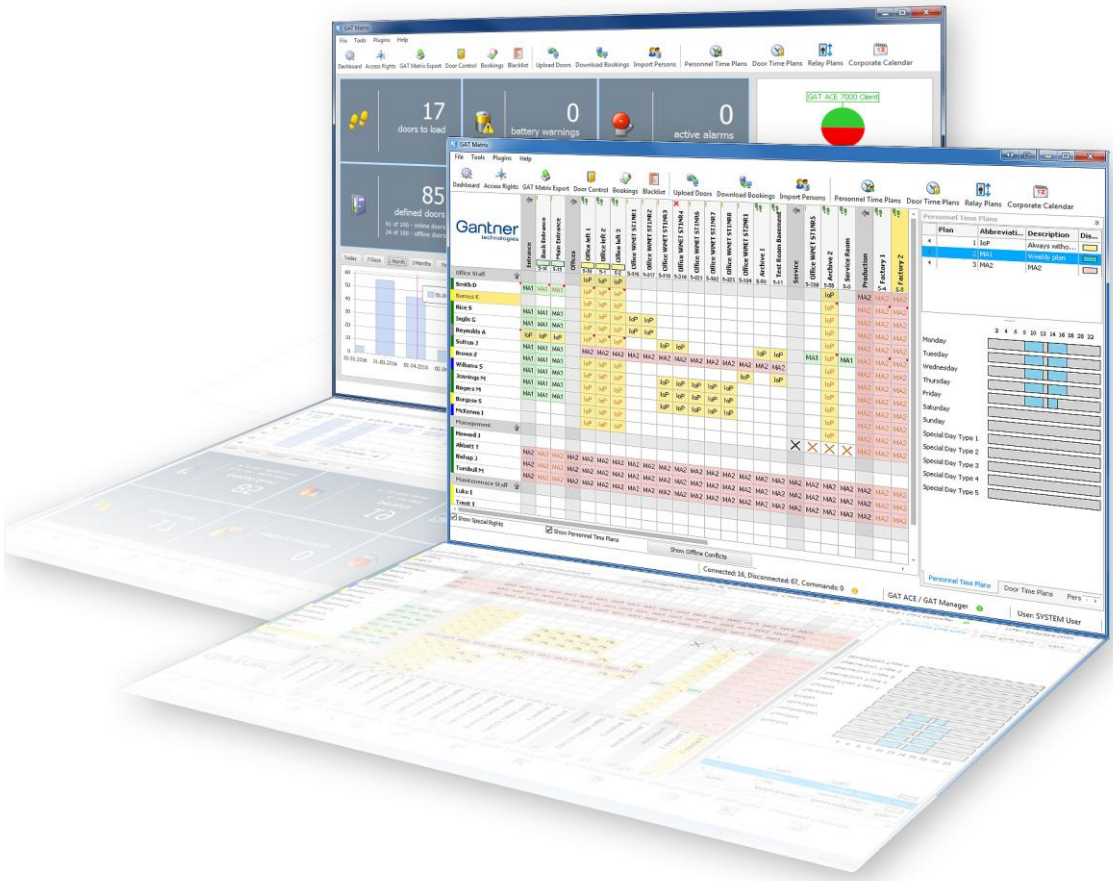
Gantner

Matrix

Software for Access, Organization, and Authorization Management



Installation, Configuration, Operation
Document version 7.1
Software version 7.1.0

© Copyright 2025 GANTNER Electronic GmbH

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

Liability

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

Trademarks

Attention is drawn at this point to markings and registered trademarks used in this manual. All product and company names that 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 Matrix or for general enquiries is listed below:

Contact address of manufacturer

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

General Warning and Safety Instructions

Dear Customer,

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

1. The installation, commissioning, operation, and maintenance of the product must be carried out in accordance with the technical conditions of operation as described in the corresponding product documentation.

2. Before installing, commissioning, operating, or maintaining the product, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.

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

4. Where not otherwise specifically documented, the appropriate installation, commissioning, operation and maintenance of the product is the customer's responsibility.

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

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

7. The installation, commissioning, and servicing of our products must be performed by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association (e.g., ÖVE [Austrian], VDE [Germany]).

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

9. It is prohibited to alter the products or remove protective shields and covers.

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

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

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

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

14. We especially look forward to hearing from you if you just want to tell us that everything is functioning perfectly.

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

CONTENTS

1. INTRODUCTION 9

1.1 About this manual 9
1.2 Formatting 11
1.3 Contact and inquiries 11

2. GENERAL INFORMATION 13

2.1 Features 14
2.2 Terminology 15

3. INSTALLATION 21

3.1 Hardware specifications 21
3.1.1 Configuration example 1 (only GAT ACE and Matrix for smaller systems) 21
3.1.2 Configuration example 2 (including larger systems with Relaxx installation) 21
3.1.3 Configuration example 3 (including SALTO ProAccess Space) 22
3.2 Software requirements 24
3.2.1 Supported operating systems 24
3.2.2 Database server 24
3.2.3 Microsoft .NET 25
3.2.4 Additional software requirements 25
3.3 Relaxx (locker locking systems) 27
3.4 SALTO ProAccess SPACE (SALTO access control) 27
3.4.1 Restrictions for the integration of SALTO devices 28
3.5 General information on Matrix communication 29
3.5.1 Communication with GAT ACE 29
3.5.2 Communication with ProAccess Space 30
3.6 Use cases and types of installation 30
3.6.1 Initial installation of Matrix 30
3.6.2 Updating Matrix 31

4. FIRST STARTUP OF MATRIX 33

4.1 Database settings 33
4.2 Database cleanup 35
4.3 TLS certificate configuration 36
4.4 Settings of the network services (clients) 39
4.4.1 License server (Licensing Client Interface) 40
4.4.2 GAT ACE client interface 42
4.4.3 Matrix Synchronizer settings for multi-user capability 43
4.4.4 Relaxx interface 45
4.4.5 TBS RemoteSync interface 47
4.5 Language selection 48
4.6 Login 48
4.6.1 Two-factor authentication 49
4.6.2 Password recovery 51
4.7 General settings 52
4.8 Global settings 53
4.9 Network settings 55
4.10 Settings for person display 56
4.11 Optional fields for personnel data 59
4.12 Activating Matrix 61
4.13 Multi-user capability 61

5. OPERATION 63

5.1 Dashboard 63
5.2 Main window 66
5.2.1 Authorization matrix 68
5.3 Person groups and door groups 69
5.3.1 Moving persons or doors between groups 70
5.4 Importing doors and locations from GAT ACE 71
5.4.1 Door import configuration 72
5.4.2 Location import configuration 76
5.4.3 Description text for doors 77
5.4.4 Display of the battery-powered or wired GAT DL 73xx electronic locks 78
5.5 Importing doors and locations from SALTO ProAccess SPACE 79
5.5.1 Configuring the import of doors and locations 81
5.5.2 Description text for doors 83
5.5.3 Display of SALTO locks and users (door import from ProAccess Space) 85
5.6 Editing the master data of a person in the authorization matrix 86
5.6.1 Defining personnel master data 87
5.6.2 Settings for persons in ProAccess SPACE 90
5.6.3 Authorizing and configuring data carriers for persons 92
5.6.4 Defining data carrier types 96
5.6.5 Reading and deleting SALTO data carriers 98
5.6.6 Automatically preparing existing persons for SALTO ProAccess SPACE 99
5.6.7 Scanning fingerprints 101
5.6.8 TBS system (biometrics) 105
5.6.9 Inserting a picture for a person 112
5.6.10 Settings for license plate recognition 113
5.6.11 Personnel settings for SALTO ProAccess Space 114
5.6.12 Assigning persons to groups 115
5.6.13 Reloading personnel data into a controller 115
5.6.14 Copying a person 116
5.6.15 Deleting a person 116
5.7 Import persons 117
5.7.1 Importing via CSV file 118
5.7.2 Importing via SAP 123
5.7.3 Importing from database 124
5.7.4 Delete actions 129
5.8 Pool groups 132
5.9 Multi-site policy 134
5.9.1 Enabling the multi-site policy 134
5.9.2 Assigning person groups 135
5.9.3 Assigning door groups 136
5.9.4 Assigning corporate calendars 136
5.9.5 Enabling locker groups 137
5.9.6 Limitations of the multi-site policy 138
5.10 Data carrier blocklist 140
5.10.1 Adding data carriers to the blocklist 141
5.10.2 Assigning data carriers to doors 142
5.10.3 Deleting data carriers and door assignments from the blocklist 143
5.10.4 Importing personnel data with blocklist 143
5.11 Defining personnel time plans 144
5.11.1 For GANTNER doors: assigning, changing, deleting day schedules 146
5.11.2 For GANTNER personnel time plans: settings for day plans 148
5.11.3 For SALTO doors: creating, changing, deleting time zones 150
5.11.4 Converting a GANTNER personnel plan to a SALTO personnel plan 151
5.12 Defining door time plans 153

5.12.1 For GANTNER doors: assigning, changing, deleting day plans 155
5.12.2 For GANTNER door plans: settings for day plans 157
5.12.3 For SALTO doors: creating, changing, deleting time zones 160
5.12.4 Converting a GANTNER door plan to SALTO time zones 162
5.13 Assigning door time plans to the doors 164
5.14 Defining authorizations of persons in the authorization matrix 165
5.14.1 Symbols and color indications used in the authorization matrix 165
5.14.2 Assigning special rights 167
5.14.3 Assignment possibilities 170
5.14.4 Deleting an assigned personnel time plan from a person 171
5.15 Relay time plans 172
5.15.1 Creating, editing, & deleting relay plans 174
5.15.2 Assigning a relay plan to a person 176
5.15.3 Assigning a relay plan to multiple persons or a group of persons (inheritance) 177
5.15.4 Denying the relay plan of a person 178
5.15.5 Deleting a relay plan assignment 179
5.15.6 Assigning a relay plan to a door (for general open plans) 179
5.16 Time switches 181
5.17 Door control 184
5.17.1 Activating door control for a door 185
5.17.2 Displaying and acknowledging alarms 187
5.17.3 Controlling the doors 187
5.17.4 Deleting doors and general control 189
5.18 Upload doors 190
5.18.1 Uploading online doors 190
5.18.2 Uploading offline doors 191
5.18.3 Loading online doors from SALTO 193
5.18.4 Loading offline doors from SALTO via programming device (PPD) 195
5.18.5 Reloading a single door 196
5.18.6 Locker authorizations 197
5.18.7 Locker matrix 199
5.18.8 Assigning locker authorizations 201
5.18.9 Locker authorizations for free locker selection 201
5.18.10 Locker authorizations for personal lockers and shared lockers 204
5.19 Locker control 209
5.19.1 Matrix display for locker control 210
5.19.2 Controlling the lockers 212
5.20 Search function 213
5.21 Creating access authorization reports 214
5.21.1 Blocklist 215
5.21.2 Excel export 216
5.21.3 PDF export of persons 217
5.21.4 When was a data carrier used for the last time? 220
5.21.5 Who has a specific time plan? 222
5.21.6 Who has access in a specific period? 224
5.21.7 Who has access? 226
5.21.8 Where does somebody have access to? 228
5.22 GAT ACE status 230
5.23 Configuring the SALTO JustIN app for access control 231

6. CORPORATE CALENDAR AND LOCATIONS 235

6.1 Defining a corporate calendar 236
6.2 Locations 240

7. BOOKINGS 243

7.1 Sorting, grouping, & filtering bookings 244

7.1.1 Sort bookings ... 244
7.1.2 Group bookings ... 244
7.1.3 Filter bookings ... 246
7.1.4 Show and hide columns in the bookings list ... 248
7.1.5 Filter authorization matrix ... 249
7.2 Export and print bookings with booking reports ... 251
7.2.1 Configuration of booking reports ... 252
7.3 Access code descriptions ... 254
7.3.1 Reload default values of the access codes ... 255
7.3.2 Add access code ... 255

8. ACTIVITY JOURNAL ... 257

8.1 Refresh, sort, group, and delete the activity list ... 258
8.2 Generate reports ... 260

9. AUTHORIZATION MANAGEMENT ... 261

9.1 Function blocks ... 261
9.2 Role management ... 262
9.3 User management ... 264
9.4 Active Directory ... 265
9.4.1 Configuring the Active Directory function ... 265

10. LICENSE MANAGEMENT ... 267

10.1 License overview ... 267
10.2 License details ... 268
10.3 Adding licenses ... 269
10.4 Product activation ... 270
10.5 Licensing for SALTO doors ... 273

11. PERSONS IMPORT SERVICE ... 275

12. MATRIX EXPORT ... 277

12.1 Usage report ... 278
12.2 Person export ... 283
12.3 Exporting the personnel data for GAT ECO.Lock Manager ... 286

13. DATA PROTECTION ... 289

13.1 General Data Protection Regulation (GDPR) ... 289
13.1.1 Perform an inventory analysis ... 289
13.1.2 Create a processing directory ... 290
13.1.3 Data protection impact assessment ... 290
13.1.4 Comply with information requirements and declarations of consent ... 290

APPENDIX A: INSTALLATION OF SQL SERVER ... 293

APPENDIX B: INSTALLATION OF MATRIX ... 297

APPENDIX C: SALTO PROACCESS SPACE INTEGRATION ... 303

APPENDIX D: FORMATS AND FILE SPECIFICATIONS ... 309

APPENDIX E: DATABASE BACKUP ... 313

APPENDIX F: PORT LIST ... 317

1. INTRODUCTION

1.1 About this manual

This manual contains all-important information necessary to install Matrix as well as instructions on how to operate the software.

The configuration software GAT ACE 3000 or GAT ACE 7000 are also required to use Matrix. This software is described in a separate manual and also via an online help accessible directly within the software. In addition, this manual also describes the information necessary to operate with the Relaxx and SALTO Space software. A detailed description of these applications and how to install them is provided in the respective documentation of Relaxx and SALTO Space.

Chapter "2 GENERAL INFORMATION" gives an overview of Matrix and its main functions and you can find a description of frequently-used terms in this manual.

Chapter "3 INSTALLATION" describes the installation of Matrix and the system requirements in general. Here you can also find a description of the different system set-ups and application types (update from GAT Access to Matrix or new installation). Please note that a detailed installation description is included in Appendix A and B.

Chapter "4 FIRST STARTUP OF MATRIX" describes the settings that must be made when Matrix is started for the first time. These settings usually only need to be made once and include the database configuration, the set-up of the network services (clients) and the selection of the display language of Matrix. The log-in process is also described here as well as the general and global settings of Matrix. In addition, the optional multi-user capability (simultaneous use of a single Matrix installation by multiple workstations) and how to define optional fields for the personnel data are also described in this chapter.

Chapter "5 OPERATION" describes in detail the work with Matrix. This includes an overview of the Matrix user interface, an explanation of groups and terminal handling, how to edit and import personnel data, how to define personnel and access time plans, how to work with the authorization matrix in the main window of Matrix, and how to define relay plans for the terminals. Here, you will also find instructions on how to control locker locks directly in Matrix using the Relaxx software and how to use SALTO Space locks in Matrix. The chapter also describes how to generate several types of reports about authorization data (excel or PDF format) in Matrix.

Chapter "6 CORPORATE CALENDAR AND LOCATIONS" describes the calendar in Matrix which is used to define special days and holidays, etc. This information is used to activate different access authorization plans on certain days.

Chapter "7 BOOKINGS" provides information on how to work with the booking data from the access terminals. In detail, how to download bookings from the terminals, how to sort the bookings, how to export bookings to external files for further processing, and also how to define the booking codes.

Chapter "8 ACTIVITY JOURNAL" describes how to evaluate (read, sort, export) the activities of the users in Matrix.

Chapter "9 AUTHORIZATION MANAGEMENT" describes how the users in Matrix are organized by using function blocks and user roles. In addition, the multi-site policy (the ability to configure which person and door groups are displayed for different locations or users) is described here.

Chapter "10 LICENSE MANAGEMENT" includes information of the license system of Matrix, how to purchase and add licenses for additional program functions and how to activate Matrix.

Chapter "11 PERSONS IMPORT SERVICE" describes the personal import of external personnel data into Matrix.

Chapter “12 MATRIX EXPORT” describes the export plugin, which allows you to export usage reports (e.g., for parking use or food expenses) and personnel data. An additional license is required for this plugin.

Chapter "13 DATA PROTECTION" informs you about the new EU General Data Protection Regulation and how Matrix supports compliance with the requirements.

Chapter "Appendix A: Installation of SQL Server" describes the installation process of the SQL Server required by Matrix. This chapter and the following are intended for users who have not used another access system of GANTNER Electronic GmbH before and who install Matrix for the first time.

Chapter "Appendix B: Installation of Matrix" describes the installation process of Matrix in detail.

Chapter "Appendix D: Formats and File Specifications" describes format settings and file formats used by Matrix - especially the exact format of the personal import files.

Chapter "Appendix E: Database Backup" shows how to save a backup of the database.

Chapter "Appendix F: Port List" shows the list of interface ports that are used by Matrix.

1.2 Formatting

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

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

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



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

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

► This symbol represents an action or instruction that you must follow.

- ○ This symbol represents the result after executing the previous action.

1.3 Contact and inquiries

If you have any questions concerning Matrix, or with any of the associated hardware and software products from GANTNER, please contact your local sales partner or directly with one of the GANTNER branch offices. The contact information is listed on the cover of this manual.

2. GENERAL INFORMATION

Matrix is a component of the GAT Management Solution software package. It is a PC application designed for fast and effortless authorization management for access control systems that use GANTNER terminals.

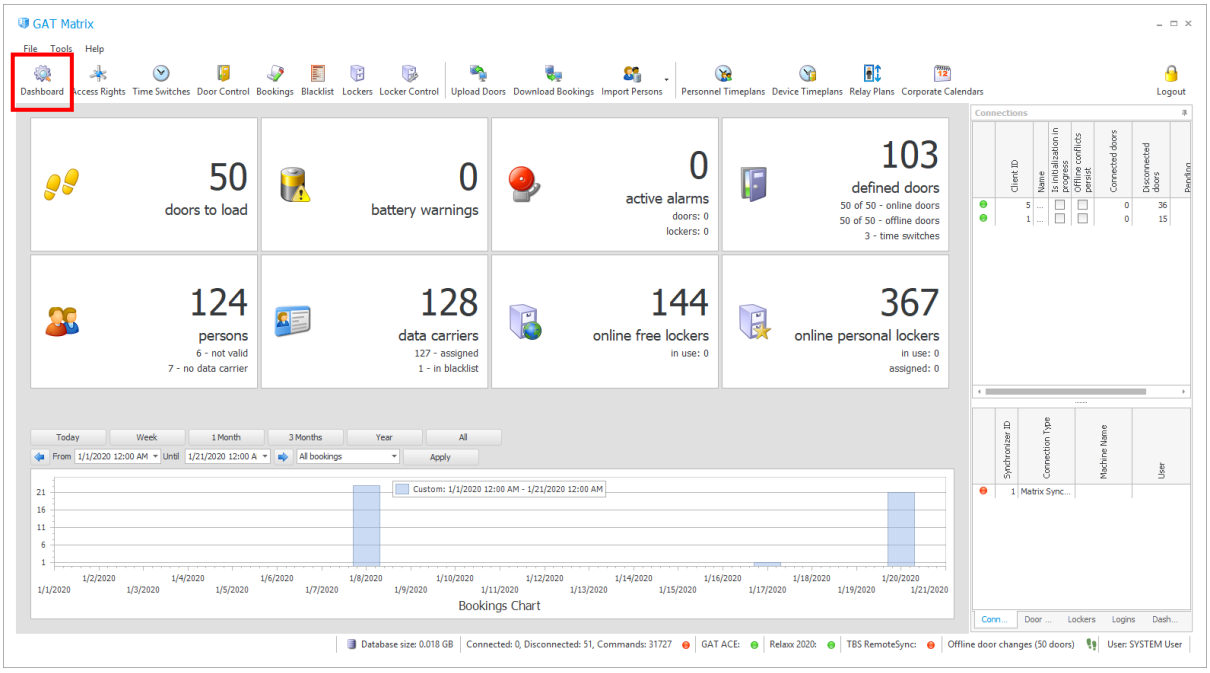


Figure 2.1 *- Matrix main page (Dashboard for the display of various system status information)*

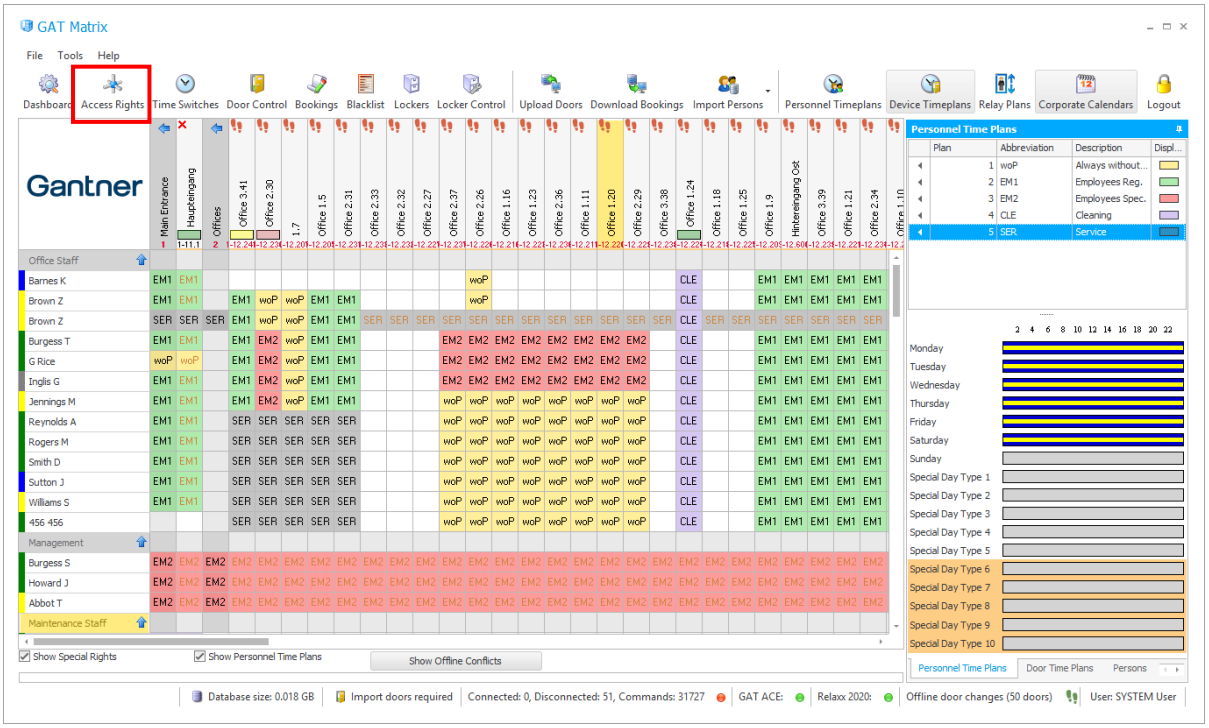


Figure 2.2 *- Matrix main page (define and manage access rights)*

Matrix operates in combination with GAT ACE software from GANTNER Electronic GmbH. The authorization of access for system users is defined and managed in Matrix while GAT ACE controls the hardware structure and access control terminals, i.e., the hardware settings, addresses, and bus parameters of all terminals in the system.

The difference between GAT ACE 3000 and GAT ACE 7000 software versions must be clarified. Matrix can operate with one of these versions, or with both versions simultaneously. The generic term "GAT ACE" is used in this manual for information that is applicable for both GAT ACE 3000 and GAT ACE 7000.

The GAT ACE 3000 and/or GAT ACE 7000 Windows Service must be installed and running before you can use Matrix. It is possible to install GAT ACE on the same PC as Matrix or on another PC.

