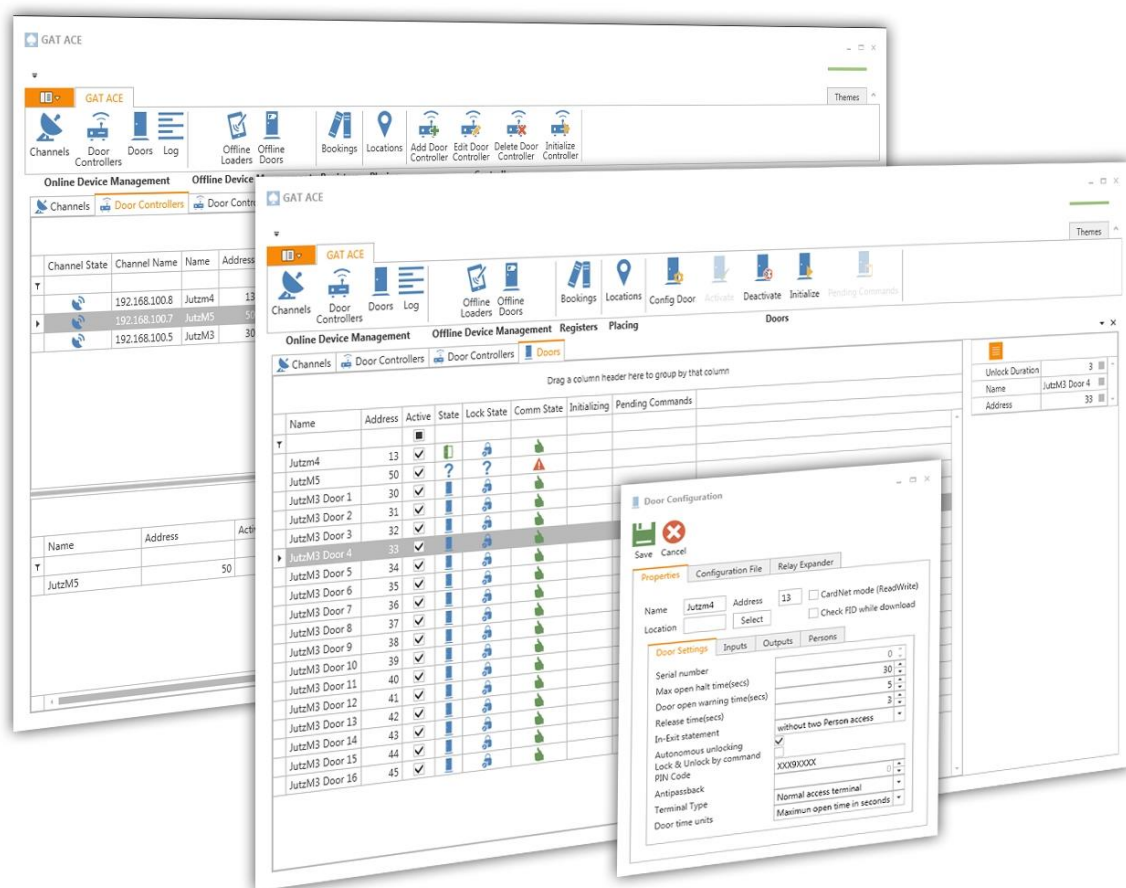


GAT ACE 3000

Middleware for Access Control by GANTNER Electronic GmbH



© Copyright 2019 by 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 this product or for general enquiries is listed below:

Contact address of manufacturer

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



General Warning and Safety Instructions

Dear Customer,

We congratulate you on having selected a product (appliance or software) from GANTNER Electronic GmbH. Our aim is to ensure that our product operates with safety and to your complete satisfaction. To achieve this aim we take this opportunity to familiarize you with the following guidelines:

1. Installation, commissioning, operation and maintenance of the purchased product must be carried out in accordance with the instructions, i.e., in accordance with the technical conditions of operation as described in the corresponding product documentation.
2. Before installation, commissioning, operation or maintenance it is therefore essential that you read the corresponding chapter of this manual and observe its instructions.
3. If there are still some points on which you are not entirely clear, please do not take a chance. All queries can be clarified by your Gantner company representative, or by ringing the GANTNER Electronic GmbH 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. Also 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. In this case, contact your Gantner company representative. They will make every effort to resolve the problem as quickly as possible.
7. Installation, commissioning and servicing of our appliances must only be carried out by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Here, the appropriate installation provisions in accordance with the relevant national Electrical Engineers construction regulations (e.g., ÖVE, [Austrian] VDE, [German]...) must be observed.
8. Where not otherwise stated, installation and maintenance work on our appliances must be carried out when disconnected from the power supply. This applies in particular to appliances which are normally supplied by low-voltage current.
9. It is prohibited to make alterations to the appliances or to remove protective shields and covers.
10. Do not attempt yourself to repair an appliance after a defect, failure or damage, or to put it back into operation again. In such cases, it is essential you contact either your Gantner company representative or the GANTNER Electronic GmbH hotline.
11. GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.
12. Although every 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, and we may carry out alterations at any time without giving prior notice.
13. Should you discover any fault with the product or in its accompanying documentation, or have any suggestions for improvement, you may confidently approach either your Gantner company 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.

TABLE OF 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 3000	9
1.5	Supported Devices	9
1.6	Terminology	11
2	INSTALLATION	15
2.1	Hardware Requirements	15
2.1.1	Configuration Example One	15
2.1.2	Configuration Example Two	15
2.1.3	Configuration Example Three	16
2.2	Software Requirements	17
2.2.1	Supported Operating Systems for GAT ACE	17
2.2.2	Database Server	17
2.2.3	Microsoft .NET Framework	18
2.3	Installation of GAT ACE 3000	18
2.3.1	Installation of Microsoft SQL Server 2016 Express	18
2.3.2	Installation of GAT ACE 3000	23
2.3.3	Windows Services Settings	26
2.4	Switching from GAT Manager to GAT ACE	27
2.5	Updating GAT ACE	27
3	STARTING GAT ACE 3000	29
3.1	Startup	29
3.1.1	GAT ACE 3000 Service	29
3.1.2	Database Settings	30
3.1.3	Login Window	31
4	CONFIGURATION	33
4.1	"User Settings" Page	34
4.2	"Roles and Users" Settings Page	35
4.3	"Anti-Pass-Back Areas" Settings Page	36
4.4	"Application Settings" Page	39
4.5	"Card and Reader Settings" Page	42
4.6	"Database Settings" Page	46
4.7	"Communication Settings" Page	48
4.8	"Time Bookings Exporting Settings" Settings Page	50
4.9	"Diagnostics" Settings Page	52
5	OPERATION	55
5.1	Functional Overview of GAT ACE	55
5.1.1	Channels	58
5.1.2	Door Controllers	58
5.1.3	Doors	59
5.1.4	Reader Configuration	60
5.1.5	Offline Doors	60
5.1.6	Scheduler	62
5.1.7	Bookings	62
5.1.8	Locations	63

5.1.9 Card Settings	63
5.1.10 Anti-Pass-Back Areas	63
5.1.11 Evaluating Log Files	64
5.2 Configuring an Access System	65
5.2.1 Defining a Communication Channel	65
5.2.2 Structuring Locations	69
5.2.3 Adding a Controller	71
5.2.4 Configuring a Controller	73
5.2.5 Configuring and Assigning a Reader to a Controller	74
5.2.6 WiNET Settings for Offline Controllers	75
5.2.7 Configuring the Time Settings for Readers	77
5.2.8 Configuring a Longrange Reader	78
5.2.9 Configuring Doors	79
5.2.10 Activating and Deactivating a Door	96
5.2.11 Initializing a Controller	96
5.2.12 Initializing Doors	97
5.2.13 Display Commands to be Sent	98
5.2.14 Offline Loaders and Offline Doors	99
5.2.15 Configuring Offline Loaders	99
5.2.16 Configuring an Offline Door	102
5.2.17 Initializing an Offline Door	104
5.2.18 Battery Warning for Offline Doors	104
5.3 Scheduler	106
5.3.1 SQL Database Backup	107
5.3.2 Cleanup of the Database Table	108
5.4 Evaluating Log Files	109
5.5 Bookings	110
5.6 Time & Attendance Terminals and Time Bookings	111
5.6.1 Time Device Settings	112
5.6.2 Time Bookings	116
6 AUTHORISATION MANAGEMENT	117
6.1 Function Blocks	117
6.2 Role Management	118
6.3 User Management	120
6.3.1 Default Users	122
7 MIGRATING GAT MANAGER TO GAT ACE	123
8 DATA PROTECTION	125
8.1 General Data Protection Regulation (GDPR)	125
8.1.1 Perform an Inventory Analysis	125
8.1.2 Create a Processing Directory	126
8.1.3 Data Protection Impact Assessment	126
8.1.4 Comply with Information Requirements and Declarations of Consent	126

1 INTRODUCTION

1.1 About this Manual

Chapter "1 INTRODUCTION" of this manual provides an overview of GAT ACE 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 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 and its additional components such as the .NET Framework and database.

Chapter "3. STARTING GAT ACE 3000" outlines the initial startup process of GAT ACE including how to complete the one-off configuration requirements such as establishing the database connection.

Chapter "4. CONFIGURATION" includes the general configuration settings for GAT ACE such as the database settings, the card and reader settings, and the role and user settings. These settings usually need only be defined once after installing GAT ACE, however, they can be accessed and adjusted at any time.

Chapter "5. OPERATION" describes the layout and how to use the interface of GAT ACE. In addition, the most important steps 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.

In Chapter "6 AUTHORISATION MANAGEMENT", information on the GAT ACE authorization 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) and employees of the facility can be assigned to the role of "Daily User" (who can access important functions in GAT ACE but cannot change the system configuration).

In chapter "7. MIGRATING GAT MANAGER TO GAT ACE", the licensing process, i.e., the licensing and activation of GAT ACE, is described. In addition, how to import a database from an existing GAT Manager access system to use in GAT ACE is available here.

Chapter "8. DATA PROTECTION" informs you about the new EU General Data Protection Regulation and how GAT ACE 3000 supports compliance with the requirements.

1.2 Formatting

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

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

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



The text accompanying this symbol contains interesting information relevant to the current section. It will help you to better understand the information in the section or provide interesting tips for the described device or software operation.

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

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

1.3 General Information

GAT ACE is a middleware application for configuring an access control system that includes 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 runs on a Microsoft Windows® operating system (see "2.2.1 Supported Operating Systems for GAT ACE").

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

GAT ACE consists of a Windows® service, which operates in the background and manages the communication requirements, and a graphical user interface that is used for system configuration and management of the service. As the user almost always interacts with the application via its graphical user interface, the term "GAT ACE" in this manual is widely used to refer to the user interface of GAT ACE 3000.

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. For this purpose, GANTNER provides GAT Matrix as an ideal partner to combine with GAT ACE. In addition, building management and monitoring systems can also operate effectively with GAT ACE.

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

1.4 Features of GAT ACE 3000

- Multilingual (English & German)
- Runs on all modern Windows operating systems (32- and 64-bit)
- Communication channels limited only by the hardware
- Communication via TCP/IP and RS-485
- 999 total devices per system
- Hardware configuration of the controller:
 - Function of the controller inputs
 - Function of the controller outputs
 - Configuration of connected peripheral devices
 - Setting of the reader
- Interface to GAT Matrix and other access management systems
- Rapid communication speeds with the controllers (parallelization) and management software
- Service runs without requiring user login
- Direction of movement recognized
- Special functions included (anti-passback function, repeated-access blocking, dual-person access, etc.)
- Harassment PIN code
- Controller initialization
- Setting of controller addresses
- Memory allocation
- Supports both online and offline controllers
- View access and time bookings
- Direct control of controller via commands
- Logging of events and communication

1.5 Supported Devices

All devices that are connected to and configured by GAT ACE must support the FLEX protocol by GANTNER Electronic GmbH. It is possible to use both online and offline terminals.

Currently GAT ACE supports the following GANTNER devices:

- GAT Terminal 3100 AK / PLUS / DUO / QUAD / ECO / WiNET
- GAT Terminal 3000
- GAT Terminal 2500 AB / AK
- GAT Terminal 1002 AB / AK
- GAT Control Module 04
- GAT SR 300 / 305 / 310 / 315 / 345 / 347 / 350 / 355 / 357
- GAT SR 7300 / 7305 / 7307 / 7310 / 7315 / 7317 / 7340 / 7345 / 7347 / 7350 / 7355 / 7357
- GAT SR 180

- GAT SR 380
- GAT SLR 300 / 310
- GAT SLR 7300 / 7307 / 7310 / 7317
- GAT SA 300 / 305
- GAT Reader 405 AP
- GAT Reader 500 UP
- GAT Reader 868 / 800 / 810 / 860 / 861 / 900
- GAT Reader 500 UB / 600 UB
- GAT SLA 500
- GAT Terminal 1015 Access AK / AB / AP
- GAT Terminal 1015 Access UK / UB / UP
- GAT Terminal 600 UB / UP
- GAT Terminal 605 UB / UP
- GAT Terminal 500 UB
- GAT ST 210
- GAT ST 220 / 225
- GAT DL 320 / 325 / 340 / 350 / 360 / 370
- TAC
- GAT REX 118 / GAT REX 118 RS485 / GAT IO 013 / GAT IO 054 / GAT IO 055

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 communication between GAT ACE and the device is possible.

Transferring data to offline devices is done using the following devices. Additional requirements to complete this process include the PC software GAT Config Manager or an SD card reader.

- GAT MT 010
- GAT DL 090
- GAT DL 092

Currently GAT ACE supports the following GANTNER devices with some restrictions:

- GAT Terminal 1015 Time AK / AB / AP
- GAT Terminal 1015 Time UK / UB / UP
- GAT Terminal 1022 AK / AB / AP
- GAT Terminal 1032 AK / AB / AP
- GAT ST 180 / 280 / 380 / 381 / 580
- GAT ST 290 / 390 / 590
- GAT ST 180 EVO / 380 EVO / 381 EVO
- GAT ST 390 EVO

1.6 Terminology

Some terms are frequently used in this manual. Please read the definition of these terms and remember their meaning.

Access Control Software

In this manual, this term describes software of a higher level than GAT ACE for the granting and administration of authorizations, e.g. the software package GAT Matrix offered by GANTNER Electronic GmbH.

User

In this manual, the term "user" describes the person operating GAT ACE. Several users can be created, each with a personal user name and a distinct password.

Person

In this manual, "person" describes the person using the access system. Every person holds a data carrier with a unique number. For every person (every data carrier) who (that) should have access, an individual data set must be created in the access control system (e.g. GAT Matrix). This staff 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 / Card

Data carriers, also called cards, are used for identification at readers connected to a controller. Depending on the reader unit used, various types of data carriers can be used, e.g. contactless cards (RFID) or magnetic and infrared cards. The contactless data carriers are available in various shapes, such as cards, key chains wristlets and for different kinds of identification systems (LEGIC, PROXY, MIFARE®, ISO 15693).

Controller / Terminal

The terms "controller" and "terminal" are used as synonyms in this manual and describe the units mounted at the doors and used to read the persons' data carriers, check the authorizations and electronically open and lock the doors accordingly. Controllers are available with integrated or separate readers. The controllers are configured and administrated in GAT ACE.

A distinction is made between online and offline controllers. Online controllers are equipped with a network interface, enabling their connection to a local network. Depending on the type of controller, both LAN networks (Ethernet) and serial RS-485 networks are possible. 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, or via corresponding data carriers or via radio signals.

Inputs / Outputs

Most controllers are equipped with one or more digital optocoupler inputs to identify the 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" is used in a general sense to describe the object to be controlled. In most cases, this will be a door within a room, where the access should be monitored. It is also possible to control and monitor a rolling gate or a driveway with an opening barrier. The principle of access control, i.e. the configuration in GAT ACE is identical in each of these cases.

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

Reader

One or several readers are connected to each controller or are installed on a permanent basis. At the readers, identification is performed with data carriers, the read data is transmitted to the controller, where the evaluation takes place. Depending on the model, data can also be written onto the carriers at the readers.

There are various reader models, e.g. separate reader units connected to the controller via reader or RS-485 interface or reader units integrated into the controllers, where the identification takes place directly at the controller. There is a further distinction made between close range readers and longrange readers, the latter enabling an identification at a distance of several meters.

Channel

GAT ACE communicates with the controllers via so-called channels. For every interface connection, a channel is defined, e.g. in a TCP/IP connection, every controller (every IP address) is connected via its own channel with settable parameters. In a serial RS-485 connection, several controllers using the same communication parameters may be connected to an interface (a channel).

CardNET

This term describes an offline controller operating mode. CardNET means that for the configuration of the terminals a programming device is used to configure the controllers on site. The authorizations of the persons are transferred via cards.

The authorization data of the persons for offline doors (controllers) can be sent by the access control software (e.g. GAT Matrix) to specific controllers within the access system. The data carriers of the persons can then be programmed directly at these controllers. The controllers must support the Read/Write or CardNet functionality. The data carrier must be suitable and prepared for this use.

WiNET

This term describes an offline controller operating mode.

WiNET means that the offline terminals are equipped with a radio connection, linking them to a controller. The configuration and authorizations are administrated via the radio network.

Schedule

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

Generally Open Schedule or Door Schedule

A Generally Open Schedule can be assigned to a controller and determines which controller functionalities should be active at what point in time. With a Generally Open Schedule, it is possible, for a certain period of time, to unlock a door, activate a special relay schedule or suppress alarms, without requiring a personal identification.

Staff Schedule

A staff schedule includes the definition of access authorizations for all days of a week, as well as for 5 types of special days. Staff schedules are assigned to the persons and controllers in the access control software and thus define the type of access authorization granted at each single controller.

Special Authorization

In the staff data set, a special authorization can be assigned to anyone. By configuring controller inputs and outputs accordingly, different functions can be executed depending on whether a person is granted a special authorization or not.

Possible functionalities for the special authorization are:

- The special relay is additionally activated in the event of identification with a special authorization. This can be used for example to control a second parking barrier.
- Authorization for a two-person access with master functionality.
- Access authorization at a controller using the controller keypad.
- Possibility of activating or deactivating the alarm system at a controller equipped with a control relay.

Double Check Principle

This functionality is also called "Two-Person Access". In order to gain access, two different valid identifications are required one after the other.

Anti-Pass-Back Functionality

If the "Anti-Pass-Back" option is activated, it is always required to access and leave in a logical combination, i.e. it is impossible to execute two access bookings without a leaving booking between them.

Repeated Access Barrier

If the "Repeated Access Barrier" option is activated, it is impossible to regain access at a door within a set timeframe, using the same data carrier. Once this timeframe is lapsed, it is again possible to gain access using the data carrier.

Attack PIN Code (=Duress Code)

Depending on the configuration and staff data, an access can require not only a valid identification via data carrier, but also the entry of a PIN code. In this case, it is possible to define a so-called attack PIN code (duress code) in addition. This code can be combined with the respective personal PIN code in order to trigger a covert attack alarm, if the door opening is obtained by force to allow unauthorized access.

Bookings

Whenever an event (e.g. identification of a person, alarm messages, etc.) occurs at a controller, it generates a booking into an internal booking log. These bookings can be read, saved and evaluated with 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 and the accompanying access control software, e.g., GAT Matrix.

2.1.1 Configuration Example One

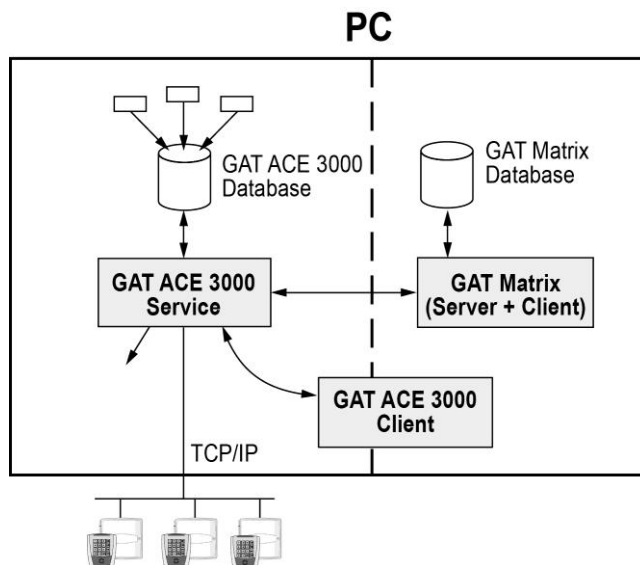


Figure 2.1 - Installation of GAT ACE and GAT Matrix on the same PC

2.1.2 Configuration Example Two

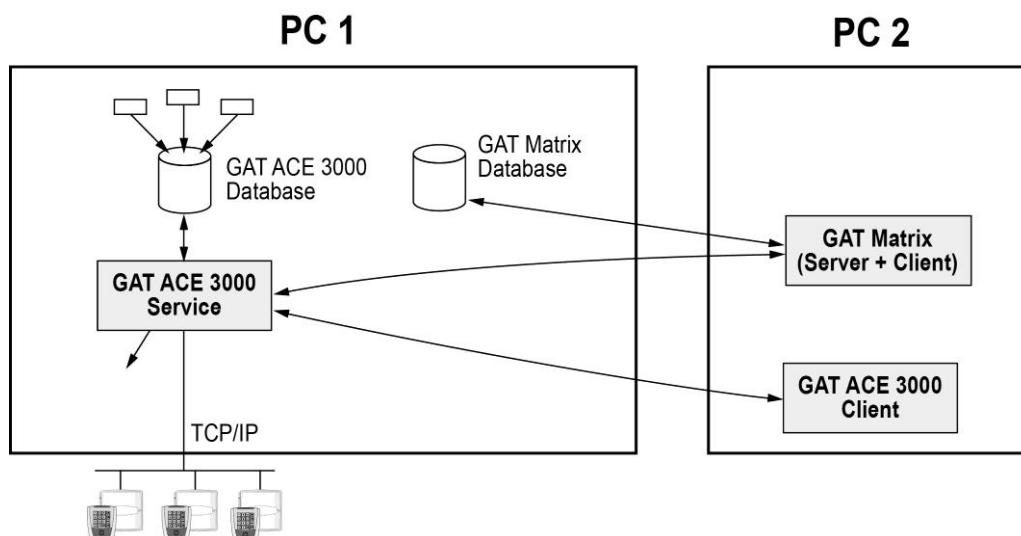


Figure 2.2 – Installation of GAT ACE and GAT Matrix on multiple PCs with GAT Matrix database on GAT ACE PC

2.1.3 Configuration Example Three

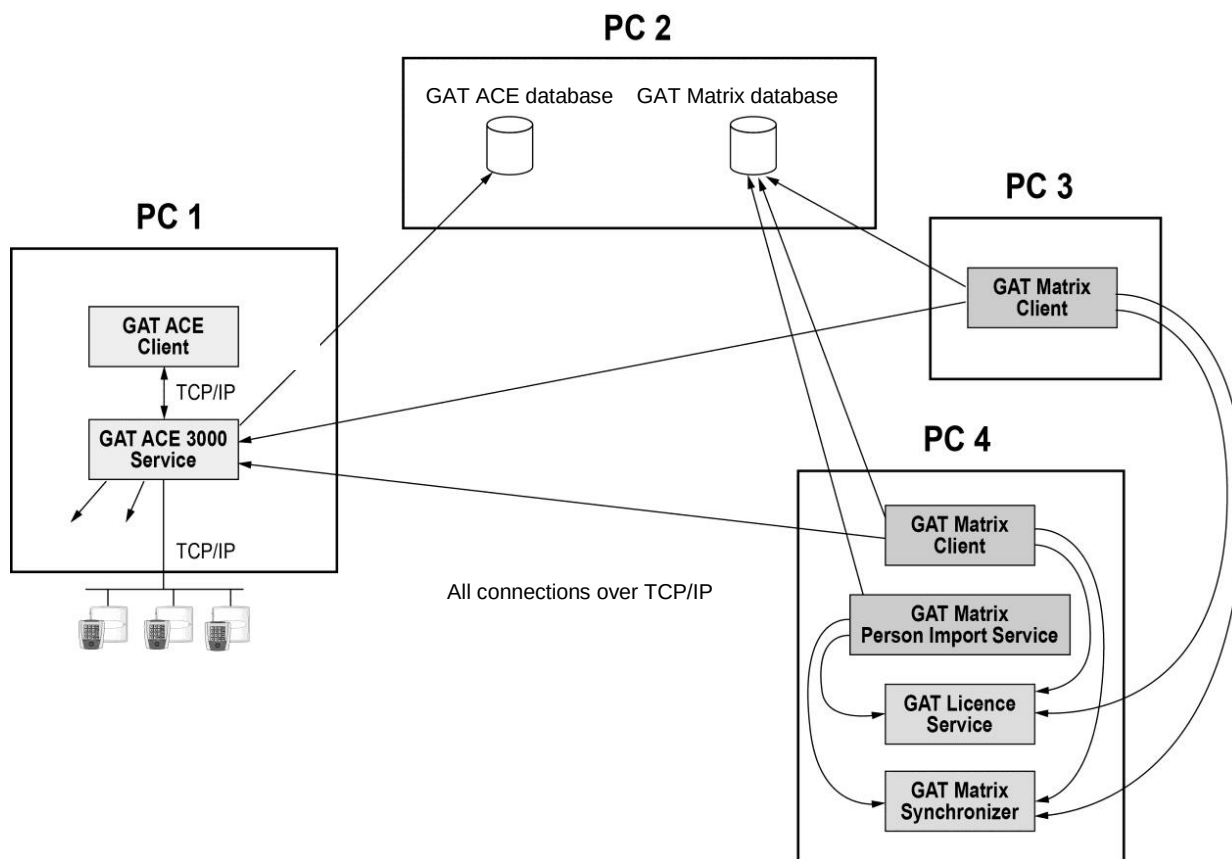


Figure 2.3 – Installation of GAT ACE and GAT Matrix on multiple PCs with GAT Matrix and GAT ACE databases on standalone PC

Hardware recommendations for PCs:

- IBM-compatible PC, for example, Core i5, 3 GHz or equivalent CPU.
- CD ROM drive
- 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. 2 GB for GAT ACE 3000
Additionally approx. 2 GB for Microsoft SQL Server Express
- Free hard drive: 20 GB (for protocol and configuration data)

The total minimum requirements for the PCs increases when more software is installed, e.g., GAT Matrix, GAT Mobile Access Management, GAT ACE 7000, etc. The requirements of these applications must be added to the values above. For further information, see the GAT Matrix manual.

2.2 Software Requirements

2.2.1 Supported Operating Systems for GAT ACE

- Microsoft® Windows® 7 (all except Home-Edition), 32- and 64-bit
- Microsoft® Windows® 8 (all except RT), 64-bit
- 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 R2 and 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 the GANTNER Support Team can only offer assistance when GAT ACE is installed on a German or English version of Windows. In addition, support can only be given when the customer provides all access authorizations required by the Support Team, e.g., access to the Windows account or the SQL database.

NOTE! The customer is responsible for providing any additional licenses required, 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® 2016 Express
- Microsoft® SQL Server® 2017

 The Microsoft® SQL Server® 2016 Express database can be downloaded from the partner page on the GANTNER homepage. The updated system requirements for Microsoft® SQL Server® 2016 Express are available via the following link: <https://technet.microsoft.com/en-en/library/ms143506.aspx>
From version 2016 onwards, Microsoft® SQL Server® is only available in 64-bit format.

NOTE! Please note that the GANTNER partner page only contains the free Microsoft® SQL Server® Express database. If a full version of 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 SQL download archive on the GANTNER partner page.



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/en-en/library/ms144228.aspx>).
- Automatic backups of the folder are not permitted.

2.2.3 Microsoft .NET Framework

For the operation of GAT ACE 3000, the .NET Framework 4.6.1 must be pre-installed.

2.3 Installation of GAT ACE 3000

This section describes the GAT ACE 3000 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 3000 by double-clicking the "Setup.exe" file in the installation package.

2.3.1 Installation of Microsoft SQL Server 2016 Express

An SQL database is required for GAT ACE 3000. If an SQL server is already available, the database can be installed on this server and the following section can be skipped. Otherwise, install Microsoft SQL Server 2016 Express as described on the following pages.

In the partner area on the GANTNER homepage, you can download Microsoft SQL Server 2016 Express for 64-bit operating systems.

NOTE!

- Microsoft SQL Server Management Studio is also included in the download archive. It is recommended to also install this application to ensure the optimal environment for the maintenance and service of GAT ACE.
- The installation program for Microsoft SQL Server 2016 Express is only available in English.
- This section describes the most important points for installing Microsoft SQL Server 2016 Express. MS SQL servers have many more configuration settings. To define these, MS SQL Server Management Studio Express is included on the GAT ACE installation CD. Contact your database administrator for advice on configuring these advanced settings.

- ▶ Log in to the partner area on the GANTNER homepage and download Microsoft SQL Server Express (menu "Products" -> "Software" -> "GAT ACE 3000").
- ▶ Extract the downloaded archive in a new folder.
- ▶ Start the setup process by running the extracted "Setup_x64.bat" file as administrator.

Attention: The Setup_x64.bat file includes all necessary presets and parameters for the installation. If the Setup_x64.bat file is not used, the required presets and parameters are not automatically inserted in the user interface during installation.

 - The installation program checks whether all prerequisites for the installation of the SQL server are met.
 1. .NET framework 3.5 must be installed.
 2. Microsoft Visual C++ 2015 x86 Redistributable must be installed.
 - If one of these software components is not found, a corresponding message is shown and the missing software can be automatically installed now.
 - If all prerequisites are met, the SQL Server 2016 Express installation wizard starts. This guides you through the installation process step by step.
- ▶ Confirm the license conditions by marking the "I accept the license terms" option and clicking on "Next >".
 - The "Setup Support Files" are installed then the following dialog opens. The individual installation steps are shown on the left and the installation settings are made in the middle.

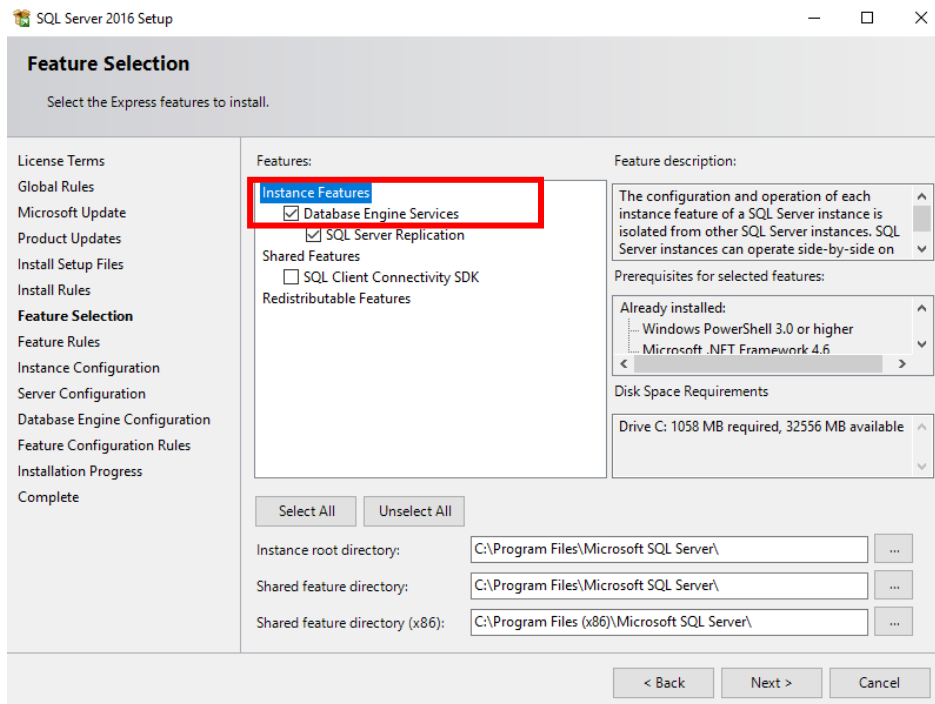


Figure 2.4 - Microsoft SQL Server 2016 Express – Option configuration

- ▶ The required options are pre-selected (see Figure 2.4).
- ▶ Click on "Next >" until the following window is shown ("Server Configuration").

