of the encrypted TLS communication is shown:

 The connection to the controller is encrypted and the certificate used is valid.

 The connection to the controller should be encrypted, but the certificate is invalid.

 An unencrypted connection with the controller is used.

- In the “Info” column, more information on the connection status is available.

- The “Enabled” column indicates whether the controller is enabled or disabled. A disabled controller does not communicate with GAT ACE 7000 and continues to operate autonomously. Booking data from access activity is stored locally in the controller and this information is not available for display and evaluation in GAT ACE 7000.

- o In the information display to the right of the main view, the “Settings” tab displays the main settings for the selected controller. You can edit the information here, however, not all information is editable.
- o The following controller tasks are available in the taskbar.



- Click on the “Add” icon to add a new controller to the list.
 - o A message is displayed to ask whether to search the network for controllers.
- Select “Yes” when the desired controller is connected via the TCP/IP network.
 - o The TCP/IP network is scanned, and all controllers found displayed in a new window.

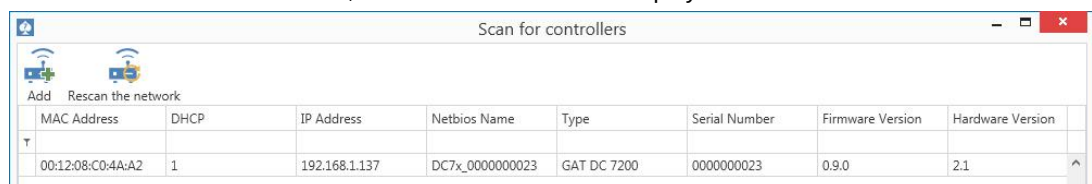
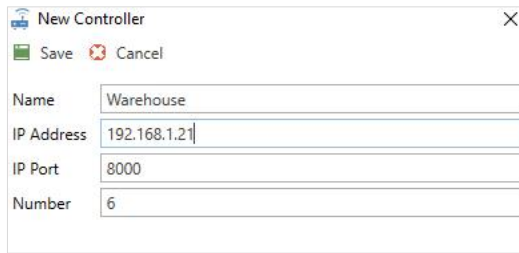


Figure 5.6 – Scanning the network for controllers

- Select the desired controller from the list.

 Controllers marked in green have already been added to the controller list of GAT ACE 7000. The controller's IP address is used for identification.

- Click on the “Add” button to add the controller to the controller list.
 - o You are returned to the controller list where the new controller was added.
- To add a new controller manually, select “No” in the network scan message.
 - o The “New” controller window opens.



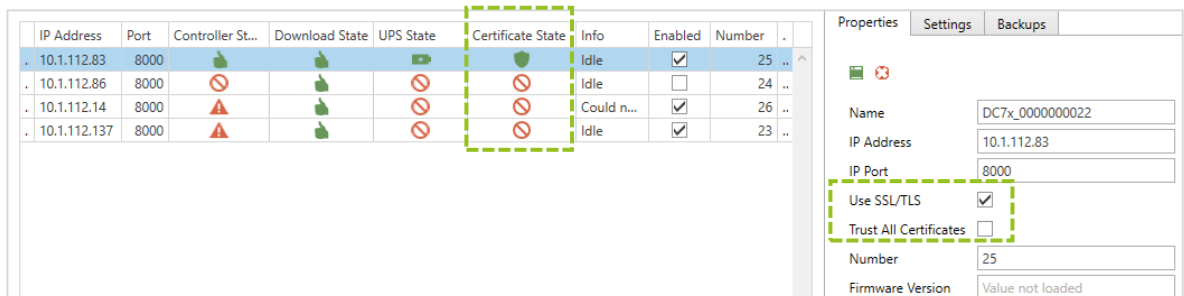
A dialog box titled "New Controller" with a close button (X) in the top right corner. It contains a "Save" button (green square) and a "Cancel" button (red X) at the top left. Below these are four input fields: "Name" with the text "Warehouse", "IP Address" with the text "192.168.1.21", "IP Port" with the text "8000", and "Number" with the text "6".

Figure 5.7 – Manually adding a new controller

- ▶ Enter the following information for the new controller.
 - Name: Name of the controller that will be displayed in GAT ACE 7000 Viewer.
 - IP address: Each controller in the system has a unique IP address by which it is identified. Enter the controller's IP address in the same format as shown in Figure 5.7.
 - IP Port: Enter the network port used for communication between the controller and GAT ACE 7000 Viewer. Default = 8000.
 - Number: Each controller and offline loader must have a unique number in GAT ACE 7000. The next available number is entered automatically into this field or you can manually enter a number. If the entered number is already in use, a corresponding message is displayed.
- ▶ Click on "Save" to confirm the information and add the new controller to the controller list.
 - You are returned to the controller list where the new controller was added.

NOTE! If you cannot find a controller or no controllers are displayed in the view, it is possible that you have chosen the wrong location in the locations list or a filter is set in the search fields that is excluding the controller.

- ▶ To delete a controller from GAT ACE 7000, right-click onto the controller and click on delete.
- ▶ To search for a specific controller, enter information into the search fields to the left of the controller list then click on the magnifying glass icon.
- ▶ To delete the entered search terms again, click on the red "X" icon.
- ▶ For larger systems where the controllers are displayed on multiple pages, use the scroll buttons beneath the controller list to navigate to the desired page and to define the number of items displayed per page.
- ▶ To enable encrypted TLS communication with a controller, select the controller in the list and check the "Use SSL/TLS" option in the settings to the right, and then click on "Save" .



The image shows a screenshot of the GAT ACE 7000 Viewer interface. On the left is a table listing controllers. On the right is a "Properties" dialog box for a selected controller.

IP Address	Port	Controller St...	Download State	UPS State	Certificate State	Info	Enabled	Number
10.1.112.83	8000					Idle	☒	25
10.1.112.86	8000					Idle	☐	24
10.1.112.14	8000					Could n...	☒	26
10.1.112.137	8000					Idle	☒	23

The "Properties" dialog box on the right has tabs for "Properties", "Settings", and "Backups". The "Settings" tab is active. It contains the following fields:

- Name: DC7x_0000000022
- IP Address: 10.1.112.83
- IP Port: 8000
- Use SSL/TLS: ☒ (This checkbox and the "Trust All Certificates" checkbox below it are highlighted with a green dashed box in the original image.)
- Trust All Certificates: ☐
- Number: 25
- Firmware Version: Value not loaded

Figure 5.8 – Controller properties - Use SSL/TLS

- If the GAT DC 7200 certificate is correctly installed in Windows (see “2.3.5 TLS certificate configuration”), a green shield symbol is displayed in the “Certificate State” column (see image).
- If the correct certificate for the GAT DC 7200 is not yet installed on the PC, a red shield symbol is displayed. You can install the certificate (see “2.3.6. Installing the TLS certificate”). After installation, the GAT DC 7200 must be deactivated once and re-activated to accept the certificate after which the shield symbol will change from red to green.
- ▶ If SSL/TLS communication is enabled in the GAT DC 7200 but the certificate is not installed on the PC, you can enable the “Trust All Certificates” option. The connection is then possible; however, this option is not recommended, and you should also always install the correct certificate for an SSL/TLS connection.

5.2.3 Configuring controllers

Complete the following steps to configure the settings of a controller.

- ▶ Select a controller in the controller list.
 - The connection settings, which are defined when adding a controller, can be viewed and edited in the information area to the right of the controller list under “Properties”.
- ▶ To modify the configuration of a controller, click on the “Configuration” icon.
 - GANTNER’s 7000 series controllers, e.g., the GAT DC 7200, are configured directly via a web server running on the controller. For this reason, your default web browser opens where the configuration settings can be accessed.



If the encrypted TLS communication is enabled but the computer certificate does not match the GAT DC 7200 certificate, an error message (“insecure connection”) is displayed in the web browser. It is possible to ignore this message and establish the connection anyway, but you should install the GAT DC 7200 certificate for a secure communication.

- For security reasons, the following window is displayed where you must enter your username and password in order to access the controller settings.



Figure 5.9 – Authentication for controller configuration

- ▶ Enter the username and password for the controller. The default login details for controllers are username = “admin” and password = “GAT”.
 - The configuration loads and is displayed in the web browser.

NOTE! Manipulation Danger! In order to prevent the unauthorized manipulation of the controller configuration, please change the default password of all controllers to secure passwords and keep them in a secure place protected from unauthorized access.

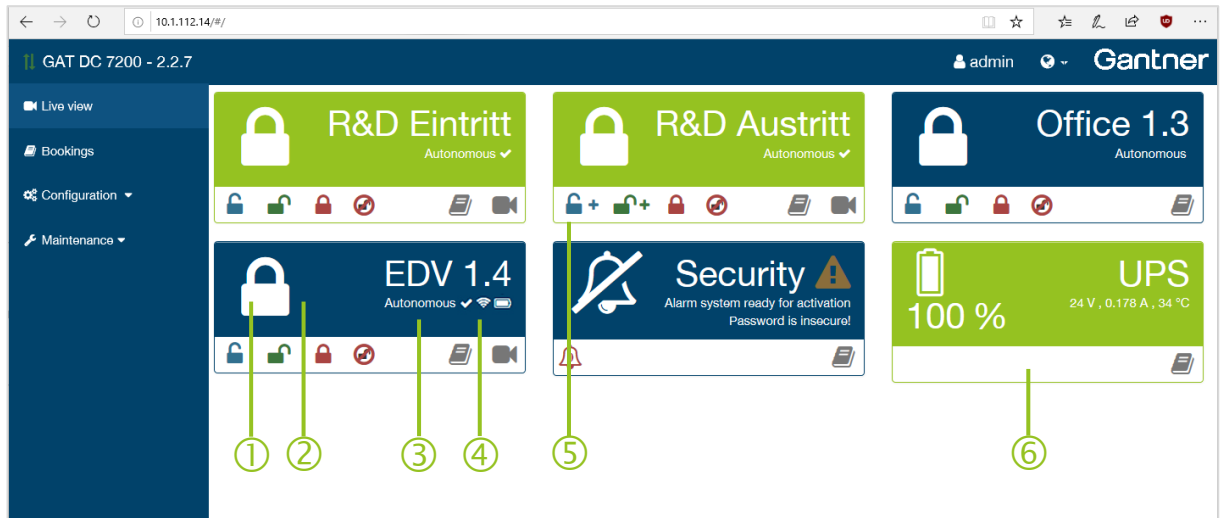


Figure 5.10 – Example configuration for a GAT DC 7200 controller – “Live view”

i The display and configuration options depend on the particular device, the device version, and the browser used. Therefore, your display may differ from the example shown here.

The main display of the “Live view” menu option shows the states (open, closed, alarm, etc.) of the doors connected to the controllers:

1 ... Symbol for the locking state:



= Door is locked.



= Door is unlocked and will be locked again after the set release time.



= Door is permanently unlocked.



= There is no locking state defined (e.g., WiNET).



= There is an alarm activated at the door.

2 ... Background color for the door contact state:

- Dark blue: Unknown (no door contact state defined)
- Light blue: Door is closed
- Green: Door is open
- Yellow: Warning
- Red: Alarm

3 ... Status information (current door state in plain text)

4 ... Symbols for the state of connected readers:

- No symbol: There is no reader connected
- Download symbol: The reader is being configured
- Tick symbol: The reader is ready
- Wireless symbol: Wireless connection to an offline lock (e.g., GDL7m) is active
- Battery symbol: Displays the battery status of a battery-powered offline lock
- X: Error

5 ... Symbols for door control:



.....Manually unlock the door for the set release time.



.....Unlock the door and set to “general open” function.



.....Permanently lock the door.

-  Set the door to autonomous operation. The access decision for users is made by the controller autonomously based on the stored authorization data.
-  Acknowledge and delete an active alarm. First determine the cause of the alarm and remove it.
-  Display the bookings for the door.
-  Display video of the door (if a surveillance camera is used).

6 ... Status of the UPS emergency power supply (if used).

► The configuration options for the controller are available in the left menu:

- Bookings: Displayed here is the controller booking data including locking/unlocking activity, alarms, configuration changes, etc.
- Configuration: The configuration of the controller can be performed via the sub-menu items of this option.
 - Doors: Configuration of the individual doors connected to the controller. This includes the door mode (normal or WiNET), entry/exit direction, fingerprint verification, unlocking and opening times, and the function of the relay outputs and optocoupler inputs.
 - Readers: Configuration of the readers connected to the controller. These include the RFID standards, corporate ID, information about the data carrier structure, and the WiNET / CardNET / Wiegand settings.
 - Extensions: Here you can find information about the extensions at the GAT DC 7200. This includes Relay Expanders, surveillance cameras and settings for the access control software with Anti-Pass-Back assignments.
 - Alarm system: Settings for the alarm system, e.g., the duress PIN code.
 - Database: In this menu item you can set the memory allocations, anonymize access bookings or backup or playback the data/bookings stored on the SD card of the controller.
 - Power over RS485: Settings for the voltage outputs to the reader interface.
 - Security and user: Security settings such as the encryption used and IP address filtering for FTP. In addition, the login password for configuring the controllers can also be changed here.
 - Ethernet: Settings for the Ethernet interface.
 - Date and time: Settings for time synchronization, automatic switching for daylight saving time, etc.
- Maintenance: Available here are the service and maintenance functions.
 - Maintenance: Display of the storage space used and the controller status. Here you can reboot the controller, reset the controller to factory settings, and save or import backups.
 - Inputs/Outputs: Here you can see the current state of the digital relay outputs and optocoupler inputs as well as the associated reader.
 - Update controller: Here you can upload a software update to the controller.
 - Update sub devices: Here you can upload a software update to the reader attached to the controller.
 - License: The MAC address and the number of licensed doors for the controller are displayed here. You can also upload an expansion license to the controller if available.



The available configuration settings depend on the respective controller. Please read the user manual of the controller for exact configuration instructions.

5.2.4 Copying the configuration of a controller

To copy the configuration of a controller (total or partial) and upload the configuration to one or more other controllers, you can use the copy function of GAT ACE 7000 Viewer as follows. GAT ACE 7000 Viewer includes this function so that you do not have to configure each controller individually.

- ▶ Select the controller with the configuration that you want to copy in the controller list of GAT ACE 7000 Viewer.
- ▶ Switch to “Settings” in the information display to the right.
- ▶ Select the settings that you want to copy from the “Settings to paste” list.

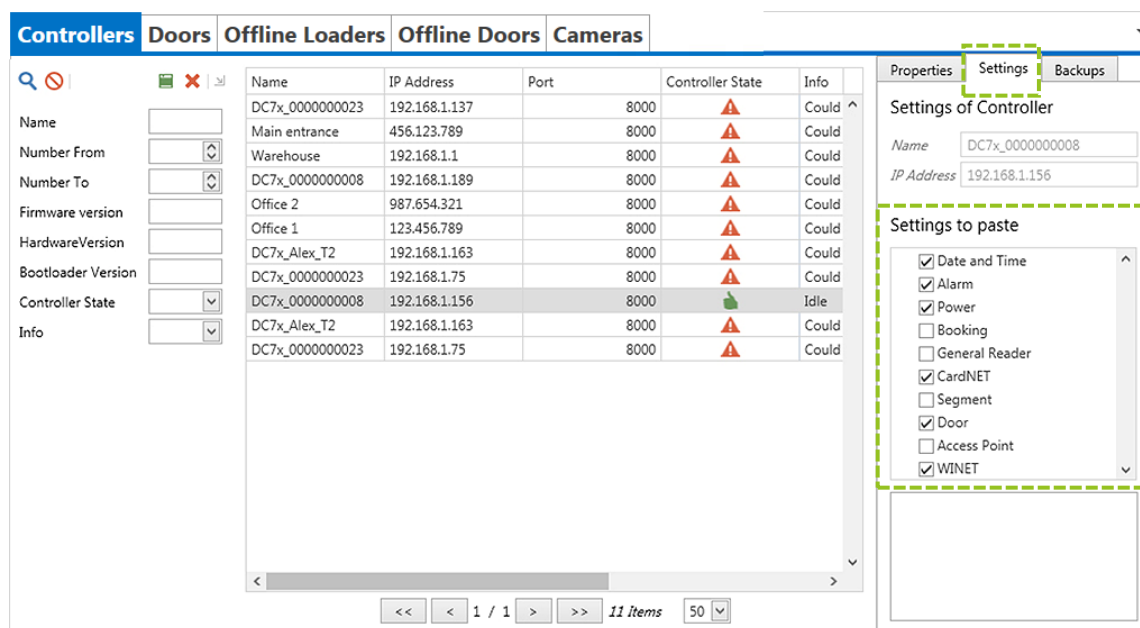
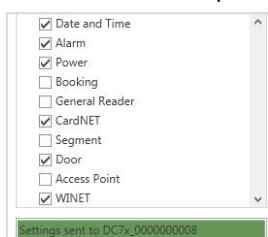


Figure 5.11 – Controller with settings selected for copying

- In the example shown for the “DC7x0000000008” controller, the “Date and Time”, “Alarm”, “Power”, “CardNET”, “Door”, and “WiNET” settings are marked for copying.
- ▶ Now select one or more controllers to which the selected settings are to be copied.
 - The copied settings, and the controller from which the settings were copied, are displayed in the information display.