NOTE! Please note that GAT Manager is no longer supported from Matrix version 3.2.0 onwards.

As of Matrix version 5.0, the ProAccess Space software can also be connected in order to use the authorization assignment of Matrix for SALTO lock technology.
As of Matrix 5.1, the JustIN app from SALTO for door control via mobile phone is also available. The authorizations can be managed directly in Matrix via the personnel data.

2.1 Features

- Simplest administration of access authorizations in a lock-plan matrix view
- Clear dashboard for the status display of various system information
- Possibility to group persons and doors for an optimized organization
- Inheritance of access authorization of persons and doors groups
- Multilingual platform (English, German, Spanish, Catalan, French)
- Multi-site policy (organization of users via the locations managed in GAT ACE 7000)
- Client-related authorization assignment for the display and processing of persons and doors groups
- Special rights definable according to the matrix
- Location-specific special day calendar with automatic calculation of holidays and special days based on specific rules
- 10 (GAT ACE 7000), 5 (GAT ACE 3000) or 3 (SALTO ProAccess SPACE) types of special days with special authorization functions
- Individual schedules for persons who can be assigned to the doors
- An individual door schedule for each door with up to 10 different authorization options per day
- Access authorizations for offline doors also definable
- Blocking of data carriers with the blocklist (for offline doors)
- Display of battery warnings for CardNET-, WiNET-, and SALTO SVN locks
- Display of the charging status of emergency power supplies (UPS) powering online controllers
- Several types of data carriers can be defined in GAT ACE 7000 (GAT ACE 3000 uses only one type)
- Vehicle recognition integrated in the personnel data
- Administration of relay plans, e.g., to activate lift controls
- Scanning and management of fingerprint data for system users
- Complete recording of all movement data
- Automatic deletion function for compliance with the requirements of the General Data Protection Regulation
- Activity journal with recording of all user actions
- Convenient formatting of access events for printing reports in various formats (PDF, HTML, CSV, etc.)

- Multi-ACE function -- connection to multiple GAT ACE 3000 and/or 7000 applications possible
- Connection to SALTO's ProAccess Space software for authorization assignment via Matrix
- SALTO JustIN app with authorization management in Matrix
- SALTO SVN support, writing permissions to MIFARE DESFire data carriers with GANTNER SVN coding
- Convenient interfaces for easy data importation (e.g., SAP)
- Manual door control, door unlocking, card release, etc., directly in Matrix
- Alarm acknowledgement
- Controller for timer function configurable
- Door status display and door control
- Status display of the GANTNER electronic locker locks via a Relaxx software connection
- GANTNER electronic locker locks can be controlled directly in Matrix

2.2 Terminology

Some terms are used often in this manual, and these are defined as follows:

User
A "user" in this manual refers to the people that use the application. Multiple users with different hierarchy levels can be defined each assigned a username and password.

Location (Site)
To structure the management of access control systems and simplify administration, GAT ACE organizes the locations in a tree-type format.
In Matrix, the multi-site policy can be used to limit the users of Matrix to see/edit doors of specific locations and selected groups of persons only. Doors and persons for whom a user has no access rights via the multi-site policy are not visible to the user.
A corresponding license is required in order to use multi-site policy.

Person
A "person" in this manual denotes any person who is registered to use the access control system. The persons are identified at the access terminals by their unique RFID data carriers. A person must be defined in Matrix and access authorization must be assigned to the person by a time plan in order to allow access for the person at certain doors. Personnel data for each person is stored in the Matrix database.

Data carrier
The data carriers are used for identification at the access terminals. Identification occurs via contactless radio - frequency (RFID). Different types of RFID technologies are available (LEGIC, MIFARE®, ISO 15693, and Proxy). Different types of data carrier media are available such as cards, key tags, and wristbands.

Controller / Terminal / Lock
The terms controller and terminal are used interchangeably throughout this manual and refer to the devices installed near doors that read the data carriers of people, verify their validity, and unlock the doors accordingly. Controllers are created, configured, and managed in GAT ACE.
The difference between online and offline terminals (i.e., doors) must be clarified. Online terminals have a network interface, by which they connect to a local network. A LAN network (Ethernet) as well as a serial RS-485 network

are possible. There is a direct connection to online controllers, which allows their direct configuration and a current update of states. The current states of online controllers are graphically represented in the matrix user interface. This data requires, for example, an appropriate response from the door.
Offline controllers in this manual refer to offline locks. These have no network interface, and the configuration of these locks is carried out on-site by a programmer or by corresponding data carriers or depending on type, via radio frequency. The configuration of both online and offline terminals is done in Matrix in the same manner.

Door
The term door is used in this manual to refer to a controlled access point. This is usually a door that controls access to a restricted area. Alternative examples of doors include a roller door, or an access barrier being controlled and monitored. The principle of access control, i.e., the configuration process in GAT ACE, is identical, however.
It should be noted that a door does not have to be equated with a controller, since a controller can, e.g., also control several doors depending on the type.
At some points in this manual, the term "door" is used to refer to a "controller" or "lock". The term door then usually designates the controller installed near the door or lock.

Read/write function (CardNET)
This term refers to an operating mode for offline controllers. It is important here to distinguish between CardNET G1 and CardNET G2.
In this mode, Matrix sends the authorization data of the persons for offline doors (locks) via GAT ACE to certain online controllers in the access control system. The data carriers of the persons can then be programmed directly at those controllers. The controller must support the read/write (CardNET function) functionality.
Matrix supports two generations of CardNET. CardNET G1 supports LEGIC prime and LEGIC advant data carriers and can store max. 10 doors and 30 door groups on the data carrier. This memory capacity is fixed and cannot be changed.
CardNET G2 is the evolution of CardNET G1 and supports LEGIC advant data carriers. CardNET G2 is also applicable for systems with flexible memory requirements since the memory capacity to be used can be individually adapted to the data carriers.
CardNET G2 is supported by the GAT DL 32x and GAT DL 34x offline controllers, the GAT SR 73xx and GAT SLR 73xx readers, the GAT DC 7200 door controller, the GAT ST 38x/39x EVO PoE time recording terminals, and the GL7p and GAT ECO.Lock 7xxx locker locks in CardNET mode. Older devices with the FLEX protocol (e.g., GAT Terminal 3100, 3000, 2500, GAT SR 3xx and GAT SLR 3xx, and the GAT ST 38x/39x) only support CardNET G1.

SALTO Virtual Network (SVN) and GANTNER SVN
SALTO Virtual Network for GANTNER coded data carriers. This function is comparable to the CardNET function. The authorization data is written to data carriers thereby authorizing the data carriers for SALTO products. With the latest Matrix and GAT ACE 7000 software versions as well as the latest firmware for the GAT DC 7200 controllers, the GANTNER SVN data can also be written and read via GANTNER readers, meaning that a data carrier can be used seamlessly in a system with GANTNER and SALTO products.
For the necessary settings and requirements, please read chapter "Appendix C: SALTO ProAccess SPACE Integration".

Time Plan
A time plan is used to define the type of access authorization of a person or the functionality of a controller. The daily schedules for weekdays and special days (max. 5 special days in GAT ACE 3000, max. 10 special days in GAT ACE 7000, max. 3 partitions in ProAccess SPACE) are defined in a time plan. Time plans defined for persons are called "personnel time plans" and time plans defined for terminals are called "door time plans".

Personnel Time Plan
A personnel time plan is a definition of the access authorizations (entrance or exit, with or without PIN and fingerprint, normal or special relay plan) of a person during certain time intervals. Personnel time plans can be assigned directly to a single person or to groups of persons at once.

Door Time Plan
A door time plan can be assigned to a controller to determine the functionality that shall be active during certain time intervals of a day. With a door time plan it is possible to unlock a door generally for a certain time period, to activate the office function, to check only the company ID of data carriers, to activate a special relay plan or to suppress certain alarms.

Day Plan
A day plan defines the functions of a controller (for door time plans) or the access authorizations of a person (for personnel time plans) for one day. A day plan can have up to 10 different time intervals with different settings. In a personnel or door time plan day plans are assigned to the weekdays and up to 10 special days in order to define the complete personnel authorization or controller functionality.

Time Interval
A time interval is a period of time with selectable start and end time during which certain controller functions or certain access authorizations of a person are active. Up to 10 time intervals can be assigned to one day plan.

Corporate Calendar
The corporate calendar is used to assign the special days (e.g., public holidays) to the corresponding days of a year. On these special days, the corresponding day plan for that special day is used for access control. The multi-site policy allows you to use a separate corporate calendar for each location.

Special Days
Special days, such as holidays, general public holidays, reconstruction, etc., can be defined in the organization time plan. This is used to activate another day plan (the plan defined for that special day), independently from the current weekday. Special days can either be at a fixed date or automatically calculated by the application every year, e.g., by using the Easter rule of Carl Friedrich Gauss. Note that offline locks and WiNET locks support max. 5 special day types, for online controllers in GAT ACE 7000 up to 10 special day types can be used, and in ProAccess SPACE 3 special days are supported.

Special Rights
Various special right functions can be assigned to each person at the doors, provided the controller that controls the door is also configured for the special rights function. It should be noted that different special rights are only supported by GAT ACE 7000. GAT ACE 3000 only supports a general special right.
The following special rights are supported by GAT ACE 7000:

- Office function special rights:
  With the office function activated, a door can be permanently unlocked after valid identification and locked again after further identification.
  NOTE: In the GAT DC 7200 the function must be configured as well.
- Alarm system: The alarm system can be activated or deactivated.
- Verify: The schedule can be overridden so that a PIN code is used for access instead of fingerprint verification.
- Anti-pass-back lock: The anti-pass-back lock can be deactivated and violations displayed.
- Pool management lock: The pool management lock can be switched to inactive and violations can be displayed.
- Double booking block: The double-booking block can be deactivated and violations displayed.
- Special relay: An additional relay output can be defined that is controlled by the special right.

For persons with special right(s), the corresponding special right is activated at the controller in addition to the normal access control. Special rights can thereby be implemented for individual persons.

Relay plan
For certain controller types, so-called Relay Expanders can be connected. These are peripheral devices with eight, 16 or max. 32 relays, which can be activated with a valid identification at the controller in addition to the normal unlocking operation. This makes it possible to realize applications such as e.g., lift controls where certain additional floors can be released after a valid authorization at the controller. A relay plan clearly defines which relays of the relay expander should be activated. Through the assignment of the relay plans to controllers and people, the behavior of the controllers can be configured for each person. There are two types of relay plans - "Normal relay plans" and "Special relay plans". A person can have a normal as well as a special relay plan assigned for each controller. Which relay of the two relay plans are used at certain times can be determined in the personnel time plan and door time plan.

Blocklist
Data carriers can be entered into the blocklist to prevent them from being used with offline doors in the access control system. This allows you to, e.g., place a lost data carrier on the blocklist to temporarily block access at offline doors.

Bookings
Each event (e.g., identification of a person, alarm messages, power failures, etc.) that occurs at a controller generates a booking that is stored in the internal memory of the corresponding controller. These bookings can be read out with GAT ACE and transferred to Matrix. The booking texts can be displayed in two languages.

GAT ACE 3000 / GAT ACE 7000
The GAT ACE 3000 and GAT ACE 7000 software applications are used to configure the access system. Here, the controllers and readers of the system are configured with GAT ACE managing the further communication between Matrix and the devices.
GAT ACE 3000 supports GANTNER's previous generations of controllers and readers (e.g., GAT Terminal 3100) and GAT ACE 7000 is used for the newest generation of these devices (e.g., GAT DC 7200).

Lockers / Locker locks
The general terms refer to GANTNER's electronic locker locks. For use in Matrix, GANTNER's Relaxx locker management software is required, which is used to communicate with the locker locks and serves as an interface to Matrix. All locker locks that are available for use in Relaxx can be displayed and controlled.

SALTO ProAccess SPACE
Software for the configuration and management of access controllers and locks from SALTO. These locks or doors can be imported into Matrix (from version 5.0). Separate documentation is available for the ProAccess SPACE software. Information about the settings for ProAccess SPACE can be found in "Appendix C: SALTO ProAccess SPACE Integration".
In this manual, this software solution is also abbreviated as ProAccess SPACE or just SPACE.
Note the following limitations:
By combining Matrix and ProAccess SPACE, the strengths of both systems can be combined. However, there are also some limitations that must be considered when planning and configuring a system:

- The combination of the systems is only possible if both systems use a DESFire data carrier or if a combination data carrier is used on which a DESFire data carrier with corresponding coding for SALTO is present.
- When using GANTNER SVN technology, authorizations for SALTO products can be updated using all online readers. When the original SALTO-coded data carriers are used, this is only possible using SALTO readers.
- Mobile identification via SALTO Justin is not possible.
- GAT Mobile Access Management only operates with GANTNER products.
- Both systems offer the possibility of anti-pass back control or pool management. These functions can only be used within the respective system, but not across both systems.

3. INSTALLATION

3.1 Hardware specifications

Matrix includes and requires several components. The installation can be done in different ways and can be distributed across several PCs/servers.

3.1.1 Configuration example 1 (only GAT ACE and Matrix for smaller systems)

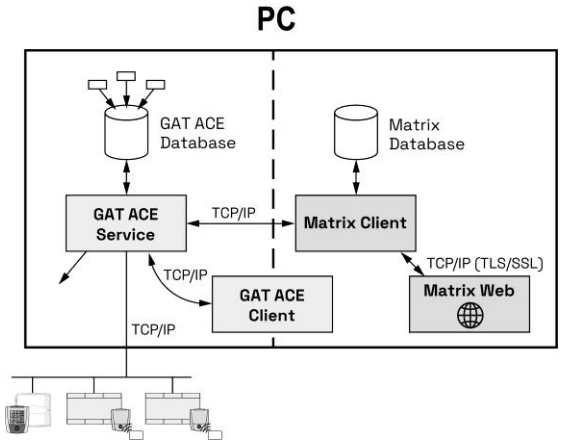


Figure 3.1 *- Matrix and GAT ACE 3000 or 7000 installation on same PC*

3.1.2 Configuration example 2 (including larger systems with Relaxx installation)

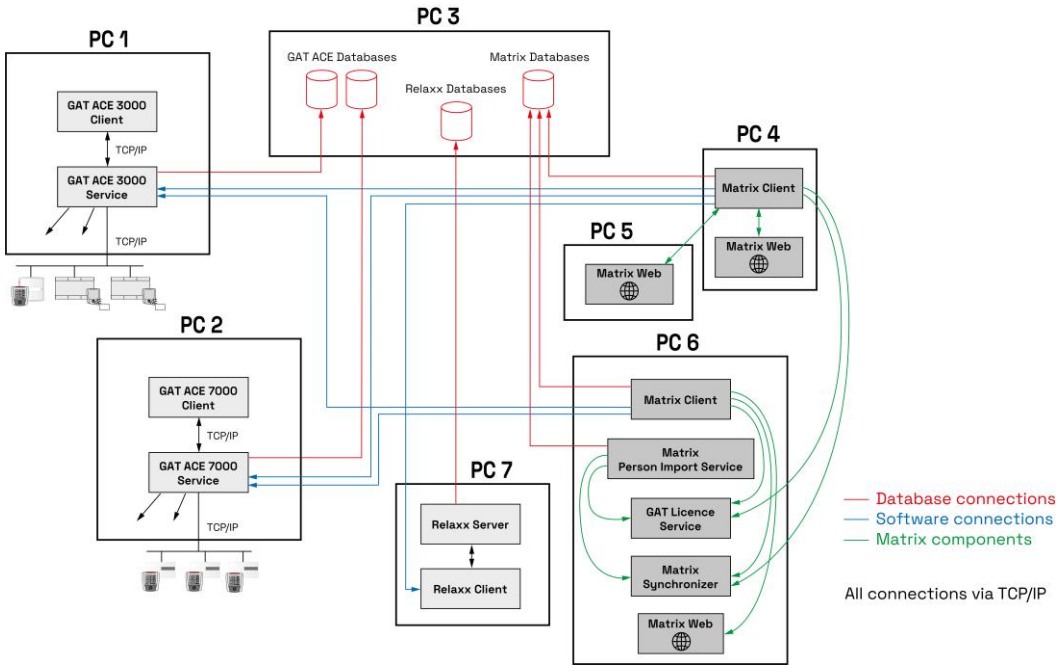


Figure 3.2 *– Matrix and GAT ACE 3000/7000 installation on different PCs, Matrix, and GAT ACE databases on own PC*

3.1.3 Configuration example 3 (including SALTO ProAccess Space)

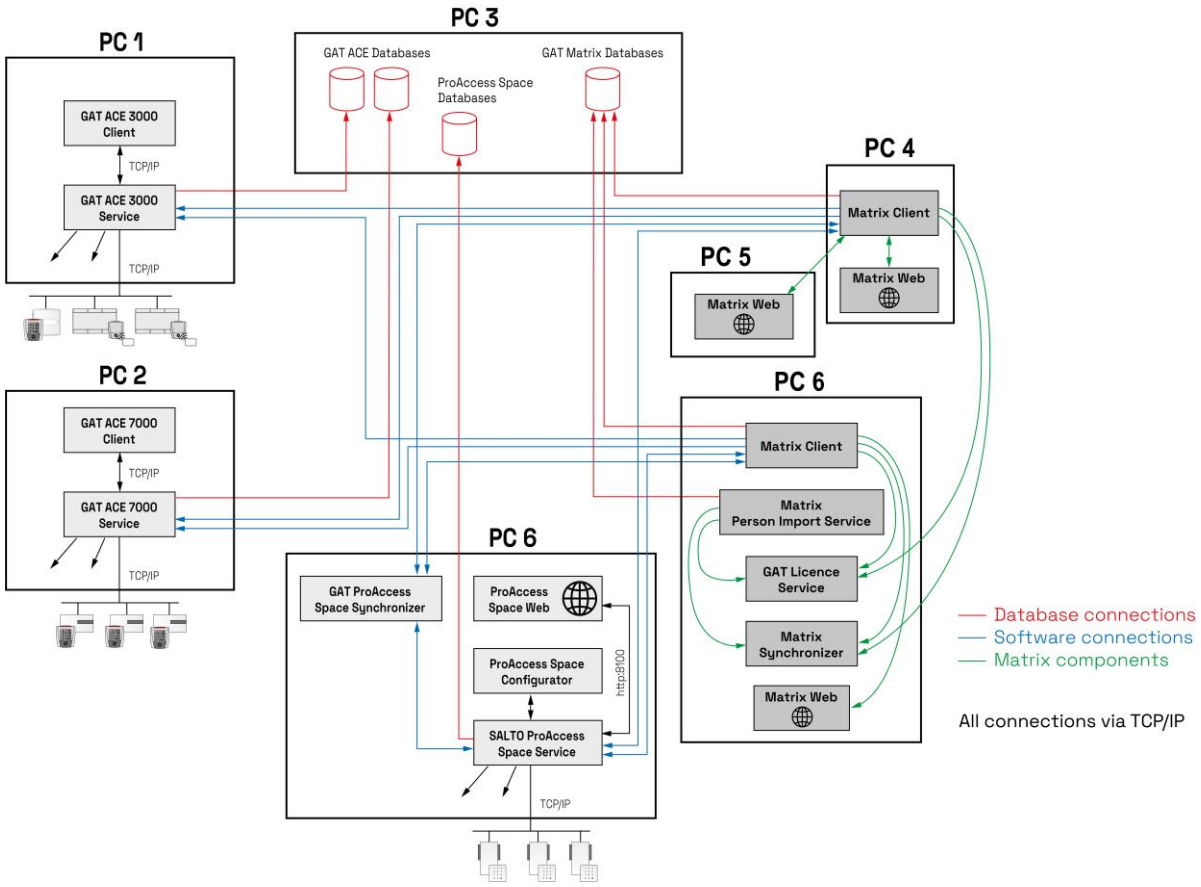


Figure 3.3 – *Installation of Matrix, GAT ACE 3000 / 7000 and ProAccess Space from Salto on different PCs. PCs, databases on own PC*

Recommended hardware requirements for the PCs:

- IBM-compatible PC, e.g., Core i5, 3 GHz or comparable CPU
- Network card (TCP/IP), 2 GBit
- PC interfaces: Ethernet (TCP/IP) and USB
- Internet access for updates
- Color monitor (HD 1920 x 1080 resolution recommended)
- Internet browser (see "3.2. Software requirements")

Additional minimum requirements for the software components:

Matrix Client Installation
- Free hard disk memory: 10 GB
- Free RAM: 2 GB

Matrix Synchronizer
- Free hard disk memory: 1 GB
- Free RAM: 1 GB

Matrix Import Service
- Free hard disk memory: 10 GB
- Free RAM: 1 GB

Microsoft SQL Server Express

- Free hard disk memory: 20 GB
- Free RAM: Recommendation 3 GB since an SQL server usually contains several databases (e.g., GAT ACE 3000, 7000, 7000 APB, eLoxx Relaxx, Matrix, etc.), additional RAM is required for the SQL server depending on the system size and automatic data backup function. This must be checked for each system.
- ***Note:*** Please note the limitations of the Express versions, such as a maximum of 1 GB of RAM, a maximum of 1 processor, and a maximum of 10 GB of database size.

GAT ACE 3000 / 7000 Service

- Free hard disk memory: 20 GB
- Free RAM: 1 GB

GAT ACE 3000 / 7000 Client

- Free hard disk memory: 2 GB
- Free RAM: 0.5 GB

GAT License Service

- Free hard disk memory: 1 GB
- Free RAM: 0.5 GB

Relaxx 2022 (also see the Relaxx 2022 system manual)

- Free hard disk memory: >30 GB (program data, database, protocol, backups for common system sizes)
- Free RAM: 4 GB

GAT ProAccess Space Synchronizer

- Free hard disk memory: 1 GB
- Free RAM: 0.5 GB

SALTO ProAccess Space (see also ProAccess Space system manual)

- Free hard disk memory: >30 GB (program data, database, protocol, backups for common system sizes)
- Free RAM: 4 GB

These additional minimum requirements for a PC are calculated depending on how many of these components are installed on the same PC. For the configuration example 2 (see “Figure 3.**2**”), this is:

- PC 1: GAT ACE Client + GAT ACE Service = 22 GB hard drive space and 1.5 GB RAM
- PC 2: GAT ACE Client + GAT ACE Service = 22 GB hard drive space and 1.5 GB RAM
- PC 3: 2 x Matrix databases (SQL Express) = 40 GB hard drive space and 4 GB RAM
- PC 4: Matrix Client and web browser for Matrix Web = 10 GB hard drive space and 1 GB RAM
- PC 5: Web browser for Matrix Web = approx. 1 GB hard disk storage and 0.5 GByte RAM
- PC 6: Matrix Client + Matrix Import Service + Matrix Synchronizer + GAT License Service = 22 GB hard drive space and 3.5 GB RAM
- PC 7: Relaxx = 30 GB hard disk space and 4 GB RAM

NOTE! Adhere to the additional system requirements of the database in use (see "3.2.2. Database server").

3.2 Software requirements

The Matrix software solution consists of various components and requires a database server with a database, as well as several software packages. The necessary components are included in the Matrix setup.

The software requirements and software packages are described below.

3.2.1 Supported operating systems

- Microsoft Windows® 10 (Pro, Enterprise) 64-bit (ends October 2025)
- Microsoft Windows® 11 (Pro, Enterprise) 64-bit
- Microsoft Windows Server® 2016 (Essential, Standard, Datacenter), 64-bit
- Microsoft Windows Server® 2019 (Essential, Standard, Datacenter), 64-bit
- Microsoft Windows Server® 2022 (Essential, Standard, Datacenter), 64-bit
- Microsoft Windows Server® 2025 (Essential, Standard, Datacenter), 64-bit

The Server Core installation option of Windows Server® 2016 is not supported by Matrix. In addition, RT, Starter, Home, Small Business, and Web Editions are not supported.