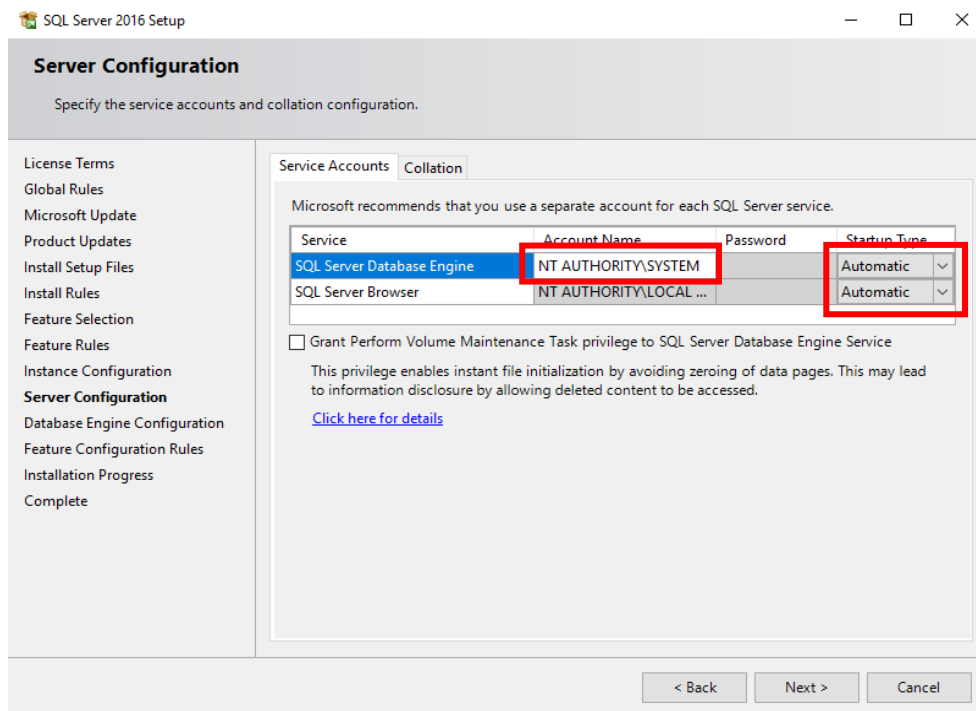


Figure 2.5 - Microsoft SQL Server 2014 Express – Server configuration

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

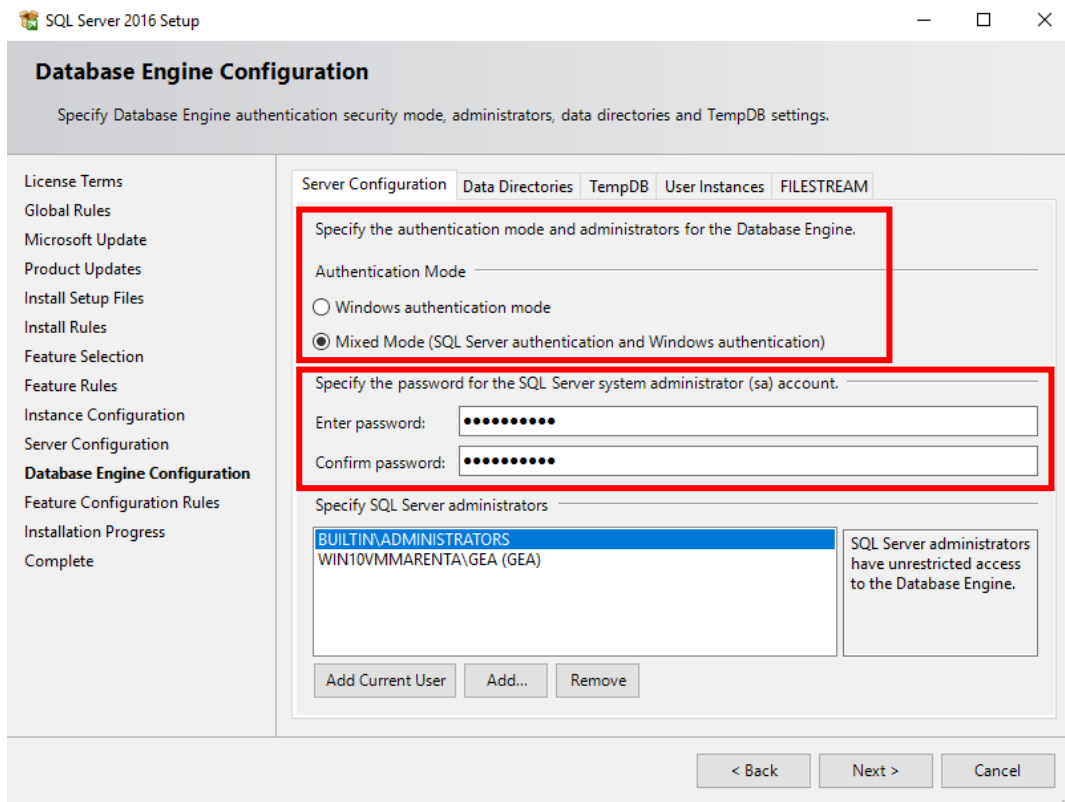


Figure 2.6 - Microsoft SQL Server 2016 Express - Database configuration

- ▶ The required options are pre-selected.
 - The password for the SQL administrator "sa" is entered automatically by the setup program (standard password = "GATMatrix1").
 - It is recommended to keep the standard password. In case you want to change the password, always use a strong password, i.e., at least 10 characters long and a combination of uppercase letters, lowercase letters, and numbers. Please follow your IT guidelines. Remember the password and keep it in a safe place. Without this password, no service access to the GAT ACE 3000 database is possible.
- ▶ Finally, keep clicking on "Next >" until the installation is complete.
 - The completed installation steps are indicated by green symbols and the status "Succeeded" in the final installation window.

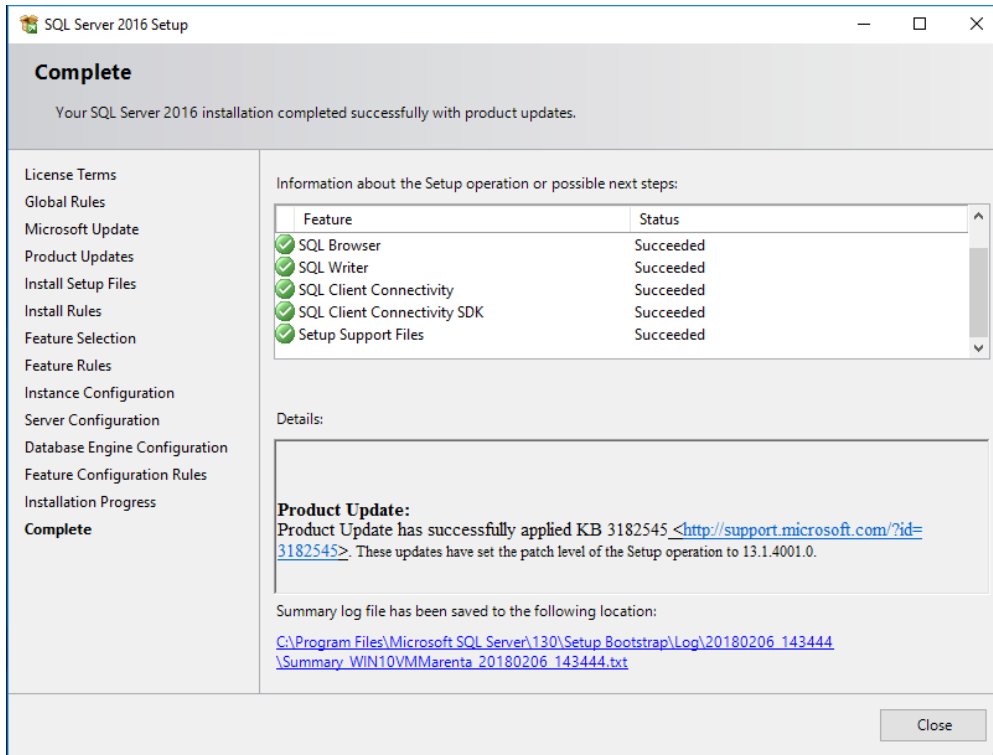


Figure 2.7 - Microsoft SQL Server 2016 Express - Installation process finished

- Click on "Close".
 - Next, the setup wizard for Microsoft SQL Server Management Studio starts.

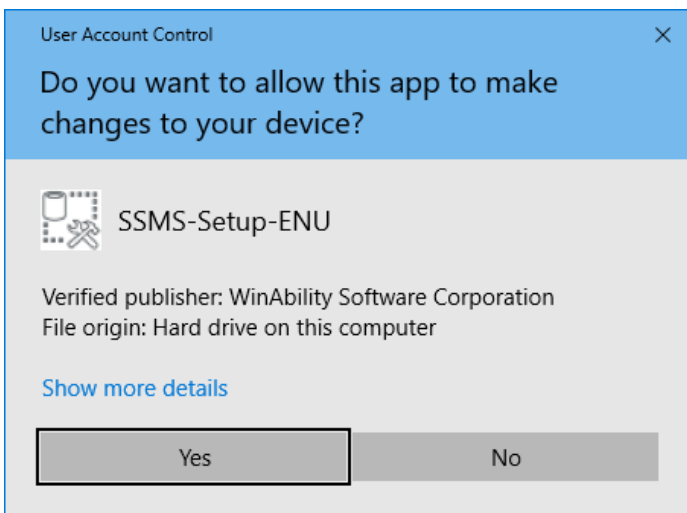


Figure 2.8 - Microsoft SQL Server Management Studio installation

- Management Studio should be installed in order to facilitate database service tasks that may be required in the future.
- Click on "Yes" and wait until the installation steps are complete. The installation is done automatically.

2.3.2 Installation of GAT ACE 3000

Once all the required components are installed, the installation of GAT ACE proceeds as follows.

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

- ▶ Insert the GAT ACE installation CD to start the setup.
- ▶ Double-click on the "setup.exe" file.
 - The installation wizard opens.



Figure 2.9 - GAT ACE installation - step 1

- ▶ Click on "Next".

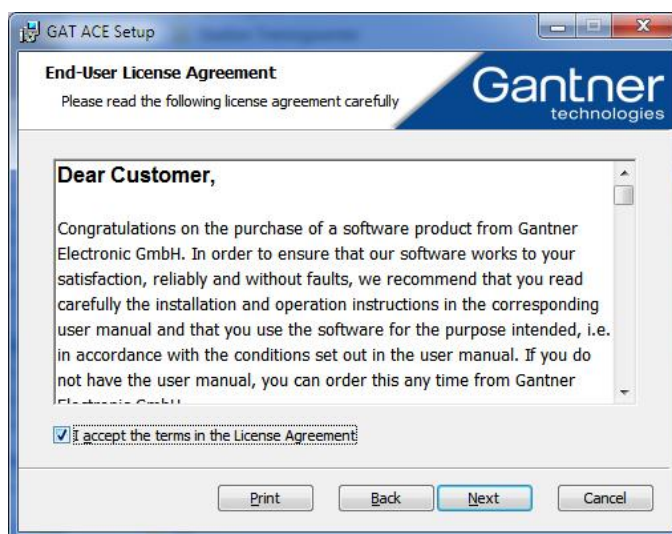


Figure 2.10 - GAT ACE installation - step 2

- ▶ 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".

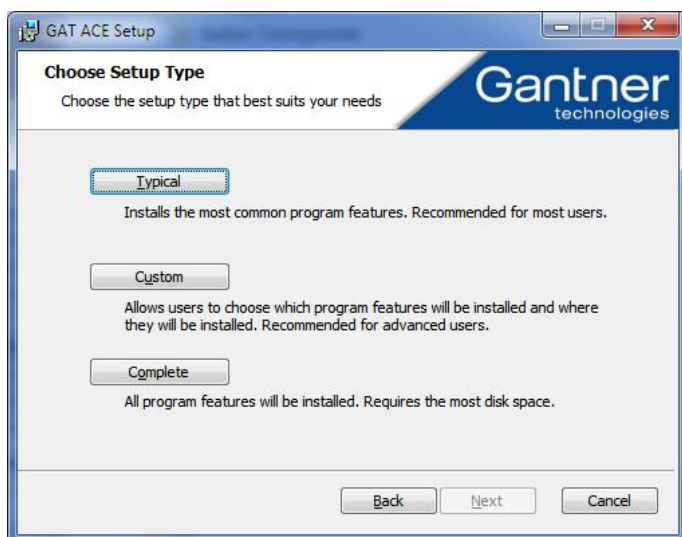


Figure 2.11 - GAT ACE installation - step 3

- Select the type of installation (standard = "Typical"):
 - Typical: Installs GAT ACE (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 Relaxx. The following window appears when this type of installation is chosen. Here GAT ACE represents the graphical user interface and GAT ACE 3000 represents the service.

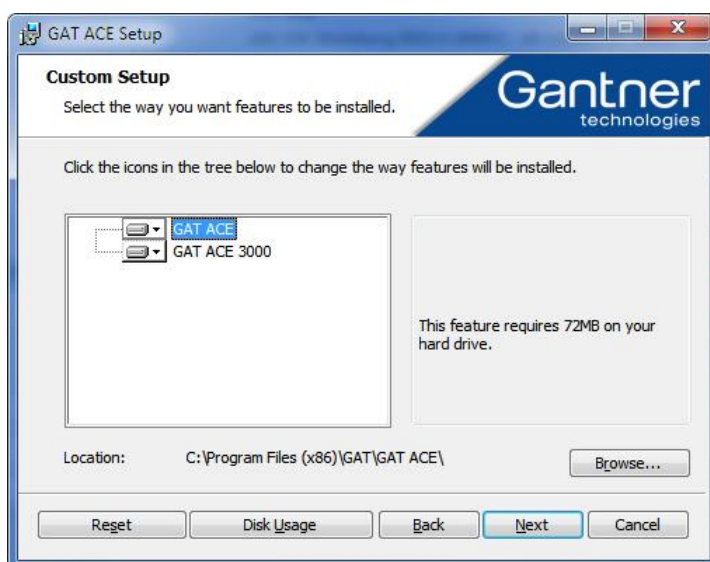


Figure 2.12 - GAT ACE installation - custom setup

- 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 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.

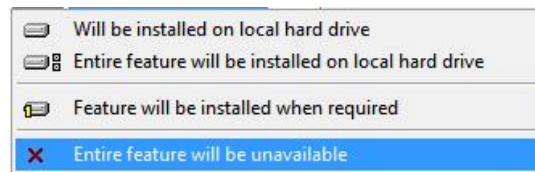


Figure 2.13 - GAT ACE installation - custom setup

- ▶ Now select the directory where you want to install GAT ACE. 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 and requires the most disk space.

- After selecting the type of installation, the following window opens in the next step.



Figure 2.14 - GAT ACE 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 is now installed and ready for use.



Attention: 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 and GAT ACE 3000 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:\Programme\GAT\GAT ACE"
 - "C:\Programme\GAT\GAT ACE 3000"
 - For 64-bit Windows versions:
 - "C:\Programme (x86)\GAT\GAT ACE"
 - "C:\Programme (x86)\GAT\GAT ACE 3000"
- The components for the GAT ACE 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 Windows service and the SQL database are installed on the same PC, it is possible that the GAT ACE service starts before the SQL database. In this situation, GAT ACE 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.

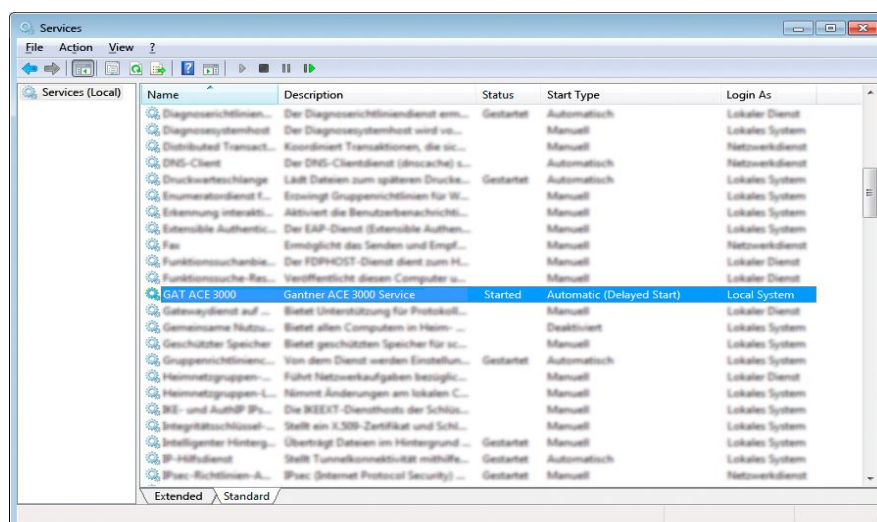


Figure 2.15 - Windows Services

- Here the "Start Type" must be set to "Automatic (Delayed Start)". Right-click on the GAT ACE 3000 service and select "Properties" from the pop-up menu.
 - The Properties window of the GAT ACE 3000 service opens.

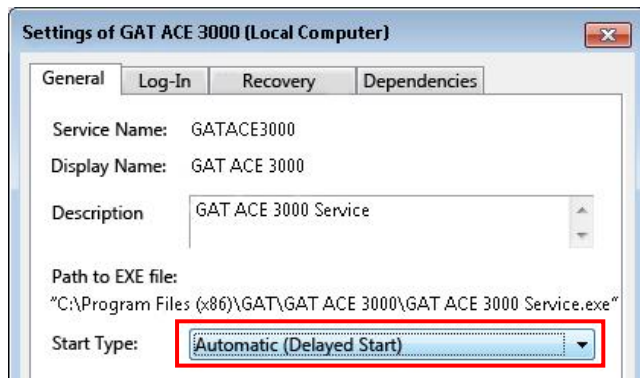


Figure 2.16 – GAT ACE service settings

- ▶ In the "Start Type" field, select "Automatic (Delayed Start)".
- ▶ Click on "OK".
 - This setting ensures that the GAT ACE 3000 service still starts automatically but the start-up process is delayed.

2.4 Switching from GAT Manager to GAT ACE

When switching from an existing access control system running GAT Manager software to the new GAT ACE software, the existing controller configurations can be imported and used.

Certain steps must be performed to ensure a faultless transition. A detailed description of this process can be found in section "7. MIGRATING GAT MANAGER TO GAT ACE".

2.5 Updating GAT ACE

GAT ACE provides the option to automatically check for software updates. An Internet connection is required for this purpose. If a newer version of GAT ACE is found, you have the option to download the update and install it. If this function does not work, please contact your IT administrator.

Once the update is complete, the same license that was used before the update can still be used. It is possible that newly created functions (e.g., the anti-passback function) are included with the update. These cannot be used with the existing license and the appropriate extension license 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 perform a backup of an SQL database please see the Microsoft documentation, e.g. on the following internet page: <https://msdn.microsoft.com/en-us/library/ms187510.aspx>.

3 STARTING GAT ACE 3000

When GAT ACE is started for the first time following installation, further configuration processes such as establishing the database connection must be completed. For each subsequent operation of the application, you will be directed to the login screen.

3.1 Startup

- Start GAT ACE by selecting "GAT Ace" from the Windows Start menu.

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

- The GAT ACE startup process begins.

During startup GAT ACE checks the connection to the GAT ACE 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 3000 Service

The GAT ACE 3000 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. Upon startup, GAT ACE checks the connection to the GAT ACE service. An error message is displayed if a valid connection cannot be established.

NOTE! Normally the service starts automatically when you run GAT ACE.



Figure 3.1 – Starting the GAT ACE 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 Database Settings

Once GAT ACE is installed, a database for GAT ACE must be created and a connection to the database established. GAT ACE 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, perform the following steps:

- The following window appears during startup if the database connection settings are not configured correctly.

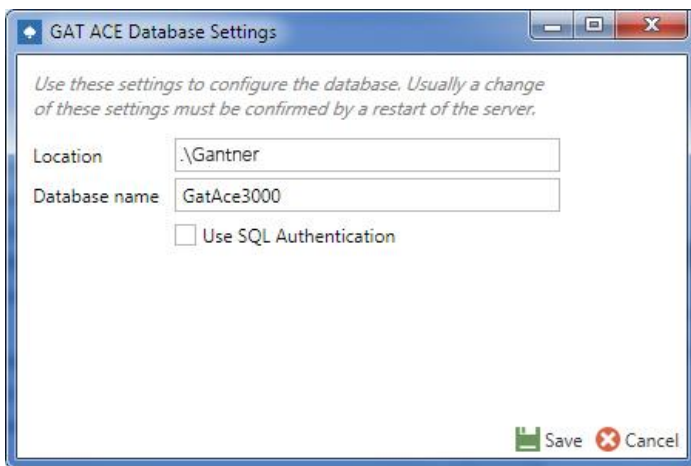


Figure 3.2 – Database connection settings

- In the "Location" field, enter the location of the database server.
 - When the database is installed on the same PC as GAT ACE and the standard settings were not changed during installation, the default location is ".\Gantner"). If the installation values are changed, the server location must indicate exactly where the database is installed (i.e., network name or IP address and SQL Server instance name).
- Enter the name of the database in the "Database name" field (default = "GatAce3000").
- The "Use SQL authentication" option allows you to select which login settings (username and password) GAT ACE uses to log into the database.
 - When this option is not selected, the Windows login settings of the respective user account are used (default setting).
 - When this option is selected, enter a username and password into the respective fields to use for database login.

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.

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

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

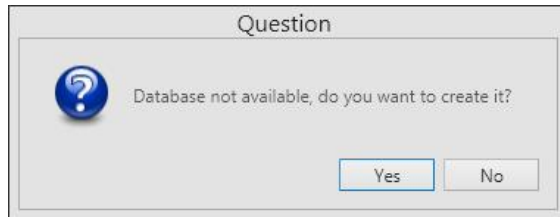


Figure 3.3 – Establishing a new database

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

3.1.3 Login Window

After GAT ACE has successfully connected to the GAT ACE 3000 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.

NOTE! You can create different users with different privileges in GAT ACE. See "6. AUTHORISATION MANAGEMENT" for more information.



Figure 3.4 - Login window for GAT ACE

- ▶ Enter your username in the "User name" field.

- ▶ Enter your password in the "Password" field. Ensure to enter your password in case sensitive format.
- ▶ Confirm your details then click on "Login".
 - When valid login details are entered, the main screen of GAT ACE 3000 opens (see "5.1. Functional Overview of GAT ACE"). Otherwise you have the option of entering the username and password again.



Change default passwords immediately after installation of GAT ACE.

After installation of GAT ACE the standard users "SYSTEM" and "Administrator" are preconfigured with their standard passwords. It is very important that you change the default passwords of these users after installation of GAT ACE to secure and secret new passwords. See more on this in chapter "6. AUTHORISATION MANAGEMENT".

4 CONFIGURATION

In the software settings, all basic GAT ACE functionalities can be set. The configurable settings are found on several different pages called "Setting Pages". These pages can be accessed as follows.

- Click on the  symbol located above the main menu bar.



- The list of setting pages for the software settings is displayed.
- Select the desired setting page.
 - The settings are displayed to the right of the list.

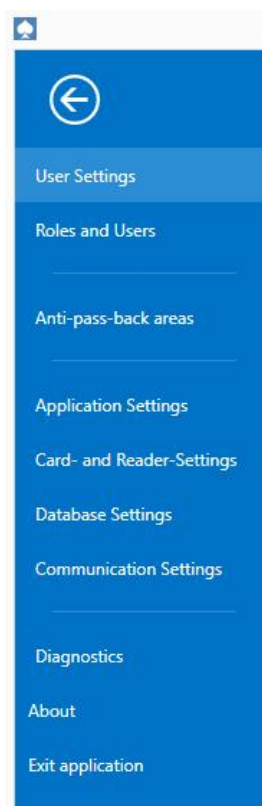


Figure 4.1 - Software settings

The various setting pages are described on the following pages.

NOTE! If changes are made on a setting page, they must be saved by pressing the "Save" button. This button is only displayed once a change has been made on a page. Setting pages with changes not yet saved are marked in red font.

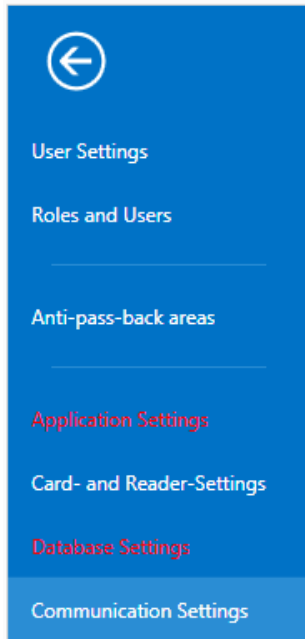


Figure 4.2 – Settings with unsaved changes

4.1 "User Settings" Page

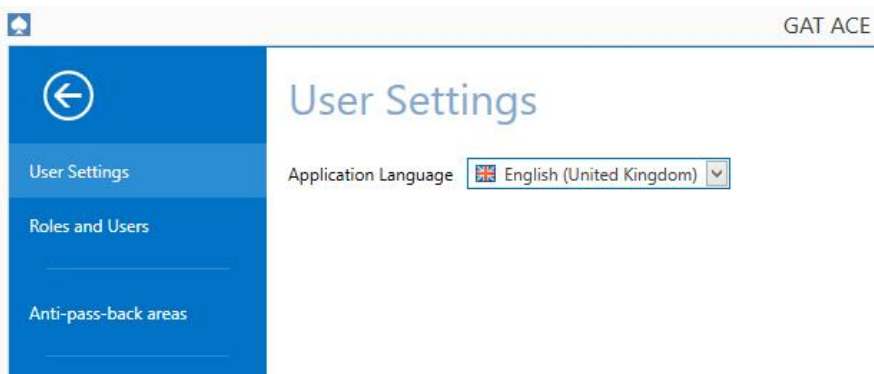


Figure 4.3 - Language selection

You can select the language here. As soon as another language is selected, GAT ACE will close the software window and reopen it immediately in the new language. A restart is not necessary.

NOTE! When switching languages, all views open in GAT ACE at the time will be closed.

4.2 "Roles and Users" Settings Page

Roles and Users

Add role Edit role Delete role Active Directory

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

Add user Edit user Delete user

User Id	User name	Display name	Role	Last login	Special rights
1	SYSTEM	SYSTEM User	SYSTEM	20/04/2018	☐
2	Administrator	Administrator	Administrator		☐

Figure 4.4 - Roles and users settings

In order to be able to work with GAT ACE, it is required to enter a user name with the associated password for safety reasons. The user system has a hierarchical structure, enabling different users to have different authorizations. These authorizations are defined using roles set and saved in GAT ACE.

In this setting window, the roles and the users are created and the roles are assigned to the users. The administration of roles and users is described in detail in chapter "6 AUTHORISATION MANAGEMENT".

4.3 “Anti-Pass-Back Areas” Settings Page

The anti-pass-back functionality prevents several people from gaining access one after the other by simply passing the data carrier to the next person. If this functionality is activated, once a person has entered, he or she has to identify him or herself when leaving in order to regain access at a later point in time. Thus, at any entrance, readers are required both for accessing and leaving, enabling the monitoring of movements.

Areas can be defined for the anti-pass-back functionality, which will then be processed separately in every area, meaning that you cannot enter the same area twice without having left it in between, using your data carrier.

The anti-pass-back functionality is an extension of GAT ACE 3000 subject to licence. Without the licence, the functionalities are not available.

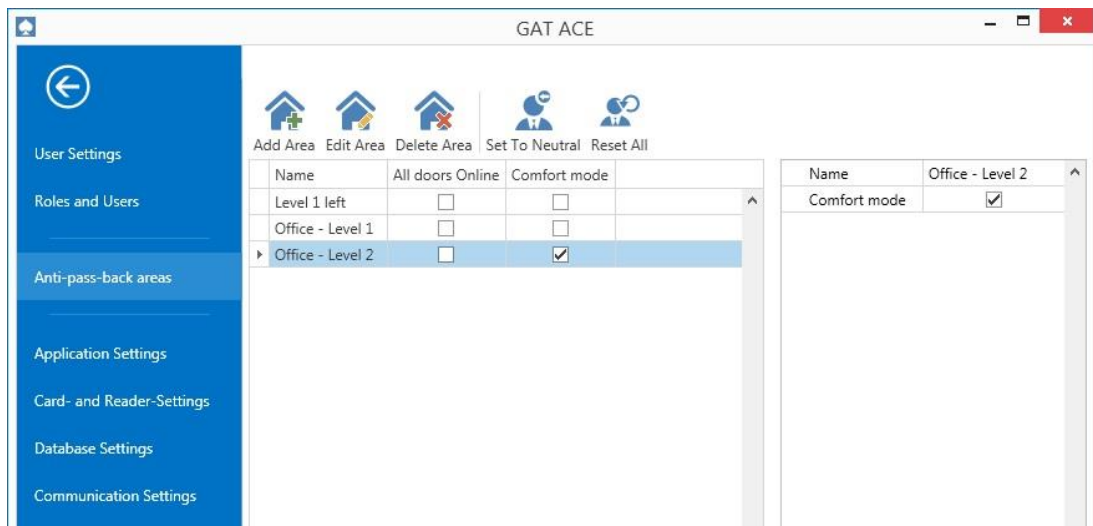


Figure 4.5 -Program settings - anti-pass-back function

This view lists all defined areas.

If the box in the column "All Doors Online" is checked for an area, this means that GAT ACE has an established connection to all doors in that area. This is important for the anti-pass-back functionality, as this functionality requires the permanent checking of who entered at which door using which data carrier in order to establish in which area the persons currently are.

If an area is activated in comfort mode, the anti-pass-back functionality of the corresponding area is deactivated when the connection to a door is interrupted, thus ensuring the operation of the access control system with as little disturbance as possible. The comfort mode should not be used for safety-critical areas. Optimum implementation of the comfort mode also requires the door(s) to be configured correspondingly.

NOTE! In addition to setting the comfort mode, the setting "Anti-Pass-Back Activated When Door Is Online?" should be selected for the controllers of the system (refer to "5.2.9 Configuring Doors"), thus ensuring a regular access check is performed in the event the connection to a door fails, without anti-pass-back checking. Deactivating the anti-pass-back functionality requires up to one minute. The anti-pass-back check will be reactivated as soon as the online connection is re-established.

- ▶ In order to add a new area, click on the "Add Area" symbol.
 - The "Area Configuration" window is opened (see below).
- ▶ In order to delete an existing area, mark it in the list and press the "Delete Area" button.
- ▶ In order to edit an existing area, mark it in the list and press the "Edit Area" button.
 - The "Area Configuration" window is opened.

Area Configuration

Save Cancel

Name: Office Floor ☒ Comfort mode

Doors in Area

Available Doors

- Office Controller Door 1-Entrance
- Office Controller Door 2-Entrance
- Office Controller Door 2-Exit
- Office Controller Door 3-Entrance
- Office Controller Door 3-Exit
- Office Controller Door 4-Exit
- T2500-Entrance
- T2500-Exit
- T310E1323551 Door 10-Entrance
- T310E1323551 Door 10-Exit
- T310E1323551 Door 11-Entrance
- T310E1323551 Door 11-Exit
- T310E1323551 Door 12-Entrance
- T310E1323551 Door 12-Exit
- T310E1323551 Door 13-Entrance
- T310E1323551 Door 13-Exit
- T310E1323551 Door 14-Entrance
- T310E1323551 Door 14-Exit
- T310E1323551 Door 15-Entrance
- T310E1323551 Door 15-Exit
- T310E1323551 Door 16-Entrance
- T310E1323551 Door 16-Exit
- T310E1323551 Door 2-Entrance

Access In Doors

- Office Controller Door 4-Entrance
- T310E1323551 Door 1-Entrance

Access Out Doors

- Office Controller Door 1-Exit
- T310E1323551 Door 1-Exit

Instructions

Figure 4.6 – Configuring areas for the anti-pass-back function

The selected area is edited here and the doors or readers to be used for the access and exit control in this area are determined. In the "Doors in the Area" list, all available doors, i.e. controllers or readers useable for the anti-pass-back functionality, are shown.

- ▶ Enter the name of the area into the "Name" field.
- ▶ Check the "Comfort Mode" option box if you want to activate this mode for this area (refer to the previous page for an explanation).
- ▶ With the mouse, pull a door from the list into the "Access to the Area" field in order to use this door as an entry access control into this area.
- ▶ Repeat this procedure with the "Exit from the Area" field in order to use this door as an exit control for this area.

- ▶ In order to remove a door from the entry or exit field, pull back the door with the mouse into the list of doors on the left.
- ▶ In order to save these settings, press the "Save" button.
 - You will return to the setting page for the anti-pass-back functionality and the area list will be updated accordingly.

Neutralizing and setting back the anti-pass-back functionality

The anti-pass-back status can be neutralized separately for each area or the status can be set back for all doors within the system. This allows all persons at the doors of the selected area to move in a desired direction. With a recorded booking, the anti-pass-back status of the person is set accordingly and checked again from that moment onwards.