- ▶ Click on the **Paste** icon in the taskbar.
 - The settings in the clipboard are copied to the selected controller. When the copy process is successful, a corresponding message is displayed in the information area.



5.2.5 Backup and restore a controller configuration

Before each update or change to a controller's configuration, a backup of the current configuration is performed by GAT ACE 7000, which allows you to restore a controller to a previous configuration.

- ▶ Select the controller that you want to restore.
- ▶ Click on the "Backups" tab in the information area.
 - All backups created for the controller are listed here.

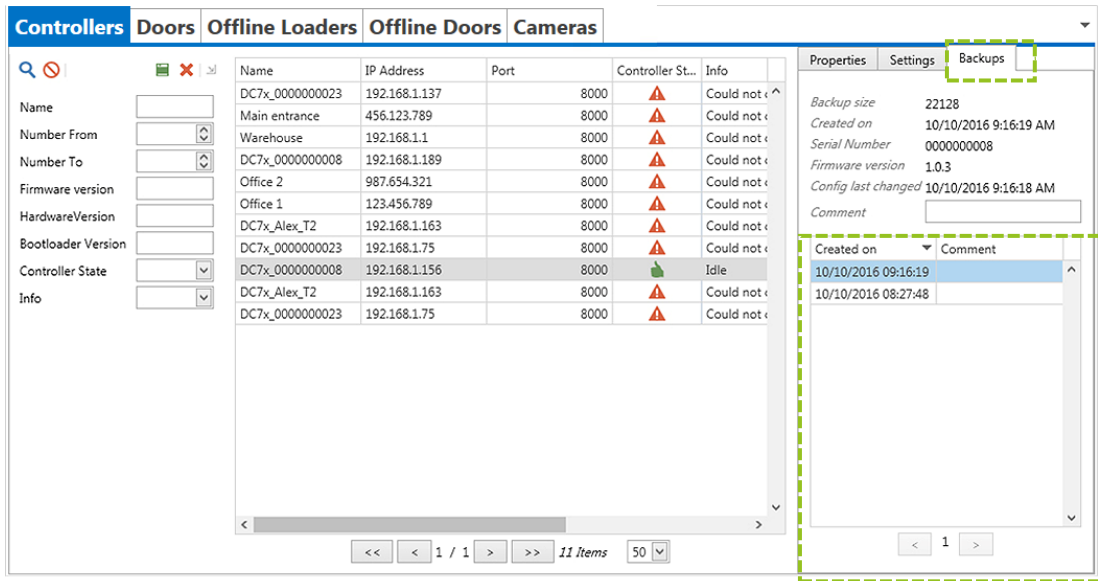


Figure 5.12 – Restoring the configuration of a controller

- ▶ For a better overview, you can enter a descriptive text for each backup by selecting the backup, entering the text in the "Comment" field, and then clicking on the "Save" icon.

NOTE! Bookings with comments are never deleted by the automatic cleanup function. See chapter "5.5 Scheduler" for more information.

- ▶ To restore a backup to the selected controller, select the backup configuration in the list.



- ▶ Click on the  icon in the taskbar.

- The settings of the selected backup are uploaded to the controller. A corresponding message is displayed when the upload is successful.



- ▶ You can also delete a backup by selecting it and clicking on the  icon in the taskbar.

5.2.6 Updating controllers and readers

To update the firmware of a controller or the readers connected to a controller, complete the following steps:

- Right-click onto a controller and select “Update Firmware” to update the controller or select “Update Reader” to update the readers connected to the controller.

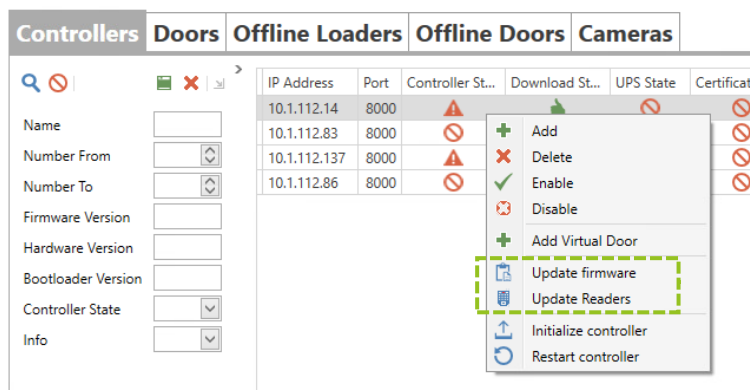


Figure 5.13 – “Update firmware” and “Update readers” options

- A window opens for selecting the ZIP or ENC file that contains the new firmware.
- Select the file with the new firmware and click on “Open”.
 - The firmware is uploaded to the controller or readers.

i The controllers and readers can also be updated in the “Updater” workspace. There you can also update each reader individually. See “5.4 Updating online controllers and readers”.

5.2.7 Initializing a controller

The “Initialize controller” function reloads all access authorization data from the GAT ACE 7000 database to the selected controller(s). This function is mainly intended for error analysis.

- Select a controller or multiple controllers in the list and right-click to open the options menu.
- Select “Initialize controller” from the menu and then click “Yes” in the confirmation window.

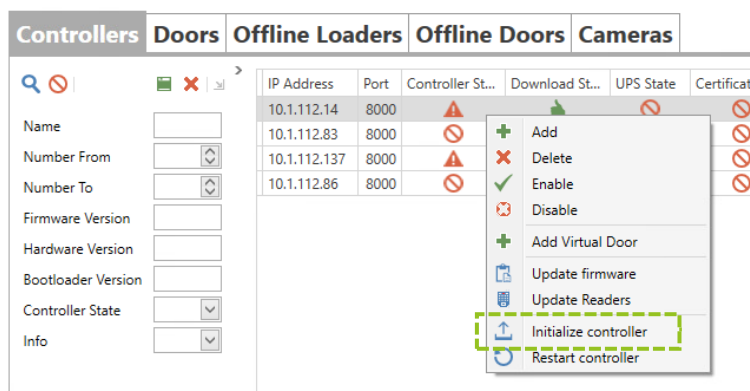


Figure 5.14 – “Initialize controller” option

5.2.8 Restarting a controller

A controller can be restarted via GAT ACE 7000. This process restarts the operating system, which can help with configuration problems.

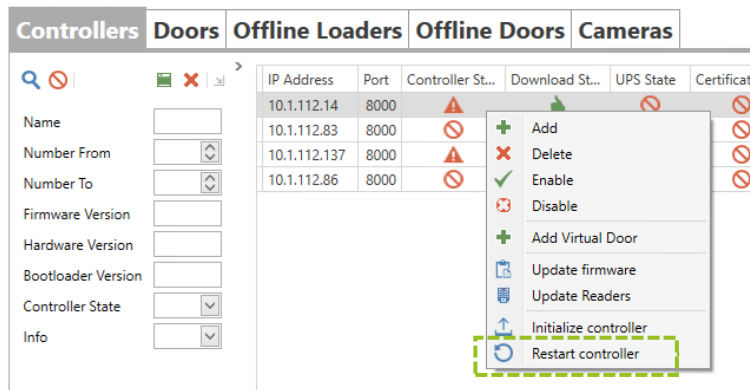


Figure 5.15 – “Restart controller” option

- ▶ Right-click on the controller and select “Restart controller” from the menu.
- ▶ Wait until the controller restarts, which can take up to one minute.

5.2.9 Assigning virtual doors to controllers

In access systems with many controllers and doors, the authorizations are often first defined in the access control software (e.g., GAT Matrix) and then the hardware is installed and put into operation. To assist with this process, the system can be pre-configured in GAT ACE using virtual doors, which are then assigned to the controllers created manually with the planned IP addresses. Now the authorization rights can be assigned to the doors in GAT Matrix. Following installation and commissioning of the hardware, the controllers are online, and the virtual doors are automatically replaced by the actual doors and readers connected to the controllers. The authorizations in GAT Matrix do not need to be changed.

i The cabling must be connected to the controllers and doors according to the preconfigured virtual doors so that the automatic updating is completed correctly.

- ▶ To insert a virtual door, click on “Controller” in the Views tab.
- ▶ In the location list, select the location with the desired controller.
- ▶ Select the controller and click on the “Add virtual door” icon in the toolbar. The same function is also provided in the sub-menu of the controller (right-click mouse).
 - The following window opens.

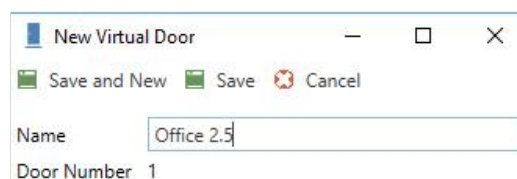


Figure 5.16 – Adding a virtual door

- Enter a name for the door. This name is displayed in the access control software (e.g., GAT Matrix).
- The door number is displayed automatically. Depending on the type, a controller can control several doors. With this door number, the virtual door is replaced by the respective actual door (or reader) after the controller is connected and put into operation.

5.2.10 Status display for online doors

A controller can monitor and control multiple doors. For each door, one or more readers are installed for reading user data carriers (e.g., one reader for entry and one reader for exit). The maximum number of doors that can be controlled depends on the controller type and the controller license used.

GAT ACE 7000 only displays those doors that have been assigned to controllers. Doors are configured and assigned to controllers via the controller configuration interface (see “5.2.3. Configuring controller”). All the door settings, such as the unlocking times, the relay output and optocoupler input settings, and other settings that determine the access functionality, are available here for each door.

i In GAT ACE 7000 and in the controller configuration, the difference between the terms “reader” and “door” must be clarified. Reader refers to the physical reading device installed near the door while door refers to the object being controlled (door, turnstile, gate, etc.). For example, four readers can connect to one controller. Depending on how the readers are installed, the controller can then control one door (all four readers are installed at this door) or - depending on the licence - up to sixteen doors (one reader per door).

- Click on the “Doors” view tab.
- From the list to the left, select the location for which you want to display the doors.
 - All defined doors for the selected location and its sub-locations are displayed.

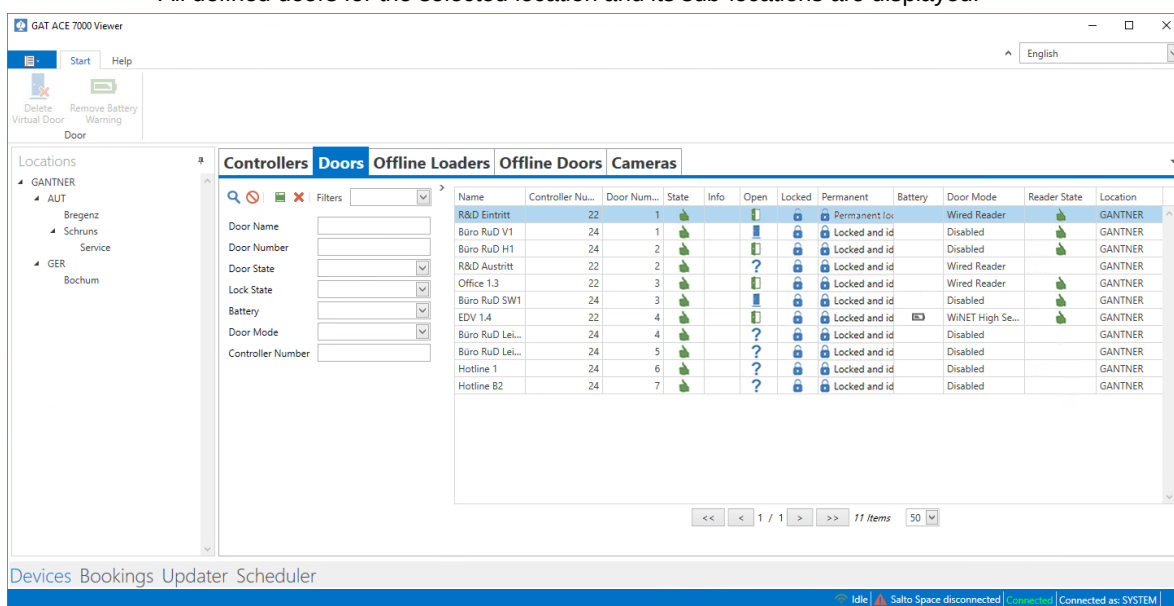


Figure 5.17 – Doors list

GAT ACE 7000 displays the following door information:

- Name: The name of the door. This is defined in the controller configuration interface.
- Controller Number: The number of the controller. Each controller in a system has a unique number. You can sort the list by the controller number and sort the readers according to their controller assignment.
- Door Number: Each door per controller is numbered. The door numbers are displayed in this column.
- State: Displays the current state of communication with the controller or door.
 -  = Communication with the door is functioning
 -  = Communication with the door is interrupted
 -  = Communication state is not known
 -  = The controller that controls the door is deactivated
- Info: This column shows additional information, if it was entered at the doors (in the controller configuration).
- Open: Displays the current opening state of the door. This function can only be displayed correctly with a connected and configured door feedback device.
 -  = Door is closed
 -  = Door is open
 -  = Door state is not known
- Locked: Displays the current locking state of the relay, which is used for door locking control.
 -  = The locking relay is set to "lock door"
 -  = The locking relay is set to "unlock door"
 -  = State of the locking relay is not known
- Permanent: Displays the "general open" state of the relay, which is used for door locking control.
 -  = The locking relay is set to "lock door"
 -  = The locking relay is set to "unlock door"
 -  = State of the locking relay is not known
- Battery: The offline controller battery status for offline doors is displayed here. The information shown is the status for when the controller was last read.
- Door mode: The mode in which the door operates is displayed here. "Wired reader" means that the reader is connected to the controller by cable. "WiNET Hight Security" is an example of a reader that operates via radio frequency using WiNET system.
- Reader status: This symbol indicates the status of the door reader.
 -  = The communication with the reader is OK
 -  = Not all update data has been transferred to the reader yet
 -  = Communication interruption with the reader
 -  = Communication status to the reader not known
- Location: The location to which the door is assigned. For more information on the locations, see "5.2.1. Structuring locations".

5.2.11 Configuring offline loaders and offline doors

Offline doors are not permanently connected to GAT ACE 7000 or the server and are supplied configuration data via a programming device. To configure offline doors, one or more programming devices ("offline loaders") are created in GAT ACE 7000 and assigned to the corresponding offline device. The following table provides an overview of the different types of offline loaders available in GAT ACE 7000 and the devices they support.

Offline loader type	Supported devices
GAT DL 092 USB wireless adapter	<u>Offline controllers</u> GAT DL 32x GAT DL 34x GAT DL 350 GAT DL 360 GAT DL 370
GAT MT 010 programming device	<u>Offline controllers</u> GAT ST 210 GAT ST 22x TAC
GAT DL 73xx	GAT DL 73xx access reader
GAT ECO.Side Lock	Electronic locker locks GAT ECO.Side Lock 7xxx CardNET, GAT ECO.Lock 7xxx CardNET, GL7p.xxxx CardNET

Table 5.1 – Types of offline loaders

These offline loaders connect to the USB port of the PC/server to allow the transfer of configuration data the respective programming device to the offline controller and transfer the bookings / status messages from the offline controllers via the programming devices to the PC. The transmission between the GAT DL 092 and the offline controllers occurs wirelessly via radio frequency. The connection between the GAT MT 010 and the offline controllers occurs via cabling. The GAT DL 73xx and GAT Locker Locks devices are directly connected via USB to the PC.

Note the following memory limits for the GAT DL 092:

Data	Max. number
GAT DL 3xx configurations	124
GAT DL 3xx configurations with max. configuration size	23
GAT DL 3xx bookings	47,000
GAT DL 3xx number of people	128
Configuration results	200
Firmware update results	1000
Information on device iteration	1000
Address list entries	4095
Max. GAT DL 370 firmware file size	409,600 bytes
Max. GAT DL 3xx configuration file size	45,056 bytes

Table 5.2 – Memory limits of the GAT DL 092

An offline loader is used to group several offline doors, which use the same operating mode and are arranged in the same building or access area, i.e., at the same location. By dividing a system into several offline loaders, the loading of the doors can be optimized so that only the data of those offline controllers, which are actually loaded by the relevant device, must be transferred to each offline loader.