NOTE! Please note that GANTNER Electronic GmbH can only provide technical support when Matrix and GAT ACE are installed on a German or English version of Windows.

NOTE! In addition to the Matrix and GAT ACE solutions, the customer must provide all additional licenses required, e.g., for the operating system or database.

3.2.2 Database server

Matrix requires a database server, in which the Matrix database is stored. The following database servers are supported by Matrix.

Supported databases:
- Microsoft® SQL Server® 2016
- Microsoft® SQL Server® 2017
- Microsoft® SQL Server® 2019
- Microsoft® SQL Server® 2022

Express versions are also supported.

No database is supplied with Matrix. If desired, you can download the Microsoft® SQL Server® 2019 Express database from the GANTNER partner page.

NOTE! Also adhere to the system requirements of the database in use. The current system requirements for Microsoft® SQL Server® Express can be found via the following link:
https://technet.microsoft.com/en-en/library/ms143506.aspx

NOTE! It is recommended to also install Microsoft SQL Server Management Studio Express. This can be downloaded from the Microsoft website.

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

NOTE! 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.

3.2.3 Microsoft .NET

The .NET 8.0 Desktop Runtime is required for the operation of Matrix. This is included in the installation package.

If the necessary .NET version is not yet installed, Matrix will prompt you for this when you start the setup wizard and ask if you want to start the Microsoft .NET installation. If you confirm, .NET 8.0 will be installed automatically.

3.2.4 Additional software requirements

- When using GAT License Servers, Version 1.1.0 or later must be used for this software.
- When using a GAT Writer read/write device, Version 2.08.28 of the GAT USB drivers must be installed for this device.
- When using a GAT FR 010 fingerprint reader, min. version 4.5.0 of the USB driver must be installed as of Matrix 5.0.
- When multiple versions of Matrix are in operation, Matrix Synchronizer must be used.
- When using eLoxx Relaxx, please note the detailed system requirements in the Relaxx manual.
- For eLoxx Relaxx, the option "Use ASCII command encoding" must be enabled (see "5.19. Locker control").
- When using SALTO ProAccess SPACE, please adhere to the system requirements in the respective documentation.

The following software and firmware versions are required to use all functions of Matrix Version 7.1.0:

- GAT ACE 7000 APB: 2.0.3
- GAT ACE 7000: V 2.2.2
- GAT ACE 3000: V 3.1.16
- GAT Mobile Access Management: V 1.7.0
- GAT License Server: V 1.1.1
- Matrix Export: V 1.7.2
- eLoxx Relaxx: V 8.0.0 Enterprise
- GT7 Room Sign & Access App: V 1.0
- SALTO ProAccess SPACE: V 6.10.4.3
- SALTO NCoder: V 01.12
- GAT SyncManager V 3.3.1
- GAT SR 73xx: V 3.5.0
- GAT SR 7000 Wiegand: V 1.2.0
- GR7: V 3.5.0
- GAT DC 7200: V 3.6.0
- GAT DL 3xx: V 4.9.0
- GAT DL 092: V 4.3.0
- GAT DL Analyzer: V 2.5.0
- GDL7p.x3xx CardNET: V 1.3.0
- GDL7m: V 1.2.0

- GAT ECO.Side Lock 7000 BA CardNET: V 2.3.0
- GAT ECO.Lock 7100 BA CardNET: V 1.1.0
- GAT IO 7054/7055: V 1.1.0

The following versions can be used; however, functional restrictions apply in Matrix Version 7.1.0:

- Matrix: V 4.5.5
- GAT Mobile Access Management: V 1.6.0
- GAT ACE 7000 APB: V 1.0.2
- GAT SR 73xx: V 3.3.0
- GAT DC 7200: V 3.5.0

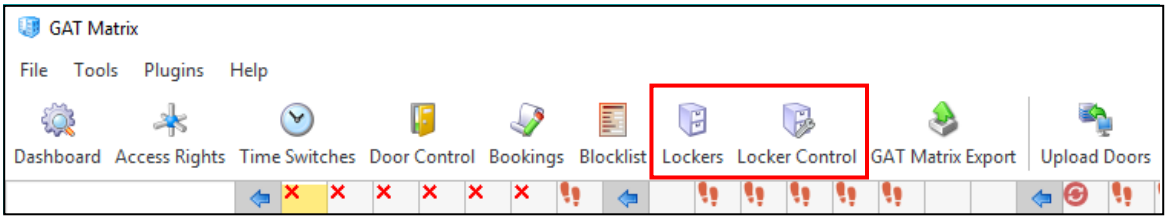
3.3 Relaxx (locker locking systems)

The Relaxx software offers you the possibility to configure, control, and monitor the status of the electronic GANTNER locker locks for locker rooms as well as the access and information terminals from GANTNER. Relaxx is installed on a computer with a Microsoft Windows® operating system (see the Relaxx Installation manual).

Relaxx consists of a Windows® service that runs in the background to provide communication with the locker system, and a user interface that is used to configure and control the locker system and online devices, and to display the statuses are of the lockers.

Matrix can establish a connection to Relaxx. It is then possible to display the lockers created in Relaxx in Matrix and to manage the authorizations here.

To integrate Relaxx into Matrix, no additional license is required for Matrix. However, it must be noted for the Relaxx version that an Enterprise license is required.



3.4 SALTO ProAccess SPACE (SALTO access control)

SALTO ProAccess SPACE is a software solution used to configure and control SALTO online and offline door locks.

Included in Matrix is an interface to SALTO ProAccess SPACE that enables the installation of access control systems with GANTNER and SALTO products. In these systems, the management of persons and access authorizations, the evaluation of events, and the monitoring and remote control of doors are performed via the Matrix user interface. In such systems, ProAccess SPACE is responsible for the communication to SALTO devices and thus functions in a similar way to GAT ACE 7000 or GAT ACE 3000 with GANTNER products.

In order to establish a connection between Matrix and ProAccess SPACE, min. Matrix version 5.0 must be used. In addition, the SALTO ProAccess SPACE synchronizer must be enabled, which is done via the "ProAccess Space Synchronization" option in the "Settings" menu (see "5.5 Importing doors and locations from SALTO ProAccess SPACE").

To integrate SALTO ProAccess SPACE with Matrix, no additional Matrix license is required. In ProAccess SPACE, certain functions must be enabled and can be used (see "10.5 Licensing for SALTO doors").

If the ProAccess SPACE is used, the mobile app JustIN can also be used. This allows users' access authorizations configured in Matrix to be saved on their mobile devices (e.g. smartphones). For access control, users can then use their mobile device (with JustIN app) instead of an RFID data carrier to identify themselves at a terminal.

3.4.1 Restrictions for the integration of SALTO devices

Note the following restrictions for the combined use of SALTO and GANTNER products in Matrix.

- The combination of GANTNER and SALTO systems is only possible if both systems use a MIFARE DESFire data carrier, or if a combination data carrier is used on which a MIFARE DESFire data carrier with corresponding coding is available for the SALTO system.
- When using GANTNER SVN technology, authorizations for SALTO products can be updated using all GANTNER online readers. When using the original SALTO-coded data carriers, this is only possible using SALTO online readers.
- Mobile identification via SALTO Justin is only possible with SALTO products.
- GAT Mobile Access Management only operates with GANTNER products.
- Both systems offer the possibility of anti-pass back control or pool management. These functions can only be used within the respective system, but not across both systems.

Further developments at GANTNER and SALTO aim at reducing the necessary restrictions. If this is interesting or important for you, please read the documentation of the respective versions or speak to your GANTNER representitative.

3.5 General information on Matrix communication

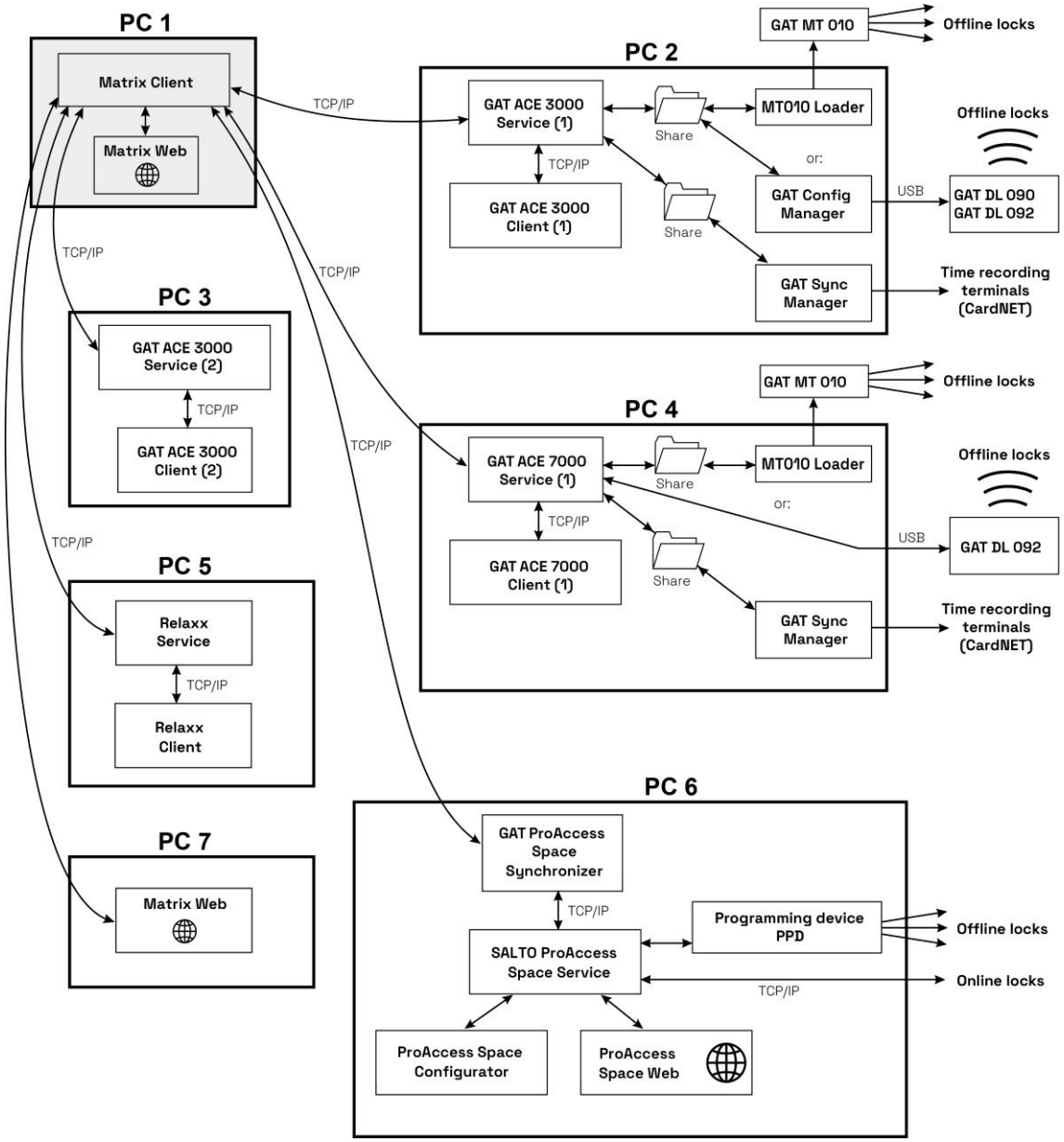


***Figure 3.4** - Communication with a Matrix and GAT ACE 3000 and/or GAT ACE 7000 system and ProAccess SPACE*

3.5.1 Communication with GAT ACE

All communication between Matrix and GANTNER controllers and door locks (online and offline) is handled by GAT ACE 7000 and/or GAT ACE 3000 software. Matrix can operate with multiple GAT ACE installations thereby allowing Matrix to access all the connected controllers. GAT ACE 3000 supports controllers prior to Generation 7 (e.g., GAT Terminal 3100) and GAT ACE 7000 supports controllers from Generation 7 onwards (e.g., GAT DC 7200).

The function of GAT ACE 7000 and 3000 is the same. Both contain a GAT ACE service (= Windows Service), which operates in the background, and a GAT ACE client (user interface). The service is responsible for all communication and operates regardless whether the user interface is running or not. In most cases, GAT ACE (service and client) is installed on the same computer with Matrix running either on the same computer or on a separate computer. The structure of the Matrix - GAT ACE system is shown in Figure 3.4.

To transfer bookings and authorization data to offline doors, the GAT MT010 Loader can be used for GAT ACE 3000 and GAT ACE 7000, the GAT DL 092 wireless modules can be used. However, it is recommended to create the offline doors in GAT ACE 7000 as GAT ACE 7000 can transfer the CardNET data to GAT ACE 7000 and to the GAT ACE 3000 controllers.

GAT ACE 7000 or GAT ACE 3000 transmit CardNET data to the time acquisition terminals via a shared directory. The software GAT Sync Manager checks the directory and transmits the data to the terminals.

3.5.2 Communication with ProAccess Space

The ProAccess Space software is used for communication between Matrix and SALTO controllers or door locks (online and offline). The principle of operation of ProAccess Space is similar to the GAT ACE software (see Figure 3.4). ProAccess Space consists of a Windows service (SALTO ProAccess Space Service) running in the background and the graphical user interface used for configuration and operation by the user.

The GAT ProAccess Space Synchronizer is responsible for transferring lock information and authorization data between Matrix and ProAccess Space. This is a Windows service that runs even when the user interface of Matrix and ProAccess Space is closed. In most cases, this service and the ProAccess Space software are installed on the same computer as GAT ACE 7000 and/or GAT ACE 3000. Matrix can operate on multiple workstations. ProAccess SPACE is installed as a web solution on a server and can be used on different workstations if required. The structure of the Matrix - ProAccess Space system may then be similar to that shown in Figure 3.4.

The transfer of the configuration to offline doors (SVN) can be done with ProAccess SPACE using a programming unit (PPD). The GANTNER SVN authorization data can be written to the data carriers (only MIFARE DESFire) at online GANTNER readers.

3.6 Use cases and types of installation

3.6.1 Initial installation of Matrix

For new installations or for systems where the Matrix software has not been installed yet, Matrix can be installed via the installation package. While installing Matrix, you can select to also install other components that are required for Matrix (.NET 8.0, database for access rights, GAT ACE, etc.). An installation wizard guides you through the installation process.

Furthermore, different settings for the firewall and network connections as well as for the database must be defined. These settings must only be configured once.

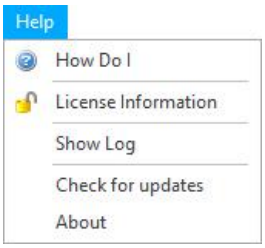
In addition, the system must also be defined in terms of hardware in GAT ACE and/or in ProAccess Space. This means that all doors or access controllers that are to be used in Matrix for the access organization must be created and configured in GAT ACE and/or in ProAccess Space. This applies to both the online and offline doors.

A detailed description of the initial installation of Matrix can be found in “Appendix B: Installation of Matrix".

3.6.2 Updating Matrix

If a new version of Matrix is available, you have the possibility to download and install the desired update from the GANTNER partner website.

Alternatively, you can also check for software updates manually in Matrix by clicking on “Check for updates” in the “Help” menu.

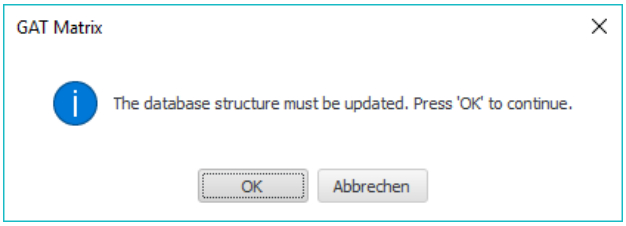


NOTE! Please note that updating Matrix to the latest version 7.x is only possible from an installed Matrix version 4.5.5 or later. For an update from version 3.4.x you must first update to version 4.5.5. After the database update, the update to version 7.x can be implemented.

NOTE! It is recommended to always backup all databases before completing an update (see "4.1. Database settings" for more information).

Please note the following points before an update:

- When upgrading the major version from version 2.x.x, 3.x.x or 4.x.x, 5.x.x to version 7.x.x, a new license is required.
- It is possible that additional packages or functions (e.g., timer function or door control as well as multi-client capability or LDAP integration) are added by the update. These cannot be used with the existing license. For their use, the corresponding extension license must be requested, and the corresponding software version must be installed.
- It may be necessary to update the database if new database fields are added by the update. In this case a corresponding message will be displayed at the first start of the Matrix after the installation.



The existing data is preserved by updating the database structure.

ATTENTION: Please note that as of Matrix V 7.0, GAT Manager is no longer supported!
If you are using Matrix 2.x.x and GAT Manager, you can upgrade GAT Manager to GAT ACE 3000 (see the GAT ACE user manual).

4. FIRST STARTUP OF MATRIX

The GAT ACE service and/or the SALTO ProAccess SPACE service must be started first. These Windows services are started automatically by default when Windows is started, but you can also configure them e.g., to "start delayed", i.e., that they are only started when enough resources are available on the PC. Please read the manuals of GAT ACE or ProAccess SPACE for further information.

GAT ACE or SALTO ProAccess SPACE can be installed on the same PC as Matrix but usually GAT ACE or SALTO ProAccess SPACE are installed on another server / PC in the network. Ensure that the installation server / PC is accessible via the network.

Double-click on the "Matrix" desktop icon or on the link available via the Windows® Start menu "Programs" -> "GANTNER Electronic GmbH" -> "Matrix", which is the default folder created during installation.

When Matrix starts for the first time, a message is displayed to inform you that the database settings must be configured correctly. Confirm the message with "OK" then define the database and network services (client connections) settings. These settings are described in the following chapters. After the settings are defined, the login window opens. The login process is described in section "4.6 Login".

4.1 Database settings

The settings for the database connection are found in the configuration window of the "Database" tab. This window is displayed upon first startup of Matrix, and it can be accessed at any time via the "Database Configuration" menu item in the "Tools" menu.

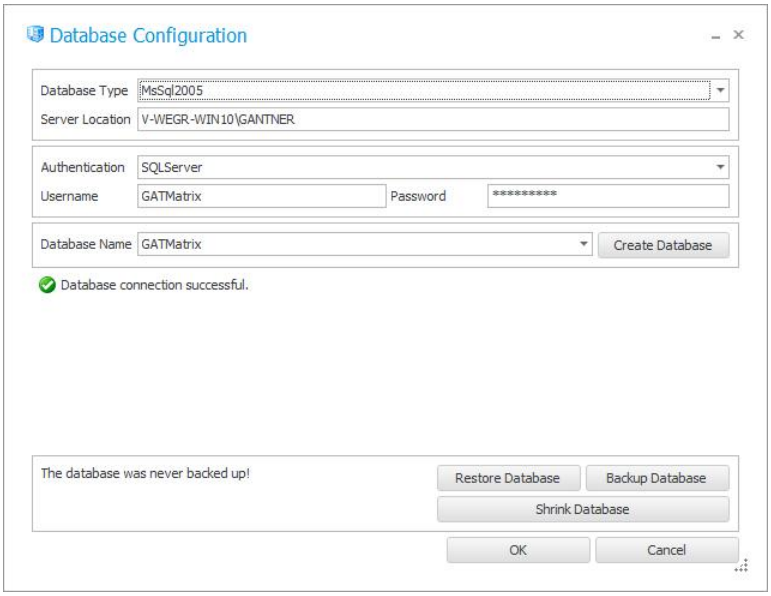


Figure 4.1 *- Database settings*

- Database Type: Select the type of database communication from the list. The default is “MsSql2005”, which is not synonymous with the installed database version.
- Server Location: Enter the network name or IP address of the server/PC where the database is located, followed by the instance name of the SQL server.
- Authentication: Select the type of authentication for the database ("SQLServer", "Windows"). Windows authentication will use the current Microsoft Windows user account to connect to MS SQL Server. The authentication type “SQLServer” allows you to specify a username + password combination to connect to the database.
  If you followed the steps described in "Appendix A: Installation of SQL Server", this is the place where you have to enter the password specified during the SQL Server Express installation. Set the authentication mode to “SQLServer” and use “sa” as a username.
- Username: If “Authentication” is set to “SQLServer”, enter a valid username to connect to the database.
- Password: If the “Authentication” is set to “SQLServer”, enter the password for the selected username.
- Database Name: A database server can manage several databases. Select the desired database that will be used for Matrix ("GATMatrixModule").
- Database Backup: This button allows you to make a backup copy of the database currently in use. This is a complete backup that includes all information used by the application. After clicking on this button, a window opens where you can enter the path where the backup file will be stored. Further information about database backup is available in "Appendix E: Database Backup".
- Database Restore: This button allows you to restore a previously saved backup of the database. Note that when restoring a backup, the current data in Matrix is overwritten.
  NOTE! This process is only possible for a database user with sufficient rights (e.g., "sa").
- Shrink Database: This button allows you to compress the Matrix database thereby releasing more storage space. This means that e.g., if the activity journal will be deleted, the used storage space remains constant.

If a Matrix database does not currently exist, click on the “Create Database” button to create a new database (**Note:** This is only possible if the current user has the SQL rights to create a database). Matrix creates a new username/password that is used afterwards by Matrix to connect to the database. Write down these login details for future use and keep them in a safe place. This information is also required for a Matrix client installation.

After entering all information correctly, the status line in the window displays the following message.



Press "OK" to confirm. A window is shown asking the user if the database should be created now. Press "OK" to confirm.

NOTE! Saving the database is intended for backup use. If you change the database server and want to override the existing database, you have to perform further steps. More information about this process is available on the MSDN homepage via the following link:
http://msdn.microsoft.com/en-gb/library/ms190209.aspx

4.2 Database cleanup

With the "Database Cleanup" menu item in the "Tools" menu, you have the option to automatically clean up the database at regular intervals, i.e., delete old bookings and log entries (see "7 BOOKINGS" and “8 ACTIVITY JOURNAL”). You can configure when the cleanup should occur, and which bookings and entries should be deleted.

NOTE!

- To use this function, the Matrix Import Service must be installed.
- If using the database cleanup function, the same configuration should also be configured on all GAT ACE clients with the same cleanup times.

► Select the "Database Cleanup" option in the "Tools" menu.

○ The "Database Cleanup Configuration" window opens.

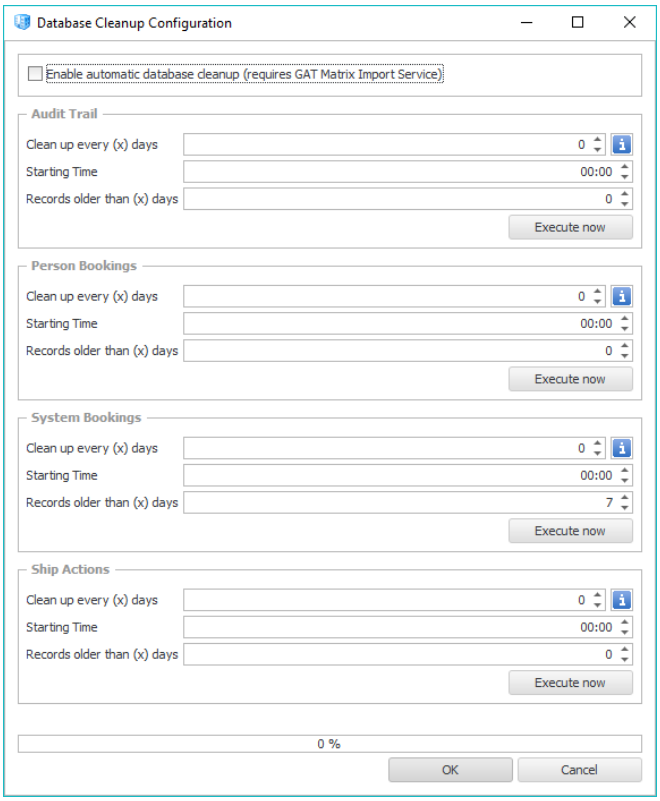


Figure 4.2 - *Settings of the database cleanup*

► Select the first option box in this window to enable the database cleanup function.