- ▶ Mark an area and press the "Set to Neutral" button in order to neutralize the anti-pass-back status for all persons at the doors of the selected area.
- ▶ Mark an area and press the "Reset All" button in order to neutralize the anti-pass-back status for all persons at all doors of the system.

If you want to reset the anti-pass-back status of a single person or door, this requires uploading from the access control software.

4.4 “Application Settings” Page

Figure 4.7 - Program settings - application settings

On this setting page, the general time and time-out settings can be performed.

- Number of attempts before door deactivation:

This value determines, how many times in the event of an error, GAT ACE will attempt to establish the connection to a door (i.e. with the respective controller of the door), that should be activated and reachable. After the set number of unsuccessful attempts, the door will be deactivated. This prevents delayed communications and reduced system performance.

- Minutes between automatic door activation attempts:

This value determines the waiting time (in minutes) after deactivating a door (refer to the previous section) until GAT ACE re-attempts establishing a connection with the door. If the connection attempt is successful, the door is reactivated.

- Global Attack PIN Code (=Duress PIN Code):

Here, an attack PIN code valid for all persons at any controller of the access control system can be entered. An individual attack code overriding the global attack code can also be defined at each controller.

In the attack PIN code, only a few digits of the code are defined, the remaining digits are shown with an "X". The corresponding digit of the personal PIN code must be entered instead of the "X"s.

Example:

X X 1 X X X X 0 ← Attack PIN code

- - - 2 4 8 8 2 ← Personal PIN code

- - 1 2 4 4 8 0 ← PIN code that needs to be entered in order to trigger the attack alarm.

Please make sure that the regular personal PIN code of a person is not identical to the attack PIN code, as an attack alarm would be triggered every time the PIN code is entered correctly.

Attack PIN codes can only be entered if entering a PIN code is required for regular access.

- Global Fingerprint Detection Threshold:

Here, enter the global threshold to be used for the fingerprint readers. This value is used as a default for all controllers equipped with fingerprint readers, but can be set individually when configuring each separate controller.

The detection threshold defines how well the fingerprints actually read at the fingerprint reader must match the stored data. Lower values imply that fingerprint checking fingerprints will be performed with a smaller number of characteristics, i.e., with a higher tolerance, which in turn means that the fingerprints will be accepted more often. Higher values imply that the fingerprints must match the stored data more precisely, which increases the safety but at the same time increases the rejection rate and this calls for more frequent multiple attempts. The detection threshold should be selected in accordance with the safety needs. The default value is 3.

- Interval for setting time of the devices (mins):

Here you can enter a time interval on which the time of the controllers shall be automatically updated with the PC clock.

- Licence for Module "GAT ACE 3000, Flex Time Bookings":

In order to use the functionality of GAT ACE to read the time bookings of GANTNER Time & Attendance terminals, you need to have the corresponding licence code for this module. This code has to be entered in this field.

- Activate "Reset Anti-Pass Back":

If this box is checked, the anti-pass-back status is reset automatically at the defined times (see below), enabling a person to access or exit. For information regarding the anti-pass-back functionality refer to "4.3. "Anti-Pass-Back Areas" Settings Page".

- Reset "Anti-Pass-Back": If the automatic reset of the anti-pass-back functionality is activated (refer to the option above), a time can be entered here for the anti-pass-back status to be reset automatically every day.

- GAT SyncManager CardNET Settings:

If the "GAT SyncManager CardNET Enabled" option is activated, access authorizations for offline locks operating in CardNET mode are written onto data carriers by the GAT p.time ST380 / ST381 / ST390 / ST380 EVO / ST381 EVO and ST390 EVO time recording devices when data carriers are read by these devices. The settings, which affect the authorization bookings on the data carriers, can be defined in the configuration of the time recording device. This allows you to, for example, grant the authorizations for "Coming" bookings and to delete the authorizations for "Leaving" bookings. In the "GAT SyncManager CardNET Directory" field, the folder for data exchange can be selected. In this folder, GAT ACE 3000 provides authorization data in the "cardnet.dat" file. GAT SyncManager provides booking data in this folder that is periodically accepted by GAT ACE 3000 in 1 minute intervals. The file for the bookings must have the designation "accessbookings.exp". By accepting the bookings, changes to the authorizations for data carriers and battery warnings in GAT ACE 3000 and GAT Matrix can be followed.

NOTE! When setting up the systems, ensure that GAT ACE 3000 and GAT

SyncManager both have read and write permission for the selected folder. Note that the read / write permission must exist for the user under which the two programs are running, e.g., network service.

- GAT ACE 7000 CardNET Settings:

These settings have the same functionality as the previously described "GAT SyncManager CardNET Settings", with the difference that GAT ACE 7000 and not the GAT SyncManager software is used for processing the offline data (authorization data for user data carriers and offline bookings).

With the option field "GAT ACE 7000 CardNET Enabled" you can activate or deactivate this function.

In the field "GAT ACE 7000 CardNET Directory" enter the path where the files for data exchange shall be stored.

NOTE! When setting up the systems, ensure that GAT ACE 3000 and GAT ACE 7000 both have read and write permission for the selected folder. Note that the read / write permission must exist for the user under which the two programs are running, e.g., network service.

In the fields "GAT ACE 7000 CardNET Filename" and "GAT ACE 7000 CardNET Bookings File" you can define the names for the files with the offline authorization data and with the offline bookings.

In the field "CardNET Card Type" enter the number of the card type to be used for the CardNET function. GAT ACE 7000 can use several different card types but GAT ACE 3000 and CardNET can only use one card type. For more information about the card types see the GAT ACE 7000 manual.

4.5 “Card and Reader Settings” Page

On this setting page, you perform the settings for the data carriers used in the system with the according reader settings. This includes the basic data structures, company IDs, etc. The reader configuration settings must match the data carrier settings used at this reader in order for the data carriers to work properly.

As several different data carriers may be used within a system, several configurations may be created.

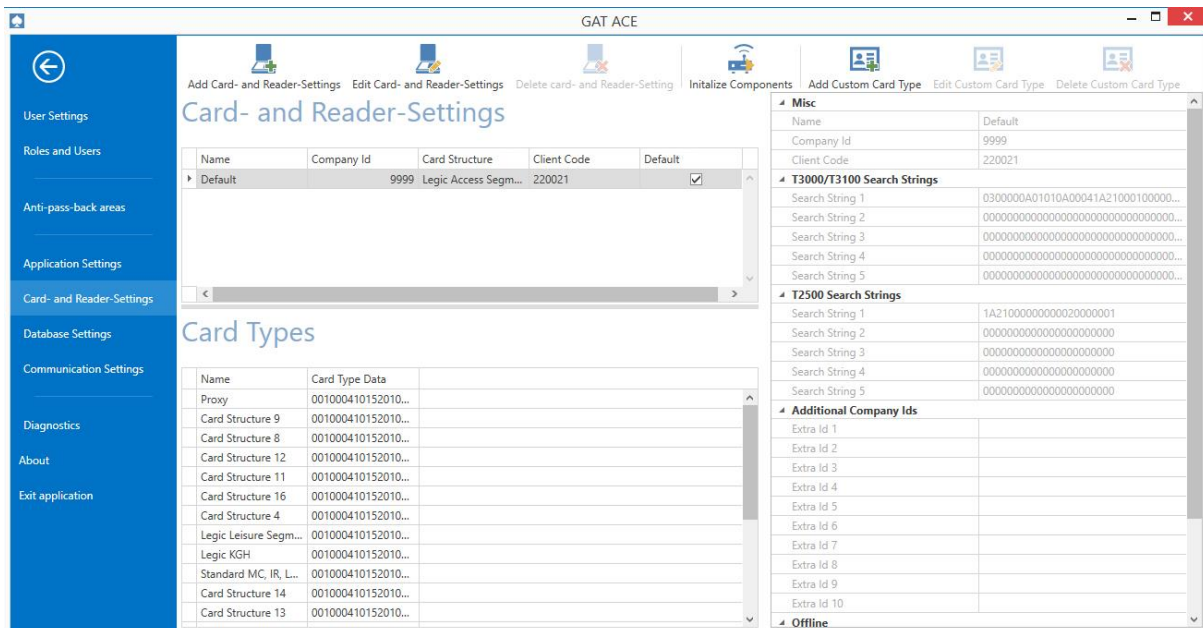


Figure 4.8 - Program settings - card and reader settings

This setting page is divided into 3 areas.

The area "Card and Reader Settings" is used for the administration of the various cards and the matching reader configurations. Normally, a system does not require more than one card setting. However, if cards of different generations or differing technologies are used simultaneously (e.g. in the event of an additional use of long-range tags), they can be recorded here. It is recommended to perform the correct settings immediately after installing the GAT ACE system and prior defining the controllers, as - to the extent possible - these settings will then be copied automatically to the readers.

In the right area, the details of the selected card settings are displayed.

In the area "Card Types", some types of technologies and special card codings are already defined. If the technology or coding you are using is not available, it can be created as a client-specific card type.

More information regarding these areas and how to edit the reader configurations is found on the following pages.

Card settings

- ▶ In order to create a new reader configuration, click on the "Add Card and Reader Settings".
 - The "Card-Reader Settings" window is opened (see below).
- ▶ In order to edit an existing configuration, mark it in the list and press the "Edit Card Settings" button.
 - The "Card-Reader Settings" window is opened.

Figure 4.9 - Program settings - reader configuration

- ▶ Enter a unique designation for the cards.
 - This reader configuration can be selected under this name when configuring the controller-configuration and can be assigned to the readers.
- ▶ Enter the following information in the fields in the upper area called "Card Data".
 - Company ID: The company ID (FID) is a unique number for your card coding. For some card types, no company ID is available. In this event, leave the default value 9999 unchanged. For other card types that have such a company ID, the correct value must be set. This ensures that external data carriers cannot gain access to your system! Your company ID is written in your order documents at the time of the delivery of your cards. Your system installer will be happy to tell you your company ID as well.
 - Card Structure: Select the type of card used in your system from the predefined list of card types. If it is not already included, it can be created under "Card Types" as a custom card type (see below).

- Client Code: The client code provides information about the card codings, the value for standard coding of GANTNER data carriers being "220021". Should you use specially coded cards, your system installer will tell you the correct client code.
 - Reader Synchro Mode: Here you can select the mode (i.e. type of interface) to use when the reader is operated in synchron communication mode (Omron or Wiegand).
- On the "Additional Company IDs " tab in the upper area, additional company IDs can be entered. This is only necessary if you consciously want holders of cards of other companies to be able to access your system. A prerequisite is that these cards show the same coding as yours, with only the company ID differing. This functionality is not available for all types of controllers.
- NOTE!** In order to delete an additional company ID from a controller it is not enough to only delete the ID number in the corresponding field in this window. To delete the ID number you have to first enter "0000" in the desired field and then initialize the controller. This will delete the additional company ID in the controller. Only now you can delete the field "0" in this window.
- On the "Technologies " tab in the upper area, you can mark the RFID technologies, that shall be activated at the reader. Please note that this setting is only used for the GAT SR 73xx and GAT SLR 73xx reader series and not for the GAT SR 3xx and GAT SLR 3xx reader series.
- In the "GAT Terminal 3000 / 3100 Settings" and "GAT Terminal 2500 Settings" areas, the search strings are entered that are required by the controller in order to read the data carriers. There are predefined requirements that can be selected. The settings must only be entered for the controllers actually used in your system.
- In the "CardNet Settings" area, the settings are defined for the functionality of a CardNet system, enabling authorizations on IDs to be transferred to offline locks.
- CardNet Segment ID: Defines the coding of the data area, where the authorizations are stored on the card. For standard codings, this value is "0A". If you are using a different coding, your installer will tell you the correct value to use.
 - Battery Segment ID: Defines the coding of the data area to which information such as battery warnings originating from offline lockers is transferred back to the online controllers. For standard codings, this value is "0C". If you are using a different coding, your installer will tell you the correct value to use.
 - Security Offline Data : If this option is activated, the person must first enter the PIN code or undergo a biometric verification at an online reader prior to being allowed to write CardNet authorizations. It is thus checked that this person is the rightful owner of the card. This ensures that lost cards cannot be used by the finder to update CardNet authorizations. This functionality can only be used if all online reader used for the updating of the CardNet authorizations also offer the possibility of entering the PIN code or are equipped with biometric readers!
 - Valid Duration (days): This value determines how long the CardNet authorizations remain valid after being written. To set this setting correctly, the next setting "Rewrite Before Expiring (days)" must also be considered.
With this value, you limit the risk associated with the loss of a card. It is recommended to keep this value low (typically 3 to 7 days) and to adapt it to your safety requirements!
 - Rewrite Before Expiring (days):
This value determines, how many days in advance the CardNet authorizations are renewed prior to expiring. This value should be set as short as possible in order to keep

the operation at the online readers as fluid as possible. Typically, this value is set to 3 days, e.g. authorizations that would expire on a Sunday are already renewed on the preceding Friday. This enables an access at offline locks on Mondays, without first having to renew the authorization at an online reader. Please adjust this value to your safety requirements.

NOTE! The validity periode is always 1 day. This means that a terminal writes the authorization onto a data carrier at 8:00 the data carrier is valid until 7:59 of the following day. But if you set the field "Rewrite Before Expiring (days)" to a higher value than the field "Valid Duration (days)" (e.g. rewrite 2 days and valid duration 1 day) the validity of a data carrier is deleted at midnight. This allows you to guarantee that the users must first identify themselves at a terminal each day (e.g. for time & attendance purposes). On this terminal the authorization data are written onto the data carrier and only after that an access is possible.

- ▶ Save the edited settings by pressing the "Save" button.
 - You return to the "Card Settings" setting window and the edited reader configuration is displayed in the list.

Card types

In the "Card Types" field, all already defined types and codings are listed. They can be used for the reader configuration. The data includes information that determines how and where data is found and interpreted on a data carrier. For that reason, it is necessary to create the correct search strings or card structures, depending on the type of data carrier in use and select them correctly during reader configuration.

- ▶ In order to create a new card type, click on the "Add Custom Card Type" button.
 - The "Card Type" window is opened (see next section).
- ▶ In order to edit an existing card type, double-click on the corresponding entry in the card type list.
 - The "Card Type" window is opened.

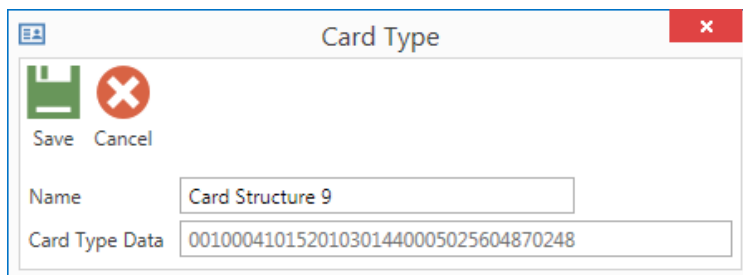


Figure 4.10 - Definition of a card type

- ▶ Enter the name of the card type into the "Name" field. During reader configuration, the card type can be selected by this name.
- ▶ Enter the search string used to find and evaluate the data carriers in the "Card Type Data" field. For client-specific cards, the installer will provide you with the necessary information.
Example for a search string for Access segment of a LEGIC prime or LEGIC advant data carrier:

The screenshot shows a configuration window with two tabs: "Card Data" (active) and "Additional Company Ids". Under "Card Data", there are fields for "Company Id" (9999), "Card Structure" (Legic GCC21 Structure), and "Client Code" (220021). Below this, there are three tabs for search strings: "GAT Terminal 3000 / 3100 Settings" (active), "GAT Terminal 2500 Settings", and "GAT Terminal 3000 / 3100 Settings". Under the active tab, there are three search string fields: "Search String 1" (0300000A01010A00041A2100010000000000000000), "Search String 2" (0300000701000700081A2400000000000100000000), and "Search String 3" (empty).

- ▶ Confirm by pressing the "Save" button.
 - The edited card type will be updated in the list.

4.6 "Database Settings" Page

The screenshot shows the "Database Settings" page in the GAT ACE 3000 configuration interface. The page has a blue sidebar with navigation links: "User Settings", "Roles and Users", "Anti-pass-back areas", "Application Settings", "Card- and Reader-Settings", "Database Settings" (selected), and "Communication Settings". The main content area has a title "Database Settings" and two buttons: "Restore Backup" and "Create Database with user". Below the buttons, there is a note: "Use these settings to configure the database. Usually a change of these settings must be confirmed by a restart of the server." The settings fields are: "Location" (.\GANTNER), "Database name" (GatAce3), "Use SQL Authentication" (checked), "Username" (GATACE3), "Password" (masked with dots), and "Confirm password" (masked with dots).

Figure 4.11 - Program settings - database settings

On this settings page, the connection settings for the GAT ACE 3000 database are defined.

- 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 “5.3.1 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 4.12 – 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 database is located. In the event of a local installation (GAT ACE Client and GAT ACE 3000 Service installed on the same PC), a "." followed by the database name can be entered as location (Example: ". \Gantner").
- Database Name: The designation chosen when creating the database.
- Use SQL Authentication: Choose whether the Windows authentication of the user or the SQL authentication (with the user name and password) should be used for the connection to the database.

NOTE! A detailed description of the database settings is found in section "3.1.2 Database Settings".

4.7 "Communication Settings" Page

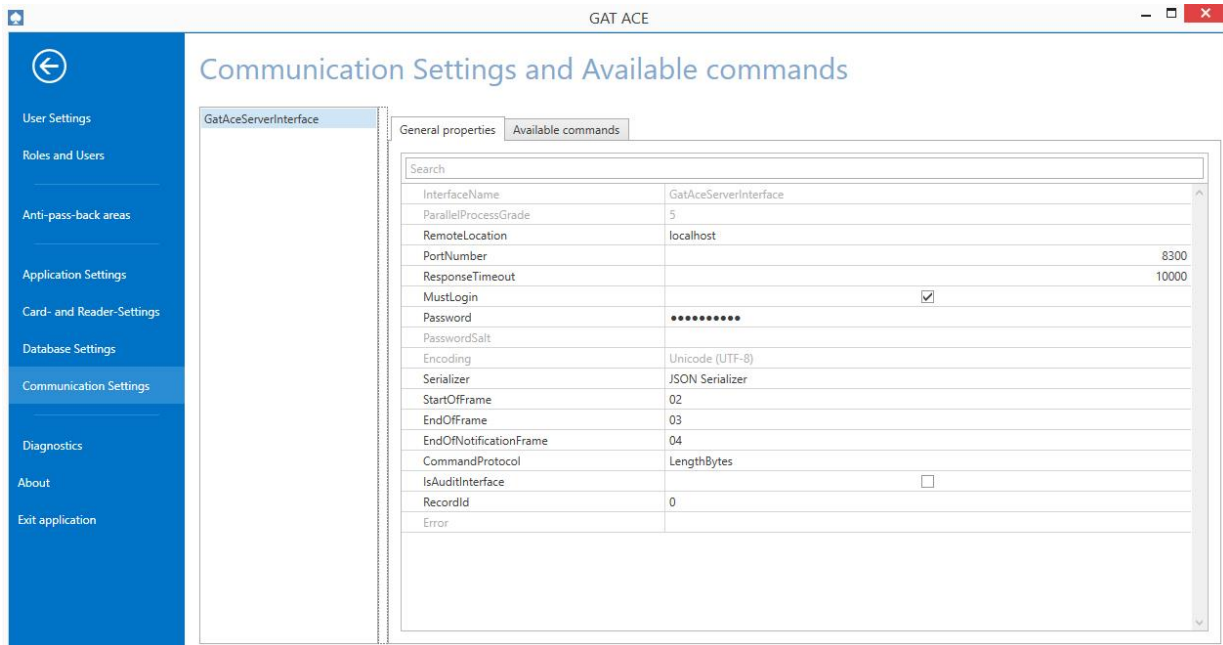


Figure 4.13 - Program settings - communication settings (general properties)

The communication settings determine the parameters used for GAT ACE Clients (graphic user interface) communicating with GAT ACE 3000 Service.

NOTE! If GAT ACE Client and GAT ACE 3000 Service are being installed on the same PC, no changes are necessary to the standard settings in order for these two to communicate properly with each other. Otherwise, you may have to change the corresponding communication parameters.

If changes are necessary:

- ▶ Select the corresponding interface (e.g. "GatAceServerInterface") in the left column.
 - The possible communication settings are shown on the right.
- ▶ Set the corresponding values and option field settings in the "General Properties" tab. Important settings are:
 - RemoteLocation: Network name or card address of the computer on which GAT ACE 3000 Service is installed. If GAT ACE Client and GAT ACE 3000 Service are installed on the same PC, enter "localhost".
 - PortNumber: Port number for communication (default value: 8300)
 - ResponseTimeout: Time (in milliseconds) waited between a request and the response to it. If no response is received within this time, an error message is displayed.
 - MustLogin: Set by default. If active, a password is required for GAT ACE Client communicating with GAT ACE 3000 Service.
 - Password: The required password for the communication between GAT ACE Client and GAT ACE 3000 Service, if the "MustLogin" option is checked. The password should be left unchanged from the default password, otherwise it needs to be changed in the GAT ACE 3000 Service as well.

NOTE! Only fields with a designation in black font can be changed. The fields shown in grey cannot be changed and serve only for information purposes.

- On the "Available commands" index page, commands that should be processed by GAT ACE can be selected. By default, all commands are selected.

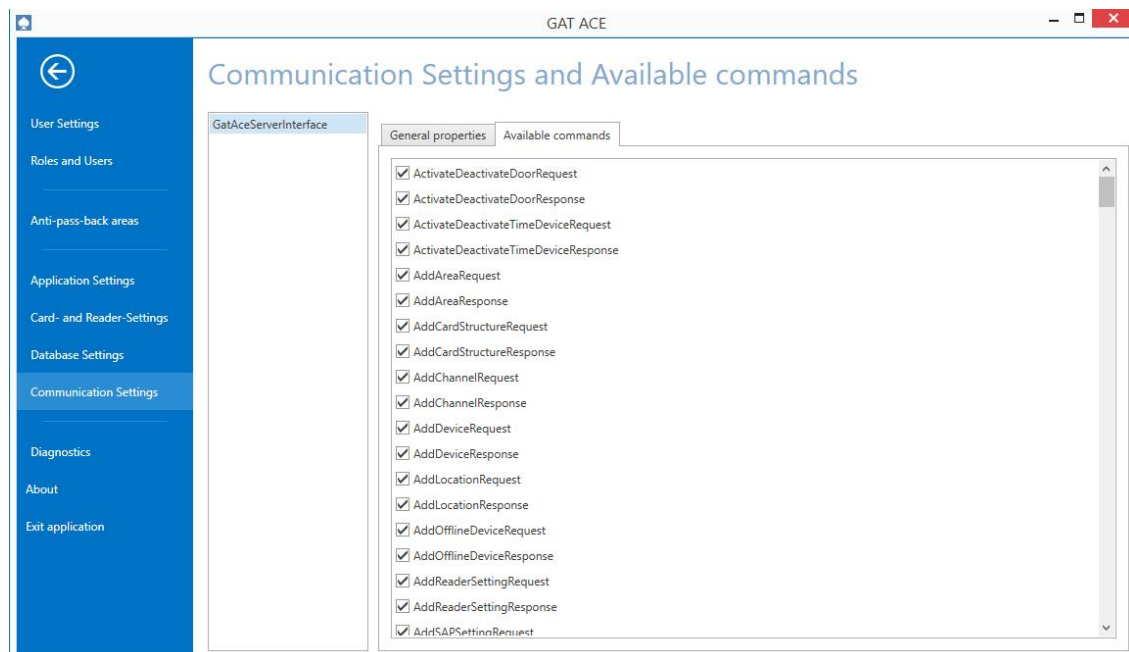


Figure 4.14 - Program settings - communication settings (available commands)

4.8 "Time Bookings Exporting Settings" Settings Page

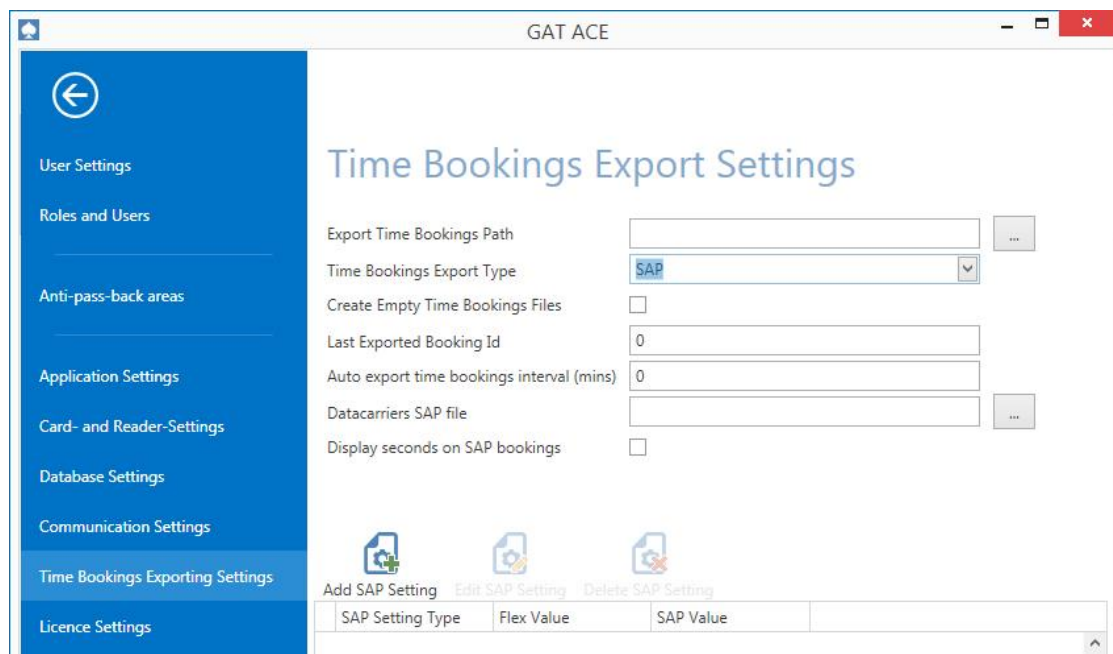


Figure 4.15 - Program settings - Time Bookings Exporting Settings

When there are time acquisition terminals (e.g. the GAT Terminal 1015 or GAT Terminal 1032) in your system and you want to use GAT ACE to read and handle the time bookings from these terminals, the corresponding licence module must be activated (see "4.4. "Application Settings" Page"). On this page you can define, how GAT ACE handles the time bookings.

► Define the following settings:

- Export Time Bookings Path: Click on the "." button and select the file path, where the exported time bookings shall be stored. Text files with the bookings will be generated in this directory.
- Time Bookings Export Type: Select the format for the time bookings.
 "Flex" uses the same format as the GAT Manager software, which makes these bookings backward compatible for older installations.
 "SAP" saves the time bookings in SAP compatible format.
- Create Empty Time Bookings Files: When this option is active, an empty file is generated when there are no time bookings. If the option is not active, no file will be generated if there are no time bookings.
- Last Exported Booking Id: Bookings are numbered with a sequential ID number. If bookings are then exported, the ID number of the last exported booking is saved. At the next export, only the newer bookings are exported. If older bookings shall be exported as well, this value can be set to the ID number of the desired booking to be exported again and the bookings from this ID to the current last ID are exported.

- Auto export time bookings interval: Here you can enter a time in minutes to automatically export the time bookings. If "0" is entered, the automatic export is deactivated.
 - Datacarriers SAP file: SAP can only handle 8-digit data carrier numbers. Data carriers with longer numbers (e.g. Proxy data carriers or UIDs) have to be converted. Here you can select a file that includes the SAP and Gantner card numbers for the data carriers. This will allow to automatically convert these numbers. Note: The same file (format) that is used for the SAP Interface CC1 for GAT Manager can be used here.
The conversions can also be defined in the table at the bottom of this settings page (no conversion file needed).
 - Display seconds on SAP bookings: Because SAP cannot use seconds in bookings, this option can be deactivated in order to set the seconds in the bookings to 00. If another time software is used, which also uses SAP format but can handle seconds in bookings, you can mark this option in order to use the seconds.
- ▶ In case you selected the SAP booking export type, add the SAP Settings in the list field on this page. Therefore click on "Add SAP Settings" and enter the SAP Settings Type ("Bookings Codes" or "Datacarriers") and the corresponding Flex and SAP values. With "Datacarriers" you can convert between SAP and Gantner card numbers without the need of a conversion file (see "Datacarriers SAP file").
 - ▶ Press "Save" to save changed settings.

4.9 "Diagnostics" Settings Page

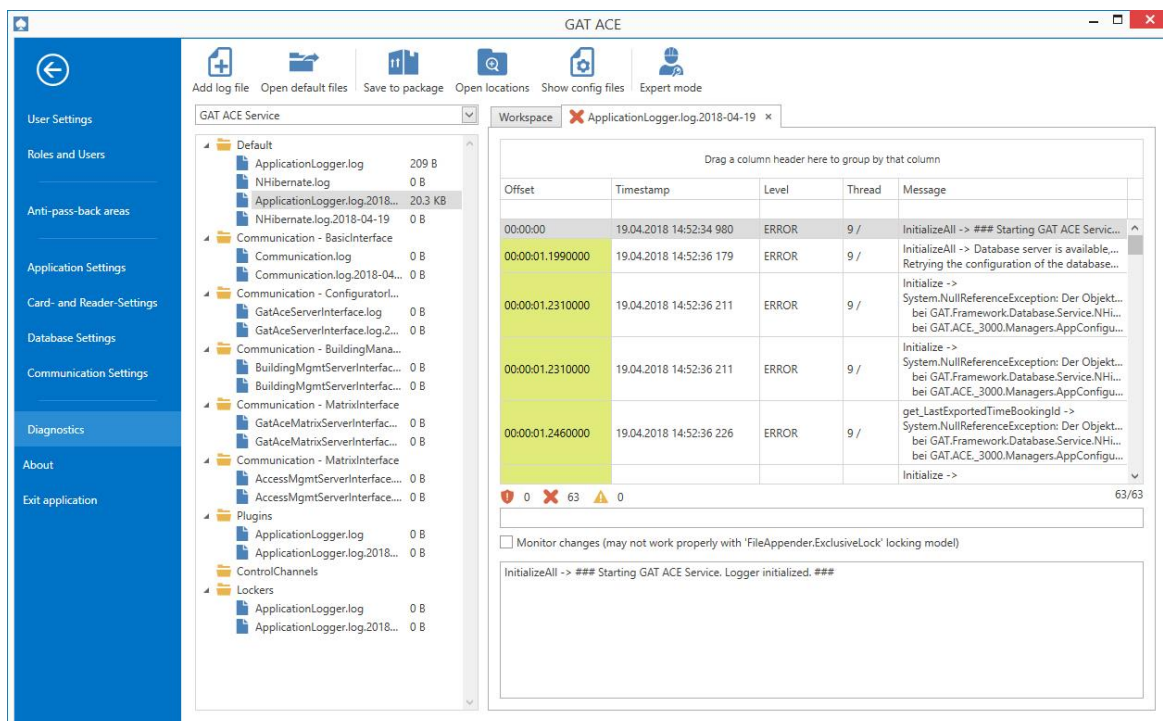


Figure 4.16 - Program settings - diagnostics settings

GAT ACE records all important events and actions in log files. In the "Diagnostics" setting page, you have the opportunity of evaluating these log files or saving them into a packet in order to send them to GANTNER Electronic or your partner for further evaluation.

- ▶ In the upper left field, select a "Collection" ("GAT ACE 3000" for the log files of the service and "GAT ACE" for the log files of the user interface).
 - The list underneath will list all log files included in this collection.
- ▶ Double-click on the log file in the left list.
 - The entries of the log file are displayed in the right field. If several log files are opened, they are selectable by their respective tab.
- ▶ Right-click with the mouse on a log file entry.
 - A pop-up window opens, which offers various setting options.

Figure 4.17 – Program settings - diagnostics settings

- www.gantner.com

5 OPERATION

This chapter contains a functional overview and a detailed description of every GAT ACE functionality.

5.1 Functional Overview of GAT ACE

This section gives an overview of the main functionalities of GAT ACE.

After starting GAT ACE, the user must log in using their username and password (see "3.1.3. Login Window"). Standard users with specific passwords and user profiles (see "6.3.1. Default Users") are already created in GAT ACE. The role assigned to a user defines which functionalities the user may execute in GAT ACE. In this chapter, the operation is described for the SYSTEM user, who may execute all functionalities.

After successfully logging in using the user name and password, the GAT ACE main screen is displayed. It is divided into several areas.