Another possibility is to use different locations and assign the offline doors to the respective locations. Divide the sites so that each location contains only so many controllers that can be transferred to a programming device in a single step, e.g., one site per building or one site per level for larger systems. Each site can be synchronized individually.

- Click on the “Offline Loaders” tab.
- Select the desired location from the location list to the left of the application window.
 - All previously defined loading groups for the selected location and its sub locations are listed. The most important information is displayed for each loading group in the workspace to the right.

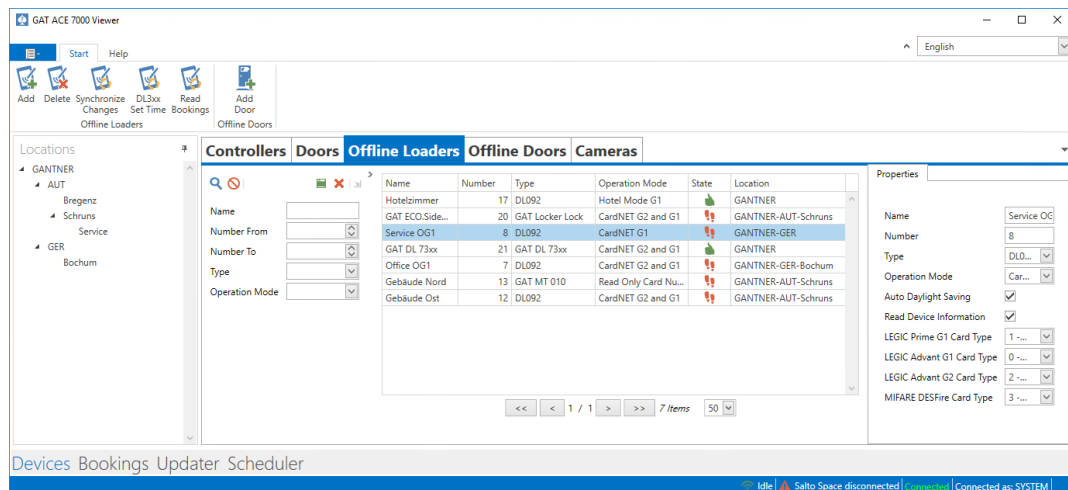


Figure 5.18 – Defining the offline loaders

- Shown in the “Location” column is the location where each offline loader is assigned. This name is also used for the synchronization file of the GAT SyncManager CardNET data.
 - In the “State” column, you can see whether one or more doors of an offline loader have configuration changes that have not yet been loaded into the door(s). In this case, a colored footprint symbol is displayed. The color depends on the type of changes. If there are several changes, the symbol with the highest priority is displayed (see section “Display of offline doors” below). If the symbol is displayed here, all door data for this offline loader are up to date.
- When you click on the workspace, the following functions become available in the taskbar.



These icons allow you to add or delete an offline loader as well as add doors to an offline loader. The three symbols for synchronization, time setting, and reading bookings are used to communicate with the offline doors (see section “5.2.12 Synchronizing offline loaders and offline doors”).

- You can edit the settings of an existing loading group via the “Properties” tab in the information window to the right of the workspace. These settings are described on the following page.

Creating an offline loader

- Click on the “Add” icon to create a new offline loader.
 - The “Offline Loader” window opens.

Figure 5.19 – Defining an offline loader – Basic Info

- ▶ Enter a name for the offline loader into the “Name” field.
- ▶ Enter the offline loader number into the “Number” field. A unique number must be assigned to each offline loader and online controller. By default, the next available number in GAT ACE 7000 is entered automatically.
- ▶ Select the type of offline loader from the “Type” menu (GAT DL 092, GAT MT 010, GAT DL73xx or GAT Locker Lock). A description of each offline loader type is provided at the start of this chapter.
- ▶ Select an operating mode for the offline loader from the “Operation Mode” menu. The following modes are available:
 - Read Only UID: The user authorization data is stored in the offline controller. The data carrier UID is used as the card number.
 - Read Only Card Number G1 and G2: The user authorization data is stored in the offline controller. The encoded card number of the data carrier is used as the card number. Depending on the operating mode selected, only CardNET G1 data carriers or both G1 and G2 data carriers are evaluated.
 - CardNET G1 (and G2): The user authorization data is stored on the employee ID cards. Depending on the operating mode selected, only CardNET G1 data carriers or both G1 and G2 data carriers can be used. Please note that the readers must also be authorized to write DESFire data carriers with CardNET G2 (as with LEGIC systems).
 - Hotel Mode G1: Authorization data for guests and staff is stored on the ID cards. This operating mode is only possible with CardNET G1 data carriers.
- ▶ If the “Auto Daylight Saving” option is selected, the offline controllers automatically switch between standard time and daylight-saving time. If this option is not selected, time changes due to daylight saving are not completed automatically and this must be considered when managing authorizations and reviewing bookings.
- ▶ If the “Read Device Information” option is selected, device information such as the firmware version, LEGIC operating system, etc., is read from the offline doors when the offline controller loads authorization data into the doors or bookings are read. The read information is displayed in the offline door list (see next point). If this information does not need to be read, you can disable this option.
- ▶ In the “... Card Type” fields, enter the card type to be used for the RFID technologies that are used. For RFID technologies that are not used, select “0 - No Card Type”. Card types are defined in GAT Matrix and allow different types of data carriers (RFID type, data structure, etc.) to be used together in an access system.
- ▶ Click on “Save” to save the settings.
 - You are returned to the list of offline loaders with the recently defined loader also displayed there.
- ▶ To assign an offline loader to another location, you can drag and drop the offline loader as desired.

Assigning offline doors



- ▶ Select the desired offline loader to which you want to assign a new door.
- ▶ Click on the “Add door” icon in the “Offline doors” area of the toolbar.
 - The “New Offline Door” window opens. The settings available in the “Basic Info” tab depend on the type of offline loader being configured.

New Offline Door

Save Cancel

Basic Info Technologies

Name: GAT MT 010

Number: 1

Silent Mode: ☐

Unlock Time: 5

Opto 1 Name:

Opto 1 Function: Not Used

Opto 2 Name:

Opto 2 Function: Not Used

Always Open: ☐

Blocklist Enabled: ☐

Calendar Outdated (Months): 10

Ignore Special Days: ☐

Figure 5.20 – GAT MT 010 settings

New Offline Door

Save Cancel

Basic Info Technologies

Name: GAT DL 092

Number: 3

Serial Number HEX: 23F870A

Silent Mode: ☐

Unlock Time: 5

Blocklist Enabled: ☐

Calendar Outdated (Months): 36

Ignore Special Days: ☐

RFID Wake-Up Enabled: ☒

Ignore Version Number: ☐

Figure 5.21 – GAT DL 092 settings

New Offline Door

Save Cancel

Basic Info Technologies

Name: GAT DL 73xx

Number: 2

Serial Number Decimal: 124125523

Article Number:

Silent Mode: ☐

Unlock Time: 5

Always Open: ☐

Blocklist Enabled: ☐

Figure 5.22 – GAT DL 73xx settings

New Offline Door

Save Cancel

Basic Info Technologies

Name: GAT ECO.Side Lock

Number: 4

Serial Number Decimal: 0

Silent Mode: ☐

Blocklist Enabled: ☐

Only Lock with Identification: ☐

Break-In Alarm Enabled: ☐

RFID Wake-Up Enabled: ☐

Figure 5.23 – GAT Locker Lock settings

“Basic Info” tab

- Name: Enter a name for the offline device into the “Name” field.
- Number: Enter a number for the offline device into the “Number” field.

NOTE! The number must be unique, i.e., not used yet in GAT ACE 7000. An error message is displayed if you enter a number that has already been used.
- Serial Number HEX / Decimal: You can enter the serial number of the offline device here. For the GAT DL 73xx, the serial number must be entered here. For the GAT DL 092, enter the serial number in hexadecimal format. For the GAT DL 73xx and GAT Locker Lock loaders, enter the number in decimal format.

- Article Number: You can enter the article number (Part No.) of the GAT DL 73xx here.
- Silent Mode: This option allows you to disable/enable the lock's acoustic beeper.
- Unlock Time: Define the time duration (in seconds) for unlocking the offline device following a valid authorization.
- Opto x Name / Opto x Function: Select a designation and a function for one or both optocoupler inputs of the offline controller (provided the controller has optocoupler inputs). The selected function defines the type of evaluation of the input signal.
- Always Open: This function is only possible with the GAT ST 210, GAT ST 22x, TAC, and the GAT DL 73xx locks. When the function is activated, the offline door can be permanently unlocked by reading an authorized data carrier and then removing the data carrier from the reading field and reading the data carrier a second time while the unlocking time is still active.
- Blocklist Enabled: Select this option to activate the blocklist as defined in, e.g., GAT Matrix. The data carriers entered in this list are sent to the offline device and blocked from access. When this option is not selected, the blocklist is not used.
- Calendar Outdated (Months): You can affect the type of loading display (footsteps symbol) in GAT Matrix or GAT ACE with reference to the operating calendar. If the operating calendar in an offline door is older than the time entered here in months (i.e., it was last updated before this time), a green footsteps symbol () is displayed for the offline door in GAT Matrix and GAT ACE to indicate that the operating calendar has to be reloaded.
NOTE! A GAT MT 010 can transfer an operational calendar for one year and a GAT DL 092 for three years to an offline door. If the operating calendar has expired in an offline door then further access to the door only occurs based on the authorization data but without taking the schedules and special days into account.
- Ignore Special Days: If you enable this option, the operating calendar with the special day definition is not loaded into the offline controller. This means that the authorization check is carried out at the offline doors concerned without consideration of the special days in the operating calendar. This eliminates the need to regularly load the offline controllers because of changes to the special days and holidays.
- Only Lock with Identification: GAT Locker Lock: When this option is enabled, the locker can only be locked by pushing the locker door shut and reading a data carrier. When not enabled, the locker door will lock simply by pushing it shut.
- Break-In Alarm enabled: GAT Locker Lock: When this option is enabled, an alarm will be triggered if the locker door is forced open. The lock indicates this state with three red LED flashes and three beeps.
- RFID Wake-Up Enabled: GAT Locker Lock: When this option is enabled, the locker door unlocks when a valid RFID data carrier is held to the reading field of the lock. When not enabled, the reading field of the lock must be activated first (with the GAT ECO.Side Lock by pushing the locker door in and with the GAT ECO.Lock and GL7p by pushing the button of the lock in).

GAT DL 092: When this option is enabled, the door unlocks when a valid RFID data carrier is read by the GAT DL 3xx lock.
- Ignore Version Number: GAT DL 092: This option is only shown when the GAT DL 092 is set to operation mode "Hotel Mode G1". This option is disabled by default, which means that the version (or index) number of the card will be considered to ensure that only the most recent card can be used.

“Technologies” tab

New Offline Door

Save Cancel

Basic Info **Technologies**

LEGIC prime ☒ ISO15693 ☒

ISO14443A ☒ ISO14443B ☐

Inside ☐ Felica ☐

Figure 5.24 – Defining an offline loader – Technologies

- ▶ Select the RFID technologies to be supported by the new door here. You can enable or disable support for specific technologies as required.
- NOTE!** Ensure that the RFID technology used on the PassKey Management data carriers is not switched off.
- ▶ Click on "Save".
 - The new door is assigned to the offline loader.

Display of offline doors

- ▶ Click on the “Offline Doors” view tab.
- ▶ Select the desired location from the location list to the left of the application window.
 - All previously defined loading groups for the selected location and its sub-locations are listed.

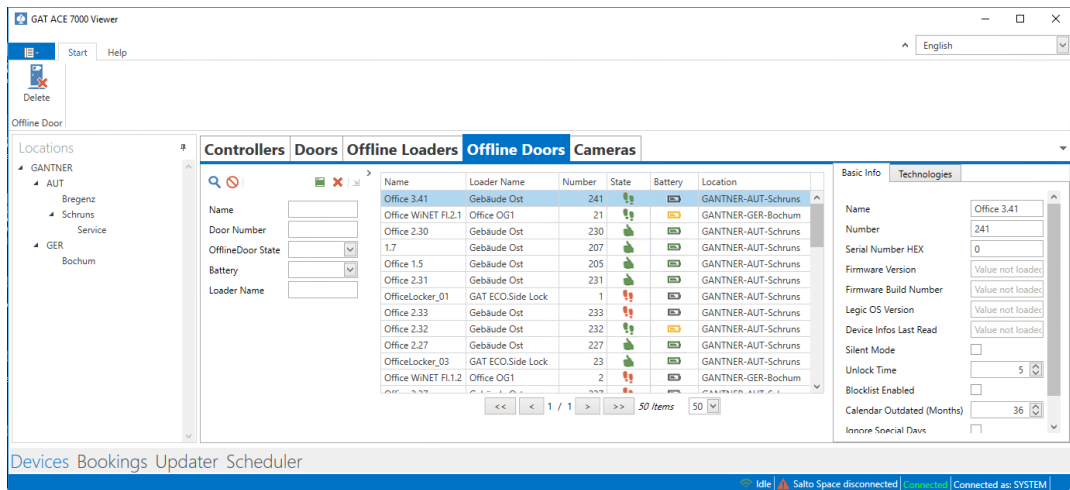


Figure 5.25 – “Offline Doors” view

- The name and number of the offline door as well as the name of the associated offline loader are displayed in the list.
- The footsteps symbol in the “State” column indicates whether there are changes that need to be loaded to the offline device.



.... The data in the offline device is current, i.e., the last changes have been loaded.

The colors of the footprint symbols indicate which data is not up to date in order of priority, which is as follows:



.... Red indicates that the access data is not synchronized.

- Violet indicates that the configuration data is not synchronized.
- Green indicates that the corporate calendar data is not synchronized.
- Blue indicates that the corporate calendar of the offline device will expire soon.

- The “Battery” column shows the battery charge status of the offline controllers at the time of the last readout of the controllers.

 ... Battery is fully charged.

 ... Battery is almost empty and must be replaced as soon as possible.

 ... Battery is empty and must be replaced.

 ... Battery status unknown (e.g., because it has not been read yet or because no battery data carrier has been used or learned at the offline controller).

- In the “Location” column you can see the location to which the doors are assigned.

► You can search for a specific door by entering information into the search fields to the left of the door list and clicking on the magnifying glass icon.

► To change the door name, the door number, or the serial number of a door, select the door and change the data in the information window. Click on the green “Save” icon to save the changes.



For information about these settings, see the information on “Assigning Offline Doors” on the previous page.

► To reset the battery warning of a controller (e.g., after the battery has been replaced), right-click on the controller and select “Reset battery warning”.

- The battery warning is reset, and the green battery symbol is displayed.



Battery warnings are also reset via the CardNET data when changing the battery (depending on the product and controller setting). If CardNET is not used (functions “Read only unique number” or “Read only card number”), the battery warnings and the resetting of bookings during readout are transferred via the programming device.

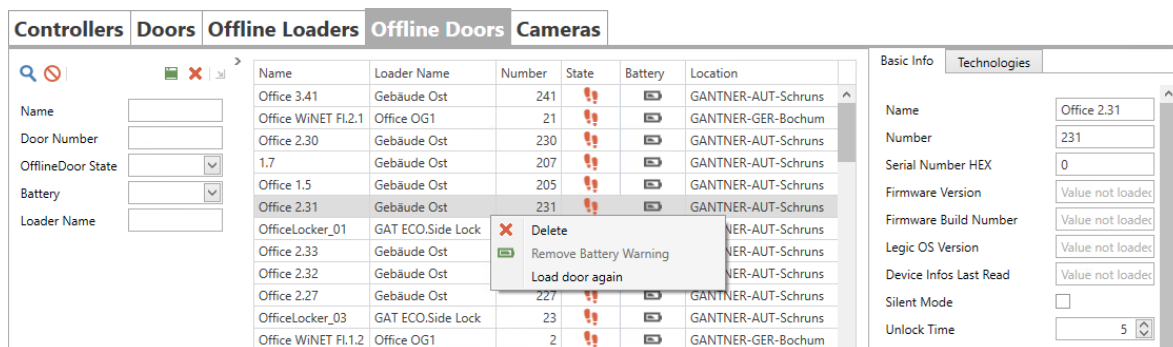


► To delete a door, select the door and click on the Delete icon.

Individually reloading offline doors

You can individually select to reload one or several offline doors with configuration data.

► Open the “Offline Doors” tab.