► Enter a value greater than "0" in the "Clean up every (x) days" field for the desired cleanup type. The cleanup is then executed at the interval in days entered here. A "0" in this field means that the cleanup for that type is disabled. The following types are possible:

- Audit Trail: Records all activity in Matrix. This includes the logging in/out of users, the creation of schedules or calendars, the changing of settings, or the assigning of schedules in the authorization matrix (see "8 ACTIVITY JOURNAL").
- Person Bookings: These include the identifications of persons recorded by the door controllers (e.g., entry, exit, access attempt, etc.). These bookings are displayed in the bookings overview (see "7 BOOKINGS").

- System Bookings: System bookings include person-independent events recorded by the door controllers (e.g., power interruptions, time setting) and also actions via Matrix during door control (e.g., opening or blocking doors via Matrix). These bookings are displayed in the bookings overview (see "7 BOOKINGS").
- Ship Actions: This function is used in conjunction with the ProAccess SPACE software. Ship is the interface to ProAccess SPACE via which Matrix sends commands to ProAccess SPACE. The Ship commands are automatically created by Matrix and stored in the database. The SPACE Synchronizer service processes the commands and then sets their status to finished. When the Ship actions are cleaned up, the completed commands are deleted from the database.

► In the "Starting Time" field, you can select the time when the cleanup should be performed.

► In the "Records older than (x) days" field, enter the date before which the records should be deleted. Records that are newer than the value entered here will not be deleted.

► You can also perform the desired cleanup manually using the "Execute now" buttons. In this case, only the value in the "Records older than (x) days" field is considered.

4.3 TLS certificate configuration

The communication between Matrix and GAT ACE 7000 and between Matrix, Relaxx, and ProAccess SPACE can optionally be encrypted using the TLS protocol. A certificate provided by the customer can be used for this, or a self-signed certificate can be generated.

For information on activating TLS encryption in Relaxx and GAT ACE, please read the instructions in the respective manuals.

If encrypted communication via TLS is activated for Relaxx and/or GAT ACE, the "Certificate" window is displayed after starting Matrix. Here, you can generate and install the TLS certificate that Matrix will operate with.

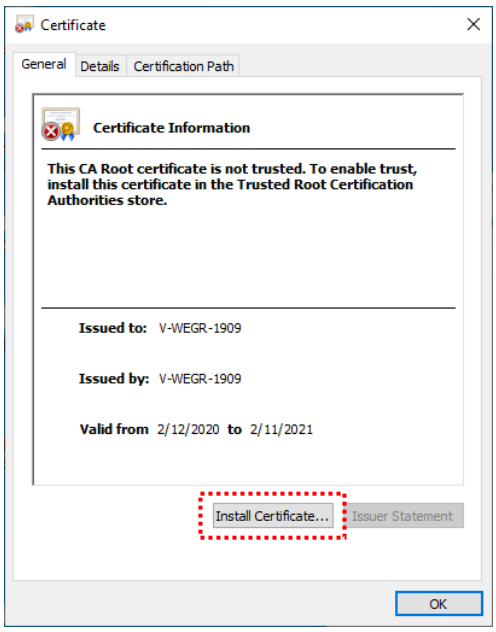


Figure 4.3 – *"Certificate" window*

► Click "Install Certificate".

  ○ The “Certificate Import Assistant” opens.

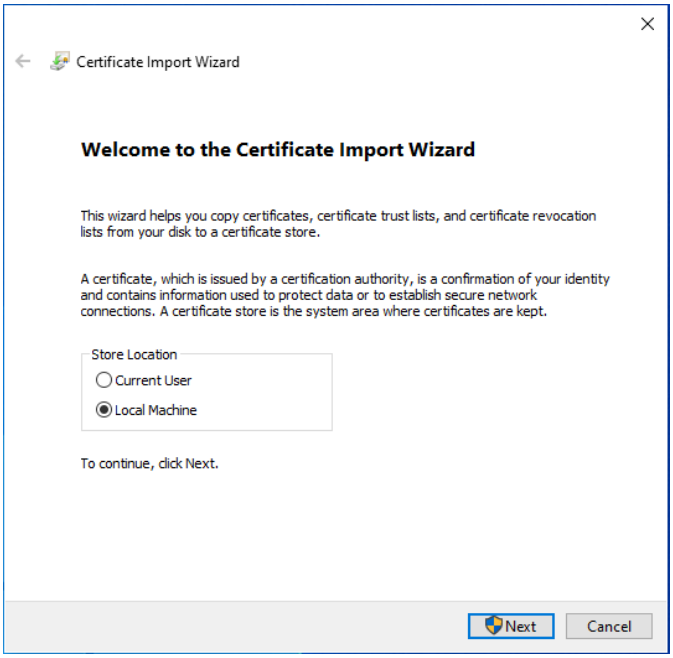


***Figure 4.4** – “Certificate Import Assistant” – Step 1*

► Select here “Local Machine”, and then click “Next”.

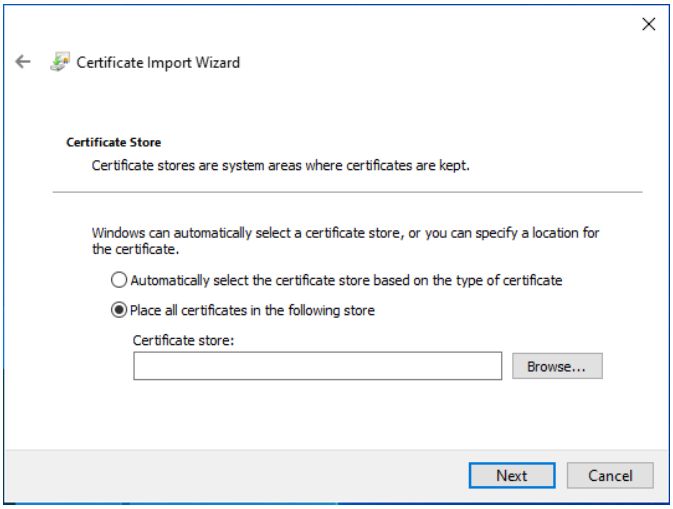


***Figure 4.5** – “Certificate Import Assistant” – Step 2*

► Select “Place all certificates in the following store” and then click “Browse…”.

► In the “Select Certificate Store” window, select “Trusted Root Certification Authorities” and then click “OK”.



Figure 4.6 *– "Certificate Import Assistant" – Step 3*

► Finally, click on "Finish" and then accept the security warning in the following window by clicking on "Next".

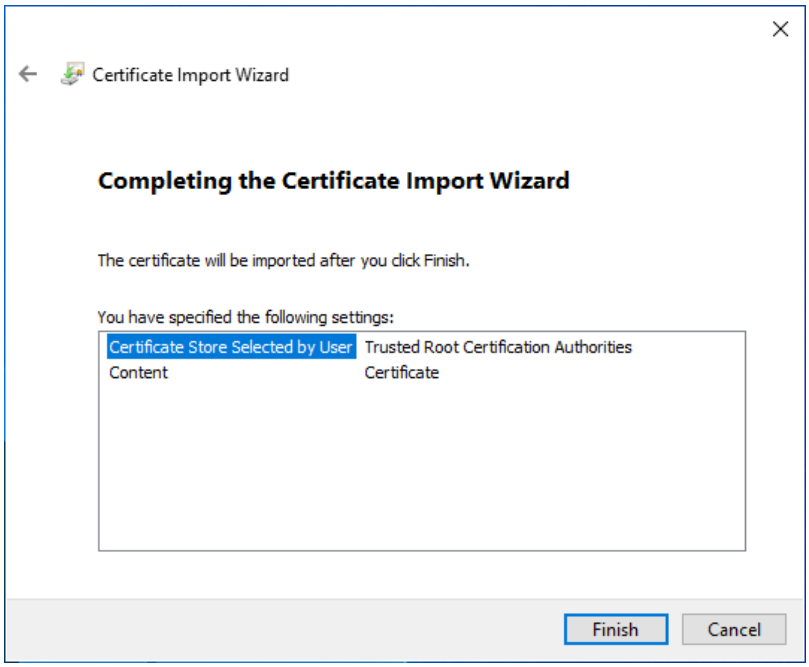


Figure 4.7 *– "Certificate Import Assistant" – Step 4*

NOTE: The certificate must be installed on all workstations where Matrix is used.

4.4 Settings of the network services (clients)

The GAT ACE 3000/7000 Client, GAT Licensing Client, and Matrix Synchronizer, GAT Relaxx Interface, and TBS RemoteSync network services enable certain functions for Matrix.

► To configure the connection for these network services, select "Options" from the "Tools" menu.

► The following window opens where you can open the "Network" tab.

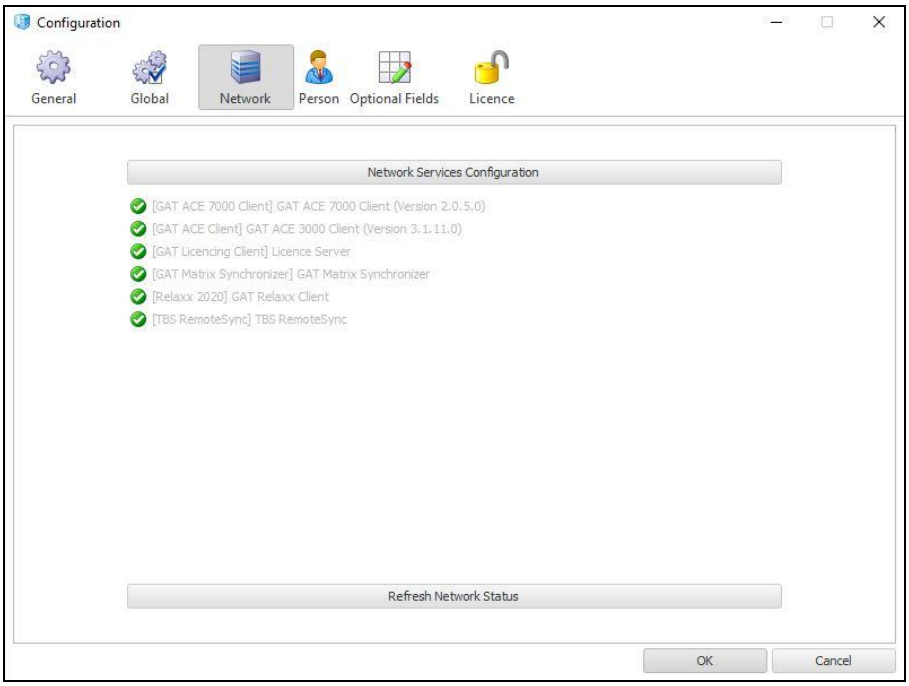


Figure 4.8 *- Settings of the network services (clients)*

The network settings for SALTO ProAccess Space can be found in a separate window (see "5.18.3 Loading online doors from SALTO").

You can see whether the connection to the respective service is active (in the example above, three connections are active and the connection to the GAT Licensing Client inactive). If any connections are inactive, you can click on the "Refresh Network Status" button to query the network and refresh the information. If a connection error remains, you will see a possible solution to the error below the corresponding error message.

Active connections are displayed with a green tick symbol and inactive connections with a red minus symbol.

Click on the button "Network Services Configuration". The window "Interface configuration" opens in which the connection settings of the service will be set. These will be described in the following sections.

4.4.1 License server (Licensing Client Interface)

Matrix allows licenses to be stored centrally on a license server. This is achieved using the Matrix Web Service, which can be installed using the Matrix installation package. To configure the license server, click on the "Licensing Client Interface" tab. The following window is displayed.

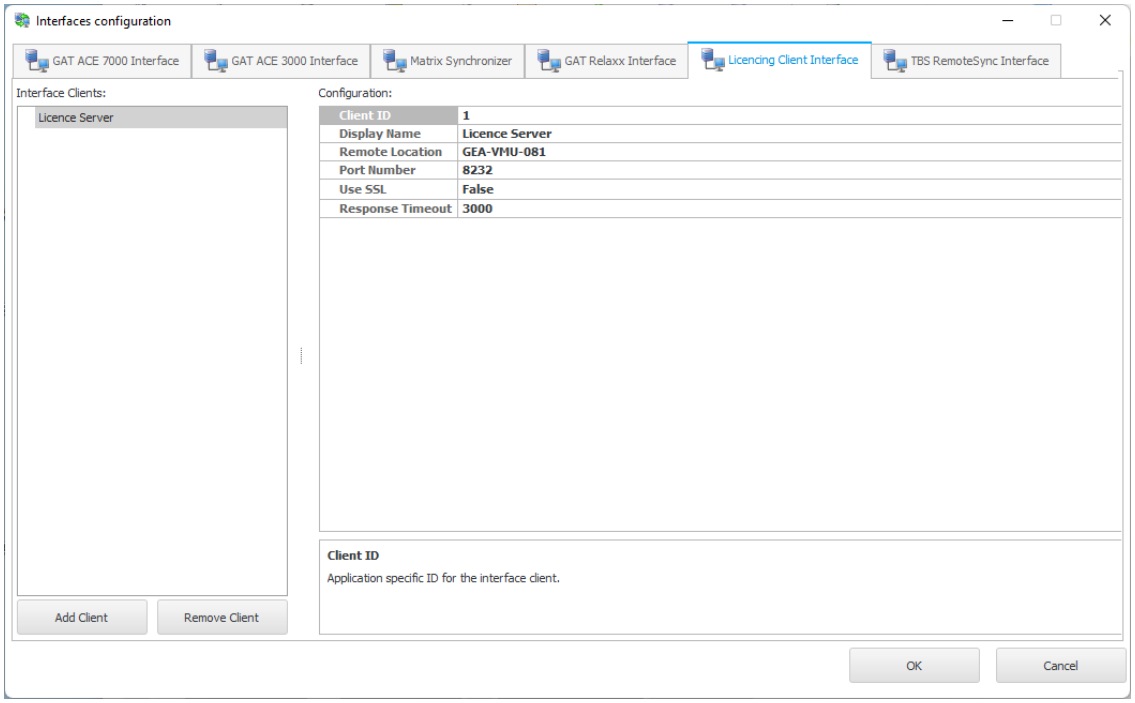


Figure 4.9 *- License server settings*

In the "Interface Clients" field, the license server is displayed. Use the buttons below the field to delete an existing license server or to add a new license server.

NOTE! Only one license server can be specified.

Should problems arise when trying to communicate with the license server, please check that TCP/IP port 8232 is open (especially when using a firewall). This is the standard port used for communicating with the license server.

The settings for the license server are defined in the right "Configuration" field. The following settings must be configured for the license server:

- Client ID: With this ID-Number, each client will be identified. This number must be unique for all clients. Since only one license server can be used, enter here 1.
- Display Name: Any name for the selected server (client). This name is only for the display of the server in the status window of the Matrix.
- Remote Location: Name or IP address of the license server.

- Port Number: Number of the port which will be used for the connection of the server. The port has to correspond with the port which was set for the GAT Manager Server. The standard value for the port is 8232.

  To test whether a connection to the entered port can be established, enter the command "`telnet hostname port`" into a Windows® console. Open the Windows console by pressing the "Windows" key + "R", then type "cmd" and press "OK".

- Use SSL: With this option, encrypted communication via TLS can be enabled for the license server. If this is enabled on the license server, set this option to "True" in Matrix as well. Otherwise select "False".

- Response Timeout: Define a waiting time in milliseconds for a response to a sent command. As the retrieval of booking data can take some time, a value of 10000 (= 10 seconds) should be entered here.

4.4.2 GAT ACE client interface

To enable communication with the GAT ACE installation(s), certain settings must be configured for each GAT ACE. Click on the "GAT ACE Interface" tab. The following window is displayed.

NOTE! Except for the SSL (TLS) settings, the settings for GAT ACE 3000 and GAT ACE 7000 clients are the same, which is why the settings for both GAT ACE variants are described together here.

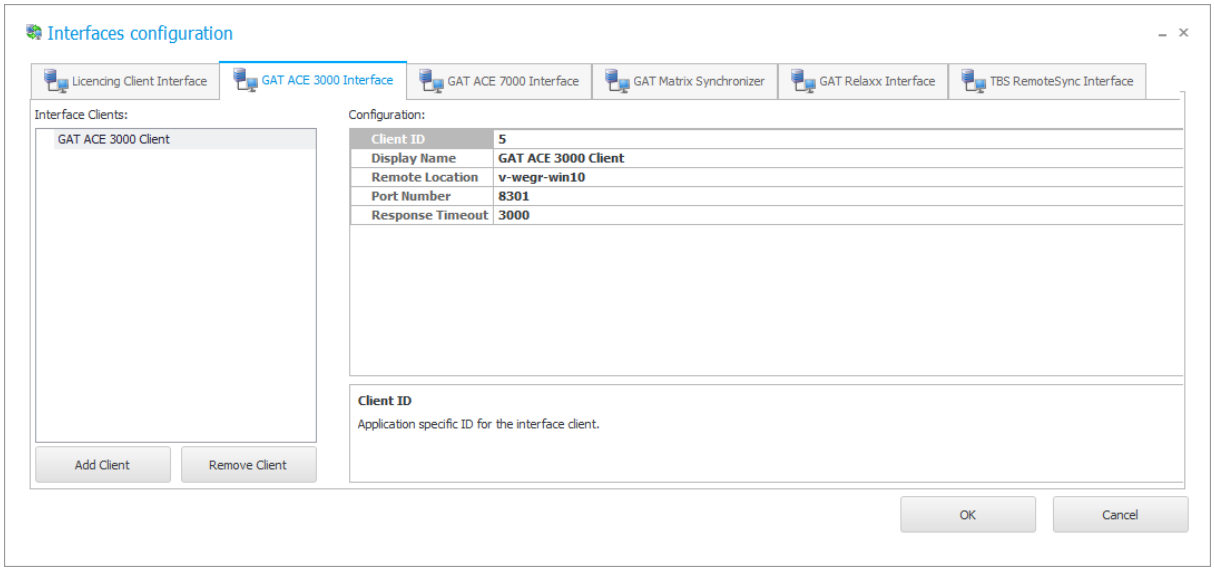


Figure 4.10 *- GAT ACE 3000 interface settings*

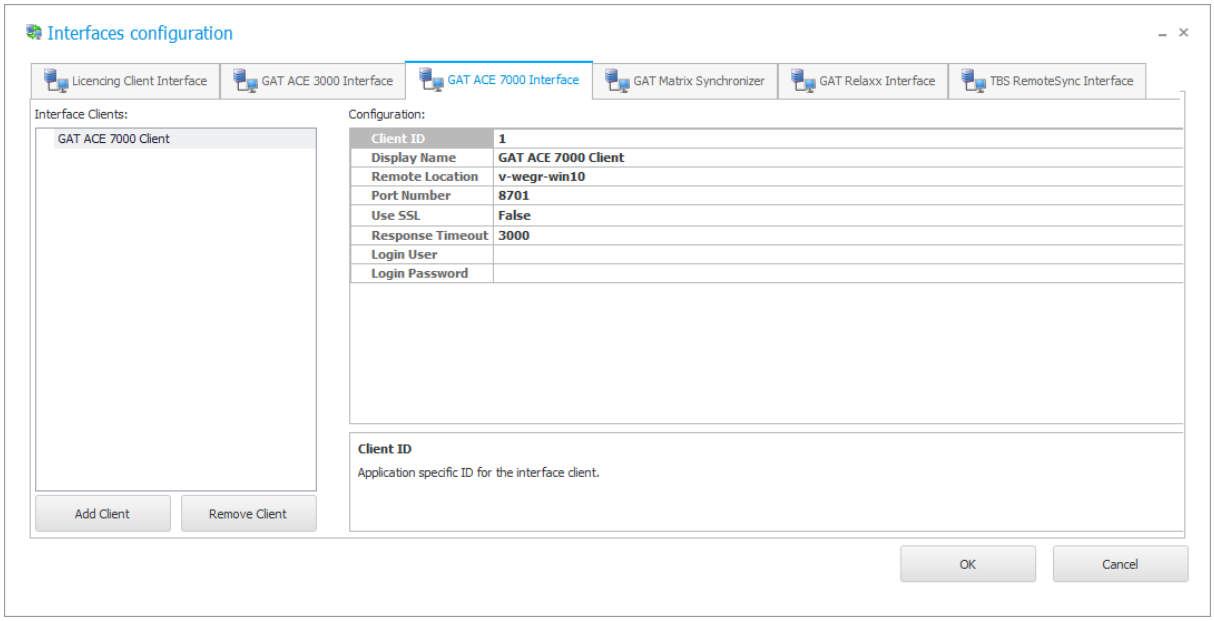


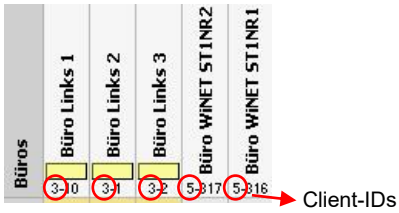
Figure 4.11 *- GAT ACE 7000 interface settings*

Listed in the "Interface Clients" area are all the GAT ACE installations that are available for use. Click on "Add Client" to add a new GAT ACE Server client.

Click on the "Remove Client" button to delete the selected entry. Note that the associated controllers in Matrix are not deleted. However, commands for the controllers are no longer sent. Furthermore, the GAT ACE ID number is no longer displayed next to the controller address.

The settings for the GAT ACE clients are configured in the "Configuration" area. When a client in the "Interface Client" list is selected, the settings of this client are displayed in the "Configuration" area. The following settings must be configured for each client:

- Client ID: Each client is identified via this ID number. The ID number must be unique (also between different GAT ACE clients) for each client. If an ID number is used twice, a message from Matrix is displayed. The ID number is also displayed in Matrix near the door address.



- Display Name: Identifying name for the selected client. This name is only used to identify each client in the status window of Matrix.
- Remote Location: Name of the server on which GAT ACE is installed.
- Port Number: Number of the port that is used to connect with the client. This port must be the same as the port configured for GAT Manager Proxy.

  To test whether a connection to the entered port can be established, enter the command "`telnet hostname port`" into a Windows® console. Open the Windows console by pressing the "Windows" key + "R", then type "cmd" and press "OK".
- Use SSL: This option is available for GAT ACE 7000 to use TLS encrypted communication. If this is activated for GAT ACE 7000, set this option to "True" in Matrix. Otherwise use "False". If TLS is activated, a username and password from a GAT ACE 7000 user must also be entered (see setting below).
- Response Timeout: Define a waiting time in milliseconds for a response to a sent command. As the retrieval of booking data can take some time, a value of 10000 (= 10 seconds) should be entered here.
- Login User/Login Password: If SSL (TLS) is activated on a GAT ACE 7000 client, the username and password of a GAT ACE 7000 user must be entered here. Only those functions that are activated in the user's authorization settings in GAT ACE 7000 are then available for communication.

4.4.3 Matrix Synchronizer settings for multi-user capability

Matrix allows several users to modify data in the software simultaneously. So that all open instances of Matrix are informed of changes occurring, a Matrix Synchronizer must be configured as the mediator between the instances. This is done via the interface configuration window (menu item "Options" in the "Tools" menu -> "Network" -> "Network Service Configuration") in the "Matrix Synchronizer" tab.