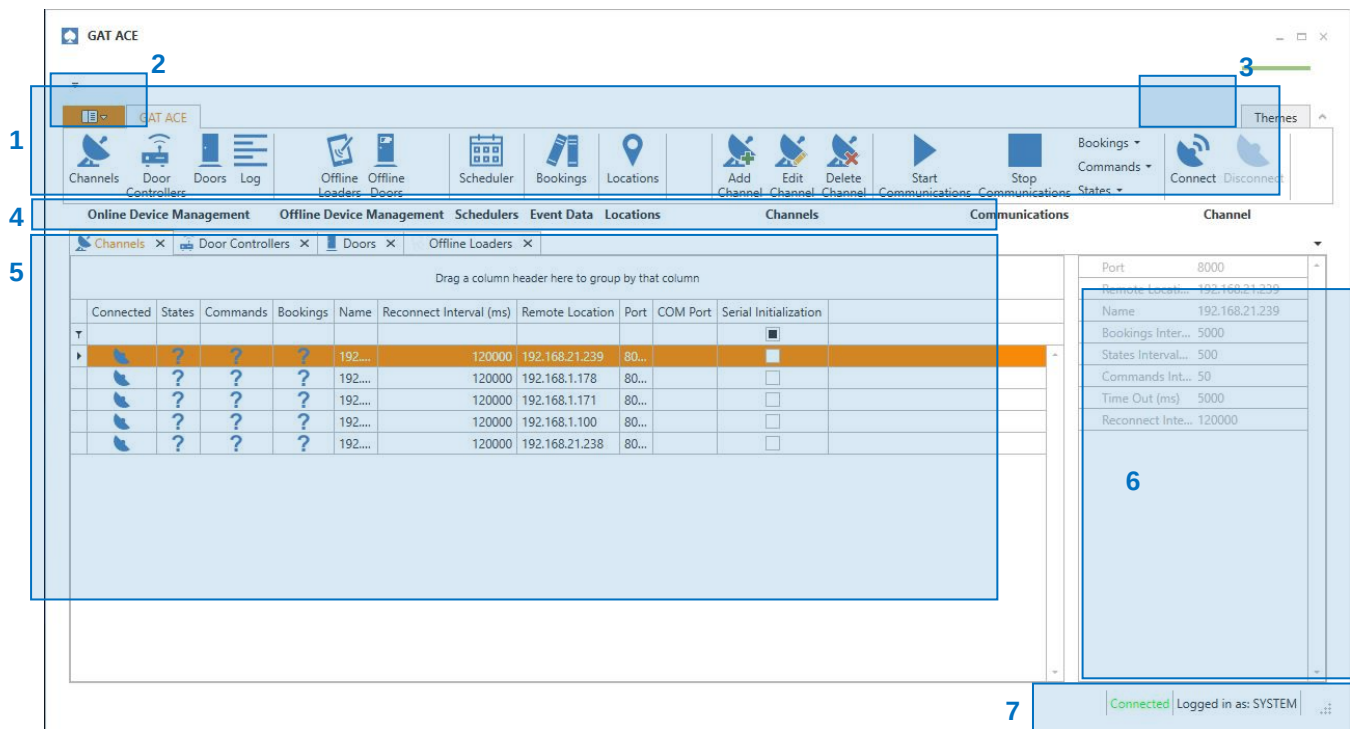


Figure 5.1 - GAT ACE – Main screen

- 1 Multifunction Bar: The left part of this bar includes the icons taking you to the various views of the GAT ACE (refer to section 4 below). Clicking on one of these items will open the corresponding view.
The right part of this multifunction bar displays all functionalities available in the currently selected view.
- 2 Software Settings: This icon takes you to the list of software settings, where various general settings are defined for the GAT ACE. Also refer to chapter "4. CONFIGURATION".

- 3 Design: This option menu allows to change the graphical interface of the GAT ACE.
- 4 List of Open Views: For the listing and processing of channels, controllers, doors, offline loaders and offline doors, log entries, bookings and locations, GAT ACE uses views. The views are displayed in this area (4).
- 5 View: In this area, different functionalities are displayed depending on the selected view. This is the main work area in GAT ACE, where all configurations are done.
- 6 Information Display: Here, more detailed information is displayed regarding the element currently selected in the view.
- 7 Status Display: Here it is displayed whether the GAT ACE Client is connected to the GAT ACE 3000 Service or not. Only if it is "Connected", a communication is possible with the devices / controllers.

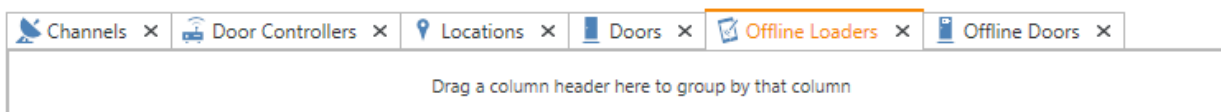


Via the icons displayed above "Online Device Management" and "Offline Device Management" in the multifunction bar, all configuration settings for the controllers, doors and readers of the system can be accessed. By clicking on these symbols, the corresponding view is opened below the multifunction bar.



These icons allow you to switch between the "Scheduler" area, where reoccurring system tasks are scheduled, the "Bookings" area, where all activity recorded in the system is displayed, and the "Locations" area, where the various locations of the access system are defined.

Several views may be open simultaneously in GAT ACE. The desired view is selected via the corresponding tab.



If a tab is moved from the tab bar using the mouse, marks appear showing where they can be moved to in the GAT ACE window. For instance, if you drag a tab to the right side of the window (as shown below) views can be arranged next to each other.

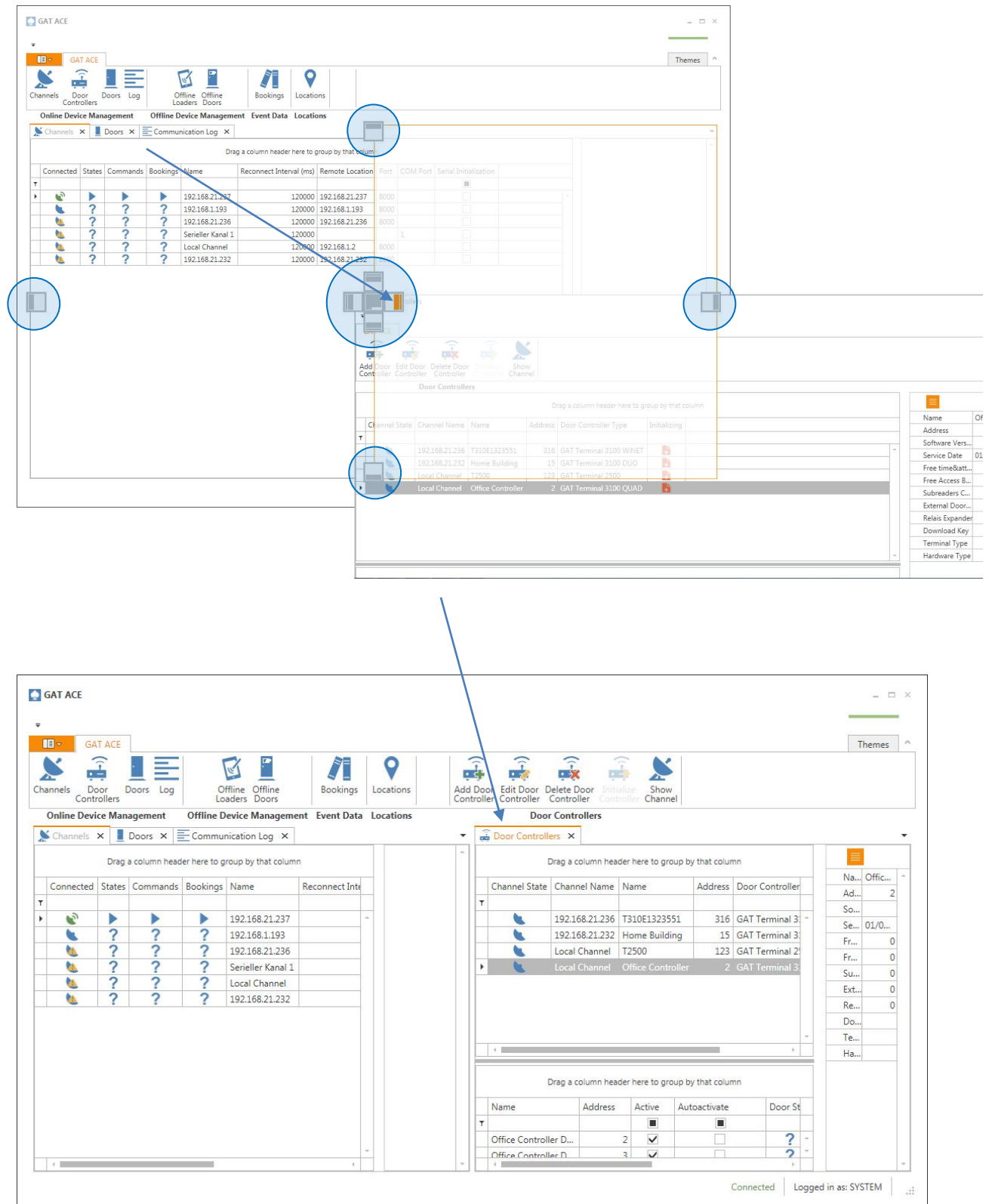


Figure 5.2 - Arranging views

5.1.1 Channels

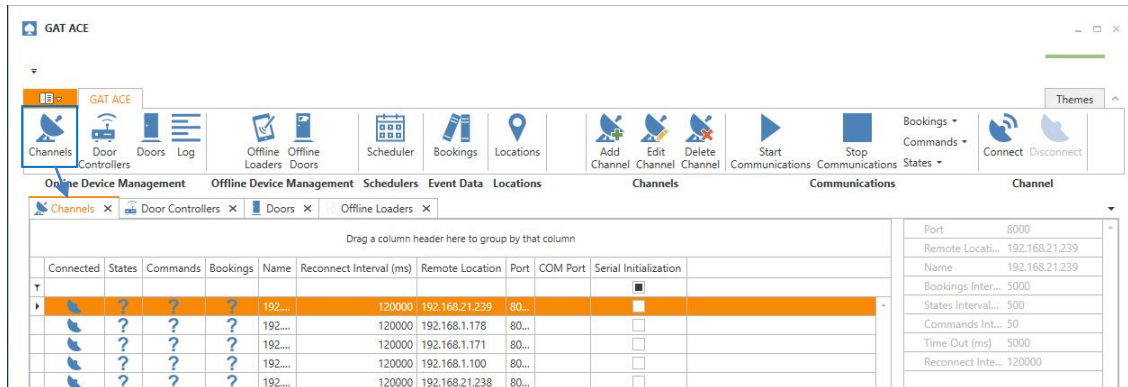


Figure 5.3 – “Channels” view

GAT ACE communicates with the GANTNER controllers via TCP/IP or serial COM connections. The connections are defined in GAT ACE via channels. For each TCP/IP address and each serial interface COM port, a separate channel is created.

The channels can be clearly administrated in the GAT ACE channel list. Within this list, it is also indicated which channels are online, i.e., connected, and which channels might possibly have problems.

For every channel, specific actions are available, e.g., the reading of bookings, the sending of commands, or the querying of the current status.

5.1.2 Door Controllers

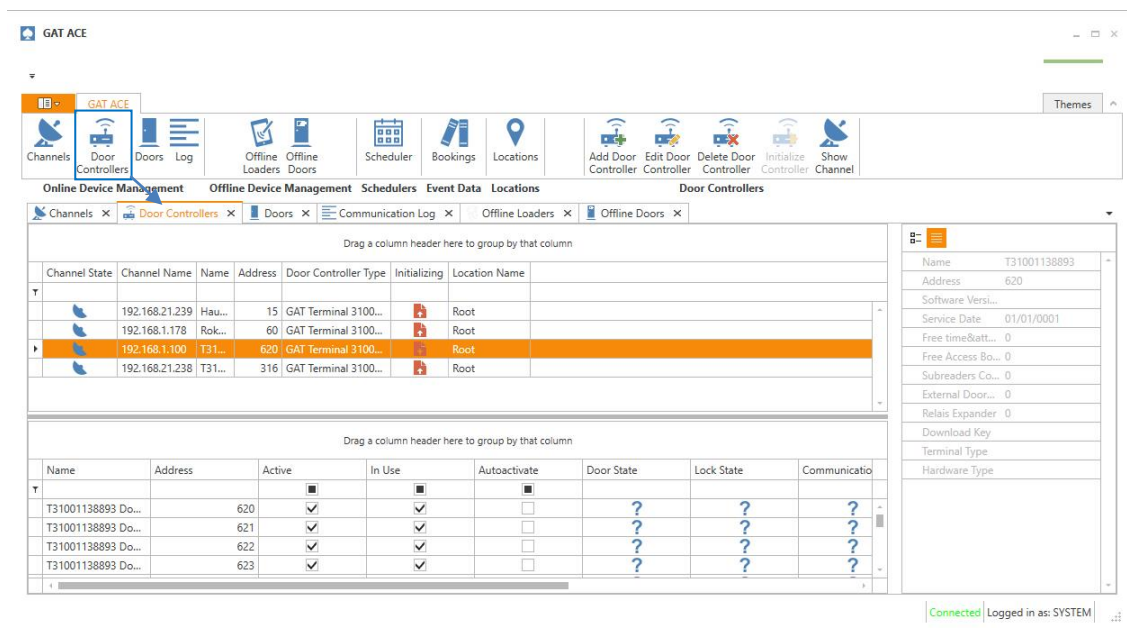


Figure 5.4 – “Door Controllers” view

The devices used for access control at the doors of a system are called controllers. A controller can be used for the access control of one or several doors. Furthermore, depending on the type of controller, one or more readers can be connected. By configuring the controllers and the reader(s) connected to each controller, the functionality of the access system can be adapted to the requirements.

GAT ACE 3000 clearly displays all controllers defined in the system in the shape of a list displayed in the controller view. The most important settings of each controller are directly displayed. Below the controller view, the doors controlled by the selected controller are displayed. Depending on the type of controller, up to 16 doors can be controlled. The unused doors can be deactivated in the list (in the example, for instance the "Quad Door 2" and "Quad Door 3"). For an improved overview, the list can be filtered to only show active doors.

In the Door Controllers view, the settings of every controller can be edited individually, e.g., the characteristics of the communication, the selection of the reader configurations of the readers connected to the controller, as well as the address of the controllers. New controllers can also be added here, while existing controllers can be deleted or reinitialized.

5.1.3 Doors

Name	Address	Active	Autoactivate	In Use	Door State	Lock State	Communication	Initializing	Pending Commands	Battery State	Last Warning Booking	Location
Hau...	15	✓	✓	✓	?	?	?					Root
Hau...	16	✓	✓	✓	?	?	?					Root
Rok...	60	✓	✓	✓	?	?	?					Root
T31...	620	✓	✓	✓	?	?	?					Root
T31...	621	✓	✓	✓	?	?	?					Root
T31...	622	✓	✓	✓	?	?	?					Root
T31...	623	✓	✓	✓	?	?	?					Root
T31...	624	✓	✓	✓	?	?	?					Root
T31...	625	✓	✓	✓	?	?	?					Root
T31...	626	✓	✓	✓	?	?	?					Root
T31...	627	✓	✓	✓	?	?	?					Root
T31...	628	✓	✓	✓	?	?	?					Root

Figure 5.5 – "Doors" view

Every controller in a system controls the access at one or several doors. The maximum number of doors that can be controlled depends on the type of controller (e.g., up to 4 readers connected to a GAT Terminal 3100 Quad) and also how many readers are to be used per door.

All doors in the system are listed in the door view. For every door, the current status of the door (open or closed, if the door feedback has been connected and configured), the locking (locked or unlocked) and whether the communication to the door is online or interrupted, are displayed amongst other information. It is also shown whether a door is already initialized or commands still need to be sent to the door.

In the Doors view, the doors can be directly configured by double-clicking. It is also possible to deactivate or initialize individual doors or to send commands to them.

5.1.4 Reader Configuration

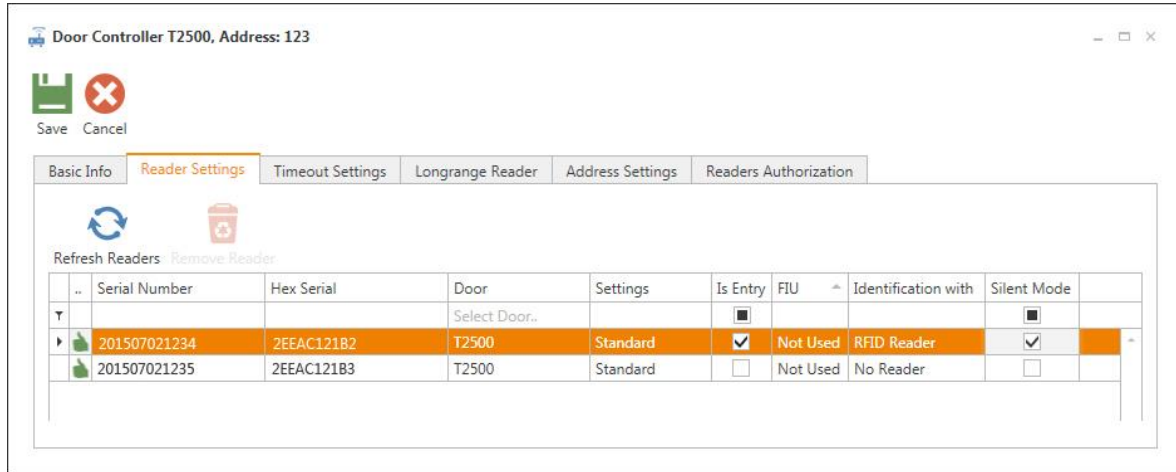


Figure 5.6 - Reader configuration

Depending on the type of controller, one or more readers can be connected to a controller. Extensive settings are available for each reader. The editing of these settings is performed on separate index cards in the controller configuration.

On the "Reader Settings", "WiNET Settings" (only for GAT Terminal 3100 WiNET) and "Longrange Reader" index cards, a functionality (access or exit) can be assigned to each reader, the type of the reader can be selected and the configuration settings can be defined. In addition, the readers are also assigned to the doors in this index card. For example using GAT Terminal 3100 Quad, it is possible to assign every reader to a different door in order to control the access at four doors or assign all 4 readers to a single door or barrier in order to provide different identification options at that door and control both access and exit.

5.1.5 Offline Doors

Offline doors or terminals are not permanently connected to the GAT ACE or a server via an interface. They are configured once and then perform access control autonomously. The configuration of these offline terminals can be performed for example with the GAT MT 010 (GAT ST 22x terminals), GAT DL 090 or GAT DL 092 (GAT DL 3xx terminals).

Per configuration channel (transport device), an interface is created in GAT ACE in the "Offline Loaders" view. By assigning the offline doors to different offline loaders, it is possible to hand over configuration and modification data to the transport device that will actually be able to forward the data to these offline doors. Furthermore, it is possible to subdivide the modification data so several staff member can be involved in uploading data to offline doors (e.g. if the doors are installed at different locations).

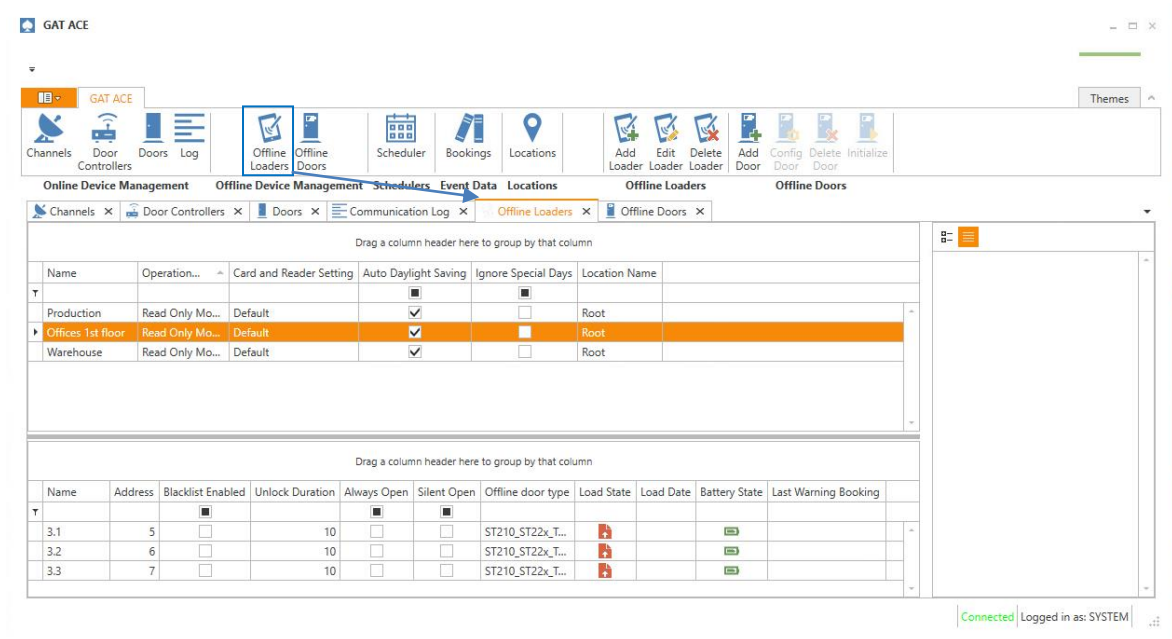


Figure 5.7 – “Offline Loaders” view

The offline terminals are then "virtually" connected via these interfaces (=loaders). An overview of the offline doors is available in the "Offline Doors" view.

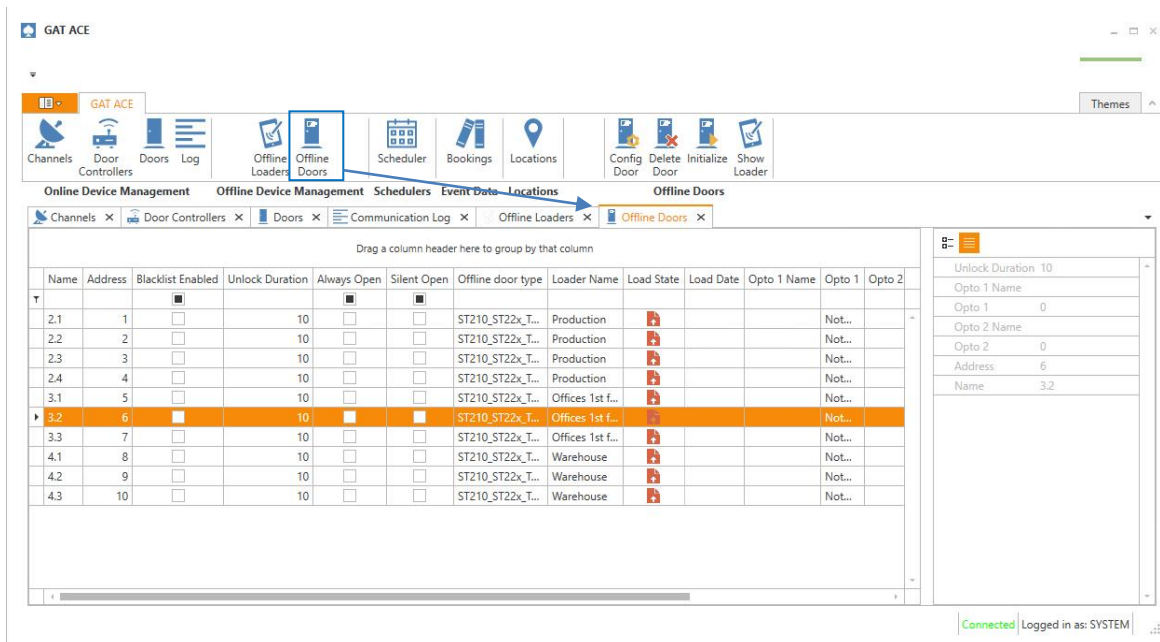


Figure 5.8 – “Offline Doors” view

Here, the most important information is displayed for every door, e.g. address, operating mode, unlock duration, and the functional settings. Via the icons in the multifunction bar, the door configurations can be edited and additional doors can be added.

5.1.6 Scheduler

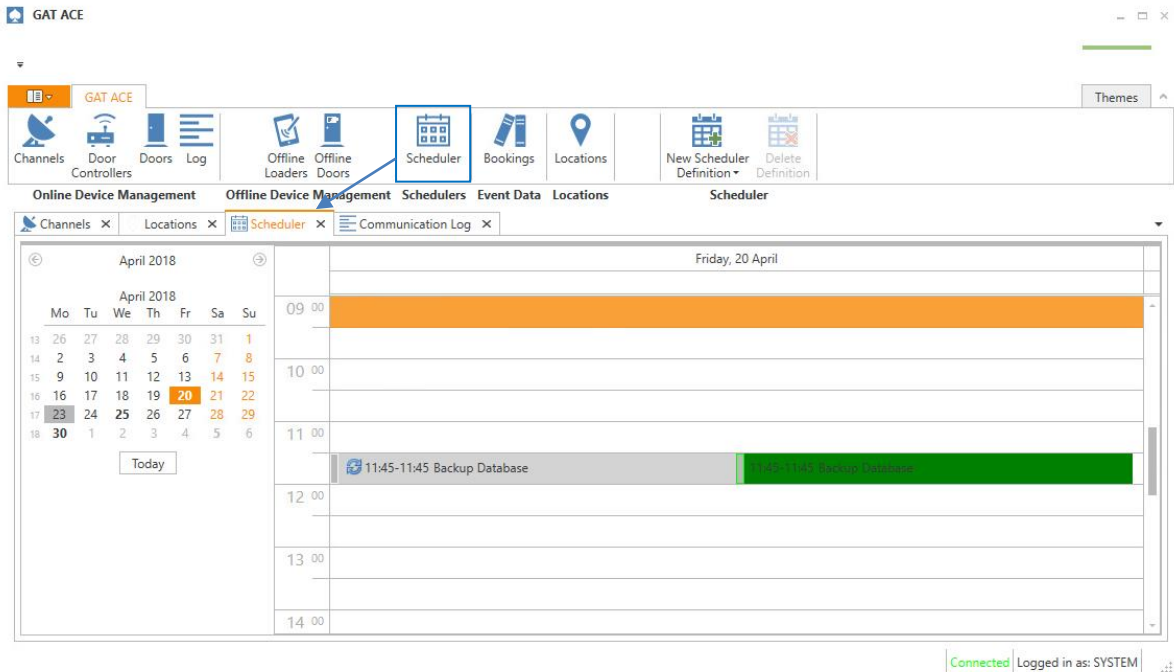


Figure 5.9 – “Scheduler” view

The “Scheduler” is used for setting reoccurring system tasks to execute automatically in GAT ACE 3000. You can use the Scheduler to perform backups of the SQL database or to delete old entries in the bookings database.

After selecting the “Scheduler” view, the current day with all tasks scheduled for the day is displayed. Use the calendar to the left to navigate to a different date.

5.1.7 Bookings

All controllers in the access control system record the movements occurring at the controllers (valid identification or attempted identification using a data carrier), and also important system events. Depending on the event, information is stored regarding the used data carrier, date and time, type of booking, and further details. These bookings thus enable a follow-up of all processes occurring at the controllers. With GAT ACE, the bookings can be downloaded from the controllers and viewed on the screen, searched, evaluated, and exported.

Time bookings from time & attendance terminals can be loaded, displayed and exported in GAT ACE as well. This function is only available if the licence for the corresponding module is activated (see “4.4. “Application Settings” Page”).

5.1.8 Locations

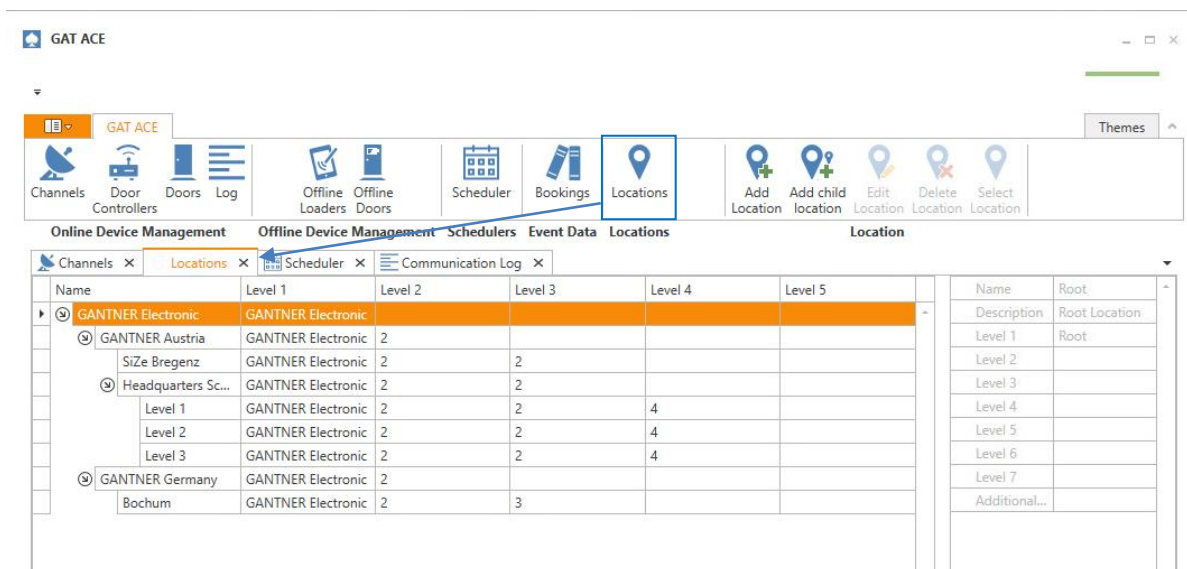


Figure 5.10 – Locations

In order to structure larger systems or the access control of a company with several business sites for example, the GAT ACE location administration can be used. The locations are defined in a structural tree. The locations can then be assigned to the individual controllers during controller configuration.

This functionality helps to sort the list of controllers. For example, it is possible in larger systems to only display the controllers and doors of a selected location.

When uploading offline doors, the uploading procedure can be simplified if the location is considered, by only displaying the doors included in the current location.

5.1.9 Card Settings

RFID data carriers are used for the identification at the access controllers. In order to guarantee the system security and assure only suitable data carrier can be used in the system, the controllers check specific characteristics on the data carriers.

In the software settings, it can be set exactly which data carriers may be used. Refer to section "4.5. "Card and Reader Settings" Page".

5.1.10 Anti-Pass-Back Areas

The Anti-Pass-Back function is used to prevent multiple persons from gaining access simply by handing the same data carrier from one person to the next. The Anti-Pass-Back Areas are configured in the software settings. For further information regarding the Anti-Pass-Back functionality refer to section "4.3. "Anti-Pass-Back Areas" Settings Page".

5.1.11 Evaluating Log Files

GAT ACE can display the communication with the controllers for analysis purposes. In this view, specific information can be searched for or filters can be activated.

NOTE! This functionality requires a significant amount of performance and system resources. It is recommended to activate this functionality only for a single communication channel and only for the time needed to conduct the analysis. If the functionality remains active too long, it may occur that the user interface becomes inoperable due to the numerous messages and has to be restarted!

For the long term recording of communications, other options are available as well. Please contact our support team for further information.

5.2 Configuring an Access System

This section describes the basic configuration procedure of an access control system with GAT ACE. The main points are described, that normally require to be set once for every system. The description of the further settings and functionalities is included in the following chapters.

5.2.1 Defining a Communication Channel

Every controller must be assigned to a communication channel. The configuration of the channels enables a communication with the controller. Channels can be started or stopped in order to start or interrupt the communication with the controllers connected to the channel.

- Click on the "Channels" icon.
 - The list of channels is displayed.

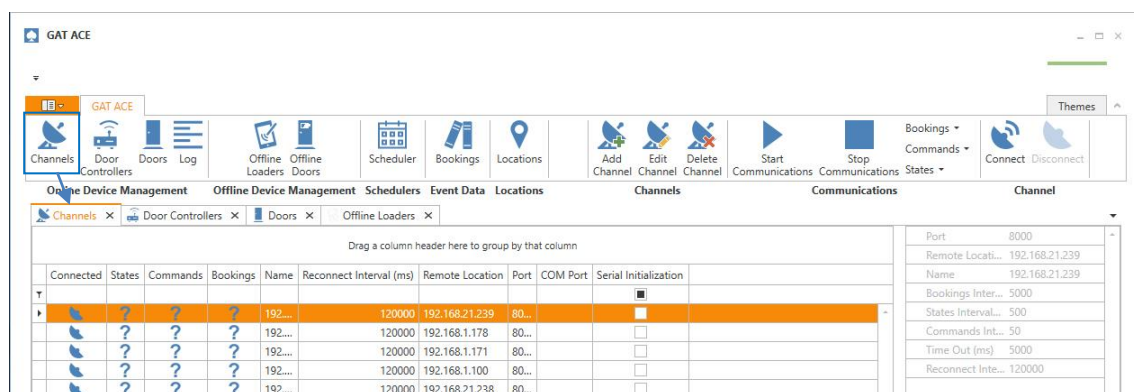


Figure 5.11 – Channel view

The status of every channel is indicated by a symbol in the "Connected" column:

-  The channel is not connected, i.e. there is no communication with the controllers via this channel. GAT ACE does not perform any connection attempts automatically.
-  The connection via this channel is momentarily interrupted, i.e. there is no communication with the controllers via this channel. GAT ACE performs connection attempts automatically. Once the connection has been re-established successfully, the symbol below will be displayed automatically.
-  The channel is connected and a communication occurs.