Name	Loader Name	Number	State	Battery	Location
Office 3.41	Gebäude Ost	241			GANTNER-AUT-Schruns
Office WiNET FL2.1	Office OG1	21			GANTNER-GER-Bochum
Office 2.30	Gebäude Ost	230			GANTNER-AUT-Schruns
1.7	Gebäude Ost	207			GANTNER-AUT-Schruns
Office 1.5	Gebäude Ost	205			GANTNER-AUT-Schruns
Office 2.31	Gebäude Ost	231			GANTNER-AUT-Schruns
OfficeLocker_01	GAT ECO.Side Lock				GANTNER-AUT-Schruns
Office 2.33	Gebäude Ost				GANTNER-AUT-Schruns
Office 2.32	Gebäude Ost				GANTNER-AUT-Schruns
Office 2.27	Gebäude Ost	227			GANTNER-AUT-Schruns
OfficeLocker_03	GAT ECO.Side Lock	23			GANTNER-AUT-Schruns
Office WiNET FL1.2	Office OG1	2			GANTNER-GER-Bochum

Figure 5.26 – Reloading offline doors

- Right-click on the controller and select “Load door again” from the menu.
 - After selecting the menu option, the status is indicated by a red footprint symbol .
 - The next time the location or offline loader is loaded, the data for the door will be transferred again.

5.2.12 Synchronizing offline loaders and offline doors

During synchronization, changed or new authorization data for offline doors is transferred to the relevant offline loaders in order to update the offline locks locally. In addition, the data stored in the offline loaders (bookings, battery warnings, etc.) of the doors are read out to make them available in GAT ACE or GAT Matrix. Depending on the type of loader, different functions are available:

- GAT MT 010: The authorizations are transferred, and the bookings are read in one step via the “Synchronize Changes” function.
- GAT DL 092: The transferal of changed data, the time setting, and the reading of bookings can be selected and carried out separately.
- GAT DL 73xx or GAT Locker Lock loader: A configuration file can be generated in order to configure the GAT DL 73xx and the CardNET locker locks. Information such as configuration results and bookings (for the locker locks) can be read and reimported into GAT ACE 7000.

i With the remote sync function for the GAT DL 092, GAT DL 73xx or GAT Locker Lock, it is possible to transfer data for offline doors over greater distances. This is helpful if the offline loader cannot be directly connected to the GAT ACE server, e.g., if a technician wants to reload the doors with an offline loader at a remote location. The data can then be transferred via a network, email, etc., between the GAT ACE server and the offline loader. See “5.2.13 Remote sync transfer of offline data”.

The functions for synchronization are either separate for each offline loader or selectable per location, i.e., for all offline loaders in one location.

- Select the offline loader or the location for which the synchronization is to be carried out.
- Select the desired function via the corresponding icon in the function bar. Alternatively, you can right click on the offline loader or the location and select the desired function from the pop-up menu.

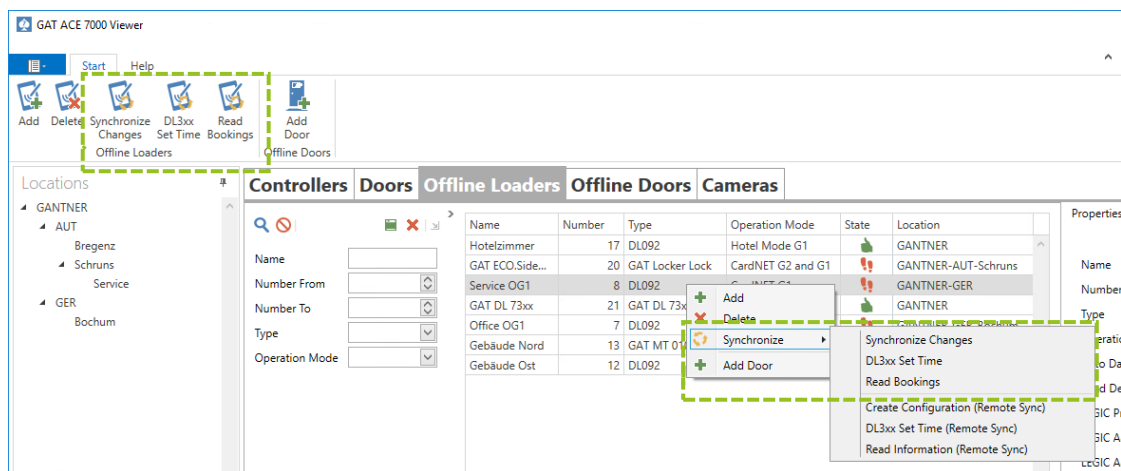


Figure 5.27 – Synchronization of a specific offline loader (GAT DL 092 selected in the example)

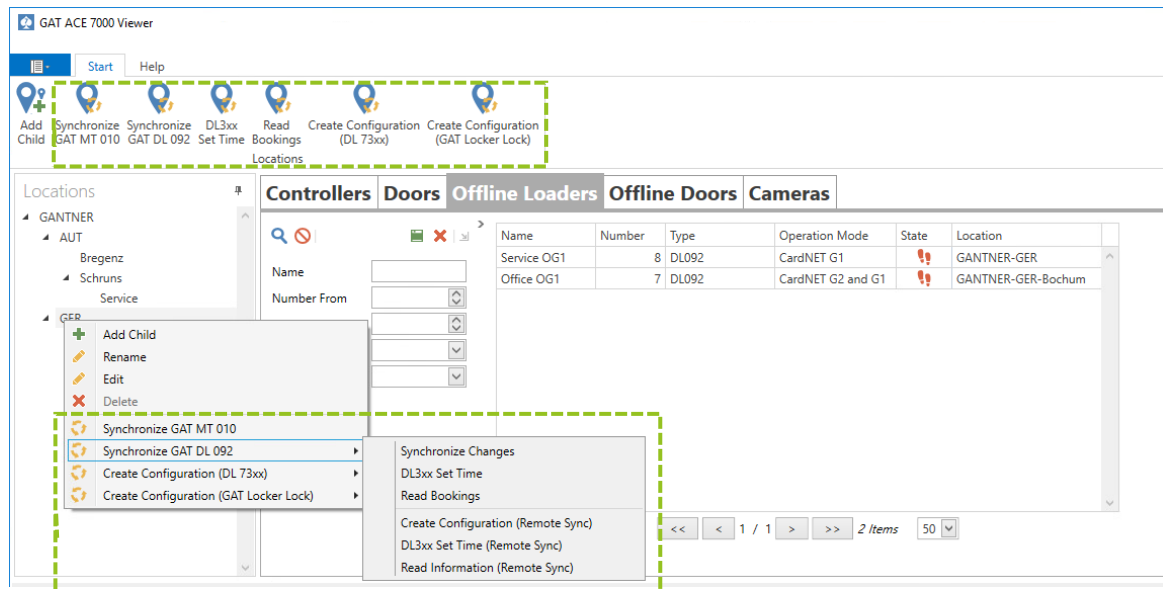


Figure 5.28 - Synchronization of all offline loaders in one location

i If the synchronization function is selected directly for a GAT MT 010 offline loader, all door data is transmitted. When synchronizing at a location is selected, only the data of the doors marked with a footprint symbol  (i.e., where data has been changed) is transmitted.

NOTE! The directories for the synchronization data as well as the synchronization with GAT Sync Manager are defined in the general settings (see “4.2 Application settings”).

GAT MT 010 – Synchronization



Use these buttons, or the menu options of the same name, to transfer all changed door data assigned to the selected offline controller or location, and to read their bookings.

- Select the desired function.
 - After selecting the function, a window opens where you can select the directory for saving the booking files.
 - Then another window opens where you can select the folder for the configuration files of the offline locks.
- Save this data, e.g., on an SD card, which is then inserted into the GAT MT 010.

ATTENTION! Before inserting the SD card into the GAT MT 010, ensure that the GAT MT 010 is switched off. After inserting the SD card, switch on the GAT MT 010 and check that the date and time are correctly set in the GAT MT 010 before loading the doors.
- Take the offline loader (programming device) and go to the affected offline doors to transfer the configuration to the offline controllers.

i Detailed instructions for loading offline doors are available in the user manual of the offline device.

GAT DL 092 – Synchronize changes



Use these buttons, or the menu options of the same name, to transfer the changed authorization data of the doors at the selected controllers or locations to the relevant offline controller.

- ▶ Connect the GAT DL 092 offline controller to a USB port on the PC.
- ▶ Select the function “Synchronize Changes”.
 - First, any saved bookings on the connected GAT DL 092 are read out (they would be deleted during writing of the changed data) and their memory is deleted. Next, the new/changed authorization data is copied to the GAT DL 092.
- ▶ Use the GAT DL 092 Controller to load the changed data into the offline doors.

NOTE! Immediately after removing the GAT DL 092, plug it into a battery pack or power bank to power it. The internal clock stops running when the supply voltage is disconnected, which leads to a large time deviation if the GAT DL 092 is left without voltage for too long.

NOTE! When transferring the changed data to an offline door, the time of the door is always synchronized (as of version 4.2 of GAT Matrix). However, if the GAT DL 092 has been disconnected more than once from the supply voltage after removing it from the PC, the time will not be synchronized when the offline doors are updated. For offline doors, where no data has been changed/transferred, the time is also not synchronized.

NOTE! If not, all changed data for all offline doors could be saved on the GAT DL 092 offline controller, a message with the missing changed data is displayed. After updating the doors, the GAT DL 092 offline controller must be reconnected to transfer the remaining data.

GAT DL 092 - DL 3xx Set Time



Use these buttons, or the menu items of the same name, to copy time synchronization data for the doors at the selected controllers or locations to the connected GAT DL 092 controller. In this case, no authorization data is transmitted. The time synchronization is transmitted for all offline doors regardless of whether the doors have changed authorization data or not.

- ▶ Connect the GAT DL 092 offline controller to a USB port on the PC.
- ▶ Select the function.
 - First, any saved bookings on the connected GAT DL 092 are read out and their memory is deleted. The time synchronization information is copied to the selected GAT DL 092.
- ▶ Go to the offline doors with the GAT DL 092 controller to synchronize the times of the offline doors.

NOTE! Immediately after removing the GAT DL 092, plug it into a battery pack or power bank to power it. The internal clock stops running when the supply voltage is disconnected, which leads to a large time deviation if the GAT DL 092 is left without voltage for too long.

If the GAT DL 092 has been disconnected from the supply voltage more than once after removal from the PC, the time will not be synchronized when the offline doors are updated. For the offline doors, where no data has been changed/transferred, the time is also not synchronized.

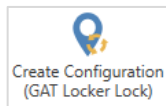
GAT DL 092 – Read bookings



Use these buttons, or the menu items of the same name, to read the bookings for the selected area via the GAT DL 092.

- ▶ Connect the GAT DL 092 offline controller to a USB port on the PC.
- ▶ Select the function.
 - The bookings stored on the connected GAT DL 092 are read out and made available to the access software (e.g., GAT Matrix).
 - If the reading of device information is selected when configuring the GAT DL 092 (see “5.2.11 Configuring offline loaders and offline doors”) then the read data, such as firmware version, etc., is also transferred from the GAT DL 092 to GAT ACE and displayed for the offline doors in GAT ACE.
 - After read-out is completed, the GAT DL 092 memory is deleted so that the bookings are not duplicated in the system when read again.

GAT DL 73xx and GAT Locker Lock – Synchronize changes



Use these buttons, or the menu options of the same name, to generate a configuration file (XML) with the authorization and configuration data for the GAT DL 73xx readers or the GANTNER Locker Locks at the selected controllers or locations respectively. The configuration file is then transferred to the GAT DL 73xx or GAT Locker Locks using the GAT DL Analyzer software. This process is described in the next chapter “5.2.13. Remote sync transfer of offline data”.

GAT Locker Lock – Read bookings



Use these buttons, or the menu items of the same name, to read the bookings for the selected GANTNER Locker Locks. After clicking the button, a window opens where you must select the correct booking file. The booking file is generated with GAT DL Analyzer as described in the next chapter “5.2.13. Remote sync transfer of offline data”.

i The GAT DL 73xx offline controller does not save bookings; therefore, the icon for importing bookings is not shown in GAT ACE 7000.

5.2.13 Remote sync transfer of offline data

With the Remote Sync function, which is available for the GAT DL 092, GAT DL 73xx and GAT Locker Locks loaders, the transfer of authorization and configuration data as well as bookings and status information is done via file transfer. GAT ACE 7000 writes the data to a file that is then sent to the location where the offline controllers or locks are located. There the files are transmitted to the offline controllers using the GAT DL Analyzer software. This software is also used to read bookings and status information from the offline controllers/locks and write this data to files that are then sent via file transfer to GAT ACE 7000 for importation.

The GAT DL 73xx and GAT Locker Locks loaders always have to use Remote Sync (file transfer with GAT DL Analyzer). The GAT DL 092 loader can be used either directly with GAT ACE or with Remote Sync file transfer. The second option is helpful if the GAT DL 092 cannot be plugged directly into the computer running GAT ACE (e.g., for IT security reasons or if the computer is accessed remotely and you are not on-site). To use Remote Sync with the GAT DL 092, the applicable “remote sync” option must be selected.

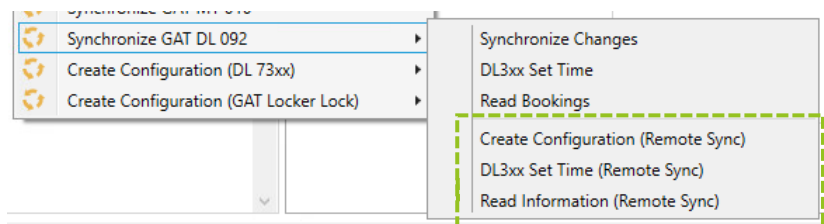


Figure 5.29 - Remote sync options for synchronization via a file interface

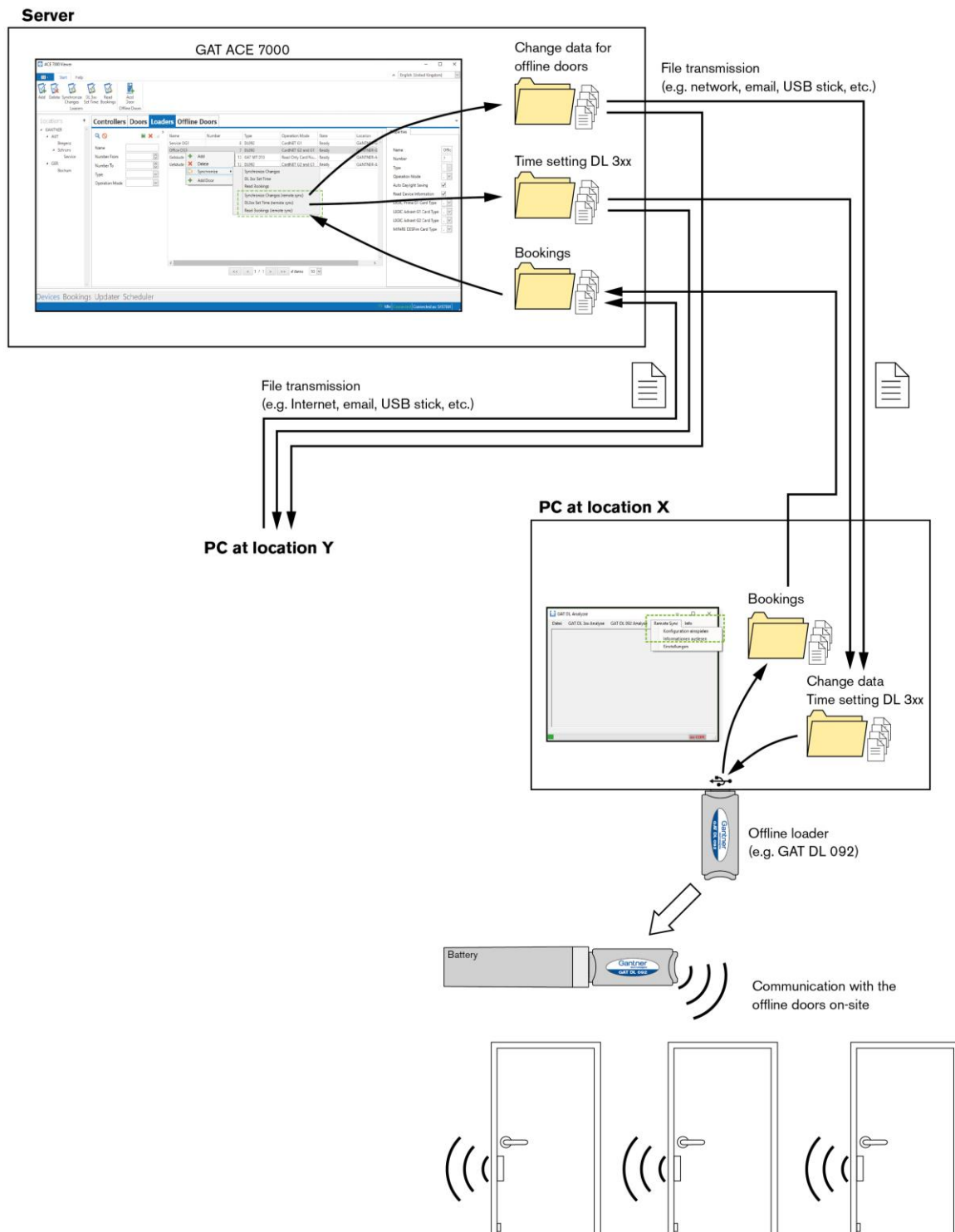


Figure 5.30 – Overview of remote sync process for offline doors (example for GAT DL 092)

This image shows the remote sync process for the GAT DL 092. The process is similar for the GANTNER Locker Locks and GAT DL 73xx except for the transfer from the GAT DL Analyzer software to the offline controller/lock (see next pages).