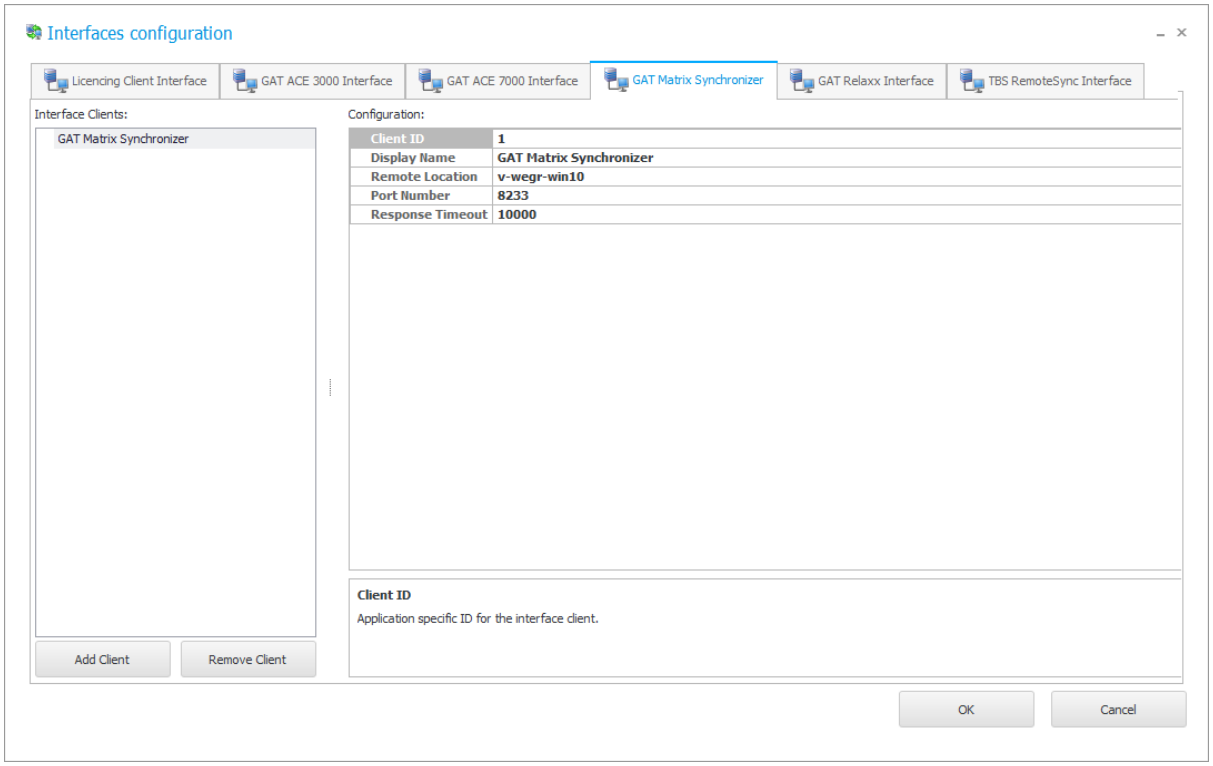


Figure 4.12 *- Matrix Synchronizer interface for multi-user capability*

In the left "Interface Clients" field, the Matrix Synchronizer, which will be assigned the role of mediator between the Matrix instances, is displayed. The buttons below the field allow you to delete the existing client or add a new one. If several GAT ACE applications are installed or in operation, you can freely select the mediator via the configuration settings to the right.

NOTE! Only one client can be defined as mediator for multi-user functionality.

The settings for a client will be determined in the right field "Configuration". The following settings are possible:

- Client ID: Each client is identified via this ID number. The number must be unique for all clients.
- Display Name: Any name for the selected server (client). This name is only for the display of the client in the status window of the Matrix.
- Remote Location: Name of the mediator, i.e., where the Matrix Synchronizer is installed.
- Port Number: Number of the port that will be used for the connection of the mediator. The standard value for the port is 8233.

  To test whether a connection to the entered port can be established, enter the command "`telnet hostname port`" into a Windows® console. Open the Windows console by pressing the "Windows" key + "R", then type "cmd" and press "OK".
- Response Timeout: Define a waiting time in milliseconds for a response to a sent command. The default value is 3000 (= 3 seconds).

After configuring these settings, Matrix is ready for multi-user operation. Changes made by one client are automatically sent to the other clients.

If problems arise when trying to communicate between the Matrix clients, please check that TCP/IP port 8233 is open (especially when using a firewall). This is the standard port used for communicating between the clients.

For further information on the multi-user functionality, see "4.13. Multi-user capability".

4.4.4 Relaxx interface

From Matrix version 4.3.0, it is possible to integrate Matrix with Relaxx - GANTNER's locker management software for electronic locker locks - thereby allowing you to assign persons to lockers in a facility via the "Lockers" page in Matrix.

See chapter "5.18.6 Locker" for detailed instructions on assigning lockers.

The settings in the GAT Relaxx Interface tab (accessed via "Tools" > "Options" > "Network" > "Network Services Configuration" > "GAT Relaxx Interface") are used to configure the connection with the Relaxx client.

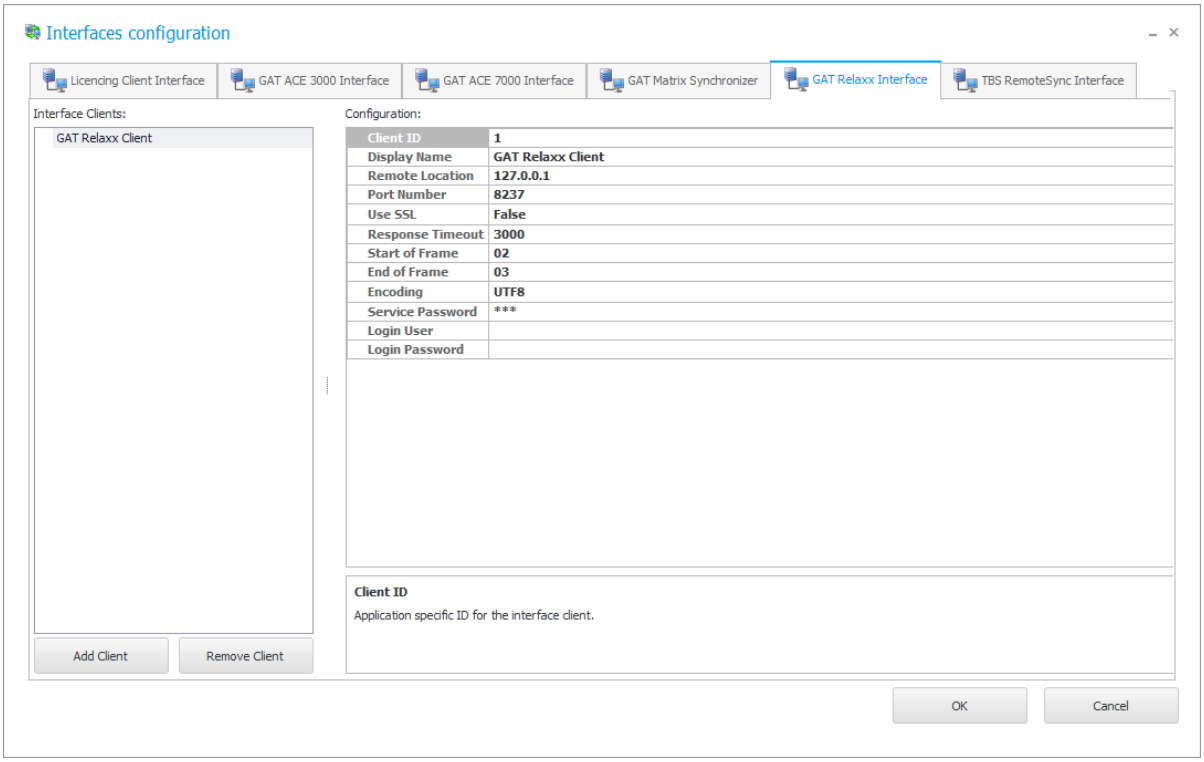


Figure 4.13 *- Relaxx Interface settings*

In the left "Interface Clients" field, all defined Relaxx clients are displayed. The buttons below the field allow you to delete the existing client or add a new one.

The settings for the client are defined in the "Configuration" field to the right. The following settings are possible:

- Client ID:	Each client is identified via this ID number. The number must be unique for all clients.
- Display Name:	The name of the selected Relaxx client. This name is only used to display the client in the status window of Matrix.
- Remote Location:	Name of the Relaxx client PC, i.e., the name of the computer on which Relaxx is installed.
- Port Number:	Number of the port that is used for the connection with the Relaxx client. The default value is 8237. A value of "0" means that connection will not be made.
- Use SSL:	This option is available for GAT ACE 7000 to use TLS encrypted communication. If this is activated for GAT ACE 7000, set this option to "True" in Matrix. Otherwise use "False". If TLS is activated, a username and password from a GAT ACE 7000 user must also be entered (see setting below).
- Response Timeout:	Time in milliseconds to wait for a response to a sent command before timing out. The default value is 3000 (= 3 seconds). For larger installations or if problems with synchronization occur, set this value to at least 10000 (= 10 seconds).
- Start of Frame:	Indicator for the data transmission start in hexadecimal format (no frames used if omitted). The default value is 02.
- End of Frame:	Indicator for the data transmission end in hexadecimal format (no frames used if omitted). The default value is 03.
- Encoding:	The type of encoding used for data transfer. The default is UTF8.
- Service Password:	The password used to establish service communication with Relaxx. This password must be the same as the password set in Relaxx.
- Login User/Login Password:	If SSL (TLS) is activated on a GAT ACE 7000 client, the username and password of a GAT ACE 7000 user must be entered here. Only those functions that are activated in the user's authorization settings in GAT ACE 7000 are then available for communication.

4.4.5 TBS RemoteSync interface

These settings are used for configuring the interface for the integration of a TBS biometric system. See chapter “5.6.8 TBS system (biometrics)” for more information.

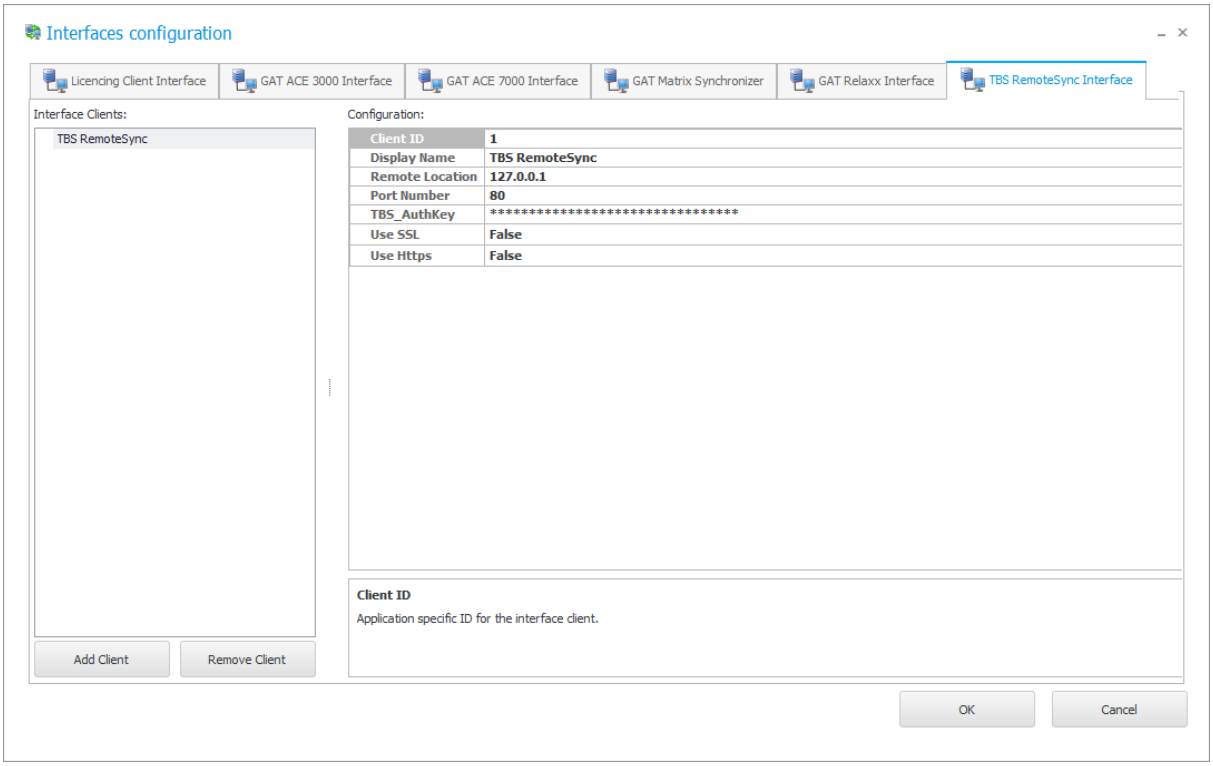


Figure 4.14 *- TBS RemoteSync Interface window*

The TBS clients can be added in the “Interface Clients” field on the left and the settings for the selected client are defined in the "Configuration" field to the right. The following settings are possible:

- Client ID: Each client is identified via this ID number. The number must be unique for all clients.
- Display Name: The name of the selected server (client). This name is only used to display the client in the status window of Matrix.
- Remote Location: Domain or IP address where the TBS WebEdition software is installed.
- Port Number: Remote port number for connection (must match the port via which the TBS WebEdition software is configured). The default value is "80". A value of "0" means that connection will not be made.
- TBS_AuthKey: Authentication key to access the TBS RemoteSync service.
- Use SSL: This option can be used to enable encrypted communication using TLS for the TBS software. If this is enabled for TBS, set this option to "True" in Matrix as well. Otherwise select “False”.
- Use Https: If this option is set to “True”, the connection will be attempted with https.

4.5 Language selection

The Matrix user interface can be displayed in different languages (German, English, French, Spanish, Catalan). Select “Options” from the “Tools” menu to access the configuration window. In the configuration window, select the “General” tab to change the application language. The following configuration window opens (see Figure 4.15).

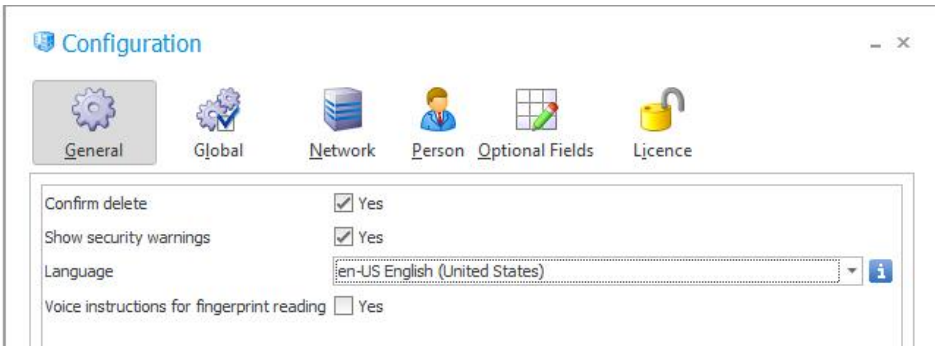


Figure 4.15 *- Language selection*

Select the desired display language and click "OK". You must either log out and log in or restart Matrix for the language to be activated.

4.6 Login



The login window is displayed after starting Matrix. Enter your username and password to begin using Matrix.

Figure 4.16 *- Login window*

► Enter a valid username into the "Username" field.

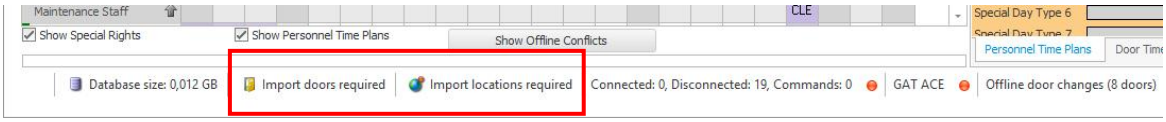
After installation, the username "SYSTEM" is predefined and the password for this user is "GAT".

► Enter the password. Note that the password input is case-sensitive.

NOTE! It is highly recommended to change this password after the initial login for security reasons. See chapter "5 OPERATION" for information about how to define users.

The main window of Matrix is displayed after logging in.

After login, Matrix checks if doors in GAT ACE 3000 and/or doors and locations in GAT ACE 7000 have changed since last working in Matrix. If so, this is shown in the status bar of Matrix.



Please note:

- *If another user imports the doors or locations, this message is only deleted for the current user after Matrix is restarted.*
- *If a GAT ACE installation cannot be reached during startup of Matrix, these messages are also shown.*

4.6.1 Two-factor authentication

It is possible to implement two-factor authentication for the login of each user. In addition to a password, it is then also necessary to enter a PIN code, which is continuously regenerated in real time using an app on a smartphone (= second factor). To enable two-factor authentication for a user, proceed as follows.

► For the role that is to use two-factor authentication, select the relevant option in the role settings (see also "9.2 Role management").

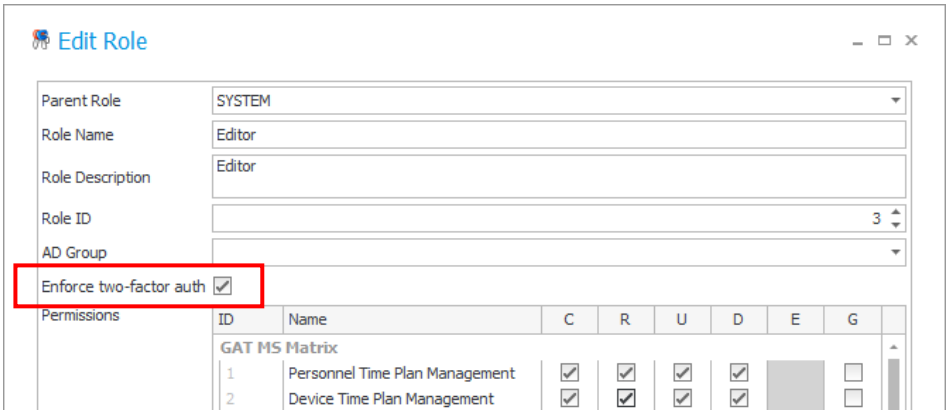


***Figure 4.17** – Role management -> activation of two-factor authentication*

► Every user assigned to this role must install an app for two-factor authentication on their smartphone (e.g., Google Authenticator or Microsoft Authenticator).
> Links for the Microsoft Authenticator:

JETZT BEI Google Play

Laden im App Store

The two-factor authentication must be configured once for each user. To do this, you as a user have to do the following.

► First, enter the username and password as described for normal login and confirm with "OK".
  - Information is displayed that the two-factor authentication must be configured.

► Confirm with "OK".
  - The following window is displayed.

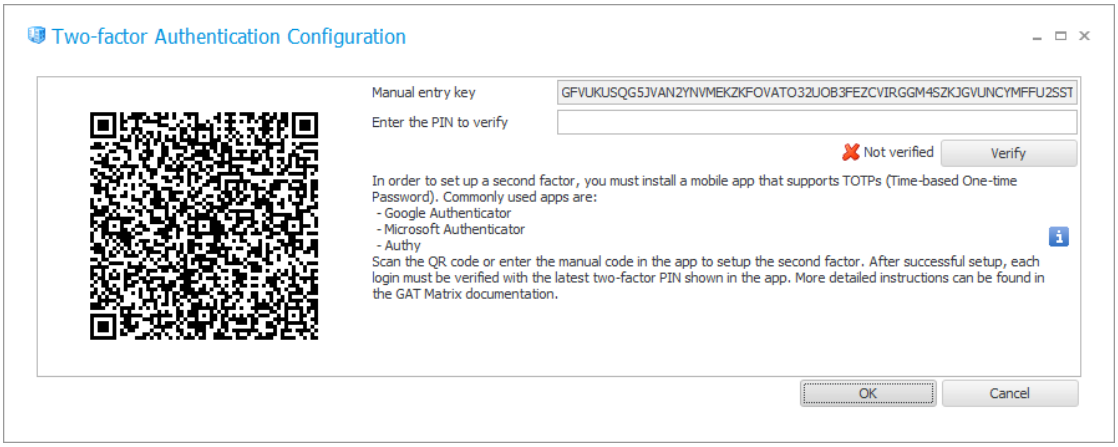


***Figure 4.18** – Configuration of two-factor authentication*

► Now create a new account in the app on your smartphone.

► Enter the key generated by Matrix for two-factor authentication in the account on the smartphone. To do this, scan the barcode via the app on the smartphone. If this does not work, you can also type the code in manually.

► The authentication app creates a PIN code for the account, which you must now enter in the window in the "Enter PIN for verification" field. The entry must be confirmed by clicking on "Verify".
  - If the code is valid, the message "Verified" is displayed.

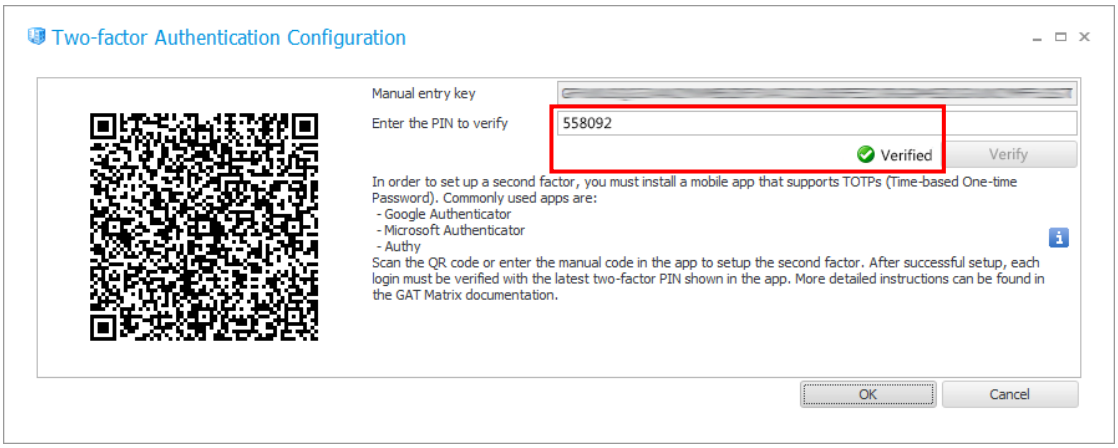


***Figure 4.19** – Configuration of two-factor authentication*

► Click on "OK".
  - When the user logs in again, the following window is displayed immediately after entering the password.

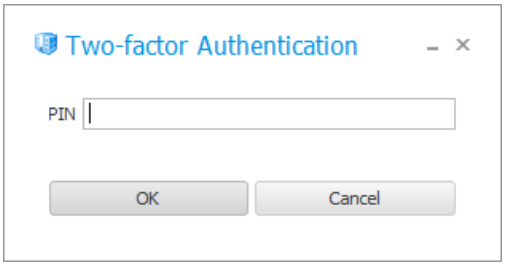


***Figure 4.20** – PIN entry for two-factor authentication*

- The smartphone app generates new codes at short intervals.

► Enter the currently displayed code and click "OK".

- If the input matches the generated code, you are logged in and can use Matrix.

4.6.2 Password recovery

If you have forgotten your password as a user, contact the system administrator to create a new password for you.

If you are a system administrator and have forgotten your password, you can request a temporary password from GANTNER Support via email (hotline@gantner.com) or telephone (+43 (0) 5556 73784-492), which you can use to log into Matrix to enter a new password for your username.

The password recovery option must be enabled in the global settings of Matrix (see "4.8 Global settings") and cannot be used when using Active Directory to log in.

► Click on "Password recovery" in the login window.

- The "Password Recovery" window opens.



***Figure 4.21** – Password recovery window*

► Enter your username into the "Username" field. Pay attention to the correct capitalization.

► Send your username and the value in the "Temporary key" field to GANTNER Support.

- You will receive a temporary password.

NOTE! Leave the password recovery window open until you have received and entered the temporary password, since the "Temporary key" is regenerated each time the window opens, and the temporary password is calculated using this key.