In the columns "Status", "Commands" and "Bookings", the following symbols are displayed:

-  The functionality (status query, sending of commands to the controller, booking query) is activated.
 -  The functionality (status query, sending of commands to the controller, booking query) is deactivated.
- Note:** The functionalities can be activated or deactivated by right-clicking with the mouse and selecting the corresponding option in the pop-up menu.
-  The status of the corresponding functionality could not be determined, as the channel is not connected.

In the list of channels, the following functions are available in the multifunction bar:



- In order to add a new channel, click on the "Add Channel" icon.
- To edit an existing channel, select the desired channel in the list and click on the "Edit Channel" icon.
 - In both cases, the "Channel Properties" window opens.

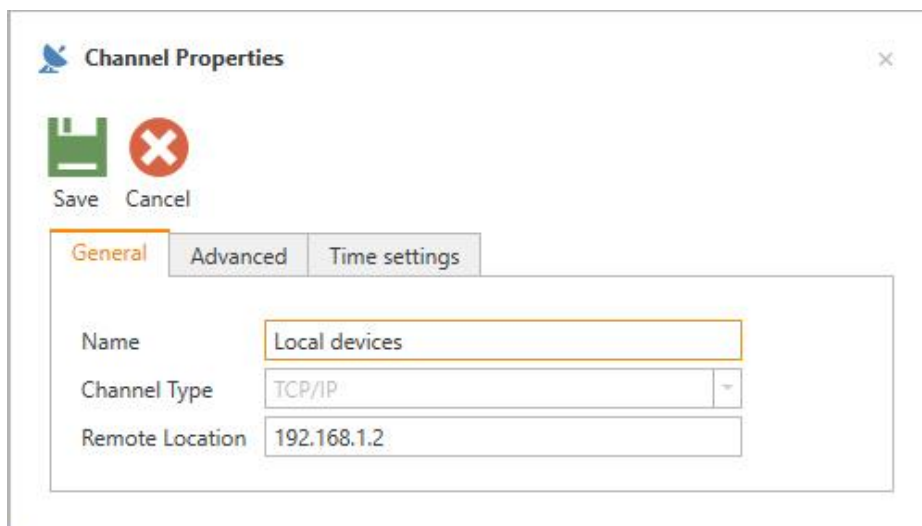


Figure 5.12 - General channel settings

- Enter the following data:
 - Name: The channel will be listed under the name entered here.
 - Channel Type: Selection of the type of connection at this channel. The options are "TCP/IP" (Ethernet connection) or "COM" (serial connection via RS-485 interface).
 - Remote Location: Only displayed for TCP/IP connections. Enter the IP address or, if available, the network name of the controller connected to this channel.
 - COM Port: Only displayed for serial COM connections. Select the PC's COM port used for the communication.
 - Baud Rate: Only displayed for serial COM connections. Select the transmission speed of the selected channel. The Baud rate must match the setting of the controllers connected via this channel.
- Switch to the "Advanced" tab in order to define further channel settings.
 - The following settings are displayed.

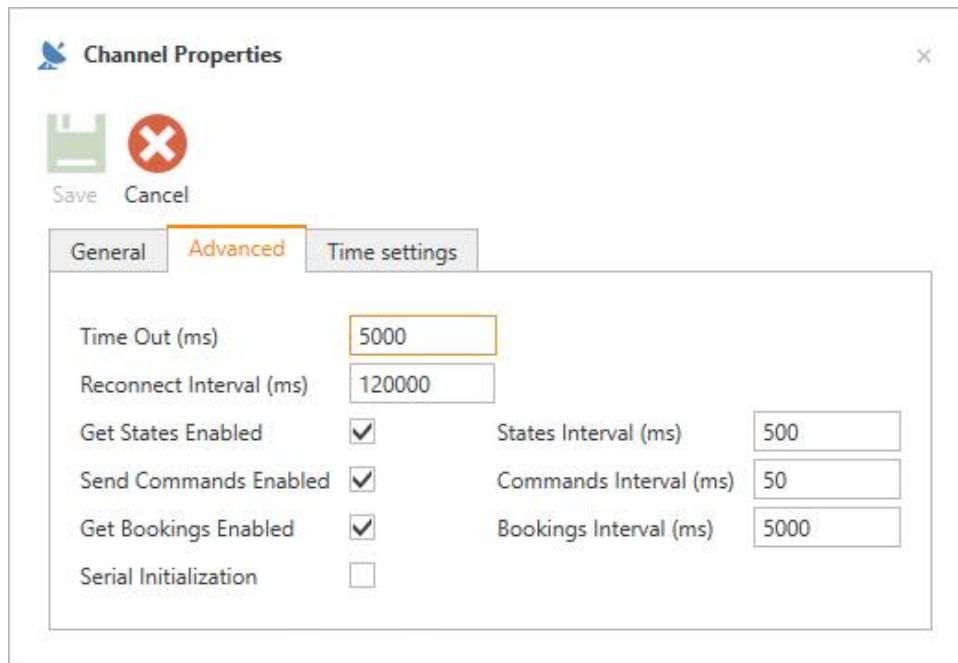


Figure 5.13 - Advanced channel settings

► Define the connection settings here:

- Port: This setting is only displayed for TCP/IP connections. Enter the port to be used for the communication via this channel (default = 8000). Make sure that the port entered here is open in the firewall configuration of the PC.
- Time Out (ms): The time (in milliseconds) a communication waits for a response to it. If no response is received within this time, the communication via this channel is interrupted.
- Reconnect Interval (ms): If the communication via this channel is interrupted, GAT ACE will attempt at the intervals set here to re-establish communication. This is indicated by the 📶 symbol in the channels list.
- Get States Enabled: If this box is checked, the state of the doors is queried via this channel at the interval indicated (in milliseconds) in the field to the right. If the door states via this channel is irrelevant, this function can be deactivated in order to improve the performance of other functions.
- Send Commands Enabled: If this box is checked, commands are sent via this channel to initialize the connected doors at the intervals indicated (in milliseconds) in the field to the right. If all initialization commands have been sent, the door is operational. In order to carry out the initialization quickly, a short interval (e.g. 50 ms) is recommended. However, if it is more important to quickly identify the bookings or changes to the door states, the interval for send commands should be increased and the other intervals decreased. If send commands are disabled, the initialization data is no longer sent to the doors of this channel.
- Get Bookings Enabled: If this box is checked, the bookings from the doors of this communication channel are read periodically in the time intervals indicated (in milliseconds) in the field to the right. If the bookings for these doors connected via this channel

are irrelevant, read bookings can be disabled here in order to gain performance for other functionalities. If the bookings should be available quickly for further processing, the interval for read bookings can be shortened.

- Serial Initialization:

When using serial channels with a lot of door controllers you should mark this option. This prevents excessive out-of-operation times of the controllers, when they are initialized.

NOTE! If this option is not marked, the memory of each controller on the channel is first erased and then the controllers are initialized one after the other. This means that the last controllers can be out-of-operation for a long time. By activating this function you can prevent this because the memories will then be erased one after the other, only if a controller is initialized.

- Switch to the "Time settings" tab in order to define the time zone and daylight saving times for the channel.
 - The following settings are shown.

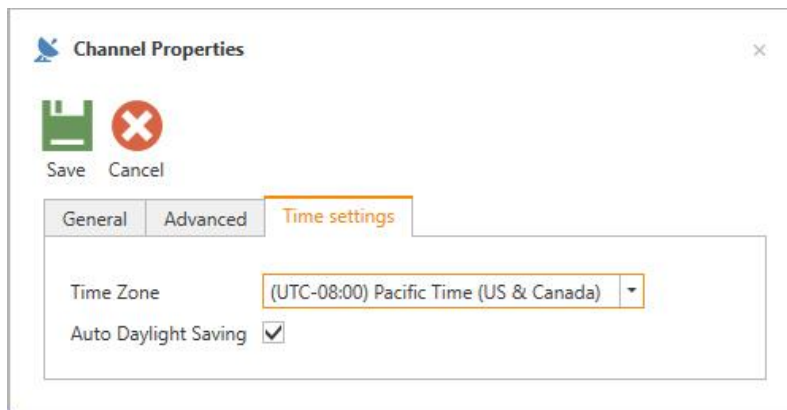


Figure 5.14 - Time settings for a channel

- Define the following settings:
 - Time Zone: Select the time zone, where the channel and connected devices are located.
 - Auto Daylight Saving: If this option is marked, GAT ACE 3000 will calculate and perform the change between standard and daylight saving time automatically.
- Save the settings by pressing the "Save" button.

5.2.2 Structuring Locations

The entering of locations is not absolutely necessary in the configuration procedure of an access control system in GAT ACE. However, a division into locations can be very useful, particularly for larger systems or if a company has several sites (locations).

- Select the "Locations" icon.
 - The "Locations" view opens.

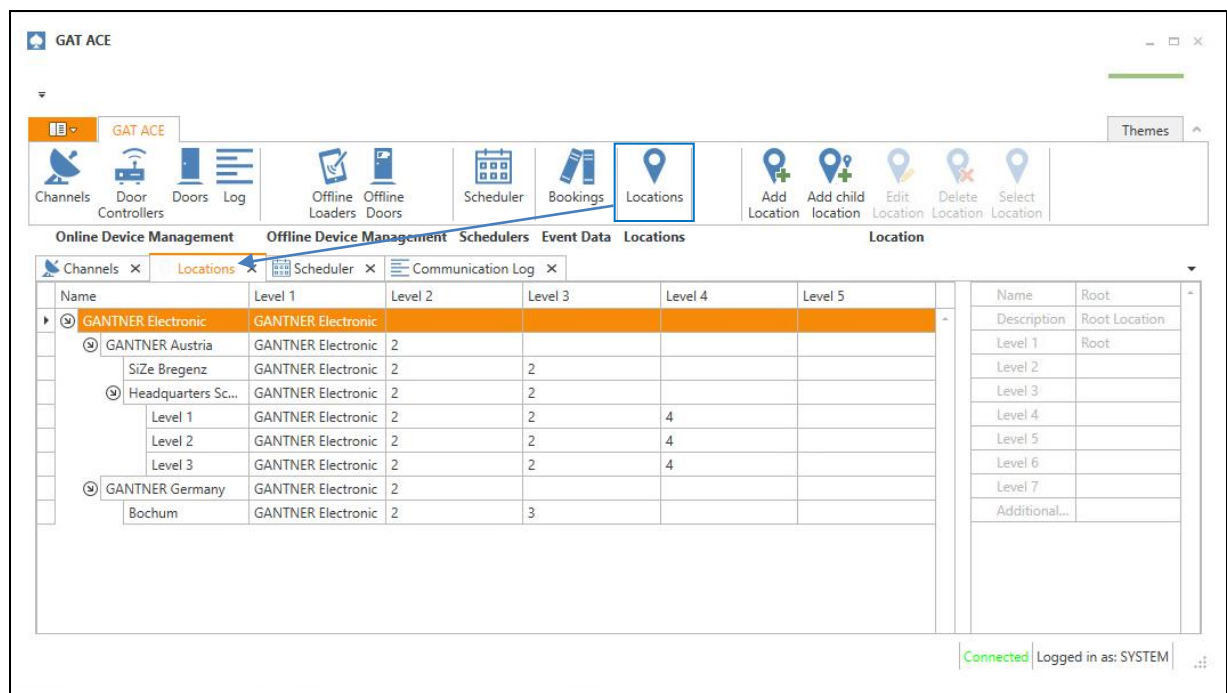


Figure 5.15 - Locations

- In the locations view, the following functions are available in the multifunction bar:



- Select the "Add Location" icon in order to add a new location.
 - The following window is displayed.

Figure 5.16 – Entering new locations

- ▶ Enter the following information:
 - Parent Location: By clicking on "Select", a list is displayed, from which an already existing location can be selected. The new location is then added to the tree structure one level below the selected location. If nothing is selected here, the new location is added at the highest level of the tree structure.
 - Level x: If a parent location is selected, the levels 1 to 6 of this location are displayed with their names. Now, a new value can be entered for the new level in order to create new locations. The higher level values cannot be changed with this functionality. In order to do this, select the editing of the higher-level locations.
 - Additional Info: If desired, additional information or a more detailed description of the location to be added can be entered here. Whenever this location is selected, this information will be displayed in the information area on the right.
 - Name: Name of the location, as displayed in the tree structure. The location name is automatically composed of the names of its levels. However, this automatically generated name can also be overwritten and replaced by another name.
 - Description: A short additional description of the location. Whenever this location is selected, this description will be displayed in the information area on the right.
- ▶ Confirm by pressing the "Save" button.
 - The new location will be added at the corresponding place in the tree structure.
- ▶ With the "Add Child Location" icon, an additional sub-location can be inserted at the marked location.
- ▶ With the "Edit Location" icon, the settings of an existing location can be changed.
- ▶ With the "Delete Location" icon, a selected location can be deleted.
- ▶ The "Select Location" icon is used during the adding of a location in order to select a higher level location.

5.2.3 Adding a Controller

In order to configure a controller, it first has to be inserted into the list of controllers.

- Select the "Door Controllers" icon.
 - The "Door Controllers" view opens.

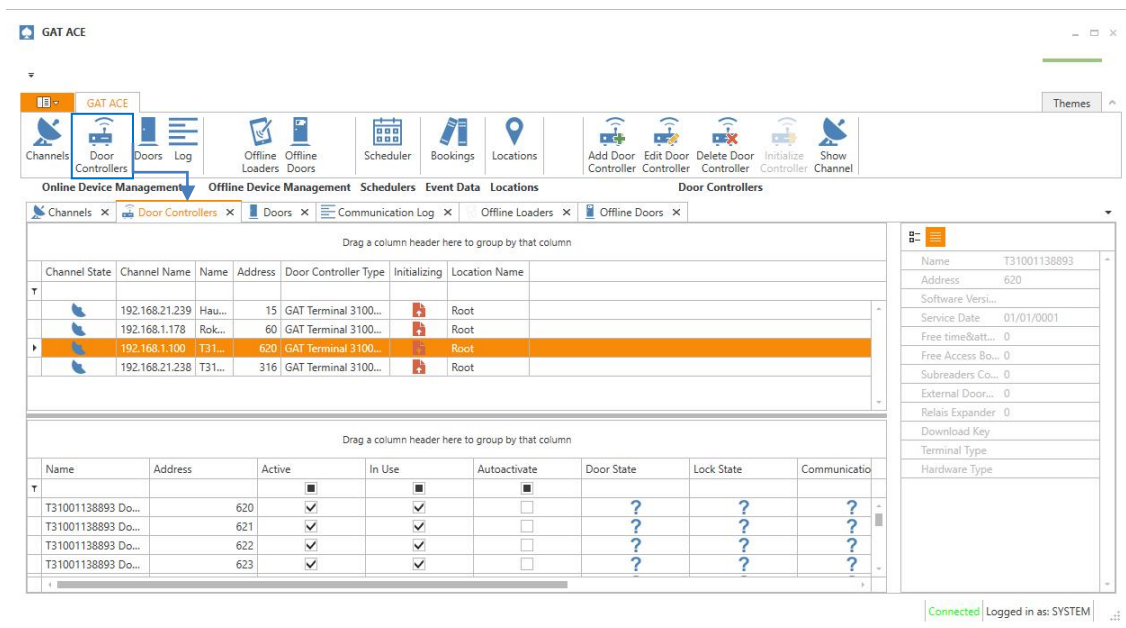
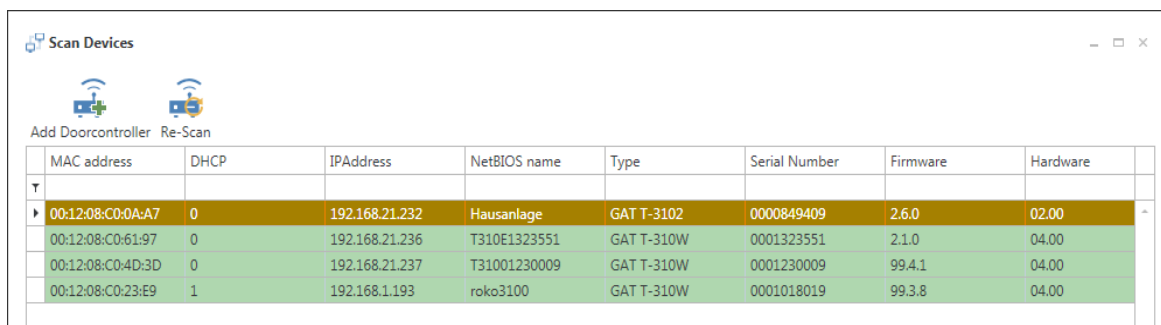


Figure 5.17 – Door Controllers view

- GAT ACE clearly displays all controllers defined in the system by listing them in the controller view. The most important settings for each controller are directly visible. In the "Channel Status" column, the current status of each controller is indicated.
 - The controller is not connected, i.e. there is no communication with the controller.
 - The controller is connected and a communication takes place with this controller.
- Below the controller view, the doors controlled by the selected controller are displayed.
- In the controller view, the following functionalities are available in the multifunction bar:



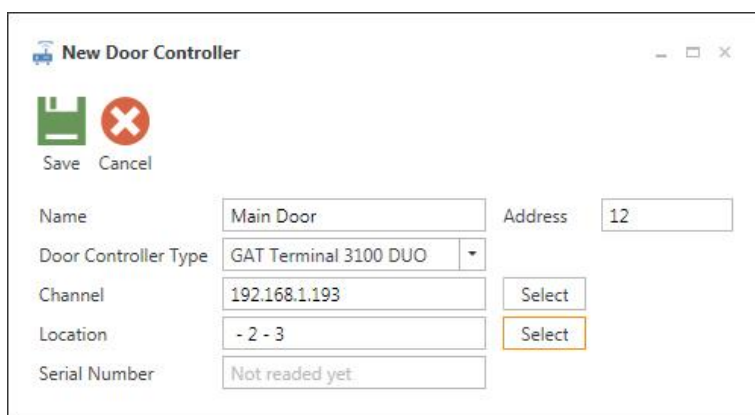
- With the "Show Channel" icon, GAT ACE directly displays the channel to which the selected controller is connected.
- Select the "Add Door Controller" icon in order to add a new controller to the list.
 - A query box is displayed, asking whether the network should be searched for controllers or not.
- Select "Yes" if the desired controller is connected to the TCP/IP network and a search should be conducted for this controller in the network.
 - The network is searched and all the controllers found are displayed in a new window.



MAC address	DHCP	IP Address	NetBIOS name	Type	Serial Number	Firmware	Hardware
00:12:08:C0:0A:A7	0	192.168.21.232	Hausanlage	GAT T-3102	0000849409	2.6.0	02.00
00:12:08:C0:61:97	0	192.168.21.236	T310E1323551	GAT T-310W	0001323551	2.1.0	04.00
00:12:08:C0:4D:3D	0	192.168.21.237	T31001230009	GAT T-310W	0001230009	99.4.1	04.00
00:12:08:C0:23:E9	1	192.168.1.193	roko3100	GAT T-310W	0001018019	99.3.8	04.00

Figure 5.18 – Searching the network for controllers

- Select the desired controller.
 - NOTE!** The controllers marked in green are already included in the GAT Ace list of controllers.
- Add the controller to the list by pressing the "Add Door Controller" icon.
 - The list of controllers is displayed again, with the new controller included.
- Select "No" if a new controller is to be added manually.
 - The "New Door Controller" window is opened.



New Door Controller

Save Cancel

Name: Main Door Address: 12

Door Controller Type: GAT Terminal 3100 DUO

Channel: 192.168.1.193 Select

Location: - 2 - 3 Select

Serial Number: Not readed yet

Figure 5.19 - New door controller

- Enter the following data regarding the new controller:
 - Name: Name of the controller, by which it will be displayed in GAT ACE.
 - Address: Every controller in a system has a unique address, by which it can be contacted.
 - Controller Type: All types of controllers supported by GAT ACE 3000 are listed here. Select the correct type.
 - Channel: Selection of the channel to which the controller is to be added. If no channel has been created for the controller, click on the "Select" button in order to create a new channel. For information regarding how to define a channel, refer to "5.2.1 Defining a Communication Channel".
 - Location: A location for the controller can be selected here. It is not absolutely necessary to select a location here. But for larger systems, the overview in GAT ACE can be improved significantly by assigning a location, as the list of controllers can then be filtered by locations.
 - Serial Number: At the initialization of the controller, its serial number is read and displayed in this field. Not all controllers offer the functionality of having their serial number read.

- ▶ Confirm by clicking the "Save" button in order to insert the new controller into the list of controllers.
 - The list of controllers is displayed, with the new controller inserted.
- ▶ In order to delete a controller from GAT ACE, mark the controller and then press the "Delete Controller" button.

5.2.4 Configuring a Controller

In order to set the configuration of a controller, proceed as follows:

- ▶ Mark a controller in the list of controllers and press the "Edit Controller" icon in order to configure the settings of the marked controller.
 - The controller configuration window opens.

The screenshot shows a configuration window titled "Door Controller T31001138893, Address: 620". At the top left are "Save" and "Cancel" buttons. Below them are tabs for "Basic Info", "Reader Settings", "WiNet Settings", "Timeout Settings", "Longrange Reader", and "Address Settings". The "Basic Info" tab is selected. It contains the following fields:

Name	T31001138893	Address	620
Door Controller Type	GAT Terminal 3100 WiNET		
Channel	192.168.1.100	Select	
Location	GANTNER Electronic	Select	
Serial Number	0001138893		

Figure 5.20 – Controller configuration

The settings of the controller are arranged on several different tabs. For every controller only the tabs, that are necessary for the controller type, will be shown.

Complete or edit the settings on the controller page, if they are incomplete or incorrect. The data is the same as the one described for the manual creation of a new controller.

5.2.5 Configuring and Assigning a Reader to a Controller

The readers connected to or installed in a controller must be configured correctly in order to function properly. The configuration is done on a separate tab in the controller configuration. For controllers controlling more than one door, the readers are also assigned to the doors.

Complete the following steps:

- ▶ Call up the controller configuration by double-clicking on the corresponding controller in the list of controllers.
 - The controller configuration window is displayed.
- ▶ Switch to the "Reader Settings" tab.
 - The "Reader Settings" tab is displayed.

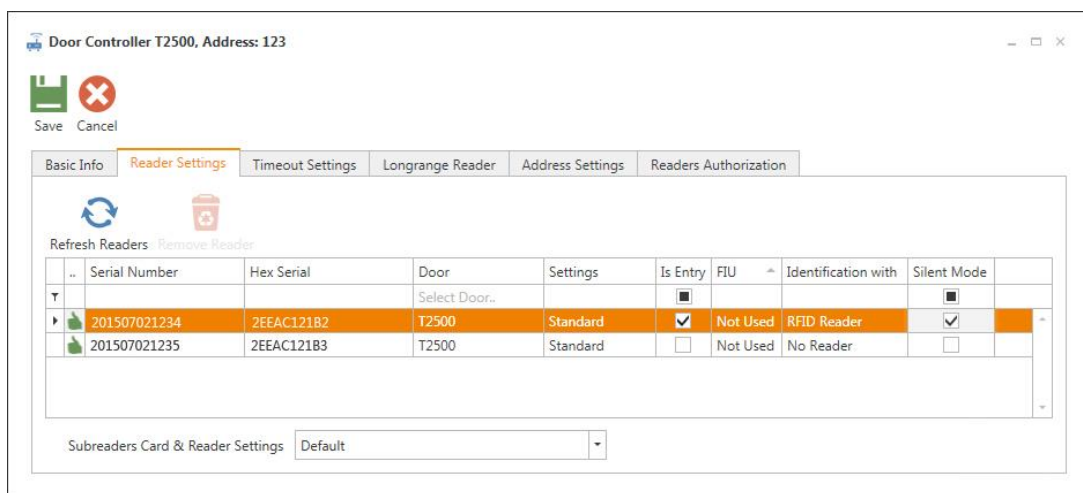


Figure 5.21 - Configuration and assigning of readers connected to the controller

- ▶ With the "Refresh Readers" icon, the readers connected to the controller via an RS-485 interface can be searched. Installed readers are displayed without a search.
 - The identified readers are listed.
- ▶ The following information is displayed for each reader:
 - Serial Number (decimal): Serial number of the reader in decimal form.
 - Serial Number (HEX): Serial number of the reader in hexadecimal form.
 - Door: Selection of the door to which the reader is to be assigned. If several readers are assigned to the same door, the separate control of entrances and exits is possible or several identification points are available (e.g. cars and trucks).
 - Settings: This selection determines which data carriers can be used at the reader (coding, RFID type, etc.). The card settings selectable here are defined in the software settings (refer to "4.5. 'Card and Reader Settings' Page).
 - (Is) Entry: This setting determines whether a reader is used as an entrance or exit reader. With 2 readers on a door, it can be determined which reader will be used for entering and which one for leaving. This setting is important for indicating the direction in the bookings, as well as for anti-pass-back.
 - FIU (fingerprint reader): This value determines the functionality of the fingerprint reader. If no fingerprint reader is connected, the setting to choose is "Not In Use". If the fingerprint is to be used to verify the card holder, choose the "Verification" setting. If the fingerprint is to be used to identify persons via fingerprint, choose the "Identification" setting.

- Identification with: With the setting "Card", the identification can only occur with cards, or in the event of a biometric identification also with a fingerprint. With the setting "Card or Keypad", persons with a special authorization can also identify themselves by entering their staff number. For these persons, it is recommended to activate verification via PIN code or fingerprint.
- Silent Mode: This setting can be used with the readers of the new generation 73xx. When the setting is activated (hook), the reader is in silent mode which means the beeper of the reader is deactivated and doesn't produce acoustic signals.
- ▶ In the field "Subreaders Card & Reader Settings" you can select one of the pre-defined card and reader settings, in order to determine which data carriers can be used at a sub reader of the selected controller.
 - The card and reader settings are defined in the configuration menu of GAT ACE 3000 (see "4.5. "Card and Reader Settings" Page").
- ▶ Confirm the configuration by pressing the "Save" button.
 - The controller view is displayed.



Please note that the controller must be uploaded again before the settings become effective. The uploading can be done automatically or manually (refer to "5.2.12 Initializing Doors").

5.2.6 WiNET Settings for Offline Controllers

For controllers of the type "GAT Terminal 3100 WiNET", the WiNET settings can be edited. This tab is not shown for other controllers. On this tab, the available door locks and the connected WiNET Access Points are shown.

- ▶ Call up the controller configuration by double-clicking on the corresponding controller in the controllers list.
 - The controller configuration window is displayed.
- ▶ Switch to the "WiNET Settings" tab.
 - The "WiNET Settings" tab is displayed.

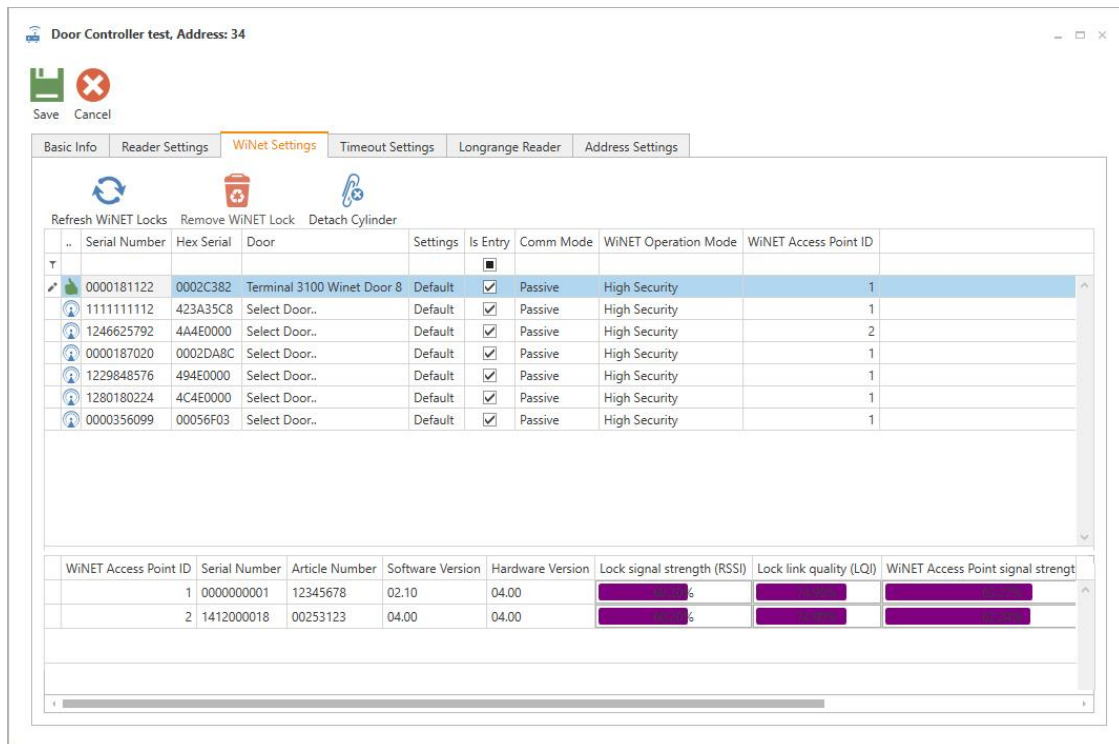


Figure 5.22 - Configuration of the WiNET settings

► Press the button "Refresh WiNET Locks".

- The controller searches for WiNET locks and shows all detected locks in the list above.
- In the list below, all WiNET Access Points, which are connected to the controller, are listed.

NOTE! If two or more Access Points are connected and one of these Access Points becomes unavailable (e.g., disconnected), the other Access Points are also not shown anymore, i.e., the list is empty.

- "Remove WiNET Lock": If a WiNET lock in the list is not in the communication range of the WiNET Access Point anymore, an error is displayed for that lock. This lock can be deleted (e.g., because it is defective), by marking it in the list and then clicking on the "Remove WiNET Lock" button.
- "Detach Cylinder": If a WiNET lock is being replaced (e.g., if the lock is being repaired or being installed at another door that is controlled by another controller), the currently used lock must be disconnected from the controller and deleted from the database by clicking on the "Detach Cylinder" button. This process must be completed in order to use the lock again at a door after repair. If this process is not completed, the WiNET lock cannot be assigned anymore since the serial number of a lock can only be used once in the system. The "Detach Cylinder" function is also necessary for when the WiNET lock is only stored in the controller list but not assigned to a door. In order to use the WiNET lock at another controller, the lock must first be reset to factory settings and WiNET mode activated again.

NOTE! Please note that when you detach a WiNET lock, the entire WiNET controller must be initialised, including memory initialisation.

5.2.7 Configuring the Time Settings for Readers

For the controllers and readers, times can be configured that are relevant for certain functionalities, e.g., the duration of a display or the time available to make an entry.

- ▶ Call up the controller configuration by double-clicking on the corresponding controller in the list of controllers.
 - The controller configuration window is displayed.
- ▶ Switch to the "Timeout Settings" tab.
 - The "Timeout Settings" tab is displayed.