GAT DL Analyzer

To use the remote sync feature, the software “GAT DL Analyzer” must be used at the remote locations where the offline loaders are being used.

i The GAT DL Analyzer software is only available in German; however, the operation is straightforward using the translations provided in the following instructions.

Complete the following steps:

- ▶ Download the “GAT DL Analyzer” software from the GANTNER partner homepage or contact GANTNER Support who will send you the software.
- ▶ Start GAT DL Analyzer by double-clicking on “GAT DL Analyzer.exe”. The software is a portable version and installation is therefore not necessary.
 - The following window is displayed.

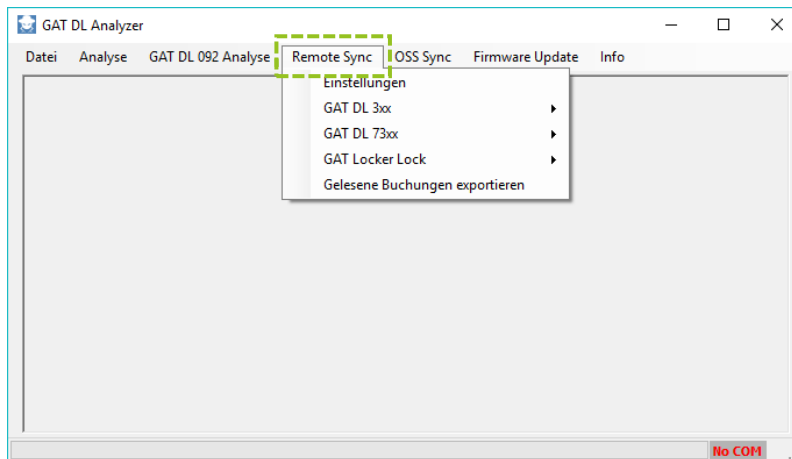


Figure 5.31 - Remote sync options for synchronization via a file interface

i Only the “Remote Sync” menu is required for the transmission of data. The other menu items are for service technicians.

- ▶ The “Einstellungen” (EN: Settings) option in the “Remote Sync” menu allows you to select the default directories where the files are to be stored by default for synchronization.
 - The following window is displayed.

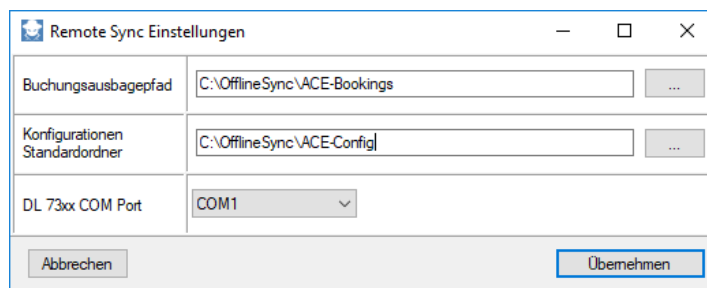


Figure 5.32 – Default directories for remote sync

- ▶ Enter the desired directories into the fields or click on the “...” buttons to select the directories. Confirm the settings via the “Übernehmen” (EN: Confirm) button.
 - You can also manually change or select the directories when selecting the files.
- ▶ For the GAT DL 73xx, select the serial interface in the “DL 73xx COM Port” field where the GAT DL 73xx configuration cable is connected.
- ▶ Use the menu items “Konfiguration einspielen” (EN: Import configuration) and “Informationen auslesen” (EN: Read information) to transfer data from and to the offline loader plugged into the USB port (see below for instructions).

Procedure for transferring change data and bookings

For GAT DL 092 to use the remote sync function in GAT ACE 7000 the menu options shown with the suffix “remote sync” are used.

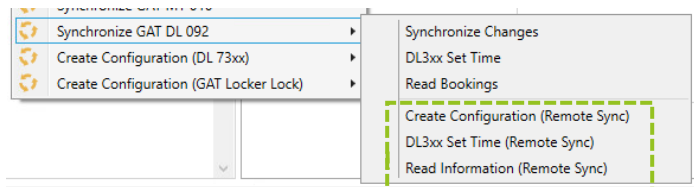


Figure 5.33 - Remote sync options for GAT DL 092 for synchronization via a file interface

The menu items are otherwise the same as for the local transfer of data. Please read section “5.2.12 Synchronizing offline loaders and offline doors” for detailed information on the three functions.

For the GAT DL 73xx and GAT Locker Lock, the menu items in GAT ACE 7000 automatically use remote sync as described in the following steps.

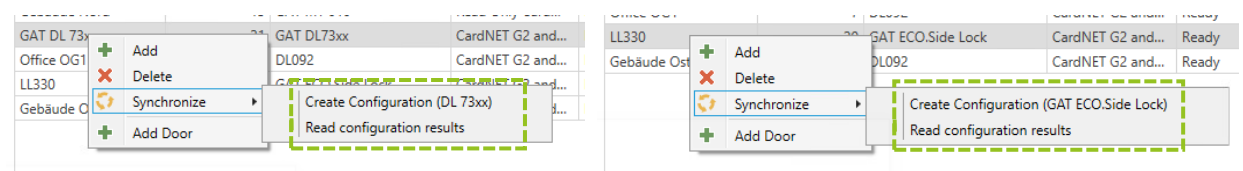


Figure 5.34 - Remote sync options for synchronizing the GAT DL 73xx and GAT ECO.Side Lock

- ▶ To read the bookings from offline doors, first transfer them from the remote locations to the current PC/server (see below).
- ▶ In GAT ACE, right-click on the offline loader or site to be loaded.
 - A context menu is displayed.
- ▶ Click on “Synchronize” or “Synchronize GAT DL 092”.
 - The menu items with the various synchronization functions are displayed.
- ▶ Select a remote sync option:
 - With the “Synchronize Changes (remote sync)” (GAT DL 092) or “Create Configuration (xx)” (for the GAT DL 73xx and GAT Locker Lock) option, the change data for the respective offline loader(s) is written to a file. A window opens where you can choose the location and file name for the file.
 - With “DL3xx Set Time (remote sync)”, commands for the time synchronization of the GAT DL 3xx locks are written to the respective offline loader(s) in a file. Thus, when transferring the file to the GAT

DL 092 offline loader, the time on the PC where the GAT DL 092 is connected (see below) is used for the time synchronization. Selecting this item opens a window in which you can select the location and file name for the file.

- With the “Read Bookings (remote sync)” (GAT DL 092) or “Read configuration results” (for the GAT DL 73xx and GAT ECO.Side Lock) option, a window opens in which you can select the file to import into GAT ACE that has the previously read offline-lock booking data.
- ▶ After confirming the selection via “OK” in the file window, the change data is written to the file or the bookings are loaded from the file into GAT ACE.
- ▶ Next, transfer the written files with the synchronization data to the remote locations (e.g., via email, remote view, or similar).
- ▶ Start the GAT DL Analyzer software on the PC at the remote location.
- ▶ Plug the offline loader into a USB port on the PC.
 - GAT DL 092: Plug this loader directly into a USB port of the PC.
 - GAT DL 73xx: Use the GAT DL 73xx Configuration Cable to connect the GAT DL 73xx (RJ 45 plug) to a USB port of the PC.
 - GAT Locker Lock: Use a standard USB cable (connector type Micro-B) to connect the lock a USB port of the PC.
- ▶ To transfer the synchronization data (configuration or time setting), open the GAT DL Analyzer and select the menu item “Konfiguration einspielen” (EN: Import configuration) in the offline loader sub menu of the “Remote Sync” menu. Then select the synchronization file generated by GAT ACE.
 - The synchronization data is transferred to the offline loader, which you can then use to load the doors.
- NOTE!** When bookings are stored in the offline loader, they are first read and saved to a file on the PC before the synchronization files are transferred (memory is deleted). This booking file can be sent to the server with GAT ACE for importation there (see above).
- ▶ To read bookings from an offline loader, select the menu item “Informationen auslesen” (EN: Read information) in the offline loader sub menu of the “Remote Sync” menu.
 - The bookings are read from the offline loader and loaded into GAT DL Analyzer.

i If several offline controllers and/or locks are loaded and read, the data is saved by GAT DL Analyzer temporarily.

- ▶ After loading and reading all the desired controllers and/or locks, select the menu item “Gelesene Buchungen exportieren” (EN: Save Read Bookings).
 - The temporarily stored data is stored in a file on the PC.
- ▶ This bookings file can be sent to the server with GAT ACE for importation there (see above).
 - Afterwards, the offline loader memory is deleted.

5.2.14 Updating firmware of the GAT DL 73xx offline controllers and GAT locker locks

The GAT DL Analyzer software enables new firmware to be loaded into the GAT DL 73xx controllers and the GAT locker locks.

i For the GAT GAT ECO.Side Lock 7000 NW BA CardNET (Part No. 1105111) only a firmware of this lock type can be used. Using a firmware for the locker locks GAT ECO.Side Lock 7xxx (without CardNET) with identical hardware is not possible. The same applies for the GAT ECO.Lock 7100 NW BA CardNET and the GL7p.xxxx CardNET locks.

- ▶ Connect the controller to the PC.
The GAT DL 73xx connects to the PC via the GAT DL 73xx Configuration Cable. The GAT locker lock connects to the PC via a standard USB cable (plug type Micro-B).
- ▶ In the GAT DL Analyzer software, open the “Firmware Update” menu and in the menu entry for the correct type of offline controller select the function to load the intended firmware of either a GAT DL 73xx component (“Leser” = EN: reader, “Funkmodul” = EN: RF module or “Funkschloss” = EN: wireless lock) or of the GAT locker lock.

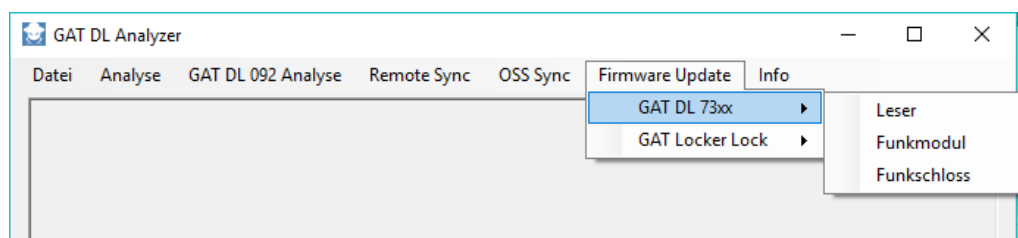


Figure 5.35 - Firmware update of an offline controller GAT DL 73xx component.

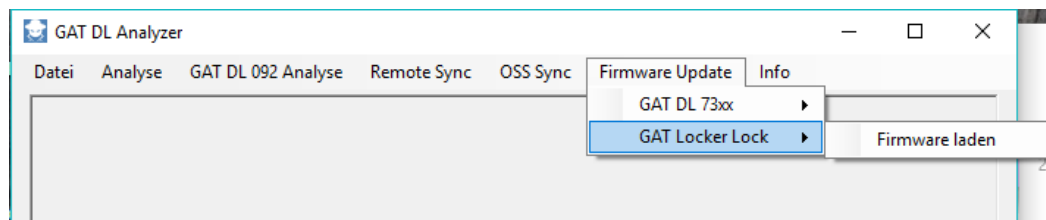


Figure 5.36 - Firmware update of a GAT locker lock.

- A window is opened where you must select the firmware file.
- ▶ Select the firmware file and click “OK”.
 - The firmware is loaded into the controller or lock respectively.
 - If the connection is not established, a corresponding error message is shown in the program window of GAT DL Analyzer.
- ▶ After transmitting the firmware, a corresponding message is displayed, and the controller or lock is restarted.

5.2.15 Configuring cameras for license plate recognition systems

As of GAT ACE 7000 version 2.2 and GAT Matrix version 5.2, cameras for license plate recognition are supported. The ID information and license plate numbers of all persons defined in GAT Matrix are transferred from GAT ACE 7000 to the camera systems. The GAT SR 950 camera available from GANTNER validates the read license plates and, if the validation is approved, transfers the ID number to the access controller (e.g. GAT DC 7200) via the Wiegand interface. In this case, the GAT DC 7200 then checks whether a local decision is possible based on the stored authorizations or whether an online decision is required, e.g., if a pool management or anti-passback decision is required. With this system solution, all requirements can be mapped.

In the GAT Matrix software, the vehicle license plates information are inserted in the personnel data. For more information about the license plate entry, please refer to the GAT Matrix manual.

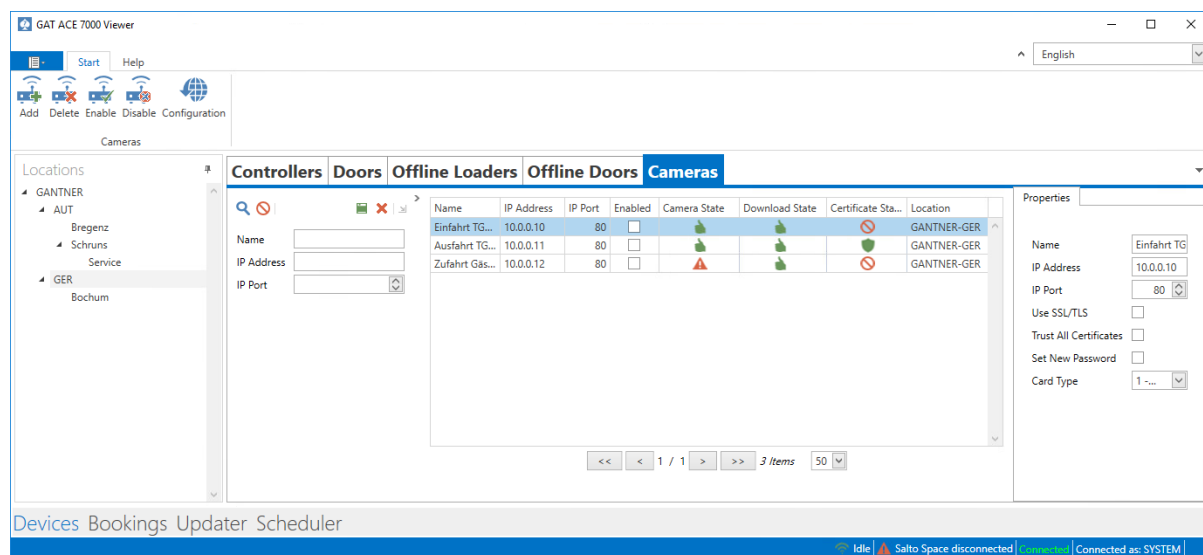


Figure 5.37 - Updating the firmware of a GAT Locker Lock

All cameras configured in the system are listed here.

- Name: The name of the camera. This is set when the camera is added.
- IP Address: Is the IP address of the camera. Each camera in a system has a unique IP number that is used to communicate over the network.
- IP Port: Port for communication with the respective camera (default = 80).
- Enabled: The Enabled column indicates whether the camera is enabled or disabled. With a deactivated camera, no communication is performed, which means that license plate recognition is currently not possible on this camera.
- Camera Status: Displays the current status of communication with the camera.
 - Communication with the camera is OK
 - Communication interruption with the camera
 - Communication status is unknown
 - The camera is disabled
- Download Status: This icon shows the status of communication from GAT Matrix to the cameras.
 - The last changes in GAT Matrix have been successfully downloaded to the camera.

- ? The connection to the camera is interrupted and the latest data in GAT Matrix has not yet been loaded into the camera. It will automatically be tried to reload the data every few minutes. If loading is not possible for about 15 minutes, the next status is displayed.
- ! The last configuration data has not yet been loaded from GAT Matrix to the camera. Reload the changes after establishing the connection to the camera.
- 🔄 The loading of the data to the camera in question was not successful and GAT ACE 7000 tries to load the data to the camera again every 2 minutes.

- Certificate Status: In this column you can see the current status of the encrypted TLS communication:

- 🛡️ The connection with the camera is encrypted and the certificate used is valid.
- 🛡️ The connection with the camera should be encrypted, but the certificate is invalid.
- 🚫 An unencrypted connection with the camera is used.