► Enter the temporary password in the "Temporary password" field and click on "Login".
  ○ You are now logged in to Matrix.
► Go to “File” -> “User Management” and change your password to a new, secure password.

NOTE! For security reasons, the following is checked for each password recovery request:

- Who made the request:	GANTNER requires the customer's address data and customer number or, if the request is made via a third party, the declaration of liability on the behalf of the customer. Furthermore, the agreement of the facility operator or customer with signature (name in block letters) and contact details for queries are required.
- Reason for the request:	Please tell us the reason for the restoration.
- Liability and costs:	Information regarding GANTNER Support’s disclaimer and costs (15 minutes technical support).

4.7 General settings

To configure the general settings of Matrix, select the "Options" menu item in the "Tools" menu and go to the "General" tab. This window is automatically displayed when starting Matrix for the first time.



Figure 4.22 *- General settings*

- Confirm delete:	When this option is selected ("Yes" is marked with a tick) a window will open whenever you try to delete any object or setting in Matrix (e.g., when deleting a person, controller, or time plan). You have to confirm the deletion with "OK". If this option is not selected and you delete an object, the object will be deleted without additional confirmation.
- Show security warnings:	When this option is selected, security warnings that open for certain actions while working with Matrix will be displayed. This setting is recommended for advanced users, who have knowledge of these warnings, to speed-up their work process. An example for this warning can be seen when a personnel time plan is being deleted. Matrix will display a message that the time plan is still assigned to a person and also the number of active assignments for the personnel time plan.
- Language:	Here the display language of Matrix can be selected (see "4.5 Language selection").
- Voice instructions for fingerprint reading:	If this field is selected, additionally to the text instructions a voice will guide through the process of reading fingerprints of persons (see "5.6.7 Scanning fingerprints").

4.8 Global settings

In the global settings, there are different options about the updates and licenses defined and it is possible to activate certain functions. The difference to the "General Settings" is that the global settings are valid for all users of Matrix and the general settings are only valid for the currently logged-in user.

In order to define the global settings, select the menu option "Options" in the "Tools" menu of Matrix and then open the "Global" tab.

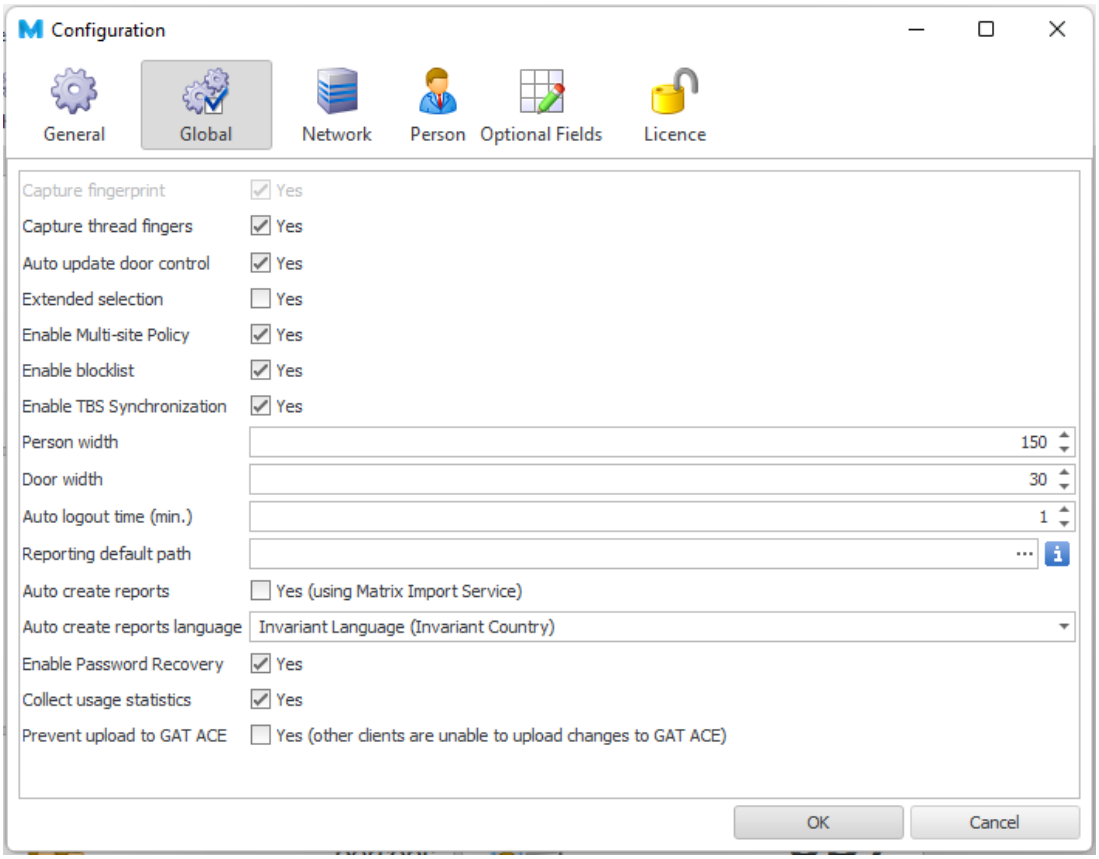


Figure 4.23 *- Global settings*

- Capture fingerprint: The identification or verification of a person can also be completed via fingerprint provided the corresponding hardware is installed. Therefore, you must mark this option, or else the identification with fingerprint is not possible (this is then set in Matrix).
- Capture threat fingers: A person can trigger a silent alarm by identification with a finger that was defined as the "threat finger" in Matrix. If the option "Capture threat fingers" is marked, the possibility to capture up to two threat fingerprints will be available when capturing the fingerprints of persons (see “5.6.7 Scanning fingerprints"). If this option is deactivated, the capturing of threat fingerprints is not possible.
- Auto update door control: If this option is selected, the door states in the door control module will automatically be updated. Else one must press F5 to update the states manually.

- Extended selection: If this option is selected, all persons or doors in a person or door group will be selected at once, if you click with the mouse onto a person group or door group header. This is, for example, helpful if you want to select many persons, or else you would have to select each person one by one.
- Enable multi-site policy: The multi-site policy is used to restrict a user/location to only see/edit specific door and person groups (see "5.9 Multi-site policy"). This function is linked to the locations in GAT ACE 3000, GAT ACE 7000, and ProAccess SPACE ("Partitions") and also allows different corporate calendars to be used for the different locations (see "6.2 Locations").

  NOTE! Enabling the multi-site policy can result in extended loading times.

  NOTE! If you change the multi-site policy setting (enable when disabled, or vice versa), you must log out of Matrix and log in again for the change to take effect.

  NOTE! Multi-site policy rules in Matrix Web allow users to utilize location and organization filters. The corresponding Multi-site policy license is required for this function; otherwise, it will not be supported.
- Enable blocklist: If this option is checked, the blocklist can be used globally for the entire access control system. This is only relevant when offline doors are being used in CardNET or Hotel mode. When online doors and offline doors are only being used in WiNET or Read-Only mode, the use of the blocklist has no advantage. For further information see "5.10 Data carrier blocklist".
- Enable TBS Synchronization: This option is displayed after the TBS Integration license has been activated in Matrix. Select this option to allow the TBS fingerprint reader system to be used in Matrix.
- Auto. import bookings: This function automatically imports bookings from GAT ACE to Matrix. To use the function, the import persons service must be installed and configured (see "5.7 Import persons").
  SPACE Synchronizer is used to import the bookings from ProAccess SPACE.
- Person width: Define the width of the person column (left-most column in the authorization matrix) in pixels. Default value is 150. Value range is 50 to 500.
- Door width: Define the width of the door columns in the authorization matrix in pixels. Default value is 30. Value range is 25 to 75.
- Auto logout time (min.): Here you can enter a time in minutes after which the current user will be automatically logged out if continuously inactive during this time.
- Reporting default path: This and the following two options refer to “reports”, which provide an overview of the authorizations for each person. This can be found for each person in their personnel data under the "Reports" tab (see "5.6.1 Defining personnel master data").
  For the default path, you can see where the reports should be placed when increasing.
- Auto create reports: If the option for automatic creation is enabled, the person reports are created every hour. If the option is not enabled, the reports are not automatically created.
- Auto create reports language: In the language selection field, select which language should be used for the reports.

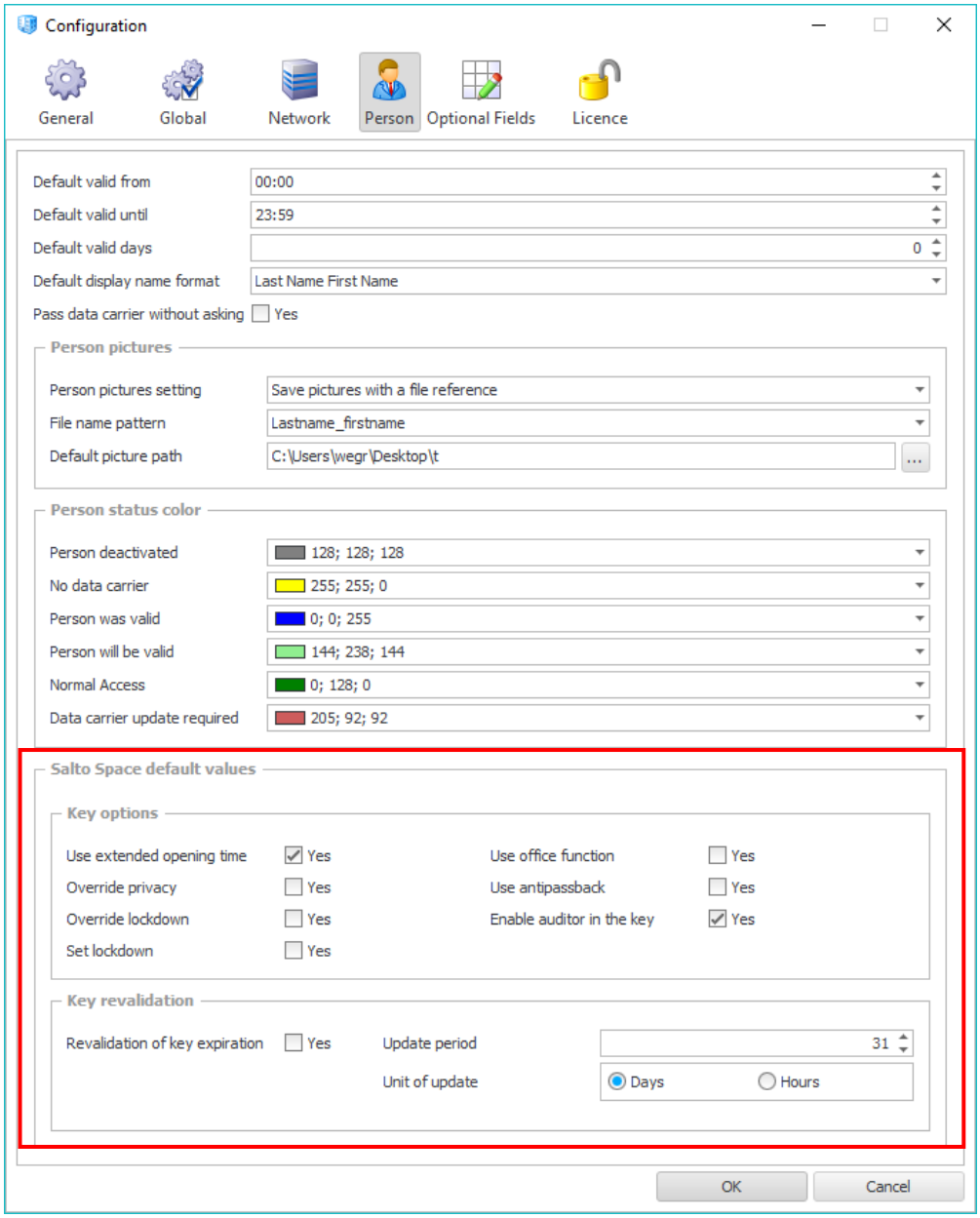
- Enable Password Recovery:	When this setting is enabled, the “Password recovery” option is displayed in the login window allowing a user to reset their password with assistance from GANTNER support if they forget it (see "4.6.2 Password recovery").
- Collect usage statistics:	If this field is selected, anonymized telemetric data about the usage of Matrix is transmitted to GANTNER Electronic. This data includes PC information (shortened IP address and GUID), usage statistics (e.g., reaction times), and error messages, which helps us in developing new features for Matrix. This information does not include personal information. You can deactivate the recording of this data by deselecting this option.
- Lock upload to GAT ACE:	This function allows an administrator to block other clients from uploading to GAT ACE. If the option is selected, the "Upload Doors" button of all other clients will be deactivated. Also, the Import Service can no longer load data to GAT ACE. In addition, you can choose whether all other clients should be closed. If so, the clients have 5 minutes to complete their work before Matrix is automatically closed. A client can then no longer be started and receives a corresponding error message at startup.

4.9 Network settings

The network settings are described in detail in chapter “4.4 Settings of the network services (clients)” and the subsequent chapters.

4.10 Settings for person display

These settings define the functionality for adding and editing persons (see "5.6 Editing the master data of a person in the authorization matrix ") and how each person is displayed in Matrix.



This area is only displayed if ProAccess SPACE synchronization is enabled (see description below).

Figure 4.24 *- Settings for person data*

The following settings are available:

- Default valid from/until: Here you can specify the times to include by default when adding authorization data for people.
- Default valid days: Here you can specify in number of days an authorization validity period to include by default when adding authorization times for people.

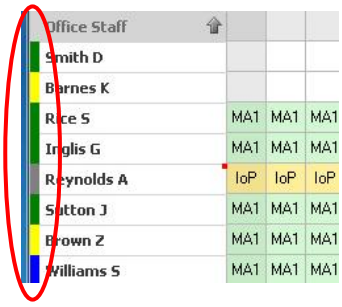
- Default display name format: Here you can select how Matrix handles the names of the users, i.e., whether to display the first name or the last name first. This is especially useful in connection with SALTO's ProAccess Space to ensure that the sorting and filtering of persons in the booking display works as intended. If this option is set differently in Matrix and SPACE, bookings will be displayed with, e.g., “Max Muster” on GANTNER devices and “Muster Max” on SALTO devices.

  Note: As of Matrix version 5.1, the name of a person is no longer used to link the person between the Matrix and ProAccess SPACE, but the "Ext ID" number is used instead. See also "5.6.2. Settings for persons in ProAccess SPACE".

- Pass data carrier without asking: When this option is selected, you will not be asked to confirm your request when assigning an expired data carrier to another person. The data carrier is unassigned from the original person without a confirmation message and assigned to the new person. When the option is not selected, a message is displayed asking you to confirm the action.

- Personal pictures: In this field, you can configure the settings for the use of pictures in personal data (see "5.6.1 Defining personnel master data").
  If "No person pictures" is selected, images cannot be used.
  With "Save pictures in the database" the images are saved in the database. This can lead to the database becoming relatively large.
  With "Save pictures with a file reference", only the paths to the images are saved. These must be in a folder accessible to Matrix. You can define how the images are named and the default image path where the images are saved.

- Person status color: Here you can assign colors to distinguish between the different states of people displayed in the matrix.

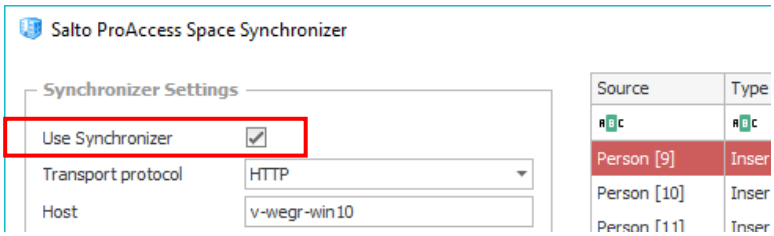


The following states can be defined for each person:

- Person deactivated: This state is assigned to a person who is still saved in Matrix but deactivated in the access control system.
- No data carrier: The person was added to Matrix but there is currently no active data carrier assigned.
- Person was valid: The validity period of the person has expired. The person has no authorization in the access system.
- Person will be valid: The person was added, and a data carrier assigned. A validity period defined for the person has not been defined yet.
- Normal access: The person is currently valid (active validity period, if defined, and valid data carrier assigned).
- Data carrier update required: For persons with this status, authorizations must be changed, and the data carriers of the persons must

therefore be rewritten. This is necessary for SALTO doors because the authorizations are stored on the data carriers.

- Salto Space default values: This area is only displayed if the "Salto ProAccess Space Synchronizer" is used and enabled. This setting can be found in the "Tools" menu -> "ProAccess Space Synchronization".



- "Key options": In this area, the default values can be defined for the data carriers/ID cards of persons that are assigned when they are added to ProAccess SPACE (e.g., when imported from an HR system). These settings can be modified and adapted individually for each person in the personnel database.

- "Key revalidation": In this area, the default values can be defined for the validity of data carriers/ID cards of persons that are assigned when they are added to ProAccess SPACE (e.g., when imported from an HR system). These settings can be changed and adapted individually for each person in the personnel database. The validity period can be entered in days or hours. Select the relevant option under the input field.

4.11 Optional fields for personnel data

With optional fields a user can add self-defined new fields, which are then displayed with the personnel data (see "5.6 Editing the master data of a person in the authorization matrix ").

Optional fields are also used for license plate recognition. This function requires at least one optional field of the type "License Plate" to be defined. Each person's personal identification number can then be entered in the personal data. Multiple license plate fields are also possible and Matrix checks every license plate entry for uniqueness.

NOTE! It must be noted that the person with the license plate number is using one or more active data carriers with the data carrier type defined for license plate recognition. This data carrier type is set in GAT ACE 7000 on the "Cameras" tab via the "Card type" setting.

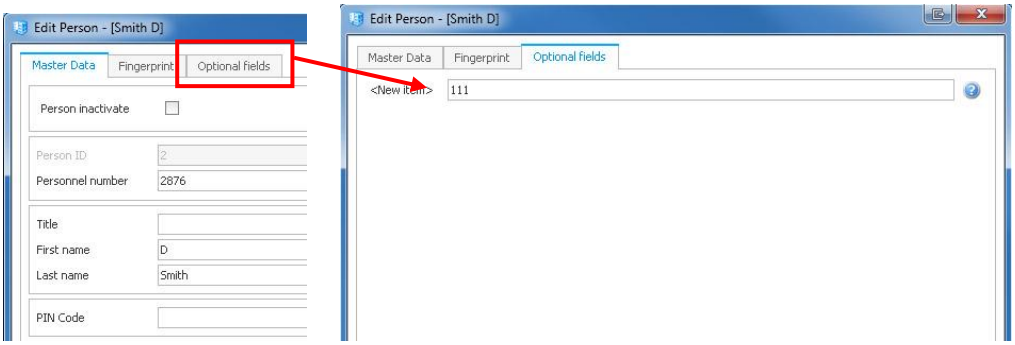


Figure 4.25 *- Optional fields in the personnel data*

To edit the optional fields, select "Options" in the "Tools" menu and then click on the "Optional Fields" tab. The settings are described in the following window.

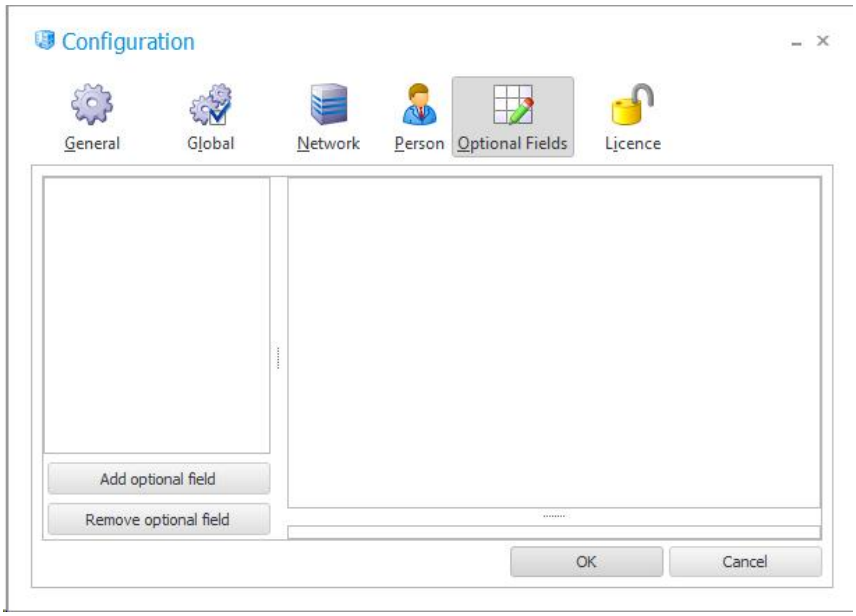


Figure 4.26 *- Optional fields*

On the left side the optional fields are displayed. At the beginning, this list is empty. With the button "Add optional field" you can add a new optional field and with the button "Remove optional field" you can delete the selected optional field to the left.

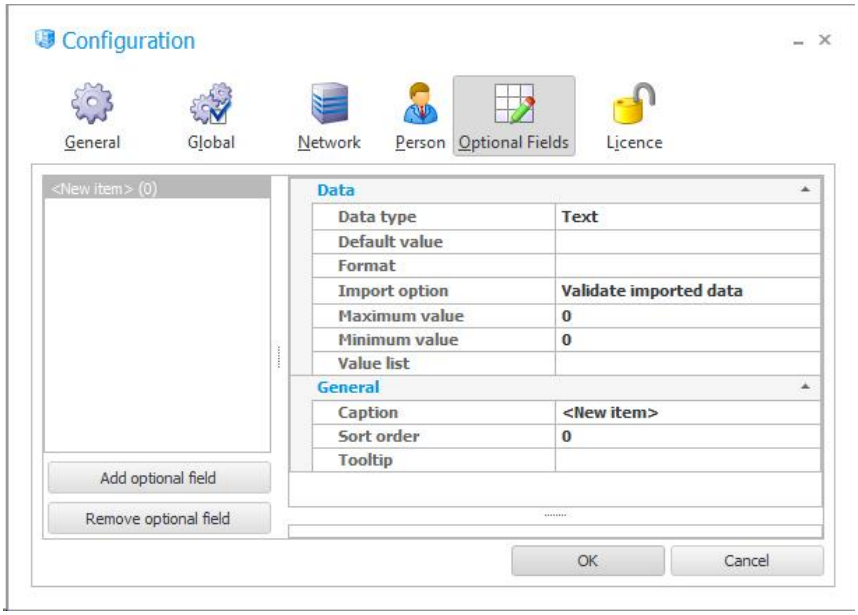


Figure 4.27 *- Optional fields, new field created*

If an optional field is selected on the left, the settings for this field can be entered in the fields to the right. The information is separated into "General" and "Data" fields:

General *(the same for all types of optional fields)**:***

- Caption: An arbitrary name for the field. The optional field is shown in the personnel data with this name.
- Sort order: If several fields are present, this number will determine how all the fields are sorted and displayed in the personnel data.
- Tooltip: A short description for the field can be entered here. If the user moves the mouse cursor over the question mark in the personnel data nest to this optional field ( ), the tooltip entered here will be shown.

Data *(depends on the type of field)**:***

- Data type: Here the type of the optional field is selected. This selection also determines, which further fields will be displayed. The following data types are possible: Number, Text, Time, Date, Checkbox, Long Text, and License Plate.
- Format: (all data types) Here you can enter a template in order to format the data in the optional field. For example, the display of the date and time can be formatted like this:
  Input = "dd.MM.yyyy HH:mm:ss"
  Output = "30.03.2012 09:10:22"
- Import option: (all data types) Define how the optional fields are managed during import:
  - "Validate imported data": During import the data of the optional field is validated (e.g. when setting the data type to "Number" it will be checked if a number is imported and not a text string). If the import is not valid, the invalid value is ignored and will not be imported.