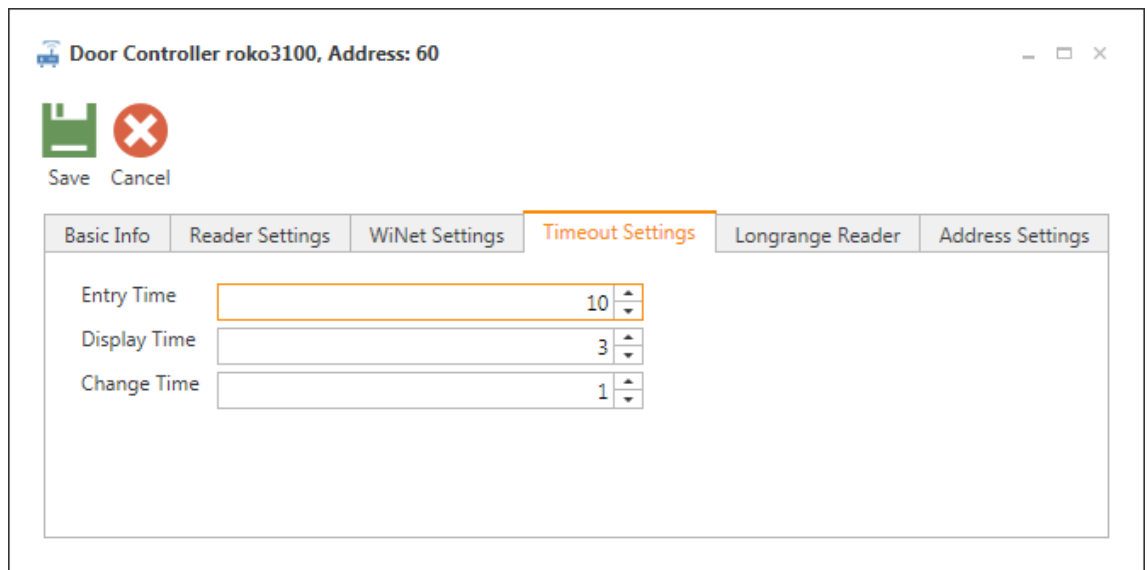


Figure 5.23 – Defining the time settings for the readers of the controller

- Entry Time: This value (in seconds) determines the available time for entering a PIN code or scanning a fingerprint.
- Display Time: This value (in seconds) determines for how long the reader will indicate a user - information on a display e.g. "Access Granted " or "Access Denied " and/or by LEDs on the reader, prior to returning to the basic state.
- Change Time: This value (in seconds) determines for how long the successful generation of a time booking will be displayed, before switching to the access display. This setting is only relevant for the configuration "Time Booking with Automatic Access", available only on some controllers.

5.2.8 Configuring a Longrange Reader

If a longrange reader GAT Reader 868 is used at a controller, this reader can be configured on a separate tab.

- ▶ Call up the controller configuration by double-clicking on the corresponding controller in the list of controllers.
 - The controller configuration window is displayed.
- ▶ Switch to the "Longrange Reader" tab in order to set the settings of this reader.
 - The "Longrange Reader" tab is displayed.

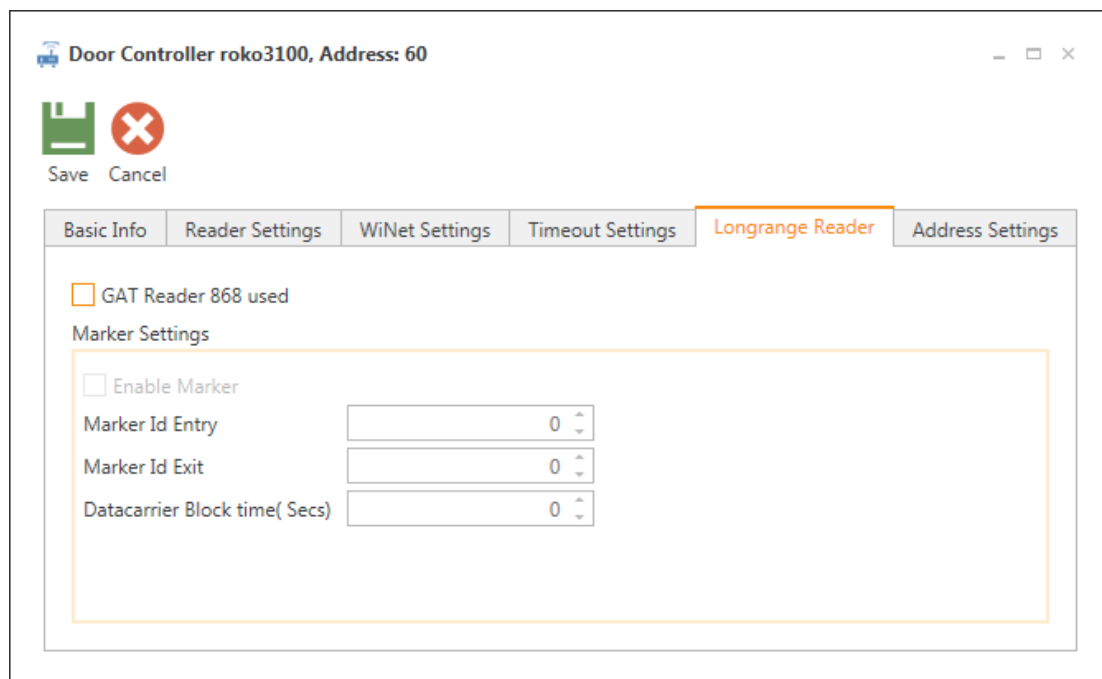


Figure 5.24 – Configuring a longrange reader

- ▶ If a GAT Reader 868 longrange reader is connected to the controller, check the "GAT Reader 868 in use" option box.
- ▶ Enter the following information below:
 - Enable Marker: Markers can be used in longrange readers to determine the direction of movement. For a longrange reader, 2 markers can be used. If a data carrier is identified, the marker is used to tell on which side the data carrier is located (inside or outside). It is also possible to use longrange readers without markers. If markers are to be used, check the "Enable Marker" option box.
 - Marker ID Entry: Enter the card number of the marker used for accessing.
 - Marker ID Exit: Enter the card number of the marker used for exiting.
- ▶ In order to conclude the controller configuration, press the "Save" icon.
 - The controller view is displayed.



Please note that the controller must be uploaded again before the settings become effective. The uploading can be done automatically or manually (refer to "5.2.12 Initializing Doors").

5.2.9 Configuring Doors

Every type of controller has a maximum number of doors it can control. If a new controller is created in GAT ACE, the maximum number of doors is displayed by default. The number of doors actually used has to be configured in order to determine the access functionality accordingly.

In the configuration of a "Door", all settings required to determine the access functionality are united, e.g. the settings for the unlocking times, the settings of the relay outputs and optocoupler inputs, as well as the other functionalities such as anti-pass-back or double check principle.

NOTE! In GAT ACE, the terms "Reader" and "Door" must be differentiated: "Reader" describes the true physically installed reader units, while "Door" describes the object to be controlled (door, gate, etc.). For example, a GAT Terminal 3100 QUAD allows the connection of four readers. Depending on the installation of the readers, the controller can control just one door (as all four readers are installed at this door) or up to four different doors (one reader per door).

There are two basic options for displaying the doors in a system.

- During the configuration of the controllers: If a controller is selected, the doors assigned to it are displayed in the list below (left figure).
- By pressing the "Doors" icon in the multifunction bar, the door view is displayed, listing all doors in the access system (right figure).

This screenshot shows the 'Doors' view for a selected controller. The table lists doors assigned to the controller, including their addresses, names, and types.

Channel S...	Channel Name	Name	Address	Door Controller Type	Initializing
192.168.1.200	T31001230009	16 - GAT Terminal 3100 WHNET			
192.168.1.193	roko3100	60 - GAT Terminal 3100 WHNET			
192.168.21.236	T310E1323551	316 - GAT Terminal 3100 WHNET			
192.168.21.232	Hausanlage	15 - GAT Terminal 3100 DUO			
Lokaler Kanal	T2300	123 - GAT Terminal 2300			
Serialer Kanal 1	CAD Büro	1 - GAT Terminal 3100 ECO			
Lokaler Kanal	Office Controller	2 - GAT Terminal 3100 QUAD			

Doors of the selected controller

This screenshot shows the 'Doors' view for the entire system. The table lists all doors in the system, including their addresses, names, and various status indicators.

Name	Address	Active	Autoactivate	Door State	Lock State	Communication	Initializing	Pending Commands
T31001230009 Door 1	16	☒	☐	?	?	?		
T31001230009 Door 2	17	☒	☐	?	?	?		
T31001230009 Door 3	18	☒	☐	?	?	?		
T31001230009 Door 4	19	☒	☐	?	?	?		
T31001230009 Door 5	20	☒	☐	?	?	?		
T31001230009 Door 6	21	☒	☐	?	?	?		
T31001230009 Door 7	22	☒	☐	?	?	?		
T31001230009 Door 8	23	☒	☐	?	?	?		
T31001230009 Door 9	24	☒	☐	?	?	?		
T31001230009 Door 10	25	☒	☐	?	?	?		
T31001230009 Door 11	26	☒	☐	?	?	?		
T31001230009 Door 12	27	☒	☐	?	?	?		
T31001230009 Door 13	28	☒	☐	?	?	?		
T31001230009 Door 14	29	☒	☐	?	?	?		
T31001230009 Door 15	30	☒	☐	?	?	?		
T31001230009 Door 16	31	☒	☐	?	?	?		

List of all doors in a system

Figure 5.25 - Doors of a system

GAT ACE displays the following information for each door:

- Address: Display of the address used when communicating with the door.
- Active: Indicates whether the door is active (the box is checked) or inactive. If not all doors of a controller are to be used, the unused doors should be set to inactive. There is no communication between GAT ACE and inactive doors.
In order to activate or deactivate a door, the functionalities in the multifunction bar or in the displayed context menu (shown when right-clicking on the door) are used.
The list can be filtered by its top field to only display active doors.

- Autoactivate: This box is checked if the communication with the door has been interrupted (refer also to the column "Communication"). In this event, GAT ACE will attempt, at configurable intervals, to automatically reactivate the door. The interval for this automatic activation is set in the system settings (refer to "4.4. "Application Settings" Page").
If this box is not checked, either the door is not active or the connection to the door is working properly.
- Door State: Indicates the current opening status of the door. This information can only be displayed correctly if the door feedback is correctly installed and configured.
 -  The door is closed
 -  The door is open
 -  The door status is unknown
- Lock State: Indicates the current status of the relay used to control the door lock.
 -  The lock of the door is locked
 -  The lock of the door is unlocked
 -  The status of the lock is unknown
- Communication: Indicates the current status of the communication with the lock.
 -  The communication with the door is OK
 -  The communication with the door is interrupted
 -  The communication status is unknown
- Initializing: The symbol indicates the initialization status of the door.
 -  The door is completely initialized and operational
 -  The door has already been initialized. But on the controller of the door there was a change on its configuration. This means the controller should be reinitialized. But the door is operational in its current state.
 -  The door has to be initialized, as modified data is available, that will only be uploaded when the door is initialized.
 -  If an exclamation mark is shown, the door is being initialized. Initialization should not last longer than a few minutes.
- Pending Commands:

When the configuration of a door is changed, the corresponding commands are generated that need to be sent to the door. This column indicates the number of pending commands (first figure) and the total number of commands, allowing to judge the progress of the initialization. At 0 / x, the door is completely initialized and the  symbol is shown in the column "Initialization".

- In order to execute a functionality at a door, mark the corresponding door in the list.
 - The following functionalities are then available in the multifunction bar.



- With the "Show Controller" icon, the controller assigned to the selected door is displayed directly.
- Press the "Config Door" icon to open the door configuration.
 - The window containing the configuration data of the selected door is displayed. The window is divided into several tabs.

Door: Roko3100, Address: 60

Save Cancel

Properties Configuration File Relay Expander

Name Address

Location

Door Settings Inputs Outputs Memory Card Net

Unlocking Time

Advance warning max. door open time (sec)

Max. door open time

Max door open time Units

Auto Unlock ☒

Unlock by command ☐

Only check FID while download ☐

Terminal Direction

Attack PIN-Code

Two persons access control

Antipassback control

Repeated access barrier (min)

Terminal Type

Time&attendance bookings

Dissable manipulation block ☐

Use attack fingerprints ☐

Fingerprint Interface Unit resolution

Show Alarm State at Readers ☐

Figure 5.26 - Door configuration - General settings

- On the "Properties " tab, define the settings of the door. The following settings are available:
- Unlocking Time: Time (in seconds) during which the door will remain unlocked in the event of a valid identification.
 - Advance warning max. door open time (sec): This time (in seconds) determines, for an open door, how many seconds prior to arriving at the "Max. Door Open Time" (see below) a prewarning is triggered.
 - Max. door open time: This time determines for how long a door can remain open from the moment of a valid identification, until an alarm is triggered. If a relay of the controller is defined as a "Door open alarm", this relay will be activated.
 - Max. door open time Unit(s): Here, it is defined in what time unit the door open time (seconds or minutes) is expressed.
 - Auto Unlock: If this option is activated, the controller decides whether an identification / access attempt is valid or not. If this box is not checked, the authorization decision has to originate from a high-level system (server).
 - Unlock by command: This option defines whether a controller can be remote-controlled with commands. This check must be set, if the "Auto(nomous) Unlock(ing)" box is not checked, or if the facility management system should be able to open the door by sending a command to the controller.
 - Only check FID while download: During the initialization of a door, the door is unable to perform a complete access check for some time. If access should, however, be granted during that time, this option box can be checked. In this case, during initialization, the controller will only check if the company ID (FID) on the data carrier matches the card settings, i.e. during this time all data carriers valid in this system have access. This functionality is only available for coded data carriers.
 - Terminal Direction: The direction is used for doors and controller of older designs to specify which reader is used for entering and which reader is used for leaving.
 - Access, no subreader
 - Exit, no subreader
 - Access, subreader leaving
 - Exit, subreader access

For doors and controllers of newer designs (where the direction is set in the reader configuration), this setting defines the unlocking direction by pressing a button.
 - Attack PIN Code: It is possible to define an attack PIN code. This code can be combined with the respective personal PIN code in order to trigger a covert attack alarm, if the door opening forced to allow unauthorized.
- NOTE!** In the software settings, a global attack PIN code can be defined. If a value is entered as an attack PIN code at the time of configuring the door, the global setting for this door is overridden. If no value is entered, the global value is used.

In the attack PIN code, only a few digits of the code are defined, the remaining digits are shown with an "X". The corresponding digit of the personal PIN code must be entered instead of the "X"s.

Example:

X	X	1	X	3	4	X	0	← Attack PIN code
-	-	-	2	4	8	8	2	← Personal PIN code
-	-	1	2	3	4	8	0	← PIN code that needs to be entered in order to trigger the attack alarm.

- Two persons access control :

This option is also called "Double Check Access ". In order to gain access, two different valid cards are required one after the other. The following settings are available:

- No two-person access
- Two-person access without mandatory master
- Two-person access with mandatory master

- Antipassback control:

If this option is activated, it is always required to perform alternating access and exit (leaving) bookings, i.e. it is impossible to perform two access bookings one after the other, without an exit booking in-between them.

A local anti-pass-back can be realized with the basic GAT ACE licence, by using an access reader as well as an exit reader on the same door. However, anti-pass-back for an area comprising several doors requires the corresponding additional license.

The following settings are available:

- Not activated:

The anti-pass-back functionality is deactivated. Also, the door cannot be assigned to any anti-pass-back area.

- Activated:

The anti-pass-back functionality is activated. In the event of an anti-pass-back in one area, the anti-pass-back check is also performed if not all doors in the area are online. This may lead to the situation, that the area must be left by the same door used for entering the area. For more detailed information, refer to "4.3. "Anti-Pass-Back Areas" Settings Page".

- Activated, if the terminal is online:

The anti-pass-back functionality is only active, if the controller is online, i.e. communication to GAT ACE is operational. However, if the communication is interrupted, the anti-pass-back functionality will be deactivated within one minute and will be reactivated automatically once the communication has been re-established.

This setting is suitable for an anti-pass-back by areas with the comfort mode activated for the areas.

For more detailed information, refer to "4.3. "Anti-Pass-Back Areas" Settings Page".

- Repeated access barrier (min): This setting prevents repeated accesses using the same card (e.g. by handing the card to another person) within a certain timeframe. After the lapsing of that timeframe, regaining access using the same data carrier is possible.
- Terminal Type: The type of checking the authorization at the controller is defined here.
 - Regular access terminal:
All read data carriers are checked completely. This is the default setting.
 - Foyer terminal with verification of branch code:
Only the first two digits of the data carrier number are verified. If they match the defined branch code, access is possible.
 - Foyer terminal with bank sorting code verification:
The bank code numbers stored on the data carriers are checked against the stored list of bank sorting codes.
- Time&attendance bookings: With this field, it can be determined whether or not time bookings should be permitted at the controller, and if yes, which access should then be executed.
 - No time bookings permitted:
No time bookings are possible at the controller.
 - Time bookings permitted, no automatic access attempt during a "coming booking":
Time bookings are possible at the controller. For accessing, a further identification is required.
 - Time bookings permitted, automatic access attempt during a "coming booking":
Time bookings are possible at the controller. If a valid "coming booking" is performed, the door is automatically unlocked provided the person has a valid authorization for accessing at that moment, according to the stored authorization data.
 - Time booking with an additional fingerprint verification permitted, no automatic access attempt during a "coming booking":
Time bookings are possible at the controller, and an additional verification via fingerprint sensor is possible. For this purpose, the reader must be equipped with a fingerprint sensor (e.g. GAT FR 055). For accessing, a further identification is required.
 - Time booking with an additional fingerprint verification permitted, automatic access attempt during a "coming booking":
Time bookings are possible at the controller, and an additional verification via fingerprint sensor is possible. For this purpose, the reader must be equipped with a fingerprint sensor (e.g. GAT FR 055). If a valid "coming booking" is performed, the door is automatically unlocked, provided the person has a valid authorization for accessing at that moment, according to the stored authorization data.

- Disable manipulation block: By default, if five entries of PIN codes are erroneous or five fingerprint identification attempts fail, the person is blocked due to an assumed manipulation attempt.
The manipulation block can be deactivated by checking this box, i.e. any number of attempts are permissible. This may imply a safety risk!
Deactivating is only possible on GAT Terminal 3100 controllers with an updated firmware. With older versions of the firmware or other controllers, the manipulation block will always remain active.
 - Use attack fingerprints: If the reader at the door being configured is equipped with a fingerprint sensor, this box must be checked in order to enable the use of the attack fingerprint function.
 - Fingerprint Interface Unit resolution: The detection threshold defines how well the fingerprints actually read at the fingerprint reader must match the stored data.
Lower values imply that the checking of the fingerprints will be performed with a smaller number of characteristics, i.e., with a higher tolerance, which in turn means that the fingerprints will be accepted more often. Higher values imply that the fingerprints must match the stored data more precisely, which increases the safety but at the same time increases the rejection rate and this calls for more frequent multiple attempts.
The detection threshold should be selected in accordance with the safety needs. The default value is 3.
NOTE! In the software settings, a global fingerprint detection threshold can be defined. If during the door configuration, a value is entered for the detection threshold, this value will be used and will override the global value. If no value is entered, the global value is used.
 - Show Alarm State at Readers: If this functionality is activated, an activated alarm system will be indicated at the reader.
- Switch to the "Inputs" tab in order to define the functionality of the optocoupler inputs for the door.
- The following tab is displayed.

The screenshot shows a software window titled "Door: T31001230009 Door 2, Address: 17". It has a "Save" button (floppy disk icon) and a "Cancel" button (red X icon). Below these are two tabs: "Properties" (selected) and "Configuration File". The "Properties" tab contains fields for "Name" (T31001230009 Door 2), "Address" (17), and "Location" (with a "Select" button). Below these are four sub-tabs: "Door Settings", "Inputs" (selected), "Outputs", and "Memory". The "Inputs" sub-tab contains four rows of configuration for optical inputs:

Input	Description	Functionality
Opto 1		Not used
Opto 2		Not used
Opto 3		Not used
Opto 4		Not used

Figure 5.27 – Door configuration – Inputs

- The functionality of the optocoupler inputs at the door is defined here with the following settings:
 - Opto x Description: Enter a name for each of the inputs in use.
 - Opto x: Select the functionality of the inputs. In order to guarantee proper functioning of the functionality, the selected functionality must match the actual wiring of the inputs. Most functionalities are available as "energized" or "not energized". This addition determines, when the respective functionality is active (i.e. active when the entrance is energized or not energized). However, the fundamental functionality is the same for both variants, which is why both variants are described together.

Setting in GAT ACE	Setting in GAT Manager	Meaning	Value
Not used	Do not use	Select this functionality for the inputs not in use.	
Door feedback, powered if door is opened Door feedback, not powered if door is opened	Door report powered if door open Door report powered if door closed	Via this input, the controller is told whether the door is open or not. Depending on which of the two versions was selected for this functionality, the door is open when the input is energized or not energized. This functionality is usually executed via a door contact connected to this input. The unlocking relay is de-energized as soon as the open door status is signalled.	

		In case there is neither identification, nor opening by pressing a button nor remote-control by command but the input still signals a door opening, a door open alarm is triggered (unless it is suppressed in the door schedule). During a regular door opening, this input also monitored the maximum door open time (unless it is suppressed in the door schedule).	
Unlocking button, powered for unlocking Unlocking button, not powered for unlocking	Unlocking button, powered if unlocking is desired Unlocking button, powered if NO unlocking is desired	If this functionality is activated (e.g. by pressing a button, pushing down a handle or activating a speaker system), the opening of a door is triggered and this procedure is logged. The direction of this booking is opposite to the direction defined for the door. The unlocking period comprises the time necessary for the de-/energizing of the button and the set unlocking period.	
Block entrance and exit, not powered for blocking Block entrance, powered for blocking	Barrier Entering and Exiting if powered Barrier Entering and Exiting if NOT powered	If this functionality is activated, neither accessing nor exiting is possible. Even the unlocking by pressing a button is deactivated. This functionality is used for instance in sasses in order to block a door as long as the opposite door is still open.	
Block entrance, powered for blocking Block entrance, not powered for blocking	Barrier Entering if powered Barrier Entering if NOT powered	If this functionality is activated, no accessing is possible. This is used for instance in sasses when a person is inside the sass in order to prevent the opening of the sass from outside. This functionality can also be used to prevent an access when an alarm system is activated.	
General alarm, powered for alarm General alarm, not powered for alarm	General alarm active powered General alarm passive powered	If this functionality is activated, an alarm is generated and saved. This can be shown as a booking and as an online status message (e.g. for a central building control). This alarm is saved until it is acknowledged by a command.	
Monitoring 0, online info, no booking by status change	General status	The current status of the access is determined and can be queried as an online status message. The status is not saved and no status changes are booked.	
Monitoring 1, booking by status change	General control 1 with booking if status changed	For every status change a booking is generated, the additional booking information shows in which direction the status changed. A query of this signal as an online status message is NOT possible.	

Monitoring 2, online info, booking by status change, relays	General control 2 with booking if status changed	For every status change a booking is generated, the additional booking information shows in which direction the status changed. A query of this signal as an online status message is possible, so the status can also be displayed at the PC. Furthermore, a relay can be defined that will be excited whenever status changes (refer to "Configuring outputs").	
Bolt feedback, powered if bolt is retracted Bolt feedback, not powered if bolt is retracted	Locker report powered if key bolt open Locker report NOT powered if key bolt open	If this input is active, the locker bar of the door is pulled back, i.e. the door is unlocked and can be opened. Contrary to the door response, the unlocking relay is not reset by this input. The other functionalities are equal to those for the door response.	
Alarm system ready, powered if ready for activation Alarm system ready, not powered if ready for activation	Enable for relay if powered Enable for relay if NOT powered	The "burglary detection ON/OFF" input (refer to Configuring outputs) can only be activated by pressing the "ON" button on the controller only if this input is activated, e.g. the readiness of an alarm system to be activated can be sent to a controller.	
Suppress door timeplan, powered for suppressing Suppress door timeplan, not powered for suppressing	Suppress generally open if powered Suppress generally open if NOT powered	If this functionality is activated while a door schedule is active, the unlocking defined in the door schedule is suppressed. People may access as long as they are allowed access in their time schedules. If this functionality is deactivated, the door schedule is active again.	
Unlocking button, unlocking by change from not powered to powered	Unlocking with button (change) if powered Unlocking with button (change) if NOT powered	If the input switches from deenergized to energized, the opening of the door is triggered and the process is logged as a booking. The unlocking period is defined in this optocoupler setting only by the set unlocking period and not by the duration of the optocoupler energizing. The other functionalities are identical to the ones of a regular door unlocking.	
Unlocking button, unlocking by change from powered to not powered	Unlocking with button (change) if NOT powered	If the input switches from energized to deenergized, the opening of the door is triggered and the process is logged as a booking. The unlocking period is defined in this optocoupler setting only by the set unlocking period and not by the duration of the optocoupler energizing. The other functionalities are identical to the ones of a regular door unlocking.	

Alarm system activated, powered if active Alarm system activated, not powered if active	Alarm system active if powered. flank Alarm system active if NOT powered	This input enables the status of the alarm system to be transmitted to a controller. The blocking of the access, use of the OFF button and signalling of the alarm system's condition can be controlled at the reader.	
--	---	---	--

- Switch to the "Outputs" tab in order to determine the functionalities of the relay outputs at the doors.
 - The following tab is displayed.

Figure 5.28 – Door configuration – Outputs

- The functionality of the relay outputs at the door is defined here with the following settings:
 - Relay x Description: Enter a name for the used relay outputs.
 - Relay x: Select a functionality for the door's relay outputs. In order to guarantee proper functioning of the functionality, the selected functionality must match the actual wiring of the outputs. Most functionalities are available as "energized " or "not energized". This addition determines, when the respective functionality is active (i.e. active when the entrance is energized or not energized)

The fundamental functionality is the same for both versions, which is why both are described together.

Setting in GAT ACE	Setting in GAT Manager	Meaning	Value
Not used	Do not use	Select this functionality for the inputs not in use.	
Unlocking entry and exit, relay active Unlocking entry and exit, relay passive	Unlocking ACTIVE Unlocking PASSIVE	The relay is used to unlock the door. If a person performs an identification and the authorization to open the door is valid, the functionality is active, i.e. the relay is energized or deenergized depending on which version was selected. The time period, date of expiry etc. are checked during the authorization. This functionality will be activated in the same way if a door schedule is active, a door is opened by pressing a button or an opening command is sent from the PC. The time set is irrelevant for this functionality.	
Alarm suppression, relay active Alarm suppression, relay passive	Alarm depression ACTIVE Alarm depression PASSIVE	This functionality is used for example to shunt a magnetic contact of an alarm loop, when the alarm system is activated, but no alarm is to be triggered in the case of a valid access. The exit output is controlled jointly with the unlocking relay. The time of this functionality determines how long the alarm shunting relay will be controlled. It remains active as long as the door is open plus the time set in the field (in order not to trigger an alarm when the locker bar hits the magnetic contact when the door closes).	
Doo-open-alarm, relay active Door-open-alarm, relay passive	Door Open Alarm ACTIVE Door Open Alarm PASSIVE	When the time set for the "Door open too long" alarm is exceeded or a door is opened with identification (e.g. break-in attempt), this functionality is activated. The precise reason for triggering the alarm can be evaluated in the online status or in the bookings. The individual reasons can be deactivated at the door (e.g. deactivating the opening without authorization). The time set for this functionality determines how long the relay remains activated (in seconds). If "0" is entered, the relay remains activated as long as the door stays open.	

Threat-alarm, relay active Threat-alarm, relay passive	Hold-up code ACTIVE Hold-up code PASSIVE	This functionality is activated, when an attack PIN code is entered as a variation from the normal personal PIN code or the identification is performed with the defined attack fingerprint. The attack PIN code is a combination of the personal PIN code and the attack code. In this functionality, the time determines how long the relay remains activated (seconds).	
Unlocking entry, relay active Unlocking entry, relay passive	Entering ACTIVE Entering PASSIVE	This functionality is active, when a person identifies herself at the access reader and is authorized to open the door. The time period, expiry date etc. are checked. The time set is irrelevant for this functionality.	
Unlocking exit, relay active Unlocking exit, relay passive	Exiting ACTIVE Exiting PASSIVE	This functionality is active, when a person identifies herself at the exit reader and is authorized to open the door. The time period, expiry date etc. are checked. The time set is irrelevant for this functionality.	
Video monitoring, relay active	Video function ACTIVE Video function PASSIVE	This functionality is activated as soon as a data carrier is read at the terminal (whether authorized or not) or a button is pressed. This relay functionality can be used e.g. to activate a video monitoring camera whenever an activity takes place at a door. The time of this functionality determines how long the relay remains activated (seconds).	
Special rights, relay active Special rights, relay passive	Special rights ACTIVE Special rights PASSIVE	If a special authorization is defined for a person at the door, this function is activated at a valid authorization with the exact same behavior as the unlocking relays.	
Alarm activation (0-24, with special rights), relay active Alarm activation (0-24, with special rights), relay passive	Relay (always with PIN Code) ACTIVE Relay (always with PIN Code) PASSIVE	With this functionality, persons holding a Special Authorization at a door can activate the burglary alarm system by pressing the "ON" button (previously the "8" button). If the time is set to 0 or an input has been defined with the "burglary alarm system activated", the relay can be set back by the "OFF" button (previously the "2" button). If the time setting differs from 0 and no "burglary alarm system activated" input has been defined, only the "ON" button will react and send an impulse of corresponding length.	

		The use of the "ON" and "OFF" buttons is reserved to persons holding a Special Authorization. For the "OFF" button, entering a PIN code is mandatory. The use of the "ON" button can be blocked by the "Alarm ready" input if the burglary alarm is not operational.	
Alarm activation (time-plan controlled), relay active Alarm activation (time-plan controlled), relay passive	Relay (PIN Code selectable via schedule) ACTIVE Relay (PIN Code selectable via schedule) PASSIVE	This functionality enables the activating / deactivating of the burglary alarm system performing the same checks as for access control. If at a given time, a PIN code is required to gain access, a PIN code must also be entered to control the burglary alarm system. Special Authorization and burglary alarm system readiness are not checked.	
Monitoring input, relay active for rising edge of monitoring 2 Monitoring input, relay active for falling edge of monitoring 2	Monitoring 2 Positive Edge Monitoring 2 Negative Edge	If an optocoupler is defined as "monitoring 2", the optocoupler of this output will be activated when switching from the deenergized condition to the energized condition ("positive flank") respectively from the energized condition to the deenergized condition ("negative flank"),. The time set for this functionality determines how long this functionality will remain activated (seconds).	
Door open output, relay active if door open	Door Open Output	If an optocoupler input is defined as a door response ("Door response energized when the door is open/closed"), the door status is made available at this output as a potential-free contact. The relay is controlled when the optocoupler signals that the door is open.	
Alarm deactivation pulse (0-24, with special rights), relay active Alarm deactivation pulse (0-24, with special rights), relay passive	Relay impulse ACTIVE Relay impulse PASSIVE	This functionality enables persons holding a Special Authorization to produce an impulse with the "OFF" button (previously "2" button) to deactivate the burglary alarm system. This functionality can only be used in conjunction with the "Burglary alarm system activated" input. Entering a PIN code is mandatory. The time for the impulse can be selected between 1 and 5 seconds.	

- Switch to the "Memory" tab
 - The following tab is displayed.

Figure 5.29 – Door configuration - Memory

- The memory (to save data) made available to the door is defined here.

NOTE! Remember that some controller types will multiply the value entered by 10, e.g. in the above example, the number of person records entered is 500 → 5000 person records can be saved.

The following settings are possible:

- Person record number: Number of person records reserved in the controller for this door.
- Offline person number: Number of person records for use in the offline mode (CardNet), where the personal data needed for the offline mode is saved in the controller, from which they can be transferred to a data carrier. If the offline mode is not used (refer to the next tab), the value in this field can be left at 0.
- Time & attendance bookings: Number of time bookings that can be saved in the terminal. If the memory is full, no more time bookings are possible.
- Access bookings: Number of access bookings that can be saved in the terminal. The memory for access bookings is administrated as a ring buffer, i.e. the oldest booking will be overwritten if the memory is full and a new booking is to be saved.

- In order to configure the CardNet mode, switch to the "CardNet" tab.

NOTE! In the CardNet mode, the authorizations for offline doors are stored on the person's data carrier. The writing of this data can be done at online doors with an activated CardNet mode. The writing is then done automatically as soon as a data carrier is read by the reader of the controller.

- The following tab is displayed.