- Location: The location where the camera is located is displayed here. For the location function, see "5.2.1. Structuring locations".

Adding a new camera



- To add a new camera, click the corresponding icon in the header.
 - The following window opens.

Figure 5.38 - Hinzufügen einer Kamera zur KFZ-Kennzeichenerkennung

► Enter the info for the camera here.

- Name: Enter a name for the camera, e.g., the location.
- IP Address/Port: The network address (IPv4) and port number (default = 80) for communicating with the camera.
- Use SSL/TLS: If communication to the camera is to be encrypted (recommended), then check this box. The corresponding certificate must then be installed on the PC (see documentation of the camera).
- Trust All Certificates: This option can be used to enable a connection to the cameras if "Use SSL/TLS" is activated but no appropriate certificate is installed on the PC. The connection is still possible, but this approach is not recommended and if SSL/TLS is used, the appropriate certificate should always be used.

- Password: Usually the cameras use a password to access the web configuration page to prevent unauthorized access. Enter the password here to facilitate the configuration, as GAT ACE 7000 will then perform the login directly when the configuration is called.
- Card type: For the car license plate recognition, the license plate is used as "data carrier" for the user identification. You can select here which data carrier type the license plate should correspond to. This is necessary for the authorization check in GAT Matrix (see GAT Matrix manual -> Card types).

- ▶ Click "Save" after entering the data.
 - The new camera is inserted in the List of cameras.

Configuring a camera

To configure a camera, the web interface of the camera is used. This can be opened as follows.



- ▶ Select the camera in the list.
- ▶ Click the "Configuration" button in the header.
 - The standard browser opens with the configuration page. This differs depending on the camera model. Please read the documentation of the camera for the configuration.
 - If a password is required to access the camera configuration (login), you can enter it in the browser window.
 - If the password is changed in the configuration page of a camera, please do not forget to change the password in GAT ACE 7000 as well. You can set a new password by highlighting the camera and checking the "Set new password" box in the settings on the right side.

Changing camera settings

- ▶ To change settings such as name, IP address, Use SLS/TLS, etc. of a camera, first select the camera from the list.
 - The camera settings are displayed in the "Properties" field on the right.
- ▶ Change the desired value here.
 - As soon as a value is changed, the Save  and Cancel  icons are displayed.
- ▶ Click on "Save"  to save the changes.

Searching for a camera in the displayed list

- ▶ To search the list for a specific camera, enter the known information such as name, IP address or IP port in the search fields on the left of the list.

Note: It is sufficient to enter only a part of the information (e.g. a few letters of the name).
- ▶ After clicking the search icon , only the cameras that match the entered information will be displayed in the list.

5.3 Bookings

All data carrier readings, access requests, and permitted entries/exits are recorded by the controllers in a bookings log. Each booking contains information on the data carrier number used, the date and time, and the type of booking, etc. This data allows all activity recorded by the controllers to be analyzed at a later date.

GAT ACE 7000 can directly download the bookings from the online controllers and display them in the “Bookings” area. The bookings can be filtered and displayed in this area according to specific criteria.

i The bookings of offline controllers (max. 500) can also be read out and displayed (see “5.2.12 Synchronizing offline loaders and offline doors” and also “5.2.13 Remote sync transfer of offline data”).

If bookings are provided by GAT SyncManager, ensure that GAT ACE 7000 expects a booking file called “accessbookings.exp”. The name of the booking file can be freely selected in GAT SyncManager and must therefore be defined exactly.

- Click onto “Bookings”.
 - The bookings area opens, and all existing bookings displayed.

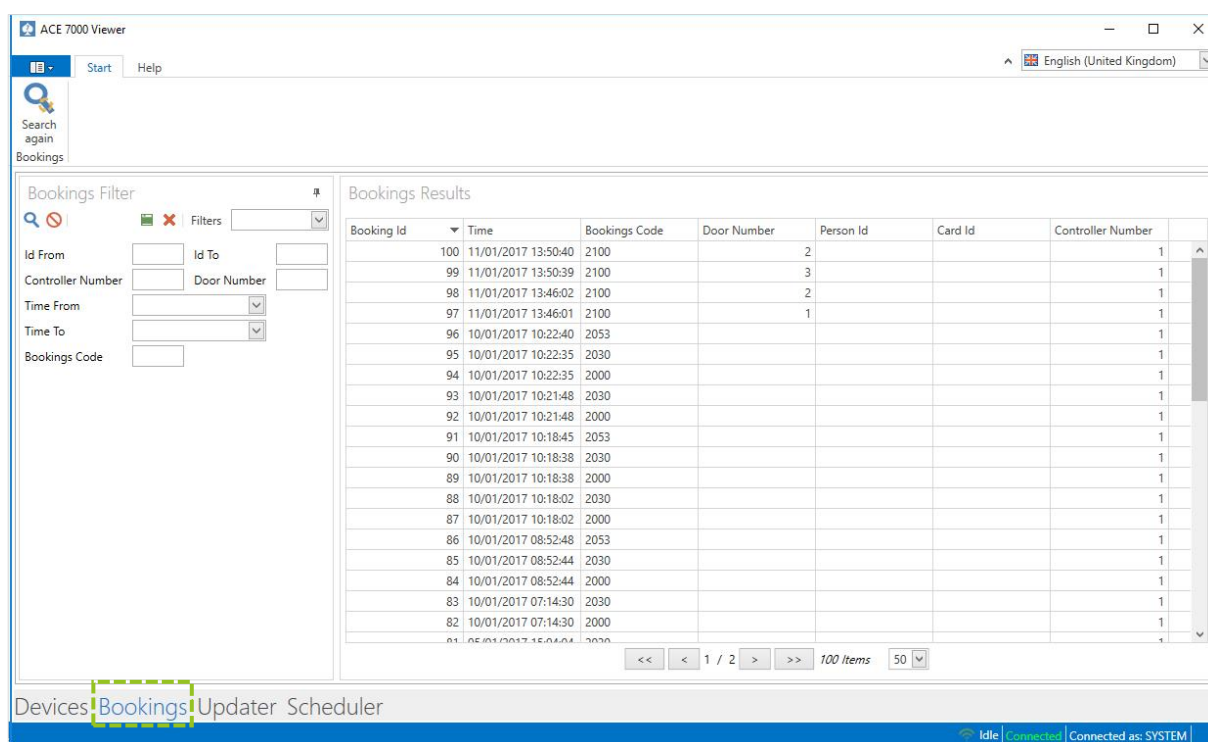


Figure 5.39 – Bookings area

The latest entries are displayed automatically.

- To view older bookings, use the scroll buttons below the list or change the number of items displayed per page.
- Use the search fields to the left of the list to filter the bookings list for specific information.
- If any new bookings occur while you are viewing the bookings, you can refresh the display by clicking on the Search button () to see the latest bookings.

5.4 Updating online controllers and readers

In the “Updater” area, you can update the online controllers of the system and the readers connected to them to a current device software.

- Click onto “Updater”.
 - The location list and the online controllers are displayed.

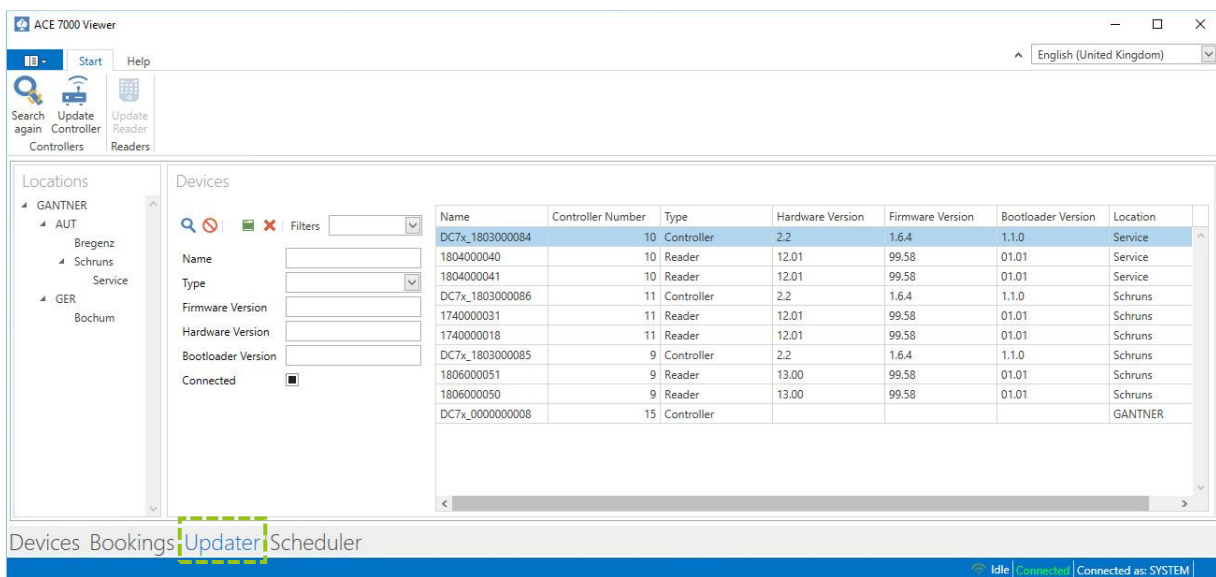


Figure 5.40 – Updater view

The list displays the online controllers that are assigned to the location and sub-locations selected to the left. The current hardware version, firmware version, and bootloader version of the controllers are also displayed.

- To update a controller with a new firmware, first select the location then select the controller in the list and finally click on the “Update Controller” icon.
 - An “Open” window is displayed.
- Select the ZIP file that contains the software update and click on “Open”.
 - The software update is transferred to the controller. The controller restarts to finalize the software update.
- Ensure that the connection to the controller and its power supply are not interrupted during the update process.
- To update the software of an RFID reader connected to a controller, select the reader from the list then click on the “Update Reader” icon.
 - A window opens where you can select the software update for the reader.
- Select the ENC file with the software update and confirm with “Open”.
 - The software update is transferred to the reader via the controller.

i Multiple controllers or readers can be selected to update with the same new software in one step. The controller restarts after the software update. The TCP/IP connection is thereby briefly interrupted but automatically restored by GAT ACE after the restart.

5.5 Scheduler

In the “Scheduler” area, reoccurring system tasks can be executed automatically in GAT ACE 7000. The following system tasks can be scheduled:

- Backing up of the SQL database
- Deleting of old entries in the bookings database
- Deleting of old controller backups

- Click onto “Scheduler”.
 - The current day with all tasks scheduled for the day are displayed.
- Use the calendar to the left to navigate to a desired date.

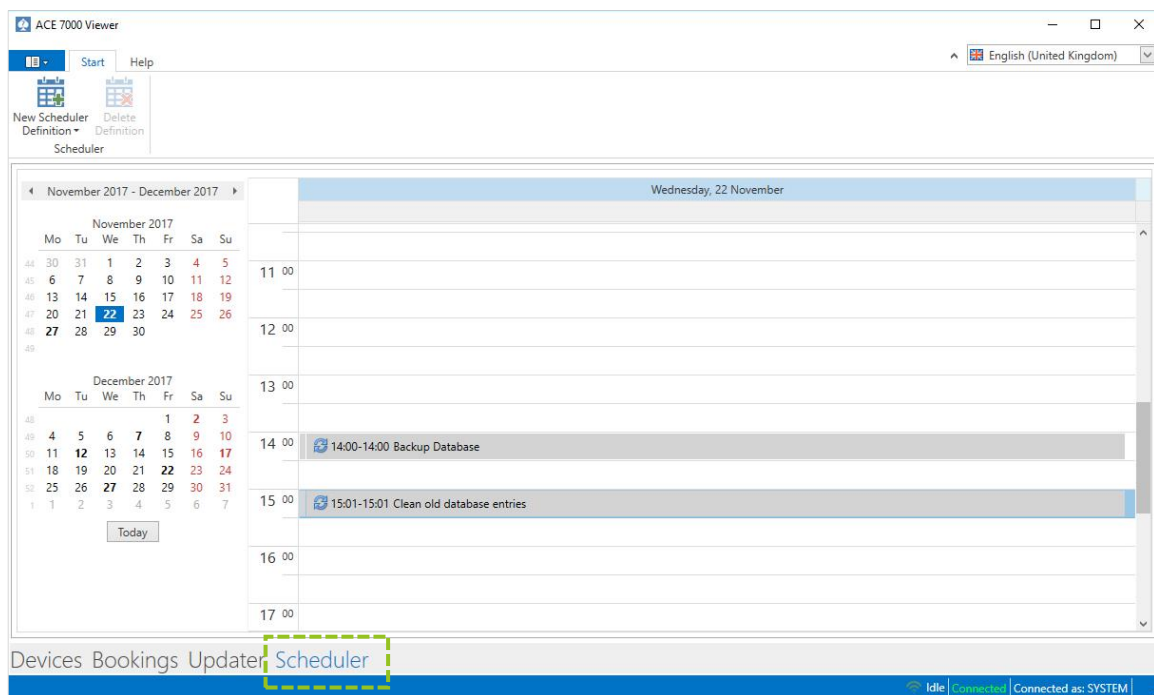


Figure 5.41 - Scheduler view

To schedule a new task, complete the following steps:

- Click on the “New scheduler definition” icon.
 - A menu with the available tasks is displayed.



- Select the desired task from the menu.
 - The “Scheduler Definition” window opens with the corresponding settings of the selected scheduler task. The scheduler tasks are described in the following sections.

5.5.1 SQL database backup

The SQL database contains all the data of the access system, e.g., the controller and door configuration settings, and the bookings data. This scheduler task allows you to automatically create backups of the SQL database at regular intervals. During every database backup, a new file is created. The date and time of the backup is included in the file name. Should an error occur in the system, the database backup file can be imported into GAT ACE 7000 so that operation can continue using the data saved at the time of the backup.

NOTE! Data deleted after performing this scheduler task cannot be recovered!

Figure 5.42 – Scheduling an automatic backup of the SQL database

- In the “Number of saved backups” field, enter the number of backups that should be kept. In order to save space, GAT ACE 7000 automatically deletes the oldest backup when performing a new backup. The value entered here is the number of backups to retain, e.g., if “5” is entered and 5 backups have already been made, the oldest backup file is deleted so that the total number of saved backups remains at 5. If backups are made frequently, e.g., on an hourly or daily basis, it is recommended not to set this value too low. Should an error not be detected immediately, more backups will be available.
- In the “Backup path” field, enter the location where the backups are to be saved. It is recommended to select a network path here so that backups are not lost if the GAT ACE 7000 PC/server is damaged.
- Click on the “Is Enabled” option to enable (field is marked) or disable (field is unmarked) the task.
NOTE! A disabled task remains saved in the scheduler but is not executed at the scheduled time.
- From the box to the left, select the interval for each reoccurrence of the task, e.g., hourly, daily, etc.
- In the fields to the right, enter the start date for the task and define the interval, e.g., every 5 hours, or every 5 days, between each subsequent backup. The options available here depend on the type of interval selected.
- Click on “Save” to confirm the scheduler definition.
 - The new task is added to the scheduler.
- With the “Execute now” button, a backup of the database according to the data entered (days and backup path) is created immediately.

5.5.2 Cleanup of the database table

This scheduler task performs a cleanup, i.e., deletion, of old table entries in the database, thereby releasing space. Currently, only data in the bookings database table can be selected for cleanup. The bookings database table records all system activity such as denied entries and permitted entries (see chapter “5.3 Bookings”).

NOTE! Booking data that has already been transferred to the access control software (e.g., GAT Matrix) remains available in the access control software after the bookings are deleted in GAT ACE 7000.

Figure 5.43 – Scheduling an automatic cleanup of a database table

- In the “Table” field, select “Booking” from the menu.
 - NOTE!** This is currently the only option available for this scheduler task.
- In the “Older than days” field, enter the number of days after which the database table entries will be deleted. For example, in Figure 5.43, all entries older than 30 days will be deleted.
- Click on the “Is Enabled” option to enable (field is marked) or disable (field is unmarked) the task.
 - NOTE!** A disabled task remains saved in the schedule but is not executed at the scheduled time.
- From the box to the left, select the interval for each reoccurrence of the task, e.g., hourly, daily, etc.
- In the fields to the right, enter the start date for the task and define the interval, e.g., every 5 hours, or every 5 days, between each subsequent task. The options available here depend on the type of interval selected.
- Click on “Save” to confirm the scheduler definition.
 - The new task is added to the scheduler.
- With the “Execute now” button, a cleanup of the database table according to the data entered is performed immediately.