	- "Extend with imported data": With this option, the personnel data will be extended by the imported field. - "None": The imported data will not be validated. In this case it is possible that invalid values will be stored. If, for example, the value "Office 3" is imported even if only a value list with the values "Office 1" and "Office 2" is allowed, the value "Office 3" will be imported but the value list will not be automatically updated.
- Default value: (all data types)	The value entered here will be used as standard value for all new persons.
- Value list: (for types "Text" and "Checkbox")	Here you can enter a list of predefined values or texts, which can then be used for the optional fields. The values in this list must be separated by the hash symbol (#). **NOTE!** The difference between the Text and Checkbox types is that only one value from the value list can be selected for type Text whereas several predefined values can be selected for the type Checkbox.
- Maximum value: (for type "Number")	Here you can enter a maximum value for the field. Higher values will not be accepted.
- Minimum value: (for type "Number")	Here you can enter a minimal value for the field. Lower values will not be accepted.

Matrix displays the status of the cameras, which are used for license plate recognition, in the dashboard (see "5.1. Dashboard").
One or more optional fields can be used for vehicle license plate recognition, for which you then must select "License plate" as the data type.

4.12 Activating Matrix

After installation, a valid license for Matrix must be entered (either by manual input of the license code or via a license file). After the license it is further necessary to activate Matrix. If Matrix is not activated, it cannot be used anymore after 14 days past installation.

To enter a license and to activate Matrix you can select the menu item "License Information" in the "Help" menu. A detailed description about the licensing can be found in chapter "10. LICENSE MANAGEMENT".

4.13 Multi-user capability

Matrix offers the possibility to operate simultaneously on several workstations being used by different users. To achieve this functionality the Matrix Client must be set up correctly as a mediator. See "4.4.3. Matrix Synchronizer settings for multi-user capability".

This multi-user operation can lead to operational conflicts if several users are working on one dataset simultaneously. Matrix draws your attention to these situations.

Matrix informs you when another user has just changed the dataset that you are currently editing. This is indicated by a yellow exclamation mark on the "OK" button, e.g., if you want to change the settings of a door and you open the edit window. If another user opens the edit window, changes the settings, and closes the window again while you are still in the edit window, a yellow exclamation mark on the "OK" button is shown. This means that saving your changes is no longer possible and you must close the window and reopen the dataset for editing.

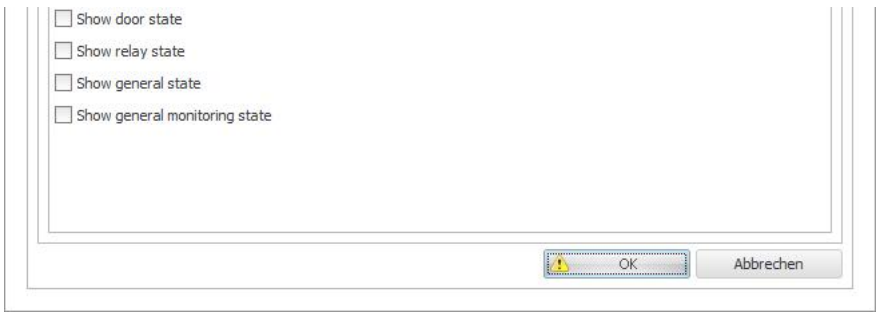


Figure 4.28 *- Dataset was changed by another person indicator*

Furthermore, it is possible that a dataset is deleted while you are editing it. In this case, a red "X" is shown on the "OK" button.



Figure 4.29 *- Dataset was deleted by another person*

The updating of the user interface according to the previous principle is implemented for the following areas of Matrix:

- Access overview
- Relay plan overview
- Booking overview
- Time plan overview (personnel- and door time plans)
- Personnel window
- Persons/door group window
- Door window
- Time plans
- Operation calendar
- Relay plan window

5. OPERATION

After starting and logging into Matrix (see previous chapter), the dashboard area of the main Matrix window is displayed first. Use the buttons in the upper toolbar to switch between the different areas.

5.1 Dashboard

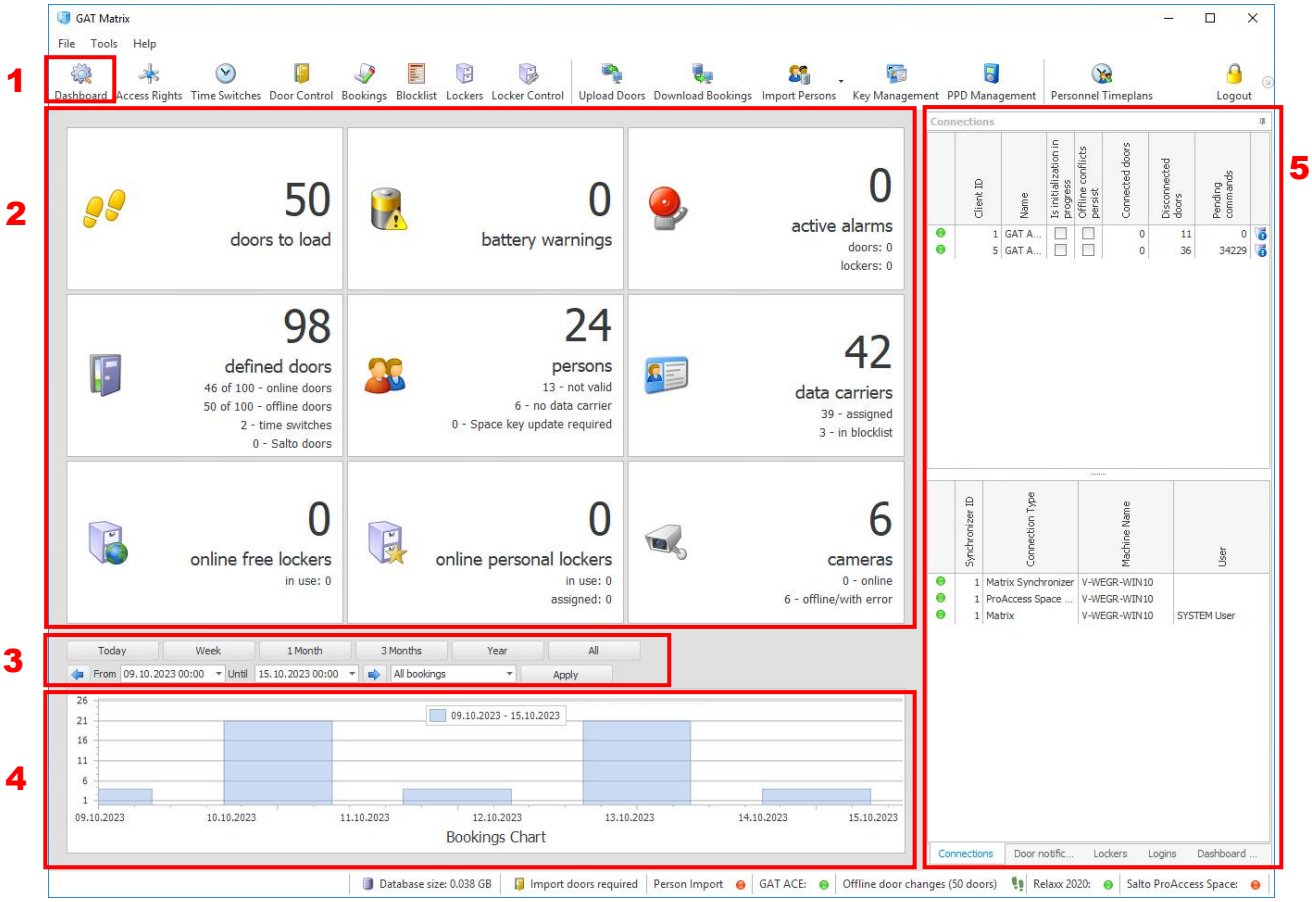


***Figure 5.1** - Main window (Dashboard) of Matrix*

Here you will find the most important information about the access system at a glance, divided into the following areas:

1 – Dashboard icon: Displays the dashboard in Matrix.

2 – System information: Shown here are tiles with current information about the access system in Matrix:

- Doors to load: The number of offline doors that still have to be loaded with the latest configuration or authorization data (see "5.18.2 Uploading offline doors").

  Note: By right clicking on this tile, you can select "Show list", i.e., the door list opens in the right column (5). In addition, a report on the doors to be loaded or a complete report in text form can be copied to the clipboard for pasting in an editor program. The complete report contains a listing of all doors to be loaded, alarms, battery warnings, and the locker status of free and personal lockers.

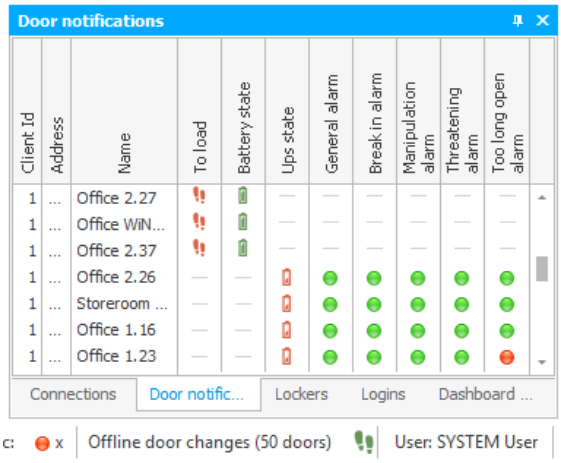
- Battery warnings: The number of offline doors where the battery level is (almost) discharged and must be changed.
- Active alarms: The number of alarms present in the system. The alarms for the doors (GAT ACE) and lockers (Relaxx) are displayed separately. Alarms can be acknowledged via the door management matrix, a building management system, the GAT Mobile Access app, or in the Relaxx software. For systems with the GAT DC 7200, the alarms can also be acknowledged via the web interface of these controllers.
- Defined doors: The number of online and offline doors in Matrix and display of the max. possible number of doors (according to license).
- Persons: The number of persons defined in Matrix with additional display of invalid persons (their validity period has expired or begins at a later date) and persons without data carriers.
- Data carriers: The number of data carriers defined in Matrix. Also shown are the number of data carriers assigned to persons and the number of data carriers currently entered in the blocklist (see "5.10. Data carrier blocklist").
- Online free lockers/personal lockers: The number of available and currently occupied (locked) lockers is displayed here when using and connecting the Relaxx locker management software and user display authorization. For the personal lockers, you can also see how many lockers are assigned to people or data carriers.
  Note: By right clicking on this tile, you can "Show list", i.e., the door list opens in the right column (5). In addition, a report on the doors to be loaded or a complete report in text form can be copied to the clipboard for pasting in an editor program. The complete report contains a list of all doors to be loaded, alarms, battery warnings, and the locker status of free and personal lockers.
- Cameras: This field displays how many cameras have been configured for license plate recognition and how many of these cameras are online or offline. The cameras are defined in GAT ACE 7000. The vehicle license plates are assigned to the persons in their personnel data (see "5.6.10. Settings for license plate recognition").

3 - Booking period: Select the period for which the booking activity (see 4) is displayed.

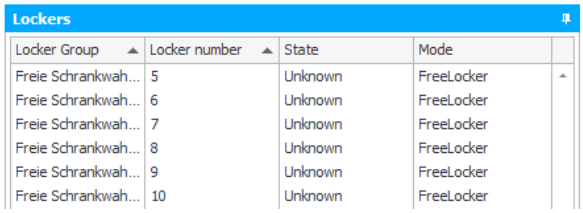
4 - Booking activity: Here you see the number of bookings recorded by the controllers in the system for the selected period. The bookings include entries and exits, access attempts by persons, alarms, system messages, error messages, etc. The bookings must be read first for the correct number to be displayed (see "7. BOOKINGS").

5 - Tabs: Connections: The upper section of this tab shows the connections to the GAT ACE installations. Green signals an active connection with red signaling a disconnection from the respective GAT ACE client. The lower section displays the connections to other software components, e.g., Matrix Synchronizer (for the multi-user function) or GAT Mobile Access Management and lists the users who are currently logged into Matrix.

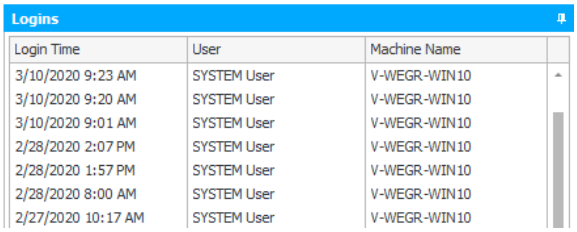
Door notifications: This tab shows the current messages such as loading information, the battery state of offline doors, UPS states, and alarm messages for the doors in Matrix.



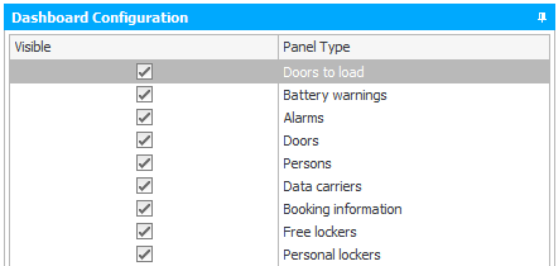
Lockers: Shown on this tab are all lockers (if Relaxx is used) and the locker numbers and locker groups.



Logins: This tab displays a list of all user logins recorded for Matrix (with date and time).



Dashboard Configuration: Use this tab to hide or show dashboard elements by selecting or deselecting the options.



You can arrange the tabs by dragging the header of a tab to the desired position.

5.2 Main window

The main window of Matrix is blank after the first start and login. The following figure shows an example of the authorization display ("Access Rights" icon) after access terminals (doors) have been imported from GAT ACE and persons have been created in Matrix. In the example, the persons have been assigned access rights.

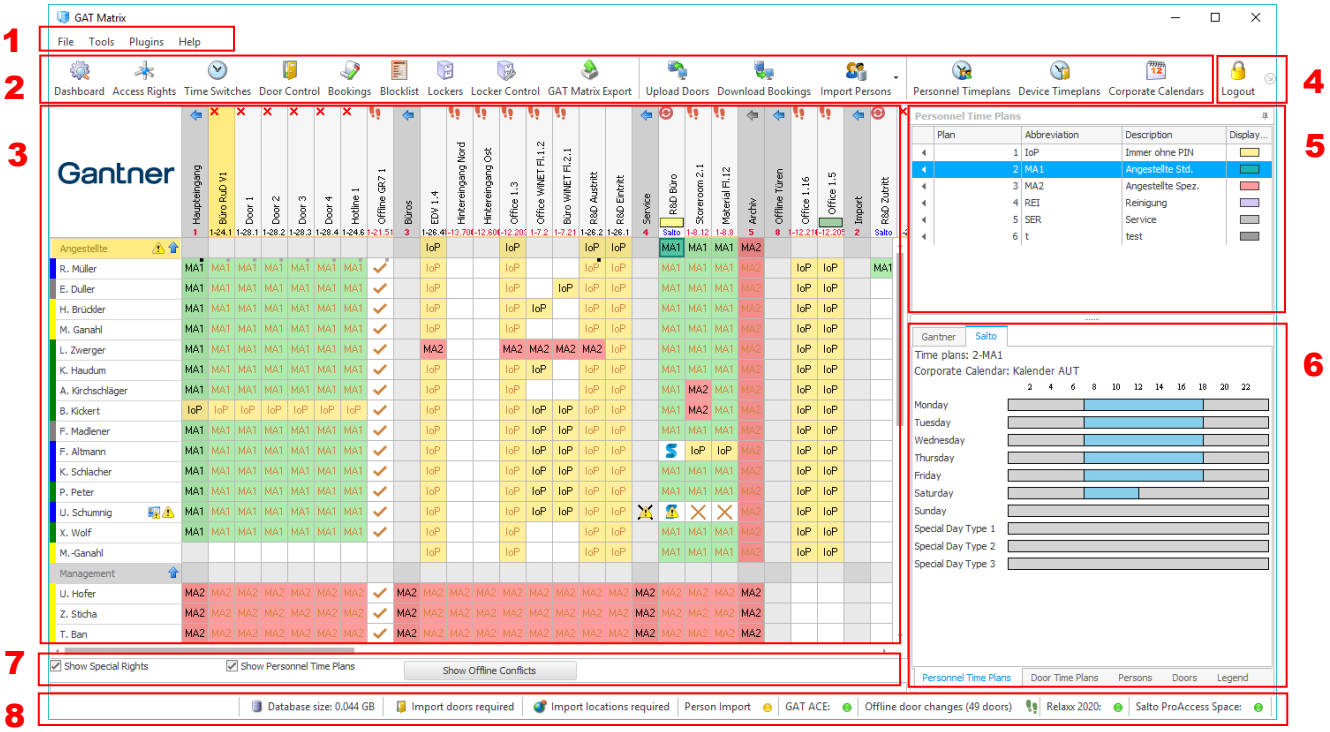


Figure 5.2 *- Main window of Matrix with authorization matrix*

The main window is divided into the following areas:

1 - Main Menu: Access all functions of the Matrix application by selecting the various menu items.

2 - Toolbar Buttons: Access important functions directly with one mouse click. With the "Access rights" icon, you can display the access rights area at any time. Depending on the features or licenses that are enabled or disabled, some of the icons may not be displayed, e.g., Key Management and PPD Management are only displayed when the SALTO ProAccess SPACE software is being used.

3 - Main Area: This area is the main information window. It can show different information such as the authorization matrix (shown in Figure 5.**2**), the bookings list, or the time plans.

4 - Logout: By clicking on this icon, the current user is logged out of Matrix.

5 - Time Plan List: Here all defined time plans (personnel or door time plans) are displayed and can be assigned to selected persons or controllers respectively.

6 - Time Plan Info / Search: Three different types of information are shown here depending on which view was selected with the tabs at the bottom of this area:

a) Settings of the time plan that is selected in (5) or the time plan assigned to the cell selected in (3). If no time plan and/or an empty cell in (3) is selected, no information is displayed here. You can also see which corporate calendar is assigned to the selected door.

b) List of the persons or controllers (or doors) with search function. The hierarchy of the "locations" of GAT ACE 7000 is also displayed in the door list.

c) Legend that describes the icons used in the authorization matrix.

7 - Options:

These options allow you to change the display mode of the matrix and the terminal loading function:

a) "Show Special Rights": When this option is selected, the matrix fields that have the "special rights" option assigned are marked with a black dot, otherwise this dot is not shown.

b) "Show Personnel Time Plans": When this option is selected, the assigned time plans are shown in the authorization matrix (with color and abbreviation). Otherwise, the matrix will be empty.



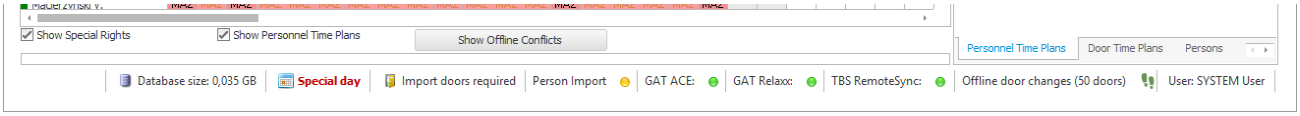
c) "Show Offline Conflicts": When this option is selected, problems with offline rights are indicated with a yellow exclamation mark in the fields concerned – for both individuals and doors as well as directly in the respective groups. Such problems can arise if too many offline rights are defined for a person (i.e. for a data carrier) so that those offline rights cannot all be saved on the data carrier (see "5.18.2 Uploading offline doors").
For offline doors with the Read Only function (or in GAT ACE 3000 also with CardNET), only the “Valid to” time of the validity period is written onto the data carrier. Therefore, the "Valid from" time must be in the past and not in the future. Offline conflicts for these doors are indicated by a yellow triangle with exclamation mark and a clock icon when the valid from date is set in the future.



d) The offline conflicts are computed by Matrix each time authorization data is changed. As this computation can take a long time it is executed as a background process and the progress of the computation is indicated by a blue bar below the option fields.

8 - Status Bar:

The status bar shows various information about Matrix (e.g., the connected controllers and logged-in user), for example:



The following information is shown:

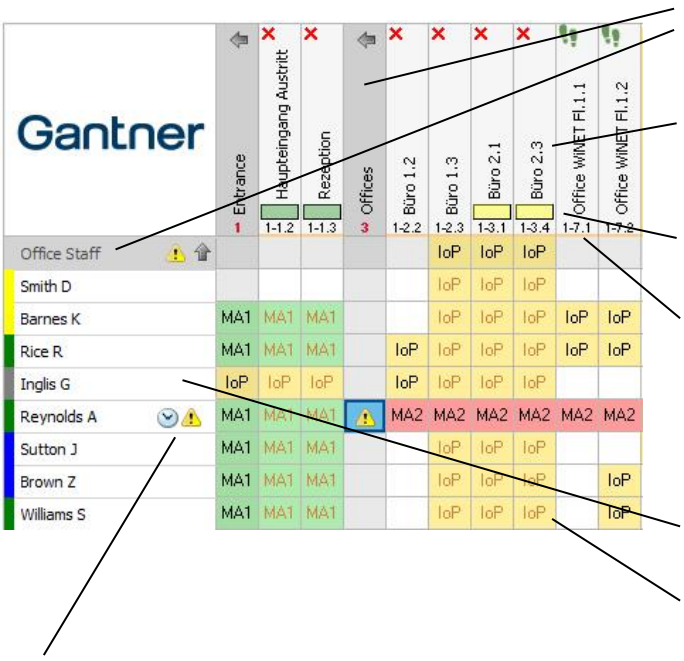
- Logged-in user
- Connection status to GAT ACE, Relaxx, and SALTO ProAccess Space (if used). A green dot indicates that the connection to the respective GAT ACE / Relaxx 2022 / TBS / Space system is active. A red dot indicates that the respective connection could not be established.
- Number of connected and disconnected controllers and number of commands that are still to be sent to the controllers.
- The "CardNET change" footsteps symbol () indicates that authorization data for offline doors has been changed and must be uploaded to the relevant offline doors with various symbol colors indicating which data is not up to date (see "5.18.2 Uploading offline doors"). When all authorization data in the offline doors is current, the footsteps symbol is not displayed.
- Conflicts in the authorization data of offline doors (see "5.18.2 Uploading offline doors").
- Notification whether there are changes to the door configurations in GAT ACE 3000 and GAT ACE 7000 since the last usage of Matrix. Changes need to be imported (see "5.4 Importing doors and locations from GAT ACE").
- Notification whether a special day is active at the current date. The name of the special day is displayed (for information on special days see "6. CORPORATE CALENDAR AND LOCATIONS").

5.2.1 Authorization matrix



You can view the authorization matrix by clicking on "Access Rights" in the toolbar.

The authorization matrix is used to define the individual access authorization of people for each controller. The doors, which are controlled by the controllers, and the persons are arranged in groups.



Door groups and **person groups** are displayed in dark gray and can be expanded and collapsed (see next page).

The **doors** are organized in the upper row of the matrix. Each door has a door name[1)], which is defined in GAT ACE.

When a **door schedule** is assigned to a door, a field with the color of the schedule is displayed.

The **numbers** under each door indicate the GAT ACE Client ID (here "1") followed by the door controller ID ("7") and door number (2). If the number is red, it is an offline door operating in CardNET mode or Hotel mode. For ProAccess Space doors, the text “SALTO” is displayed here.