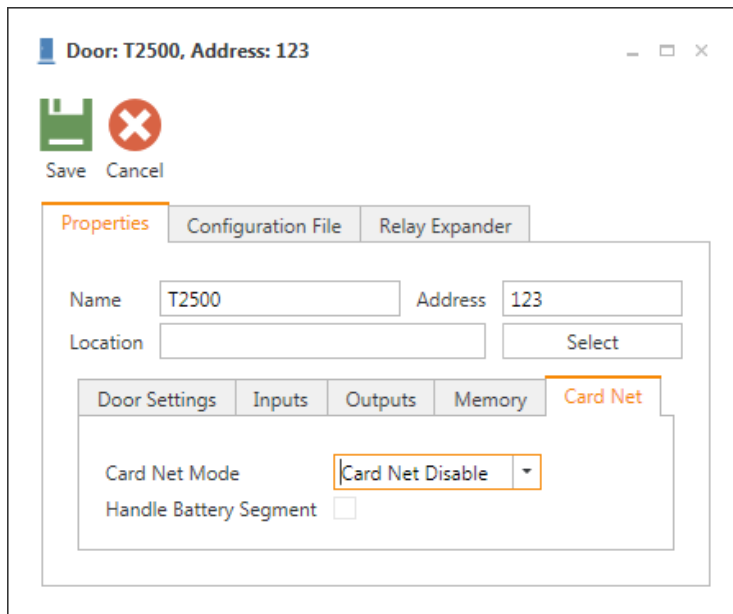


Figure 5.30 - Door configuration - CardNet

- Define the functionality of the Card Net mode. The following settings are available:
 - CardNet Mode: Select the desired Card Net mode:
 - CardNet Disabled:
At this door, no CardNet authorizations are written onto data carriers.
 - CardNet default (R/W):
Authorizations for offline doors are written onto data carriers at this door. Even if writing was unsuccessful, access is granted, if access is authorized for this person at the corresponding point in time.
 - CardNET Access after write success:
Access is only granted if writing was completed successfully.
NOTE! This functionality may only be activated if all data carriers are coded with corresponding data areas for CardNet authorizations. Otherwise, access would be impossible for persons holding cards without these data areas.
 - Handle Battery Segment: If this option is activated, battery warnings and other feedbacks from the offline lock are evaluated and treated and information regarding a necessary battery replacement is returned.
NOTE! This functionality should only be deactivated if no data area for battery messages has been coded on the cards.
 - The available parameters for doors are read from configuration files and the settings are entered into a command file, which can be displayed in the "Configuration File" tab.
- NOTE!** Please make changes to these files only after having been in contact with our support, as otherwise the functionality of the system can be impaired.
- If one or more relay expanders are used at a door, they can be configured on the "Relay expander" tab.

The following tab is displayed.

Door: T2500, Address: 123

Save Cancel

Properties Configuration File **Relay Expander**

Relay expander Mode: Relay expander for elevator control

Value	Description
0	Relay expander for elevator control
1	Relay expander for locker control

Relays

Drag a column

Number	Name	Is Enabled
1	Relay 1	☒
2	Relay 2	☐
3	Relay 3	☐
4	Relay 4	☐
5	Relay 5	☐
6	Relay 6	☐
7	Relay 7	☐
8	Relay 8	☐
9	Relay 9	☐
10	Relay 10	☐
11	Relay 11	☐
12	Relay 12	☐
13	Relay 13	☐
14	Relay 14	☐

Figure 5.31 - Door configuration – Further outputs via relay expanders

- ▶ In the "Relay Expander Mode" field, select the mode for the expanded relay outputs. The following options are available:
 - .. for elevator control: Up to 32 relay outputs are activated according to the authorizations of the person. The relays are controlled simultaneously with the unlocking relay. This functionality is used to select a floor on the elevator floor selection panel.
 - .. for locker control: The number (1 - 32) of the desired locker must be entered after identification. After valid authorization, only the relay of the selected locker is controlled. The number of the locker is logged.
Note: This functionality is only possible if the used reader is equipped with a keypad to enter the number!
- ▶ Mark the relay of the relay expander that is to be used and enter a meaningful designation for the relay. This significantly simplifies the administration of authorizations in GAT Matrix.
- ▶ Press the "Save" button in order to save the configuration of the door and return to the door view.

5.2.10 Activating and Deactivating a Door

For authorizations to be uploaded to a door, it has to be activated in GAT ACE. All doors not in use can be deactivated. This gives a better overview in the list of doors and the controller view, as the lists displayed there are filtered to contain only active doors.

Whether a door is activated or not is visible in "Active" column of the door view. A checked box indicates an activated door.

- ▶ In order to activate or deactivate a door, mark it in the list of doors.
- ▶ Press the "Activate" icon in order to activate a door. Every door to be used in the system must be activated.
- ▶ Press the "Deactivate" icon in order to deactivate a door.
- ▶ Another option is to select either of the above from the pop-up menu that appears when right-clicking with the mouse on the desired door in the list.

Automatic activation:

If the "Automatic Activation" option is active for a door, the communication with the door has been interrupted. GAT ACE will periodically attempt to re-establish the connection and activate the door. The periodicity of these attempts can be defined in the software settings (refer to "4.4. "Application Settings" Page").

5.2.11 Initializing a Controller

During the initialization of a controller, the corresponding configuration parameters for the controller itself and all doors connected to this controller are sent. This procedure is required for the first putting into service of the controller, but also in the event of hardware changes (e.g. connected readers).

As soon as changes are made to the controller settings, this is indicated in the list of controllers, by the  symbol in the "Initialization" column. This column can be filtered, so only controllers requiring initialization will be listed. In this case, all displayed controllers can be marked and then initialized simultaneously.



By initializing the controller and formatting the memory, the controller is set back to its factory settings with the exception of the communication parameters. For some controllers, this can imply a loss of bookings. For this reason, make sure all bookings have been read from the controller prior to memory formatting.

NOTE! If a WiNET lock is detached from a WiNET controller, the entire controller must be initialised again, including memory initialisation.

- ▶ Mark the controller to be initialized in the controller view.
- ▶ In order to initialize it, press the "Initialize" icon.
- ▶ Select whether memory should be formatted or not
- ▶ In the "Initialization" column, the duration of the initialization is indicated by a progress bar, showing the number of pending commands.

- ▶ Once the initialization has been completed correctly, a green thumb  is displayed in the "Initialization" column.
- ▶ In the event of a failure, a red exclamation mark  is displayed in the "Initialization" column. This indicates that there has been a problem with the initialization and the door may not work properly. For further information, please contact our support team.
- ▶ If the memory was formatted, once the controller initialization has been completed, an automatic initialization of the doors connected to the controller will be started in order to make the doors operational again. Further details are found in the next chapter.

5.2.12 Initializing Doors

If configuration changes of doors are made in GAT ACE, the corresponding doors have to be initialized, i.e. the changes have to be sent to the doors. This is done with the "Initialize door" functionality.

As soon as changes are made to a door configuration, this is indicated in the "To Load" column of the list of doors. This column can be filtered, so only the doors requiring an initialization will be listed. In this case, all displayed doors can be marked and then initialized simultaneously.

Authorizations sent by GAT Matrix to GAT ACE are automatically forwarded to the doors, so no initialization in GAT ACE is necessary in this case.

NOTE! The changes in configurations and authorizations become effective only once a door has been initialized correctly. Make sure that the GAT ACE 3000 Service is running, as otherwise no uploading takes place and configuration changes cannot become effective.

- ▶ Mark the door to be initialized in the door view.
- ▶ In order to initialize the door, press the "Initialize" icon.

In the "Pending Commands" column, the duration of the initialization is indicated by a progress bar, showing the number of pending commands.

- Once initialization has been completed successfully, a green thumb  is displayed in the "Initialization" column.
- In the event of a failure, a red exclamation mark  is displayed in the "Initialization" column. This indicates that there has been a problem with the initialization and the door may not work properly. In this case, the commands that could not be correctly sent are displayed in the context menu under "Display Commands".

5.2.13 Display Commands to be Sent

After changing a door configuration, or whenever the door requires initialization, GAT ACE generates corresponding commands that have to be sent to the door. The number of commands already sent and still pending are indicated in the "Pending Commands" column. These commands can also be displayed and, if desired, commands can be sent or deleted one-by-one.

Normally, it is not necessary to delete any commands, as all commands must be processed by the controllers. However for reasons of backwards-compatibility, it might be necessary to delete specific commands in order to be able to put the system into operation.

- ▶ Mark the desired door in the list of doors.
- ▶ Click on the "Pending Commands" icon.
 - The "Pending Commands" window is opened, listing all commands.

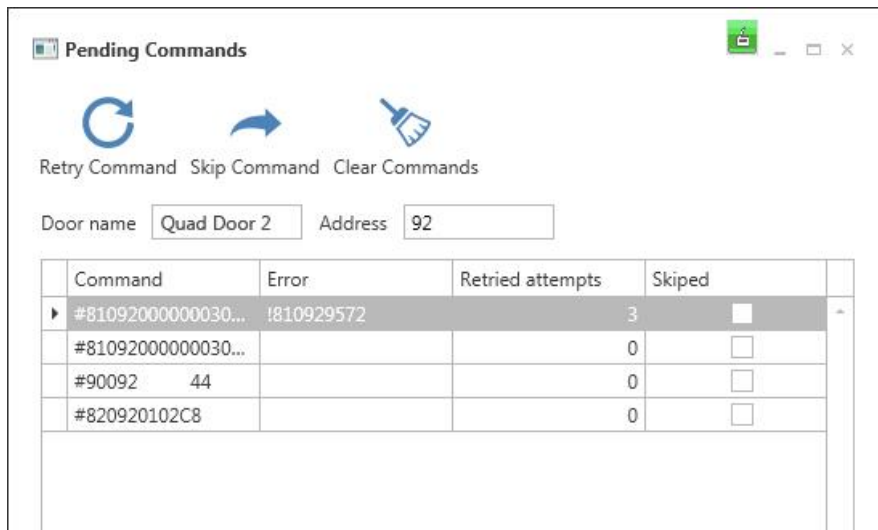


Figure 5.32 - Door configuration – Pending commands to be sent

- If an error occurs during the sending of a command, a message to this effect is displayed. GAT ACE will attempt to re-send this command. These attempts will also be indicated.
- ▶ In order to deactivate a command in the list, so that it will not be sent (e.g. because error messages are displayed for this command), mark the command and click on the "Skip Command" icon.
 - The skipped command is marked with a checked box in the last column "Skipped".
- ▶ In order to re-send a command, mark the command and select the "Re-send the Command" icon.
- ▶ In order to delete all commands, click on the "Delete Commands" icon.
 - All commands are deleted from the list and thus not sent any longer to the door or controller.

NOTE! The skipping or deleting of commands can lead to a condition, where a door will not operate correctly any longer! Please perform these steps only after having been in contact with our support team.

5.2.14 Offline Loaders and Offline Doors

Offline doors are not connected permanently via an interface to GAT ACE or the server, but are supplied with data by a programming device. For configuring these offline doors and the transport devices, offline loaders and offline doors are required.

The following types of offline doors can be configured by GAT ACE:

- GAT ST 21x
- GAT ST 22x
- TAC
- GAT DL 32x
- GAT DL 34x
- GAT DL 350
- GAT DL 360
- GAT DL 370

For GAT ST 21x, GAT ST 22x and TAC, the configuration data is transferred to these offline doors using the handheld device GAT MT 010 (transfer of the configuration data on site per cable connection). For GAT DL 32x, GAT DL 34x, GAT DL 350, GAT DL 360 GAT DL 370, the data is transferred with the GAT DL 090 or GAT DL 092 (transfer of the configuration data per radio connection). If these offline doors are operated in the WiNET mode, they communicate via a permanent radio connection. Thus, these doors are treated as online doors and are also configured as online doors.

5.2.15 Configuring Offline Loaders

Offline loaders are used to join several offline doors having the same operating mode, being uploaded with the same handheld device and located in the same building or access area.

By dividing a system in several offline loaders, the uploading of the doors can be optimized in the sense that all doors close to each-other can be uploaded via the same handheld device.

- Select the "Offline Loaders" icon.
 - The "Offline Loaders" view is displayed.

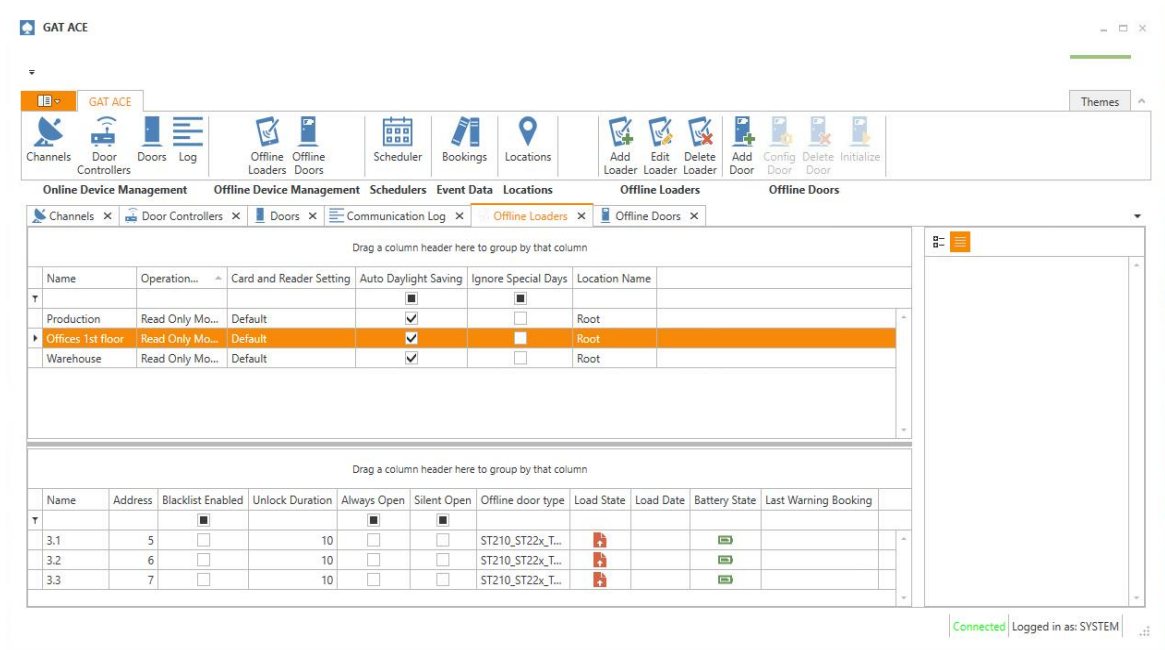


Figure 5.33 - Defining offline loaders

- All defined offline loaders are listed here. The most important data is displayed for each interface.
- Underneath the list of interfaces, the offline doors assigned to the selected interface are displayed.
- In the offline loader view, the following functions are available in the multifunction bar (the last three icons are described in the configuration of offline doors).



- ▶ Select the "Add Loader" icon in order to define a new interface.
- ▶ Select the "Edit Loader" icon in order to edit the settings of the selected interface.
 - In both cases, the "Offline Loader" window is opened.

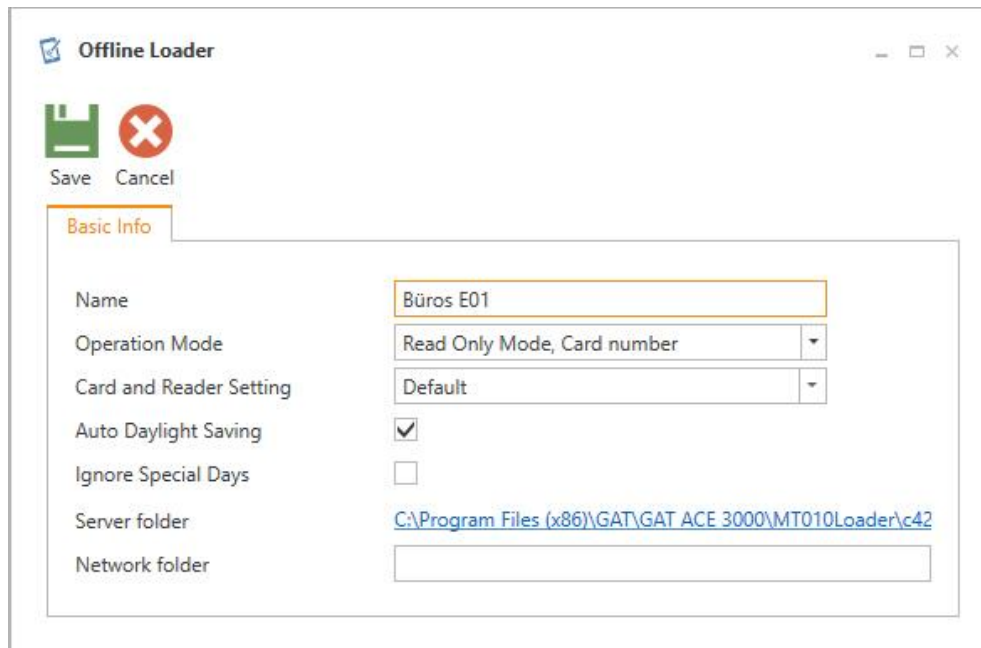


Figure 5.34 – Configuring an offline loader - General settings

- ▶ Enter a name for the interface into the "Name" field.
- ▶ Select the operating mode for the interface in the "Operating Mode" field. The following operating modes are available:
 - Read Only Mode, Unique Number: Authorized persons are saved in the lock. The unique number of the data carrier is used as card number.
 - Offline (CardNet) Mode: The authorizations of the persons are saved on the staff cards and transferred to the lock in this manner.
 - Company ID Mode: It is only checked whether the data carrier belongs to the system.
 - Hotel Mode: Authorizations for guests and staff are saved on the cards.
 - Read Only Mode, Card Number: Authorized persons are saved in the lock. The coded card number of the data carrier is used as card number.
- ▶ Select the preset configuration for the reader or data carrier in the "Card and Reader Settings" field.
- ▶ Check the "Automatic Summer/Winter Time Switch" box, if this functionality is to be used in the terminals connected to the interface.
- ▶ If the field "Ignore Special Days" is active, special days will be ignored by the offline locks. Special days are defined in the organisation calendar and on these days it is possible to activate other time plans than the one that would be active on that day. The normal day plan will be used on these days.
- ▶ In the "Server Folder" field, the folder is displayed, where the configuration files for the offline doors are saved by the GAT ACE 3000 Service. This storage location is assigned automatically. A click on the link opens the folder (if you work on a server). With "Ctrl" + "Click" on this link, this path can be edited.
- ▶ The server folder must be shared in the network, so access to the data from work stations and transfer devices is enabled. The network name can be entered into the "Network Folder" field. A click on the link opens the folder. With pressing "Ctrl" and clicking on this link, the data can be edited.
- ▶ Save the settings by pressing the "Save" button.
 - The list of offline loaders is displayed again.

5.2.16 Configuring an Offline Door

All offline doors are assigned to the corresponding offline loaders. If an offline loader is selected in the offline load view, the offline doors assigned to this interface are displayed below. How to configure offline doors is described in the following.

- Mark an offline loader and click on the "Add Door" icon in the multifunction bar in order to add a new offline door.
 - The "Offline Door" window is displayed. This window is divided into two 2 index cards.

Figure 5.35 - Configuring an offline door - Basic info and inputs

- Enter the following information for the new door.
 - Name: Give a name to the offline door.
 - Address: The offline terminal is identified at the offline door by its address, which is why every offline terminal must have an unambiguous address not already used by another offline terminal. If an address already in use is entered, an error message will be displayed when saving the door data.
 - Location: With the "Select" button, a location to which the offline door will be assigned to can be selected.
 - Offline Door Type: Select the type of the offline door.
 - Serial Number: Enter the serial number of the offline terminal installed at the offline door. For some type of device, this enables the automatic addressing and thus facilitates putting into operation.
 - Unlock Duration (seconds): This time determines for how long a door will remain unlocked in the event of a valid identification.
 - Blacklist Enabled: This setting is relevant for the CardNet and hotel modes. If this box is checked, all deleted data carriers are entered into a blacklist. Once this blacklist is transferred to a lock by a handheld device, the card is not authorized any longer, even if the data on the staff card would result in a valid authorization. This enables immediate blocking of lost cards.

- Silent Open(ing): If this box is checked, no signal sounds are emitted at the offline door. By default, the sounds are emitted, i.e., this box is not checked.
This function can only be used with readers of type GAT SR 73xx and GAT SLR 73xx and has no influence on readers of type GAT SR 3xx and GAT SLR 3xx.
 - Always Open: This function is only supported by the previous generation TAC and GAT ST 2xx offline locks. If this function is activated, the door is permanently unlocked when an authorised user makes 2 valid accesses (data carrier read) within 2 seconds of each other. The door will be locked again when an authorised user makes a valid access at the door.
- Switch to the "Inputs" tab in order to configure the inputs of an offline door. Depending on their type, offline doors can be equipped with up to two optocoupler inputs, which can register status signals. Enter a description into the lower fields and select functionality. The following functionalities are available:
- Door Feedback (not energized/energized, when the door is open):
A door contact is connected to this input, signalling whether the door is open or closed. Depending on which of the two versions of this functionality has been chosen, an open door is signalled by an energized or a not energized state.
 - Unlocking by Pressing a Button (not energized / energized for opening the door):
A button is connected to this input, enabling the unlocking of the door.
Depending on the version selected, the door opening occurs when energizing or de-energizing the door opening button.
- Save the door configuration by pressing the "Save" button.
- The new offline door is added to a list of offline doors and assigned to the previously selected offline loader.
- NOTE!** If an address is entered that is already used by another offline terminal, the configuration cannot be saved.
- It is also possible to display an overview of all offline doors by clicking on the "Offline Doors" icon.
- The "Offline Doors" view is displayed.

Name	Address	Enabled	Blacklist Enabled	Unlock Duration	Always Open	Silent Open	Offline door type	Loader Name	Load State	Opto 1 Name	Load Date	Opto 1	Opto 2
aaa	55	✓	✓	3	☐	☐	ST210_ST22x_TAC	asas			01/01/0001	Not used	
333	50	✓	✓	3	☐	☐	ST210_ST22x_TAC	asas			01/01/0001	Not used	
Keller	11	✓	✓	3	☐	☐	ST210_ST22x_TAC	Produktion			02/01/1759	Not used	
Werkstatt2	5	✓	✓	3	☐	☐	ST210_ST22x_TAC	Produktion			01/01/0001	Not used	
Büro2	0	✓	✓	3	☐	☐	ST210_ST22x_TAC	Produktion			01/01/0001	Not used	
Werkstatt1	4	✓	✓	3	☐	☐	ST210_ST22x_TAC	Produktion			01/01/0001	Not used	
Technikraum	3	✓	✓	3	☐	☐	ST210_ST22x_TAC	Produktion			01/01/0001	Not used	
Büro1	1	✓	✓	3	☐	☐	ST210_ST22x_TAC	Büros			01/01/0001	Not used	
Büro2	2	✓	✓	3	☐	☐	ST210_ST22x_TAC	Büros			01/01/0001	Not used	

Figure 5.36 - Offline doors

- For every door, the most important information, i.e., address, operating mode, unlocking duration and various functional settings are displayed.
- Using the icons in the multifunction bar, the door configurations can be edited and new doors can be added.
- ▶ Configure the offline doors as described for offline loaders on the previous page.
- ▶ In order to activate or deactivate an offline door, click on the corresponding "Activate" or "Deactivate" icons in the GAT ACE icon bar. A deactivated door will not be processed by GAT ACE.
- ▶ With the "Show Loader" icon, the offline loader to which the currently marked door is connected can be displayed directly.

5.2.17 Initializing an Offline Door

When initializing an offline door, the data for the offline door is generated and made available to the handheld device in the correct folder. The  symbol indicates that initialization was successful.

- ▶ In order to initialise an offline door, mark it in the list of offline doors.
- ▶ Click on the "Initialize" icon in the multifunction bar.
 - If changes have been made, the data is generated, which is indicated in GAT ACE and in GAT Matrix by the  symbol, i.e., the data in the handheld device has to be transferred to the offline door.
- ▶ Use the handheld device as indicated in its description.
 - If the correct transmission via handheld device is confirmed by a feedback message, the door is shown as correctly initialised by the  symbol. The possibility of feedback messages depends on the type of handheld device and the software version.

5.2.18 Battery Warning for Offline Doors

The offline locks generate battery warnings for different battery conditions.

Offline Loaders											
Drag a column header here to group by that column											
Name	Operation Mode	Card and Reader Setting	Auto Daylight Saving	Ignore Special Days							
CardNumber	Read Only Mode, Card number	Default	☒	☐							
CardNet 2 100 - 131	CardNet Mode	Default	☒	☐							
CardNet 1 500 - 511	CardNet Mode	Default	☒	☐							

Drag a column header here to group by that column											
Name	Address	Blacklist Enabled	Unlock Duration	Always Open	Silent Open	Offline door type	Load State	Load Date	Battery State	Last Warning Booking	
CardNET 500	500	☐	3	☐	☐	DL32x		01/12/2016			
CardNET 501	501	☐	3	☐	☐	DL32x		03/12/2016		12/11/2016	
CardNET 502	502	☐	3	☐	☐	DL32x		03/12/2016			
CardNET 503	503	☐	3	☐	☐	DL32x		03/12/2016		02/12/2016	
CardNET 504	504	☐	3	☐	☐	DL32x		03/12/2016			
CardNET 505	505	☐	3	☐	☐	DL32x				05/12/2016	
CardNET 506	506	☐	3	☐	☐	DL32x					
CardNET 507	507	☐	3	☐	☐	DL32x		06/12/2016			
CardNET 508	508	☐	3	☐	☐	DL32x					

Figure 5.37 - Offline doors – Battery warnings

-  ... The battery status is good.
-  ... The battery is partially discharged and must be replaced soon.
-  ... Battery warning. The battery is empty and must be replaced.
The battery warning is visually and acoustically signaled at the

- ▶ A person uses an offline door following battery replacement. If the person subsequently uses an online door with CardNET function, the battery warning is reset automatically. This option is available for GAT DL 3xx series locks.
- ▶ A person uses an offline door following battery replacement. If the person subsequently uses a time recording device with CardNET function, the battery warning is reset automatically. This option is available for GAT DL 3xx series locks.
- ▶ If the transport device uploads the bookings of an offline door following battery replacement then synchronizes with GAT ACE 3000, the battery warning is reset automatically. This option is available for all offline locks.
- ▶ It is also possible to reset the battery warning in GAT ACE 3000. To do so, right-click onto a battery warning symbol (red) in the offline lock list and select "Remove battery warning" in the pop-up menu. This option should only be used in exceptional cases as the data circuit is not closed and further battery warnings are ignored for a period of one month.

Drag a column header here to group by that column											
	Name	Address	Blacklist Enabled	Unlock Duration	Always Open	Silent Open	Offline door type	Load State	Load Date	Battery State	Last Warning Booking
▼	CardNET 500	500	☐	3	☐	☐	DL32x		01/12/2016		
	CardNET 501	501	☐	3	☐	☐	DL32x		03/12/2016		12/11/2016
	CardNET 502	502	☐	3	☐	☐	DL32x		03/12/2016		
	CardNET 503	503	☐	3	☐	☐	DL32x		03/12/2016		02/12/2016
	CardNET 504	504	☐	3	☐	☐	DL32x		03/12/2016		
▶	CardNET 505	505	☐	3	☐	☐	DL32x				
	CardNET 506	506	☐	3	☐	☐	DL32x				
	CardNET 507	507	☐	3	☐	☐	DL32x		06/12/2016		
	CardNET 508	508	☐	3	☐	☐	DL32x				
	CardNET 509	509	☐	3	☐	☐	DL32x		06/12/2016		
	CardNET 510	510	☐	3	☐	☐	DL32x		06/12/2016		
	CardNET 511	511	☐	3	☐	☐	DL32x				08/10/2016
	CardNET 512	512	☐	3	☐	☐	DL32x				
	CardNET 513	513	☐	5	☐	☐	ST210 ST22x T...				

NOTE! Following battery replacement, it is necessary that the battery data carrier is read by the reader of the offline door in order to document the replacement. To set the correct time and load a current operating calendar following battery replacement, it is strongly recommended to load the offline door with current data! This process also resets the battery warning after the transport device is synchronized with GAT ACE 3000.

www.gantner.com

5.3 Scheduler

In the "Scheduler" area, reoccurring system tasks can be planned. These are automatically executed. The GAT ACE 3000 service must run. The following system tasks can be scheduled:

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

► Click on the "Scheduler" icon.

- The current day with all tasks scheduled for the day are displayed. Use the calendar to the left to navigate to a different date.

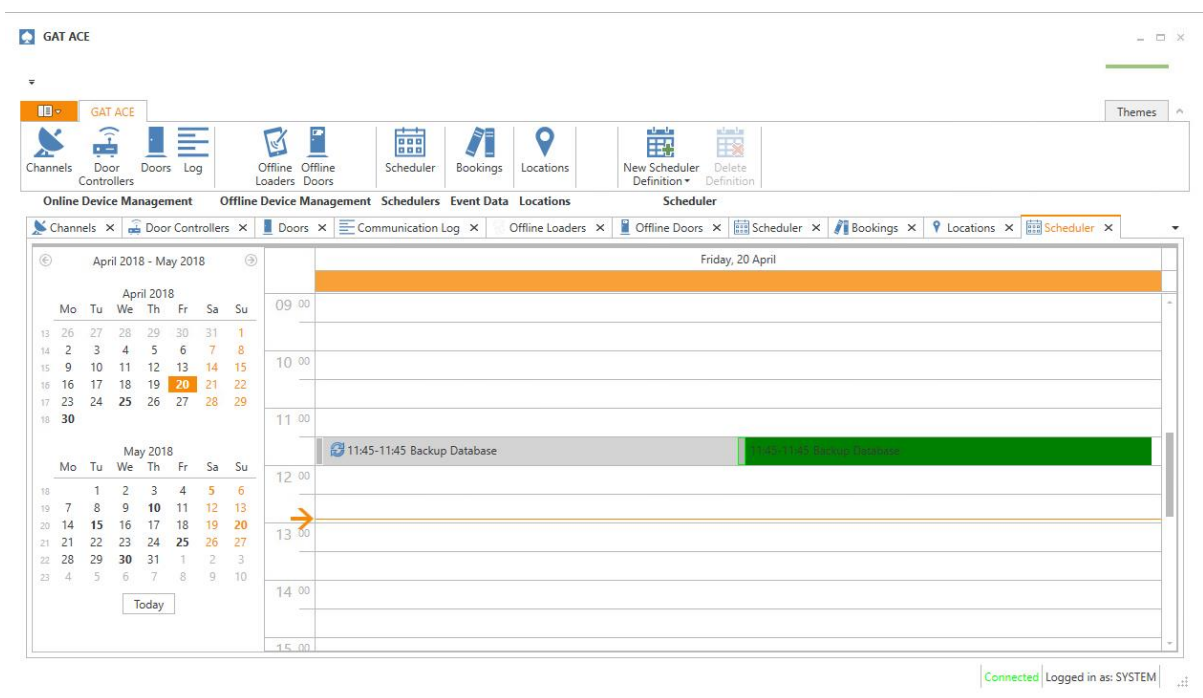
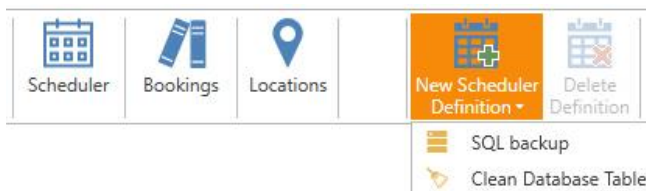


Figure 5.39 - Scheduler view

► To schedule a new task, click on the "New Scheduler Definition" icon and select the desired task from the menu.



- The "Scheduler Definition" window opens with the corresponding settings of the selected task. The scheduler tasks are described in the following sections.

► To delete an existing task, click on the task in the scheduler and click on the "Delete Definition" icon.



5.3.1 SQL Database Backup

The SQL database contains all the data of the access system, e.g., the controller/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 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 5.40 – 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 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 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.

5.3.2 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 “5.5 Bookings”).

NOTE! Bookings 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.

Figure 5.41 – Scheduling an automatic cleanup of a database table

- In the "Table" field, select "Booking" from the menu. 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 5.41, 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 scheduler but is not executed at the scheduled time.

- In 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 Bookings

For all identification attempts and access/entry events the controllers store a booking entry in the internal memory. Each booking contains information about the used data carrier number, time and date, type of booking etc.. This makes it possible to later check and evaluate all events that occurred at the controllers.

GAT ACE can read the bookings from the controllers and will display them in the view "Bookings". In this view you can sort and filter the bookings by different criterias.

- Select the symbol "Bookings" from the multifunction bar.
 - The bookings view is opened and the read bookings are displayed.

Booking Id	Device	Address	Type	Partner	Person N°	Booking Time	Creation Time
280			22	Access	-1	28/04/2015 10:41:27	28/04/2015
279			21	Access	-1	28/04/2015 09:43:12	28/04/2015
278			22	Access	-1	27/04/2015 16:39:26	27/04/2015
277			20	Access	-1	27/04/2015 16:25:20	27/04/2015
276			19	Access	-1	27/04/2015 16:43:29	27/04/2015

Figure 5.43 - Bookings view

The latest bookings will be shown first. If you want to see older bookings, select the corresponding function from the icon bar:



- With the symbol "More Bookings" the next, older bookings are loaded from the server. The amount of read bookings is limited, in order to reduce the waiting time in case there are a lot of bookings. You can select this function multiple times in order to see older bookings until the desired booking periode is displayed.
- With the symbol "All Bookings" all bookings saved on the server will be loaded at once. This can take a long time if there are a lot of bookings.
- With the symbol "Stop reading bookings" you can stop the loading of bookings, if the bookings of the desired time frame are already shown. This symbol is only displayed if bookings are being loaded.
- With the symbol "Export to Excel" the shown bookings are exported into an Excel file.
- If the function „Display new bookings“ is active, newly created bookings are automatically shown in the bookings list. If this function is not active, the bookings list will not be refreshed, until you make a manual refreshment with the buttons "More Bookings" or "All Bookings".