5.5.3 Cleanup of the door controller backups

This scheduler task performs a cleanup (i.e., deletion) of old door controller backups in the database, thereby releasing space. Before each update or change to a controller's configuration, a backup of the current configuration is performed by GAT ACE 7000, which allows you to restore a controller to a previous configuration (see chapter "5.2.5 Backup and restore a controller configuration").

NOTE! Backups with a comment are not deleted, even if they are older than the set value.

Figure 5.44 – Scheduling an automatic cleanup of the door controller backups

- In the “Keep at least (x) backups” field, define the minimum number of door controller backups to keep in the database. For example, in Figure 5.44, at least 5 backups will always be kept even if they are older than the value defined in the “Older than (x) days” field.
- In the “Older than (x) days” field, enter the number of days after which the door controller backups will be deleted. For example, in Figure 5.44, all entries older than 30 days will be deleted provided the number of backups is more that the value defined in the “Keep at least (x) backups” field.
- Click on the “Is Enabled” option to enable (field is marked) or disable (field is unmarked) the task.
NOTE! A disabled task remains saved in the schedule but is not executed at the scheduled time.
- From the box to the left, select the interval for each reoccurrence of the task, e.g., hourly, daily, etc.
- In the fields to the right, enter the start date for the task and define the interval, e.g., every 5 hours, or every 5 days, between each subsequent task. The options available here depend on the type of interval selected.
- Click on “Save” to confirm the scheduler definition.
 - The new task is added to the scheduler.
- With the “Execute now” button, a cleanup of the door controller backups according to the data entered is performed immediately.

5.6 Help functions

The “Help” menu contains links to useful information, software support, and a diagnostics tool for analyzing log data. The following icons are displayed in the taskbar.



Figure 5.45 – Help menu

5.6.1 Show Manual

This function opens a Windows Explorer directory where the user manuals for GAT ACE 7000 (PDF) are located. Double-click on the desired user manual to open it in Adobe Reader.

5.6.2 Quick Support

This function opens “TeamViewer”, a software program that allows other people to access your computer desktop. TeamViewer is very useful if you encounter a problem while operating GAT ACE 7000 and need assistance from the GANTNER Support Team. Via TeamViewer, the Support Team can remotely view your PC configuration to identify and resolve the issue.

Proceed as follows when you are prompted to start a TeamViewer session.

- ▶ Click on “Quick Support” in the “Help” menu of GAT ACE 7000.
 - The following window opens.



Figure 5.46 – Quick Support window

- ▶ Give the Support Team your ID number (“Your ID”).
 - Your PC desktop is shared only when the Support Team logs in to TeamViewer with your ID number.

- If you close TeamViewer via the “X” or “Cancel” buttons, the remote session with the Support Team is aborted and they no longer have access to your PC.

The configuration settings for the TeamViewer session, e.g., the video or audio settings, can be viewed and changed by clicking on the settings icon (⚙️). There are three configuration options in the “TeamViewer Settings” window:

- General: Enable event logging recording. Network settings – configure the proxy settings.
- Audio conference: Settings for audio output and voice input, e.g., for microphone use.
- Video: Settings for video transmission, e.g., via a webcam.

Please refer to the TeamViewer website for more information about configuring and operating the software.

5.6.3 Diagnostics

GAT ACE 7000 records all important events and access activity in log files. The “Diagnostics” help function allows you to evaluate the log files and, if required, to save them in a package and send them to GANTNER or your partner for further evaluation.

- Click on “Diagnostics” in the “Help” menu of GAT ACE 7000.
 - The diagnostics window opens, which is empty after opening for the first time.
- In the upper-left menu, select a “collection” of log files to display. Select between “GAT ACE service” for the service log files and “GAT ACE” for the GAT ACE 7000 Viewer log files.
 - All log files that are included in the collection are listed in the left column.
- Double-click on a log file in the list.
 - The entries in the log file are displayed in the main window. If multiple log files are opened, they can be selected via tabs.

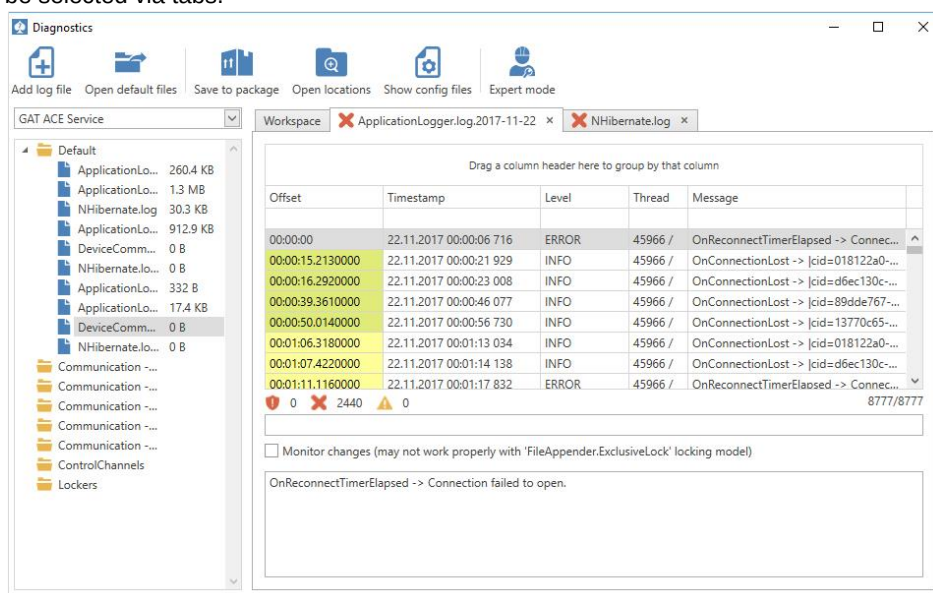


Figure 5.47 – Diagnostics tool for evaluating log files

- ▶ Right-click onto a log file entry.
 - The following pop-up window opens with various settings.

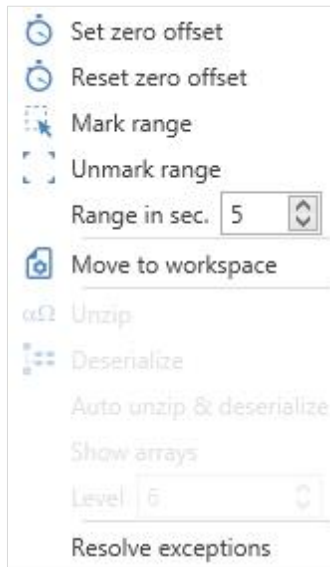


Figure 5.48 – Diagnostics settings

- ▶ The options in this menu allow you to filter the display of the log files according to time. You can also reset the time reference point (= green marker in the log entries) by which the log files are calculated for display.
- ▶ To open all commonly used log files at once, click on “Open default files” in the taskbar.
- ▶ To send log files to a specific location for analysis, click on “Save to package” in the taskbar. The log files are compressed into a ZIP file and sent directly via email. After selecting this taskbar option, you can select whether to send only the files displayed in the log list or all files.
- ▶ The “Open locations” taskbar option opens Windows File Manager and the folder where you will find the log files.
- ▶ For some log files, e.g., “Communication – ConfiguratorInterface” and “Communication – MatrixInterface”, the log entries are stored in packaged form. To read these files, you can use the “Expert mode” taskbar option for which a password is required for security reasons.

5.7 Troubleshooting

5.7.1 VPN Connection Problem

A problem can occur in GAT ACE 7000 when trying to establish a connection to the server via a virtual private network (VPN). This is due to the packet size of the interface being set too large, so that with VPN or VLAN connections, the packet size allowed by the router is exceeded.

Reducing the server's maximum transmission unit (MTU) value so that the maximum packet size of the VPN is not exceeded can assist to solve the problem. Complete the following steps:

- Click on the Start button and enter `command` in the search box at the bottom of the Start Menu and then click Command Prompt when it appears in the results.
- Display the current network settings by entering the following command into Command Prompt:

```
netsh interface ipv4 show subinterface
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh interface ipv4 show subinterface
```

MTU	MediaSenseState	Bytes In	Bytes Out	Interface
4294967295		1	0	503424 Loopback Pseudo-Interface 1
1500	1	1987541724	42923187	GEA
1500	1	54217789	18272722	Test

Figure 5.49 – Displaying network settings

- Reduce the MTU value of the applicable network interface to 1280 bytes:
`netsh interface ipv4 set subinterface "test" mtu = 1280 store = persistent`

NOTE! Replace "test" with the name of the applicable interface.

```
C:\Windows\system32>netsh interface ipv4 show subinterface
```

MTU	MediaSenseState	Bytes In	Bytes Out	Interface
4294967295		1	0	503424 Loopback Pseudo-Interface 1
1500	1	1990884393	42951208	GEA
1500	1	54319452	18293947	Test

```
C:\Windows\system32>netsh interface ipv4 set subinterface "Test" mtu=1280 store=persistent
OK.

C:\Windows\system32>netsh interface ipv4 show subinterface
```

MTU	MediaSenseState	Bytes In	Bytes Out	Interface
4294967295		1	0	507528 Loopback Pseudo-Interface 1
1500	1	1990281193	42973554	GEA
1280	1	54331964	18299836	Test

Figure 5.50 – Reducing the MTU value

- Check to confirm that the MTU value has been reduced by entering:
`netsh interface ipv4 show subinterface`
- Finally, connect to GAT ACE 7000 via a VPN to confirm that this now operates as expected.

6 AUTHORIZATION MANAGEMENT

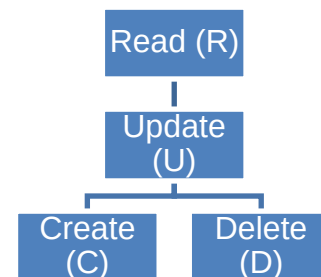
GAT ACE 7000 offers the possibility to assign individual users with different levels of system control. This is done using a “role” based access system. Each user is assigned to a role with the user's control in the system inherited from this role. A role represents a collection of permissions that allow the user to modify certain functions within the application. Furthermore, the system allows overriding of the permissions at user-level.

6.1 Function blocks

A function block is a group of basic actions in GAT ACE 7000 (e.g., manage device settings, manage database settings, manage anti-passback zones) for which the permission to modify can be granted instantly. Depending on the function block, the permission to Read (R), Update (U), Create (C), Delete (D), Execute (E), and Grant (G) can be assigned to system users.

An example of this is the “Manage device settings” function block for which RUCD permissions can be assigned. It is therefore possible that some users are only allowed to view the device settings but not modify them, while other users are allowed to view and modify the device settings.

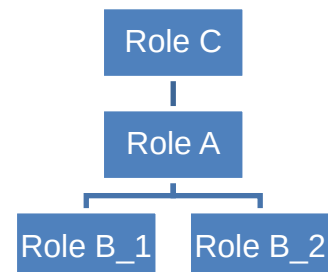
The RUCD permissions are organised in a hierarchical way. This means that it is not possible to assign Update permission without having Read permission. The diagram to the right shows the hierarchy of access levels.



The “User Management” and “Role Management” function blocks are assigned to allow users to manage users and roles.

In addition to RUCD and Execute permissions, Grant (G) permission can also be assigned. Grant permission allows the user to assign their permission for a certain function block to another user. To achieve this, the user must have Grant permission for the function block. Users who are assigned function block permission from another user become a child role of the user granting permission.

The diagram to the right represents a permission hierarchy. The user in Role A has Grant permission for a certain function block and is allowed to assign this permission on to Roles B_1 and B_2. The maximum permissions that can be passed on are the permissions currently assigned to Role A. For example, RUCD permissions cannot be assigned if Role A only has RU permissions.



6.2 Role management

A role represents a collection of permissions for the function blocks defined in the software. Roles are organized in a hierarchical way. Each role is derived from a single parent role and can have multiple subordinate roles. The hierarchical structure defines who is allowed to manage which roles and, therefore, which users. Users of a role can only manage descendant roles and the users of these roles (provided the user has been assigned “User Management” and “Role Management” permission).

GAT ACE 7000 starts with one superior role called the SYSTEM role. The SYSTEM role contains exactly one user, the SYSTEM user who is allowed to do anything within the application. Each subsequent role is a descendant of the SYSTEM role.

The maximum rights a role can have are the rights of its parent role. Removing a right from a parent role also deletes the right from all descendant roles.

- To define a new role, open the “Roles and User Management” page in the software settings menu.
 - The “Roles and User Management” settings page opens.

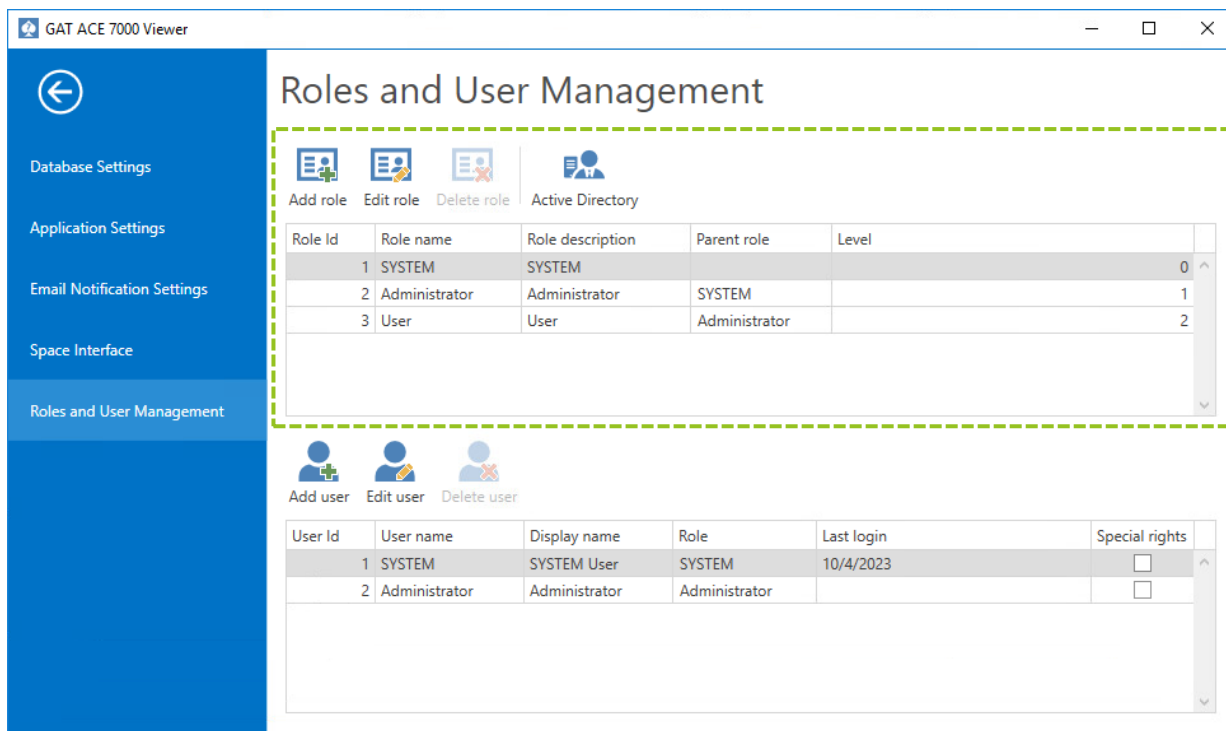


Figure 6.1 – Roles overview

- Click on “Add role” to define a new role.
 - The “Edit role” window opens in which the role settings are defined.

Name	C	R	U	D	E	G
GAT ACE 7000 Viewer						
Devices Management	☐	☒	☐	☐	☒	☐
Database Management	☒	☒	☒	☒	☒	☐
Application Management	☒	☒	☒	☒	☒	☐
Communication Management	☐	☐	☐	☐	☒	☐
Locations Management	☐	☒	☐	☐	☒	☐
Scheduler Management	☐	☒	☐	☐	☒	☐
Role management	☐	☐	☐	☐	☒	☐
User management	☐	☐	☐	☐	☒	☐

Role Id 4

Figure 6.2 - Role settings (for "SYSTEM" user)

- ▶ In the "Parent role" field, enter a parent role from which the new role inherits.
NOTE! You can only select a role from the same level or lower level as your current role, which was used to log in to GAT ACE 7000 Viewer.
- ▶ Enter a name for the new role in the "Role name" field. Each role must have a unique name.
- ▶ Enter a brief description of the role in the "Role description" field.
- ▶ Assign individual permissions for the role by marking/unmarking the function block boxes.

Depending on the selected parent role, different permissions are available to assign to the selected role. In the figure above, it is possible to assign permissions for every function available in GAT ACE 7000. This is because the logged-in user is the SYSTEM user who has grant permission for every function block. Clicking on the option boxes next to the functions define the permissions assigned to each function. The definition for each column is as follows:

- C: "Create" permission - Generate new data records for the function
- R: "Read" permission - Display data records for the function
- U: "Update" permission - Changing existing data records for the function
- D: "Delete" permission - Deleting data records for the function
- E: "Executing" permission - Execute actions concerning the function
- G: "Grant" permission - Passing on the permissions of this function to other users

The Role ID is calculated automatically and is only relevant when external applications are used.

6.3 User management

Each user in GAT ACE 7000 has their own user account. The user accounts are secured by a unique username and password, thereby preventing users from inappropriately logging into another user's account. Every user in GAT ACE 7000 must be assigned to exactly one role (see "6.2. Role management"). It is not possible to have a user who is not assigned to a role. The user inherits their system functionality and permissions from their role.

There is also the possibility to explicitly override role permissions at the user level for individual function blocks. These user permissions are retained even if the permission is changed at the role level.

- To define a new role, open the "Roles and Users" page in the system settings menu.
 - The "Roles and Users" settings page opens.

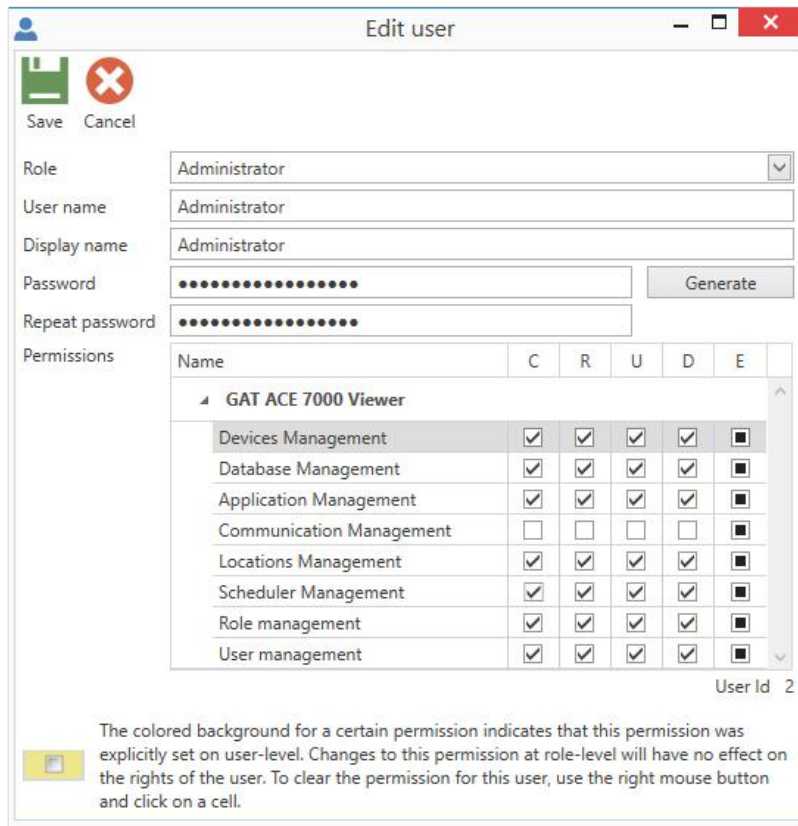
Role Id	Role name	Role description	Parent role	Level
1	SYSTEM	SYSTEM		0
2	Administrator	Administrator	SYSTEM	1
3	User	User	Administrator	2

User Id	User name	Display name	Role	Last login	Special rights
1	SYSTEM	SYSTEM User	SYSTEM	10/4/2023	☐
2	Administrator	Administrator	Administrator		☐

Figure 6.3 – Users overview

Listed at the bottom of the page are all the current user accounts. The figure above shows the default users, which are included with GAT ACE 7000, as described in section "6.3.2. Default users". To edit a user account, select the user from the list and click on the "Edit user" icon.

- To create a new user, click on "Add user".
 - The "Edit user" window opens.



Edit user

Save Cancel

Role: Administrator

User name: Administrator

Display name: Administrator

Password: Generate

Repeat password:

Name	C	R	U	D	E
GAT ACE 7000 Viewer					
Devices Management	☒	☒	☒	☒	☐
Database Management	☒	☒	☒	☒	☐
Application Management	☒	☒	☒	☒	☐
Communication Management	☐	☐	☐	☐	☐
Locations Management	☒	☒	☒	☒	☐
Scheduler Management	☒	☒	☒	☒	☐
Role management	☒	☒	☒	☒	☐
User management	☒	☒	☒	☒	☐

User Id 2

The colored background for a certain permission indicates that this permission was explicitly set on user-level. Changes to this permission at role-level will have no effect on the rights of the user. To clear the permission for this user, use the right mouse button and click on a cell.

Figure 6.4 - User settings (for "Administrator" role)

- ▶ In the "Role" field, assign a role to the user from the drop-down menu.
 - The user's authorization to use specific functions is directly linked to the selected role.
- ▶ Enter a unique name for the user in the "Username" field. The user will use this name to log in.
- ▶ In the "Display name" field, enter a display name for the user. GAT ACE 7000 uses this name to represent the user in the application, e.g., in the log files.
- ▶ Enter a password for the user. This must be entered twice for verification.

NOTE! Use a strong password. The password must be at least 7 characters long and contain at least one uppercase letter, one lower case letter, and one number. Click on "Generate" to automatically generate a strong password.

- ▶ If desired, role permissions can be overridden by explicitly setting user permissions in the table.
 - Permissions that are set explicitly on user level are marked with an ochre background. For example, in Figure 6.4 the create ("C"), read ("R") and change ("C") permissions for the "Database Settings" function blocks have been explicitly assigned for the user and will override the inherited settings from the selected "User" role.
- ▶ To revoke set permissions, right-click on the appropriate fields.

6.3.1 Active Directory

An Active Directory (AD) domain controller authenticates and authorizes all users and computers in a Windows domain network. When a user logs in to a computer that is part of a Windows domain, the Active Directory checks the login details to confirm their validity.

GAT ACE 7000 allows users to log in to the application using their Windows login details (username and password). The following window opens after clicking on the “Active Directory” icon.



Figure 6.5 - Active Directory settings window

- Enable external authentication: Select this option to enable the Active Directory function.
- Prefer external authentication: If this option is not enabled, GAT ACE 7000 uses local authentications first and only if none can be found, uses the Active Directory.
- Server type: Select the location of the Active Directory.
 - Machine: Select this option to use the authentication system from the local Windows machine. The “Test connection” button scans the PC and displays the groups and users that can be used for authentication. It is not necessary to configure these lists any further.
 - Domain: Select this option to use an Active Directory located on a server. Enter the “domain” and “container” details (see Figure 6.5), and then press “Test connection” to display the groups and users that can be used for authentication.

6.3.2 Default users

After installing GAT ACE 7000, the following default user accounts are available.

User:	SYSTEM	Administrator
Role:	SYSTEM	Administrator
Password:	GAT	Mirone59

NOTE! Immediately after installing GAT ACE 7000, change the passwords of the default users to new and secure passwords to maintain security. Keep the passwords in a secure place, protected against unauthorized use.

Access rights for the "SYSTEM" role

Name	Create	Read	Update	Delete	Execute	Grant
Device settings management	X	X	X	X	-	X
Database settings management	X	X	X	X	-	X
Application settings management	X	X	X	X	-	X
Communications settings management	X	X	X	X	-	X
Site management	X	X	X	X	-	X
Scheduler management	X	X	X	X	-	X
Role management	X	X	X	X	-	X
User management	X	X	X	X	-	X

X ... granted
O ... denied
- ... not available

Access rights for the "Administrator" role

Name	Create	Read	Update	Delete	Execute	Grant
Device settings management	X	X	X	X	-	X
Database settings management	X	X	X	X	-	X
Application settings management	X	X	X	X	-	X
Communications settings management	O	O	O	O	-	O
Site management	X	X	X	X	-	X
Scheduler management	X	X	X	X	-	X
Role management	X	X	X	X	-	X
User management	X	X	X	X	-	X

X ... granted
O ... denied
- ... not available

Access rights for the "User" role

Name	Create	Read	Update	Delete	Execute	Grant
Device settings management	O	X	O	O	-	O
Database settings management	O	O	O	O	-	O
Application settings management	O	O	O	O	-	O
Communications settings management	O	O	O	O	-	O
Site management	X	X	X	X	-	X
Scheduler management	O	X	O	O	-	O
Role management	O	O	O	O	-	O
User management	O	O	O	O	-	O

X ... granted
O ... denied
- ... not available

7 DATA PROTECTION

7.1 General Data Protection Regulation (GDPR)

As of May 25 2018, the EU's General Data Protection Regulation (GDPR) will apply. The new regulations affect all companies that process personal data. The GDPR regulates the handling of personal data and specifies the conditions under which companies may process this data (e.g., employee data). The GDPR affects single-person companies as well as large companies.

The content of the GDPR is based upon seven principles that can be used to orientate data protection efforts. These are:

- Principle of Storage Limitation
- Principle of Data Minimization
- Principle of Purpose Limitation
- Principle of Accuracy
- Principle of Integrity and Confidentiality
- Principle of Accountability
- Principle of Lawfulness, Fairness, and Transparency

Definitions of Personal Data and Data Processing

Personal data includes all data that directly or indirectly allows you to draw conclusions about a specific person, e.g., email, name, photo, etc. Sensitive personal data is personal data that is particularly worthy of protection, e.g., biometric and genetic data. However, information on ethnic origin, political opinion, trade union membership, religious or philosophical beliefs, health, and sexuality are also considered sensitive.

Data processing means the viewing and saving of data as well as any automated or manual form of processing. A data application exists when personal data is fully or partially automated.

It is therefore clear from these definitions that the GDPR is relevant for GANTNER's access control software. The following sections outline what has to be done with regard to access control and what options GAT ACE 7000 offers. The instructions are summarized in the following sections.

7.1.1 Perform an inventory analysis

Check which data in your access control system is recorded and saved. Inquire about the purpose for which the data is needed, how long it is stored, and who has access to it. Also, check whether the data is being shared externally with anyone.

Access control can often work with only a name (which could also be anonymized) and an ID number. However, sometimes additional fields, e.g., a PIN code, are included in order to ensure greater security. Additional information, stored in optional fields for example, are not directly relevant to the access control decision. In these instances, it is necessary to check whether this data needs to be stored in the software system.

7.1.2 Create a processing directory

After completing the inventory analysis, a processing directory must be created. The processing directory is one of the key innovations of the GDPR and replaces the current data processing messages. Among other things, it must include the names and contact details of the persons responsible, the purpose of the data processing (access control), the categories of persons concerned and personal data, the categories of recipients, and the description of the data security measures.

The category of persons concerned are normally employees. In exceptional cases, suppliers or customers can also be managed by the access control system.

In access control, GANTNER has paid attention to the **Principle of Data Minimization** and the **Principle of Purpose Limitation**. Only data that is necessary for the operation of the systems is stored. Essentially, an ID number, which is used as an identification feature, and the name of the person are stored. Other data, e.g., a PIN code, personnel number, or balances, is optional and serves to increase security or to provide convenience. By default, no sensitive data is stored in the systems. The exception, however, is when fingerprints are used in the system. This data is biometric data.

The access control data is normally not passed on to other systems.

The **Principle of Accuracy** of the data must be in the interest of the system operator, since in the end, the security of the company or the accounting for personnel expenditure depend on it. The **Principle of Integrity and Confidentiality** of the data is ensured by allowing only authorized persons to access the software and by limiting the software users to access only the data needed to perform their tasks (see chapter “6.3. User management”).

7.1.3 Data protection impact assessment

A data protection impact assessment is normally not required because there is no high risk to the rights and freedoms of natural persons. Known technologies are used and there are no systematic evaluations and assessments of personal aspects. If using fingerprints, an individual consideration for each situation is recommended.

7.1.4 Comply with information requirements and declarations of consent

Persons affected by data processing must be able to be informed about this (what, who, for what purpose, how long, where?). Likewise, data subject rights (e.g., information, deletion) must be met promptly, i.e., within one month at the latest.

The consent of persons for the use of the personal data for the purposes of access control and time recording should be defined in a service contract or works agreement. This will ensure the **Principle of Lawfulness, Fairness and Transparency** is upheld.

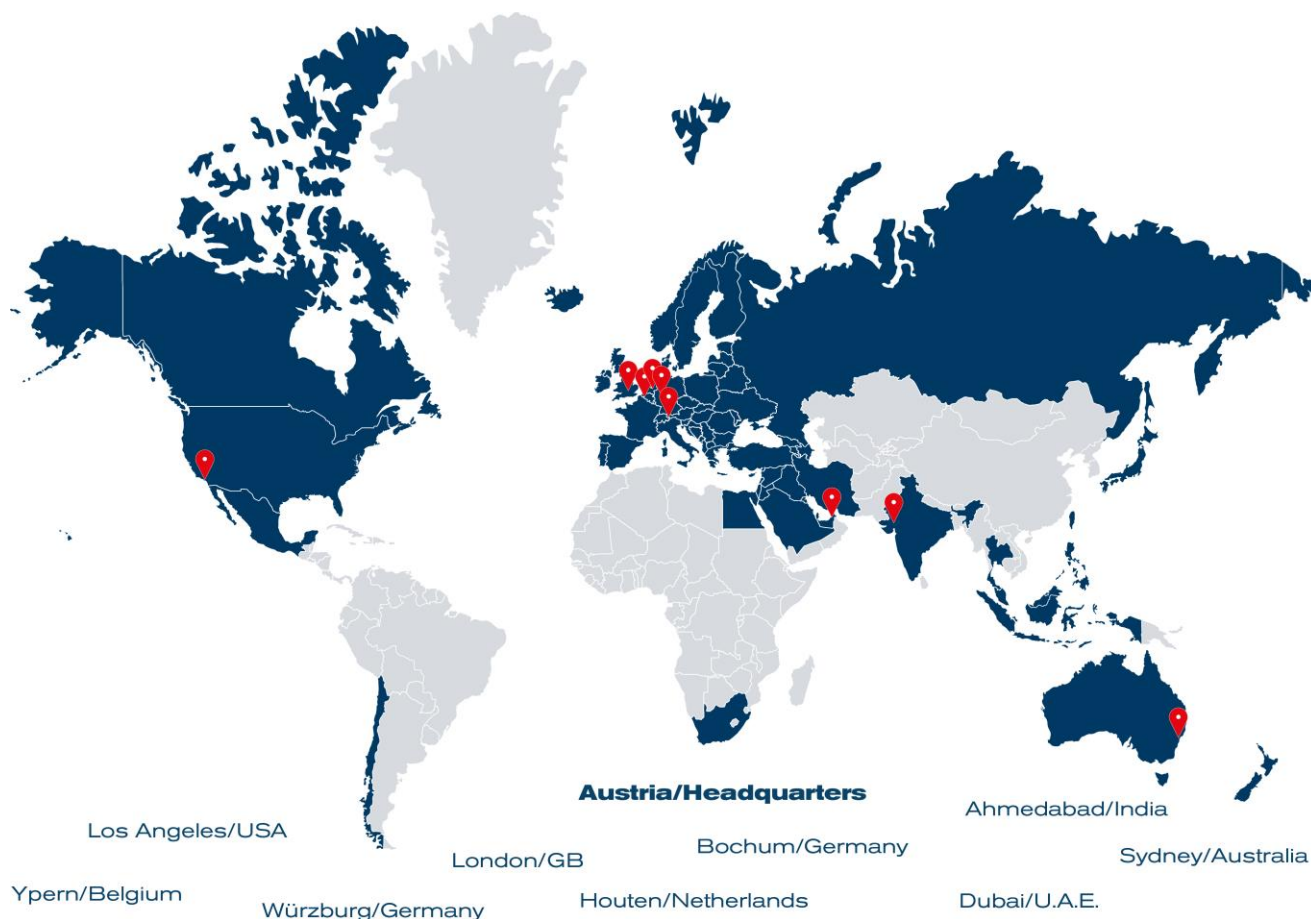
The data storage period depends on the requirements for access traceability as well as the present/absent bookings that you need in your company. By deleting data, the **Principle of Storage Limitation** can be met (see chapter "5.5.2. Cleanup of the database table").

If you have designated a data protection policy leader in your company, fulfilled the legal framework, taken technical and organizational measures, and created the documentation, you can also comply with the **Principle of Accountability** and are well prepared for meeting the GDPR.

In summary, we would like to point out that with GAT ACE 7000 version 1.5 or later you can easily comply with the GDPR. Please do not hesitate to contact your sales representative if you have any questions or concerns.

Note:

This manual is valid as of October 9th, 2023. It is subject to change.
Amendments and changes can be made without prior notice at any time.
The information in this manual is valid for GAT ACE 7000 version 2.2.0.



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