Attention: If the function „Display new bookings“ is reactivated after some time, the bookings generated while this function was deactivated are not automatically loaded and shown in the list. But of course these bookings are still stored in the database.

5.6 Time & Attendance Terminals and Time Bookings

GAT ACE offers the possibility to load and export the time bookings of time&attendance terminals (e.g. the GAT Terminal 1015 and 1032 or the GAT p.time terminals from GANTNER Electronic GmbH). First you have to add the time device(s) to GAT ACE and then you can load the bookings from the device (manually or automatically).

NOTE! To use the time booking functionality you have to enter the licence for the corresponding module (see "4.4. "Application Settings" Page").

- ▶ Select the symbol "Time Devices" from the multifunction bar.
 - The Time Devices view is opened and the already added time devices are listed.

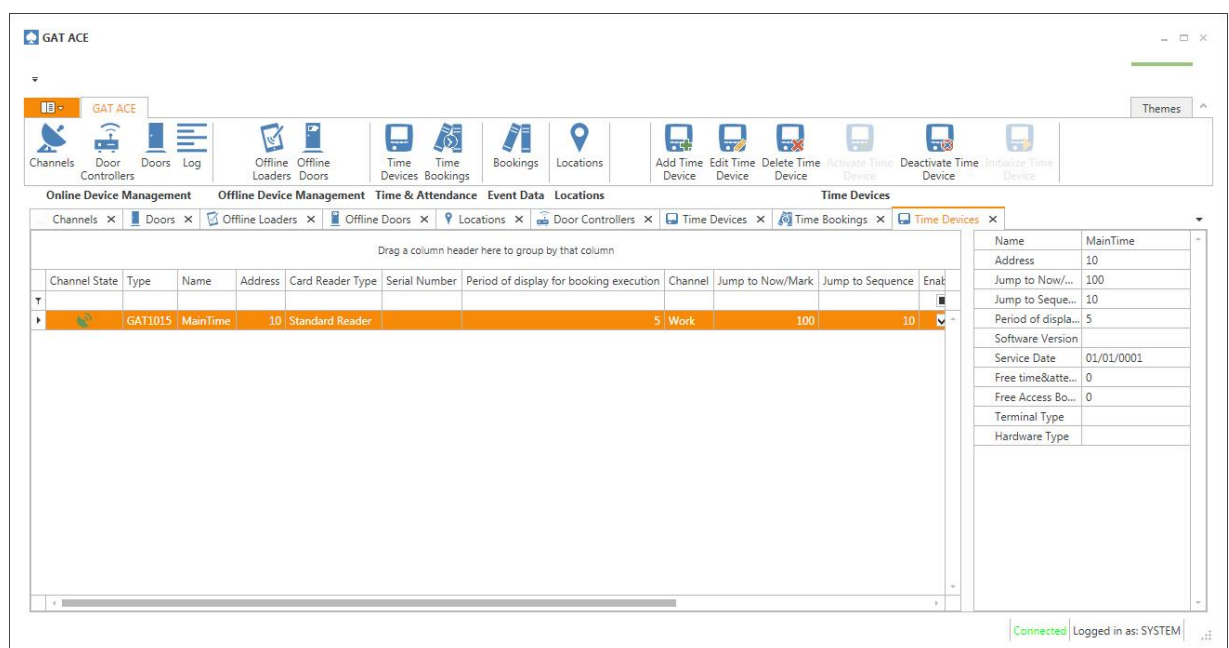


Figure 5.44 - Time devices

With the following icons in the icon bar you can select different functions:



- ▶ With the symbol "Add Time Device" a new device is added to the list. Clicking on that icon opens the window "Time Device" to define the settings of the device (see below).
- ▶ With the symbol "Edit Time Device" you can edit the settings of the device that is selected in the list. The window "Time Device" is opened (see below).
- ▶ The symbol "Delete Time Device" is used to delete the device that is selected in the list. This has to be confirmed with in a pop-up window that appears after clicking that symbol.
- ▶ The symbols "Activate Time Device" and "Deactivate Time Device" switch the time device between activated and deactivated state. When a device is deactivated no time bookings will be read.
- ▶ When clicking on the symbol "Initialize Time Device" the selected device will be initialized.

5.6.1 Time Device Settings

When a new time device is added to GAT ACE or you click the "Edit Time Device" symbol for a marked time device the windows "Time Device" is opened, where you can configure the device.

The screenshot shows the 'Time Device' configuration window. It has a title bar with a minus, maximize, and close button. Below the title bar are 'Save' and 'Cancel' buttons. The 'General' tab is selected, showing fields for Name (MainTime), Address (10), Type (GAT1015), Card Reader Type (Standard Reader), Channel (Work), Permanent Illumination (unchecked), and Reader Settings (Leser2). A 'Select' button is next to the Channel field.

Figure 5.45 - Time devices - General settings

The configuration settings are separated into different register cards.

Register Card "General"

- Name: Enter any name for the device. This name is shown in the time device list.
- Address: Enter the terminal address. Every terminal has to have a unique address.
- Type: Select the type of terminal.
- Card Reader Type: Select the type of reader, that is used at the terminal to identify the personnel. "Standard" means the contactless readers for RFID or infrared data carriers. "Magnetic Reader" is used for reading cards with magnetic stripes, and "Magnetic Reader (Var. Card Structure)" must be selected for magnetic stripe cards that don't use the Gantner Standard Segment coding.
- Permanent Illumination: If this field is marked, the illumination of the terminal's display will be switched on permanently. If the field is not marked the display will only be illuminated briefly if a data carrier is read or a button is pressed at the Terminal. By deactivating the permanent illumination of a Terminal the lifetime of the display can be increased.
- Reader Settings: Select the defined reader settings from the list. The reader settings are defined in the general Setting Pages of GAT ACE (see "4.5. "Card and Reader Settings" Page").

Register Card "Advanced Settings"

Time Device

Save Cancel

General Advance Settings Time Settings Memory

Jump to Now/Mark 100

Jump to Sequence 10

Serial Number

Period of display for booking execution 5 (seconds)

Repeated access barrier 0 (minutes)

Project registration ☒

Fingerprints control quote 50 %

Figure 5.46 - Time devices - Advanced settings

- Jump to Now/Mark: This is the jump address for Now/Mark bookings. This address depends on the sequence file.
- Jump to Sequence: This is the jump address for the sequence. This value usually is set to 10. Other values depend on the sequence file.
- Serial Number: Serial number of the terminal.
- Period of display for booking execution: This time defines, how long the generation of a booking will be shown on the Terminal display.
- Repeated access barrier: Note: This is a setting used due to compatibility issues with GAT Manager. Not supported by GAT ACE.
- Project registration: If this option is marked, any projects can be recorded (as long as this is allowed by the sequence). Otherwise only projects can be recorded for which data has been loaded into the terminal.
- Fingerprints control quote: Note: This is a setting used due to compatibility issues with GAT Manager. Not supported by GAT ACE.

Register Card "Time Settings"

Time Device

Save Cancel

General Advance Settings Time Settings Memory

Entry Time 5

Display Time 5

Change Time 5

Figure 5.47 - Time devices - Time settings

Here you can adjust the time behaviour of the terminal.

- Entry Time: This is the input timeout value for entering values at the terminal.
- Display Time: This time defines the time (in seconds) how long an information (e.g. booking) will be shown on the display of the terminal before the terminal switches back to the standard screen.
- Change Time: This is a setting used due to compatibility issues with GAT Manager. Not supported by GAT ACE.

Register Card "Time Settings"

Figure 5.48 - Time devices - Memory settings

Here you can define, how the memory of the terminal shall be used and how many space shall be reserved for certain different data. This helps to adjust the memory segmentation for different use scenarios.

- No. of Personnel records: Number of personnel records that can be stored in the terminal. The size of each record can vary.
- No. of Display Texts: This indicates how many display texts can be stored in the terminal.
- No. of Cost accounts: Number of cost accounts or projects respectively that can be stored in the terminal.
- No. of Causes: Number of causes for absence that can be stored in the terminal.
- No. of Time bookings: Number of time bookings that can be stored in the terminal. If the memory is full, no more time bookings are possible before the bookings are downloaded from the terminal.
- No. of Access bookings: This is the number of access bookings that can be stored in the terminal. The memory of the terminal is a ring buffer, which means that, if the memory is full and a new booking shall be stored, the oldest booking will be overwritten.

Register Card "Sequence File"

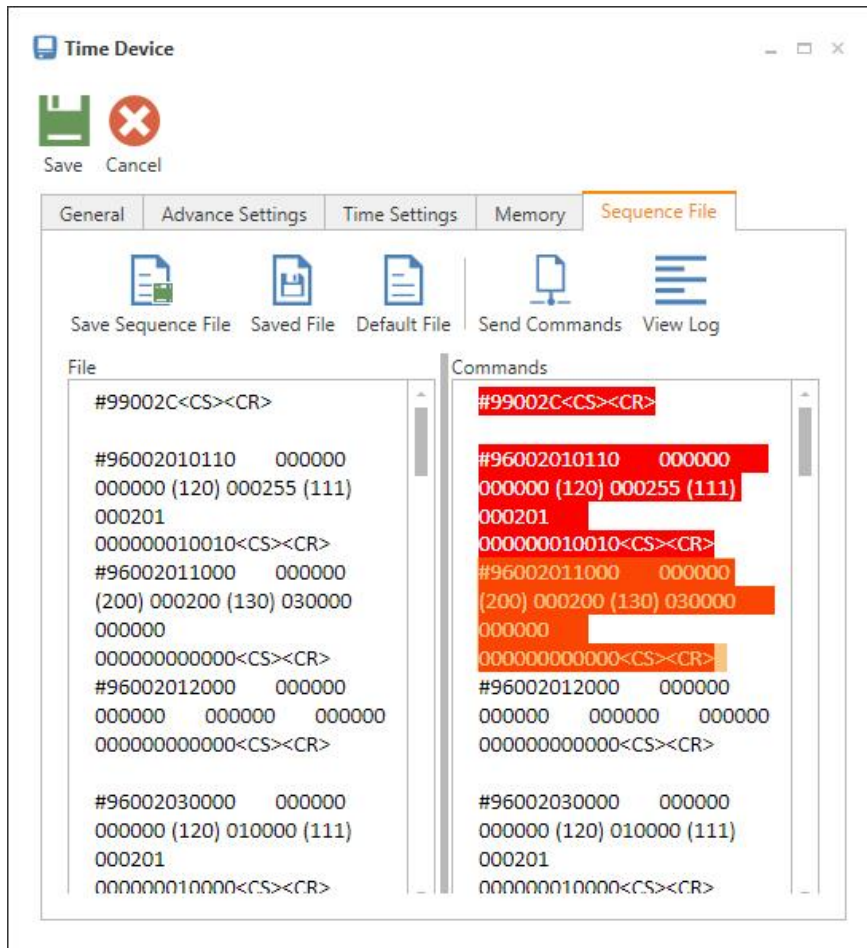


Figure 5.49 - Time devices - Sequence File

Here you see the sequence file for the terminal. The sequence file controls the functions of the terminal. If other functions than the ones that are available as standard are required a corresponding sequence file must be sent to the terminal.

- ▶ You can change the shown sequence file on the left field "File" and save it with "Save Sequence File".
- ▶ To reload the last saved sequence file, click the symbol "Saved File".
- ▶ To reload the default sequence file, click the symbol "Default File".
- ▶ To send the sequence file to the terminal, press "Send Commands".
 - The commands will be sent and the current status is shown in the right field "Commands".
- ▶ You can skip the sending of the commands by pressing the symbol "Stop Commands", which is only shown while commands are sent.

5.6.2 Time Bookings

- To view the time bookings, select the symbol "Time Bookings" from the multifunction bar.
 - The time bookings view is opened and the read bookings are displayed.

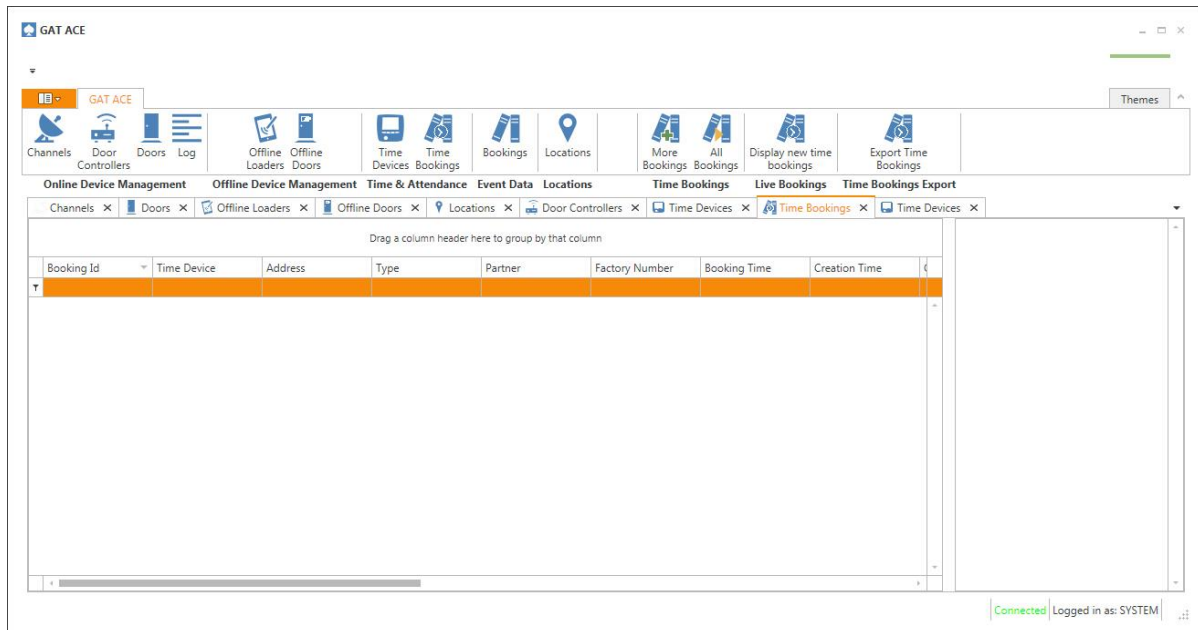


Figure 5.50 - Time Bookings view

The latest bookings will be shown first. If you want to see older bookings, select the corresponding function from the icon bar:



- With the symbol "More Bookings" the next, older bookings are loaded and displayed. The amount of read bookings is limited, in order to reduce the waiting time in case there are a lot of bookings. You can select this function multiple times in order to see older bookings until the desired booking periode is displayed.
- With the symbol "All Bookings" all bookings will be loaded at once. This can take a long time if there are a lot of bookings.
- With the symbol "Stop reading bookings" you can stop the loading of bookings, if the bookings of the desired time frame are already shown. This symbol is only displayed if bookings are being loaded.
- With the symbol "Display new time bookings" the latest time bookings will be read from the time terminals.
- With the symbol „Export Time Bookings“ the currently shown bookings are saved to a file according to the settings in the Settings Page "Time Bookings Export Settings" (see "4.8 Time Bookings Exporting Settings" Settings Page").

6 AUTHORISATION MANAGEMENT

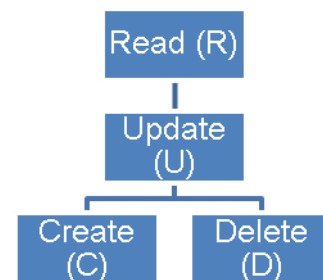
GAT ACE offers the possibility to assign individual users with different levels of system control. This is done using a simplified “role” based access system. Each user is assigned to one role and the user's system control is inherited from this role. A role represents a collection of permissions that 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 (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 for 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 to modify them, while other users are allowed to view and modify the device settings.

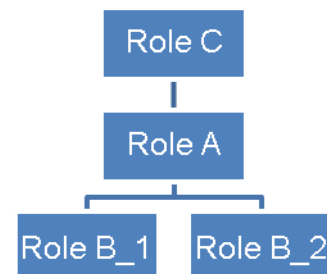
The RUCD permissions are organised in a hierarchical way. This means that it is not possible to assign Update permission without having Read permission. The diagram to the right shows the hierarchy of access levels.



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 this function block. Any future 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 organised in a hierarchical way. Every role is assigned to exactly one parent role and has multiple child 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 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. Every following role is therefore a descendant of the SYSTEM role.

The maximum permissions a role can have are the rights of its parent role. Removing a right from a parent role will also delete the right from any descendant.

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

The screenshot displays the 'Roles and Users' management page in the GAT ACE application. The left sidebar contains navigation links: User Settings, Roles and Users (selected), Anti-pass-back areas, Application Settings, Card- and Reader-Settings, Database Settings, Communication Settings, Diagnostics, About, and Exit application. The main content area is titled 'Roles and Users' and features two tables. The first table, 'Roles', has columns for Role Id, Role name, Role description, Parent role, and Level. It lists three roles: 1. SYSTEM (parent: none, level: 0), 2. Administrator (parent: SYSTEM, level: 1), and 3. User (parent: Administrator, level: 2). The second table, 'Users', has columns for User Id, User name, Display name, Role, Last login, and Special rights. It lists two users: 1. SYSTEM User (role: SYSTEM, last login: 20/04/2018) and 2. Administrator (role: Administrator). Above the roles table are buttons for 'Add role', 'Edit role', 'Delete role', and 'Active Directory'. Above the users table are buttons for 'Add user', 'Edit user', and 'Delete user'.

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	20/04/2018	☐
2	Administrator	Administrator	Administrator		☐

Figure 6.1 – Roles and users 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						
Geräte Einstellung...	☐	☒	☐	☐	☒	☐
Datenbank Einstell...	☒	☒	☒	☒	☒	☐
Anwendungs Einst...	☒	☒	☒	☒	☒	☐
Ausweis- und Leser...	☒	☒	☒	☒	☒	☐
Kommunikations Ei...	☐	☐	☐	☐	☒	☐
Konfigurations File...	☐	☐	☐	☐	☒	☐
Logfile Anzeige Ein...	☐	☒	☐	☐	☒	☐
Anti Pass Back Zon...	☒	☒	☒	☒	☒	☐
Role management	☐	☐	☐	☐	☒	☐
User management	☐	☐	☐	☐	☒	☐

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

- ▶ In the "Parent role" field, enter a parent role from which the new role inherits.
- ▶ 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. 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

Every user in GAT ACE 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 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.

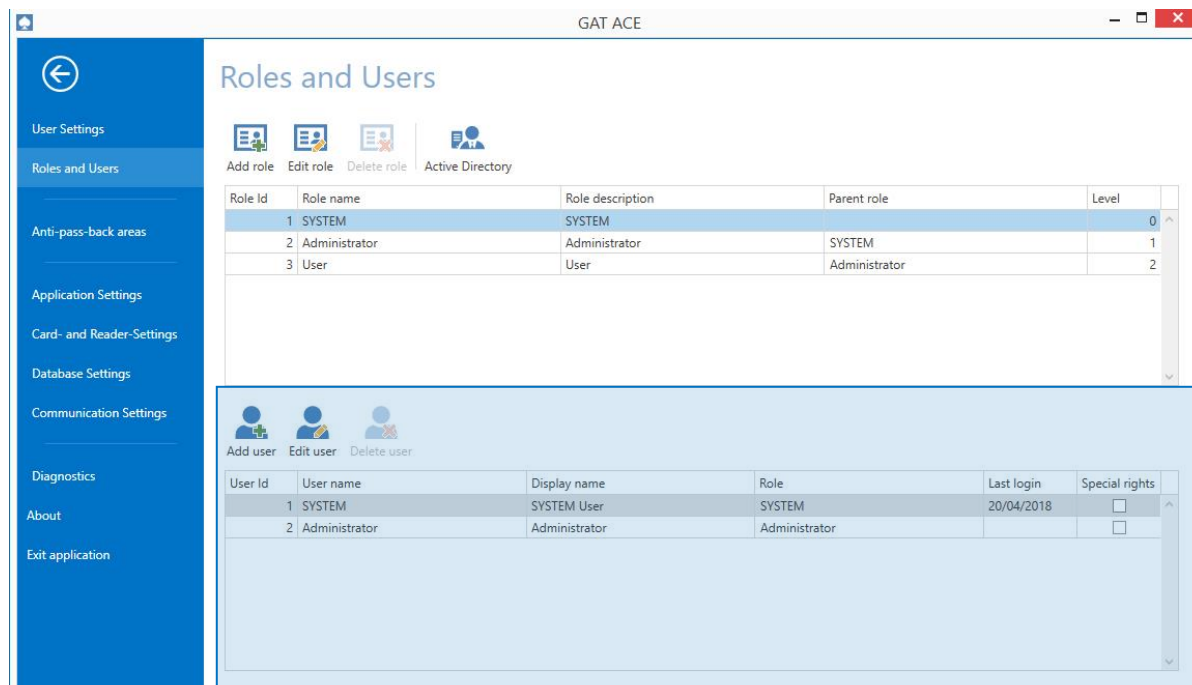


Figure 6.3 – Users overview

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, as described in section "6.3.1. 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: [dropdown]

User name: [text box]

Display name: [text box]

Password: [text box] Generate

Repeat password: [text box]

Name	C	R	U	D	E
GAT ACE					
Geräte Einstellun...	☐	☐	☐	☐	☒
Datenbank Einstel...	☐	☐	☐	☐	☒
Anwendungs Eins...	☐	☐	☐	☐	☒
Ausweis- und Les...	☐	☐	☐	☐	☒
Kommunikations...	☐	☐	☐	☐	☒
Konfigurations Fil...	☐	☐	☐	☐	☒
Logfile Anzeige Ei...	☐	☐	☐	☐	☒

User Id 3

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 overview

- ▶ Enter a unique name for the user in the "User name" field. The user will use this name to log in.
- ▶ In the "Display name" field, enter a display name for the user. GAT ACE 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.

The "User ID" is generated automatically and is only relevant for external applications.

- ▶ In the "Role" field, assign a role to the user from the drop-down menu.
 - The authorization of the user to use specific functions is directly linked to the selected role.
- ▶ 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 read permissions "R" for the "Application settings management" function blocks have been explicitly assigned for the user and will override the inherited settings from the selected "User" role.
- ▶ To revoke set permissions, click with the right mouse button on the appropriate fields.

6.3.1 Default Users

After the installation of GAT ACE, the following default user accounts are available.

User:	SYSTEM	Administrator
Roll:	SYSTEM	Administrator
Password:	GAT	Mirone59



Immediately after installation of GAT ACE you must change the standard passwords of the default users to secure and secret new passwords, due to security reasons.

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
Data carrier settings management	X	X	X	X	-	X
Communications settings management	X	X	X	X	-	X
Configuration file management	X	X	X	X	-	X
Log file view settings management	X	X	X	X	-	X
Anti-passback zone 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
Data carrier settings management	X	X	X	X	-	X
Communications settings management	O	O	O	O	-	O
Configuration file management	O	O	O	O	-	O
Log file view settings management	X	X	X	X	-	X
Anti-passback zone 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

7 MIGRATING GAT MANAGER TO GAT ACE

GANTNER Electronic GmbH has developed GAT ACE as the modern successor to the GAT Manager software. Existing systems using GAT Manager software can switch to GAT ACE using the "Gm2AceConverter" software tool by GANTNER Electronic GmbH, allowing the importation of the existing database including the controller configurations into GAT ACE. This chapter gives an overview of this tool.

The Gm2AceConverter tool is operational without installation.

- ▶ Copy the packet with the Gm2AceConverter into a folder on the PC on which GAT Manager is installed.
- ▶ In this folder, run the "Gm2AceConverter.exe" file.
 - The following user interface is displayed.

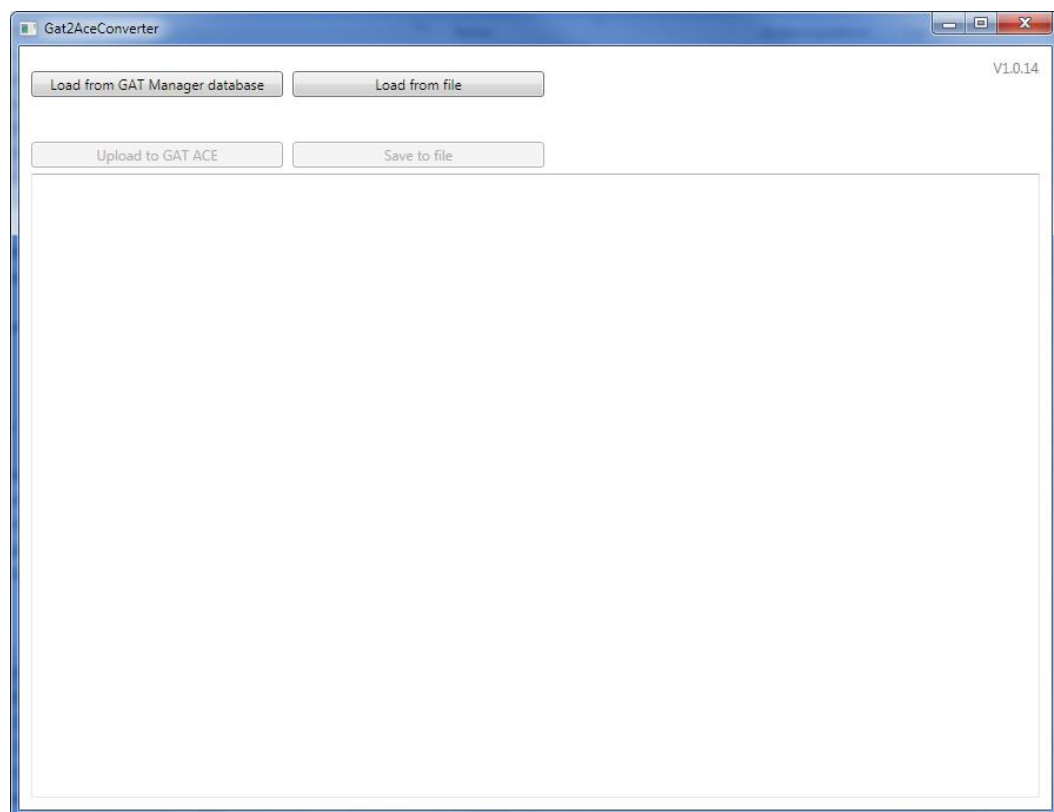


Figure 7.1 - Gat2AceConverter window

- ▶ Click on the "Load from GAT Manager Database" button.
- ▶ Select the location, where the GAT Manager database files are saved.
 - The data is read from the database.
- ▶ Save the database into a file by pressing the "Save to File" button.

- ▶ Next, copy the packet with the Gm2AceConverter into a folder on the PC on which GAT ACE is installed.
- ▶ Copy the file created previously to the GAT ACE PC.
- ▶ Start the "Gm2AceConverter.exe" tool on the PC on which the GAT ACE 3000 is already running.
- ▶ Click on the "Load from File" button and select the file created on the GAT Manager PC in order to load this file.
- ▶ Click the "Upload to GAT ACE" button in order to migrate the data into GAT ACE.
 - GAT ACE can now be started and all settings from GAT Manager are now transferred.
- ▶ Check the settings of the controller and look for missing settings that are new in GAT ACE.

NOTE! The Gm2Ace converter needs a .NET Framework 4.5. on the GAT Manager computer. If it cannot be installed due to the age of the operating system, the database of the GAT Manager and the FLEX.INI file can be transferred to another PC on which a GAT Manager or the Borland Database Engine is installed as well as the .NET Framework 4.5. The conversion can be performed on this PC as well.

8 DATA PROTECTION

8.1 General Data Protection Regulation (GDPR)

From the 25th May 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 Minimisation
- 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 or 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 3000 offers. The instructions are summarised in the following sections.

8.1.1 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 anonymised) 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.

8.1.2 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 Minimisation** 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 authorised persons to access the software and by limiting the software users to access only the data needed to perform their tasks (see section "6.3. User Management").

8.1.3 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.

8.1.4 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.

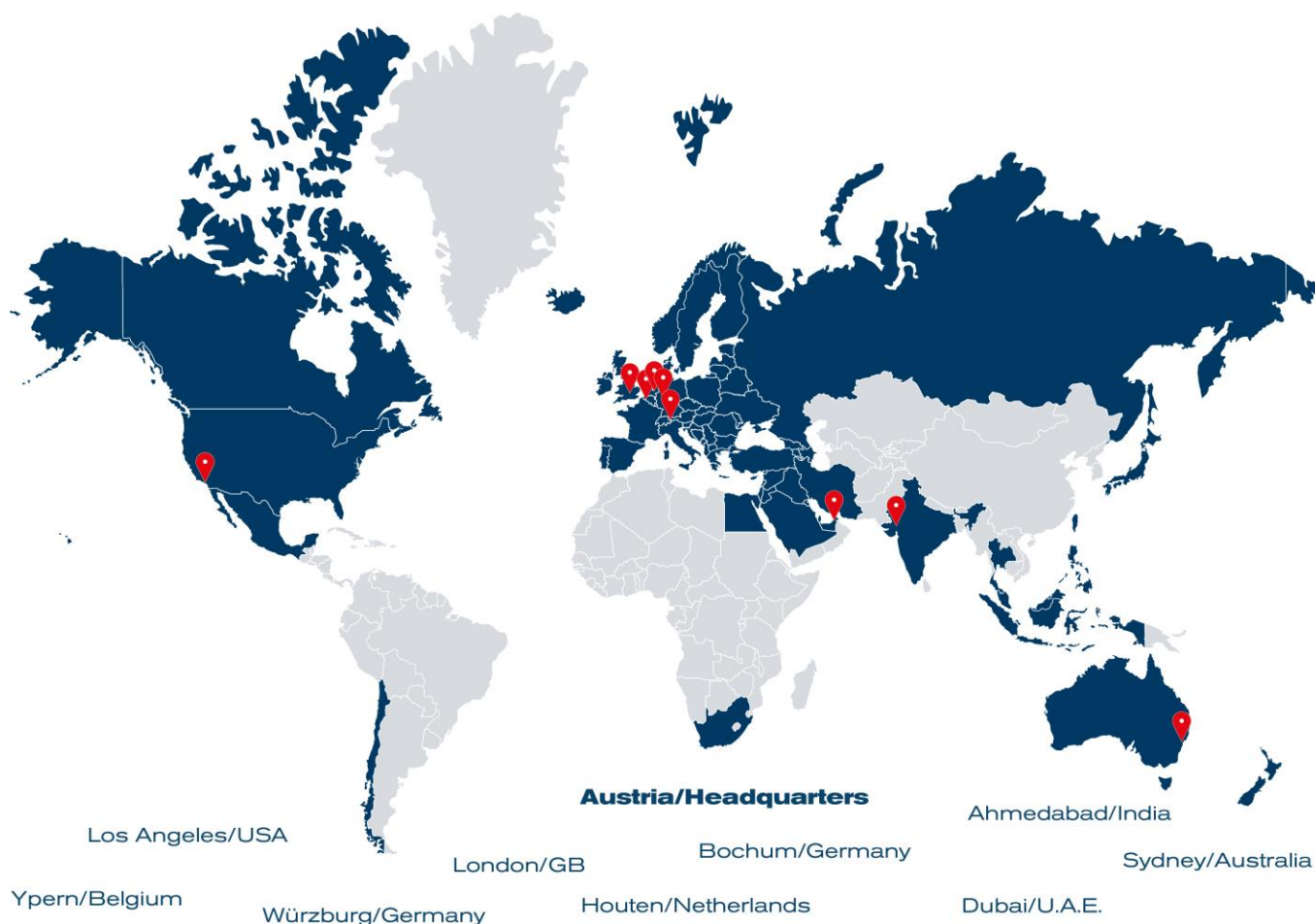
The data storage period depends on the requirements for access traceability that you need in your company. By deleting data, the **Principle of Storage Limitation** can be met (see section "5.3.2. Cleanup of the Database Table").

If you have designated a data protection policy leader in your company, fulfilled the legal framework, taken technical and organisational 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 3000 version 3.0 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 29th July 2019. It is subject to change.
Amendments can be made without prior notice at any time.
Information in this manual is valid for GAT ACE 3000 version 3.0.0 onwards.



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