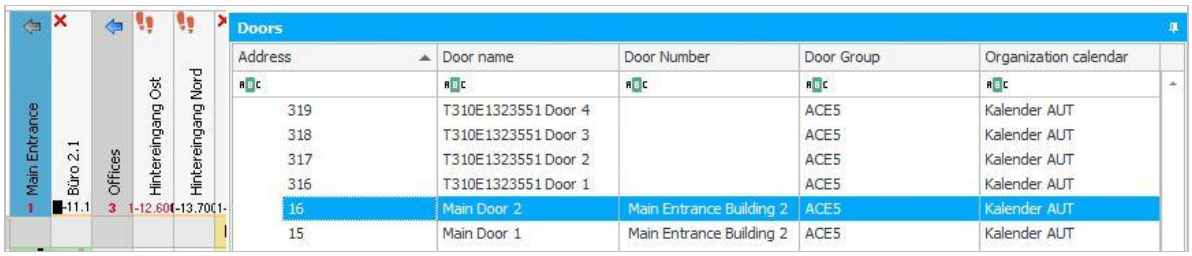
The **persons** are listed in the left column of the matrix.

Assigned **personnel schedules** are displayed in the matrix fields.

Symbols next to a person indicate the following information (see "5.14.1 Symbols and color indications used in the authorization matrix"):

… Problem with the validity period for offline doors
… Problem with the person authorization
… Number of authorizations exceeded

[1)] In GAT ACE 7000, the door name can consist of two components (separated by a vertical line or pipe symbol "|"). The part to the left of the line is used as the display name in Matrix. The part to the right of the line is displayed as pop-up text when you hover the mouse pointer over the door name. In the door list (see description on the previous page: field 6, option b in Figure 5.**2**), both components are displayed in the "Door name" and "Door number" columns.

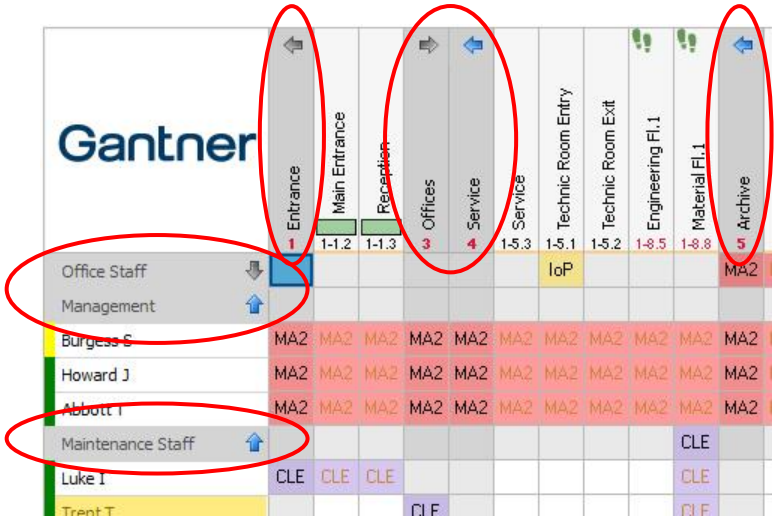


The clock symbol for a person indicates that there is a problem with the validity period in the personnel data for GAT ACE 7000 for an offline door with Read Only function (and for GAT ACE 3000 also with CardNET function).

See section "5.14. Defining authorizations of persons in the authorization matrix" for further information on working with the matrix.

You can adjust the width of the left column that lists the persons and the door columns in the global settings (see "4.8. Global settings").

5.3 Person groups and door groups



Gray arrows:
There are no plans assigned in this group or they are inherited from other groups only.

Blue arrows:
A plan is directly assigned to at least one door or person in the group.

Figure 5.3 *- Person and door groups*

Persons and doors must be assigned to groups.

Groups are shown in darker gray with an arrow (see red marks in the Figure 5.**3**). A blue arrow on a door group or person group indicates that at least one door or person in that group is assigned a personnel time plan as individual authorization. If no personnel time plan is assigned or only inherited, then a gray arrow is shown. The groups can be expanded or collapsed by pressing the arrow next to the group field. As an alternative, groups can also be expanded or collapsed by using the context menu, which can be accessed via the right mouse button.

To add a new group, right-click onto the "Gantner" logo and select "Add person group" or "Add door group". A new group is added to the matrix.

By right-clicking onto a group field a context menu is shown that offers functions to edit (change the group's name), add, delete, expand, or collapse the groups and to show the bookings that were made for the items in this group. Furthermore, the bookings of persons / doors within the group can be displayed in the menus. The persons and doors can be sorted alphabetically within a group and the doors additionally sorted by address.

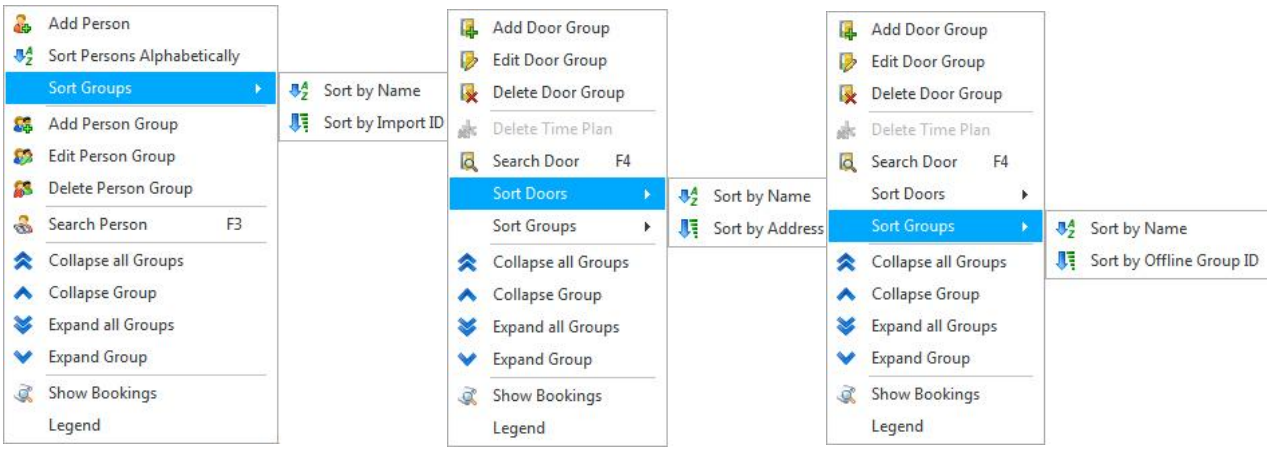


Figure 5.4 *- Context menus in the matrix*

5.3.1 Moving persons or doors between groups

With the menu item "Move Persons" and "Move Doors" in the Pop-up menus of the groups, persons and doors from a group can be moved to another.

The moving procedure is identical for persons and doors and described here using the example of persons.

If you select the menu item "Move Person", the following window opens:

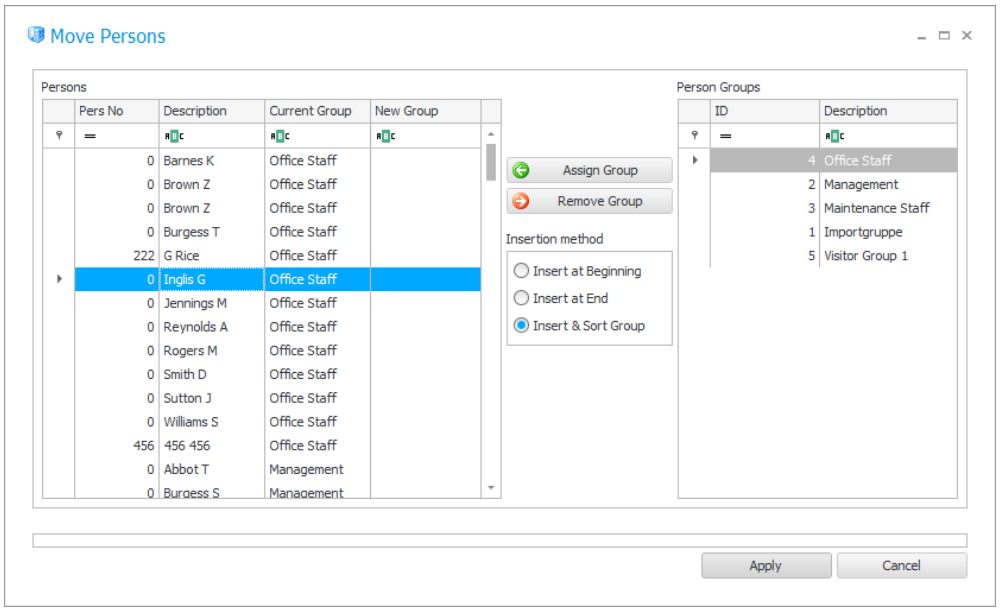


Figure 5.5 *- Moving persons between groups*

All persons previously added to Matrix are shown in the left field. Each person has a unique Personnel-ID number ("Pers Id"). The "Description" column shows the name of the person. The "Current Group" column shows the group where the person is currently assigned, and the "New Group" column shows the group they are moving to.
In the "Person Groups" list on the right, you can see all the defined groups of persons in Matrix. Only those groups that have no inherited permissions are listed here. Otherwise, if people were moved to these groups, permissions would be granted without the user being aware of this.

Assigning a person to another group

- First, select the person (or several persons) whom you want to assign to a new group.
- Afterwards, mark the new group in the right "Person Groups" field to which the person should be assigned.
- In the "Insert Position" field, you can further determine in what position the person will be inserted in this new group (at the beginning, end, or at the alphabetically correct position).
- After selecting these three settings, (Persons, New Group, Insert Position), click on the "Assign Group" button. The new group is shown for the marked person(s) in the "New Group" column.
- Additional persons can now be assigned to other groups via the same process.
- In order to cancel the assignment of a person to another new group, select the person and then press the "Remove Group" button. The group is then deleted again from the "New Group" column.
- For the effective assignments of the new groups, ensure to confirm via the "Apply" button.

NOTE! When a person is moved, the inherited group authorizations are not copied. Authorizations directly assigned to the persons will be copied.

5.4 Importing doors and locations from GAT ACE

The doors in Matrix, which are monitored and controlled by the controllers, are imported from GAT ACE 3000/7000 by selecting the “Import Doors and Locations” option from the “Tools” menu. With this option, the locations from GAT ACE 7000 are also imported into the matrix.

When using SALTO ProAccess SPACE software, the doors and locations can also be imported from this software into Matrix. This is done using ProAccess SPACE Synchroizer (see chapter "5.5 Importing doors and locations from SALTO ProAccess SPACE").

The import is completed using a wizard that helps you to classify the doors and locations accordingly in Matrix.

► For the import, select "Import Doors and Locations" from the "Settings" menu.

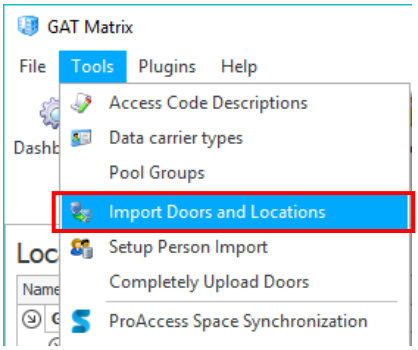


***Figure 5.6** – Option for importing doors and locations*

The doors and locations are configured in GAT ACE. The door names are also defined in GAT ACE and loaded into Matrix.

NOTE! The address of the GANTNER offline doors must always be unique in Matrix, i.e., do not use the same address twice. This is particularly important when operating multiple instances of GAT ACE as the same address could be used multiple times in every GAT ACE.

- A window opens in which a group must be selected.

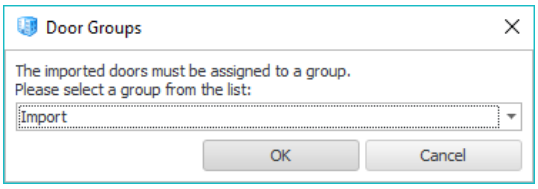


***Figure 5.7** - Selecting the door group for import*

- The doors added in the next step are inserted in the group selected here. After confirming with "OK", the following window opens.

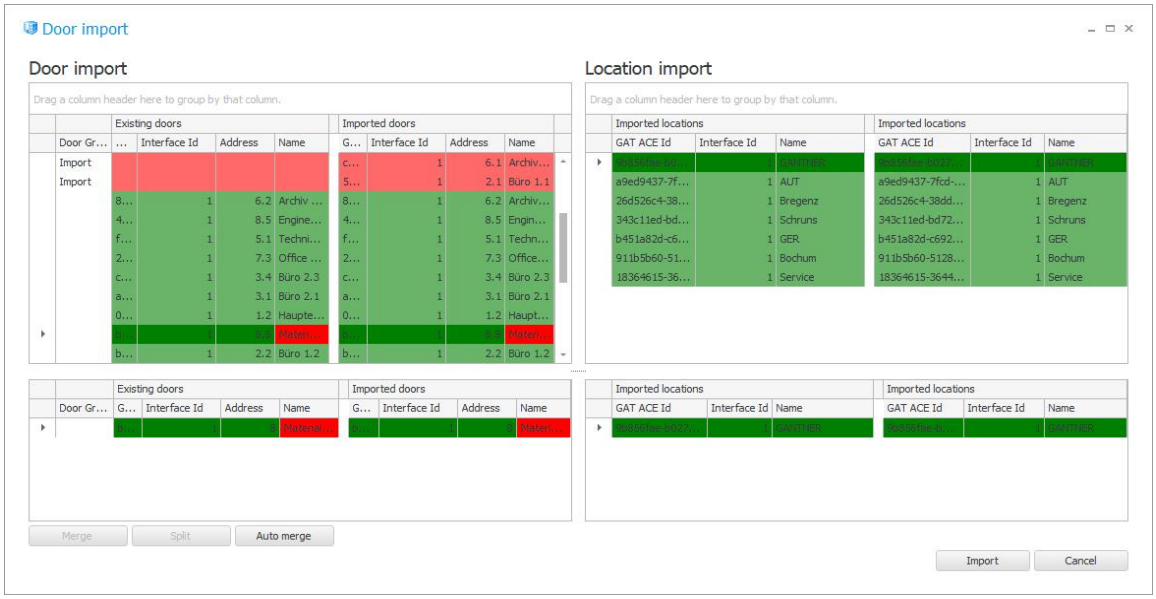


***Figure 5.8** - Importing doors and locations*

In this window, shown under "Door Import" are the existing and imported doors and on the right under "Location Import", the existing and newly imported locations from GAT ACE are shown. The door import process is described first in the following pages with the location import carried out in the same way. For more information, see "5.4.2 Location import configuration".

5.4.1 Door import configuration

Shown in the door import list are the doors and their assigned door group (left column) that already exist in Matrix. Shown on the right side are all the doors that are currently configured in the connected GAT ACE.

Matches between Matrix and GAT ACE are displayed in green. These doors are present in both Matrix and GAT ACE and their data coincides (name, address, GAT ACE ID, Interface ID). However, if data has been changed, or the doors to be imported cannot be uniquely assigned to a door in Matrix, e.g., the name of a previously assigned door has changed in GAT ACE, this is shown in red. In the figure below, the name of the door "Local 3" has been changed in GAT ACE to “Local 4 new".

With the "Split" and "Merge" buttons, you can unlink and link doors in Matrix with the corresponding doors in GAT ACE. This is useful, e.g., when after deleting a controller in GAT ACE and adding a new one you now want to assign the doors from the deleted controller to the new controller in Matrix.

Example:



Figure 5.9 *- Door import example – incorrect assignment*

The controller for the doors "Local 2", "Local 3", and "Local 4" has been deleted in GAT ACE and a new controller with 2 doors "Local 2 new" and "Local 4 new" was added. According to the existing addresses, Matrix automatically assigns door "Local 2" to "Local 2 new" and "Local 3" to "Local 4 new". However, if you want to assign the new door "Local 4 new" to "Local 4" in the existing Matrix, proceed as follows:

► Select the assignment that you want to remove (see Figure 5.**9**).

► Click on "Split".

- The assignment is separated.

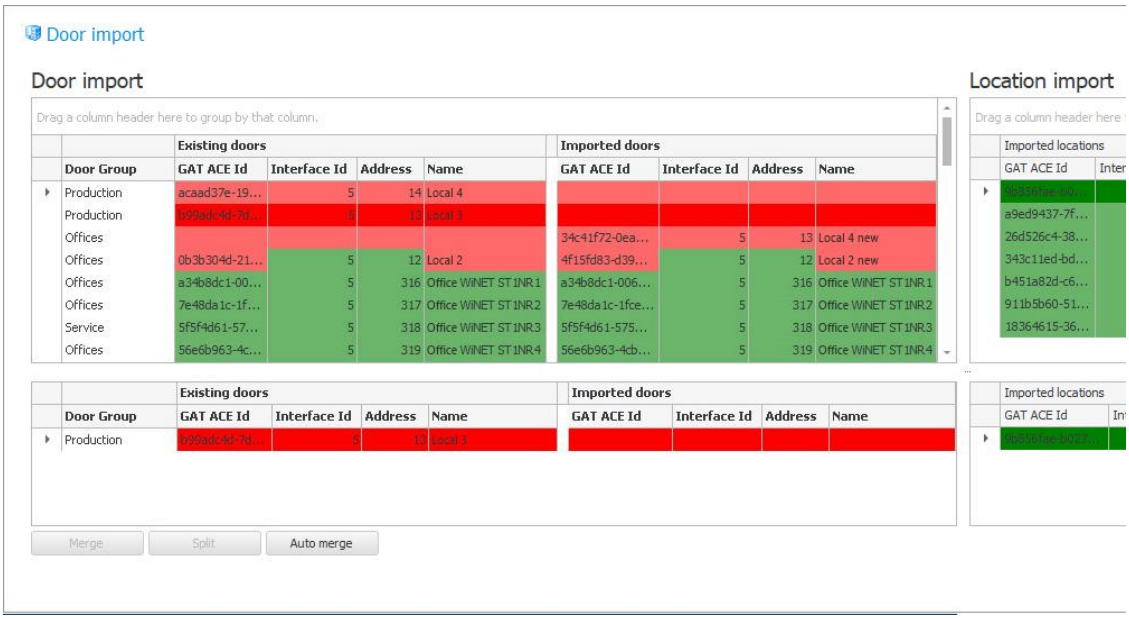


Figure 5.10 *- Door import example – assignment separated*

► While pressing "Ctrl", click on the two doors to be connected (in the following example, this is door "Local 4" in the left list and door "Local 4 new" in the right list).



***Figure 5.11** - Door import example – marking door and controller for new assignment*

► Click on "Merge".

- The allocation is redefined so that "Local 4 new" is reassigned to the door "Local 4".

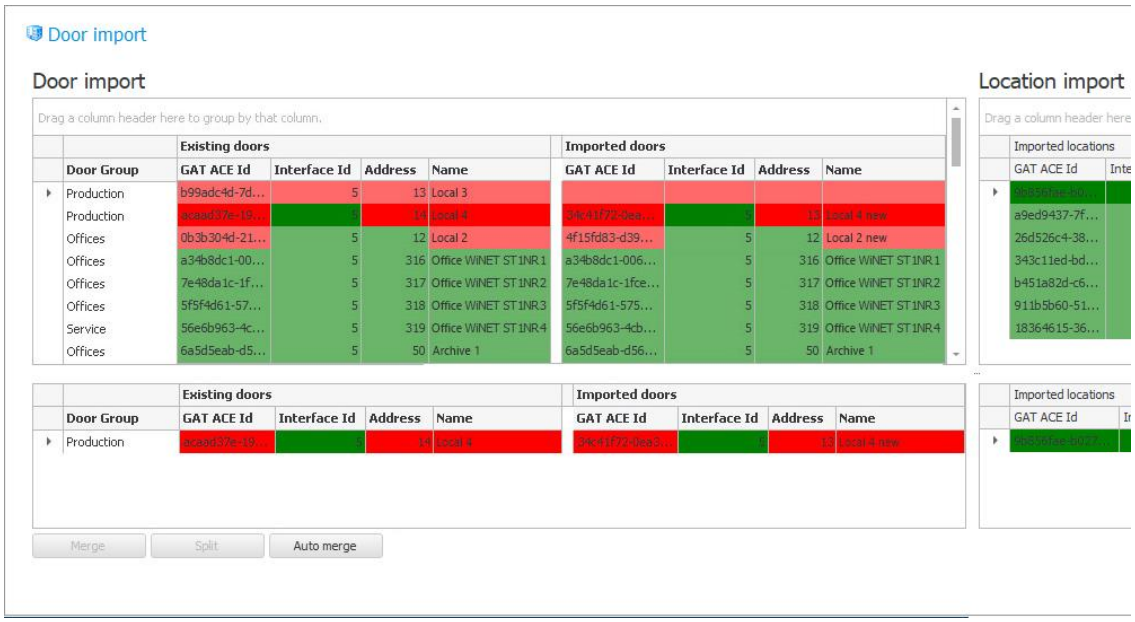


***Figure 5.12** - Door import example – new assignment*

Doors can be assigned to a different group later (see below and in “5.3.1 Moving persons or doors between groups").

After the doors are imported, they are assigned to their chosen groups and displayed in the header of the matrix.

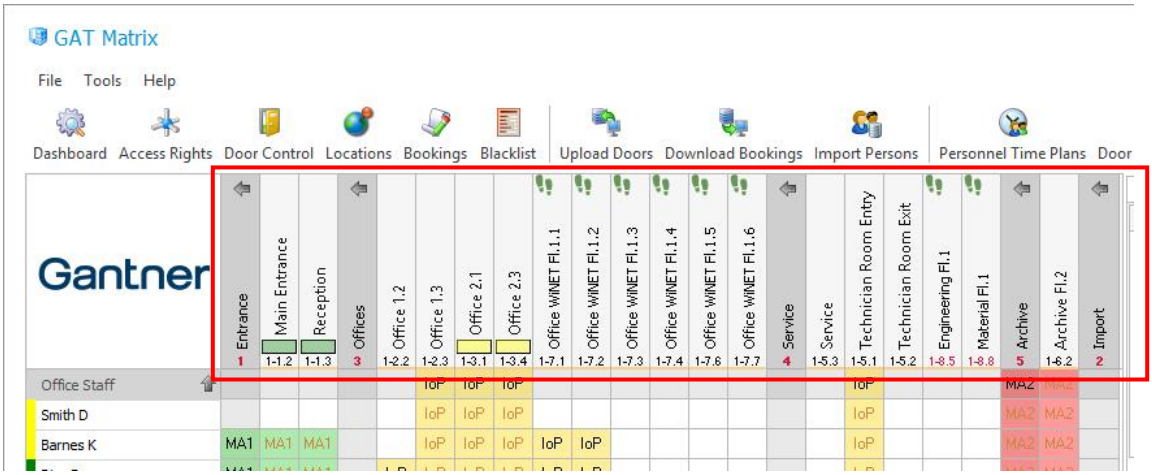


Figure 5.13 *- Controller/door display in main window*

Doors are displayed with the name and address that were assigned to them in GAT ACE. In addition, displayed before each address is the unique ID of the GAT ACE client where the door was originally configured.
For example, in Figure 5.***13*** the "Back Entrance" door has an address of "16" and was configured in GAT ACE with unique ID 5. The door address cannot be changed. The name of the door can be changed in GAT ACE. It should be noted for the next door import of GAT ACE that changed names must be linked manually to the corresponding door in Matrix (see "5.4 Importing doors and locations from GAT ACE").

For offline doors, a footsteps symbol is displayed when changes to the door settings and associated authorization data were made but the changes have not been loaded into the offline lock yet. A red X symbol indicates that the door is set to inactive in GAT ACE or that the door in GAT ACE has been deleted.

Blue colored doors represent open commands that have not been loaded from GAT ACE to the controller.

Arranging doors in the groups:
It is possible to move terminals to other locations, even to other groups, by holding down the SHIFT key while dragging the terminal to the new location with the left mouse button. In order to move several doors simultaneously, you can use the function "Move Doors" from the pop-up menu of the door groups (see section "5.3.1 Moving persons or doors between groups").

5.4.2 Location import configuration

Together with the door import, the locations from GAT ACE 7000 are also imported into Matrix. The import is configured in the same window.

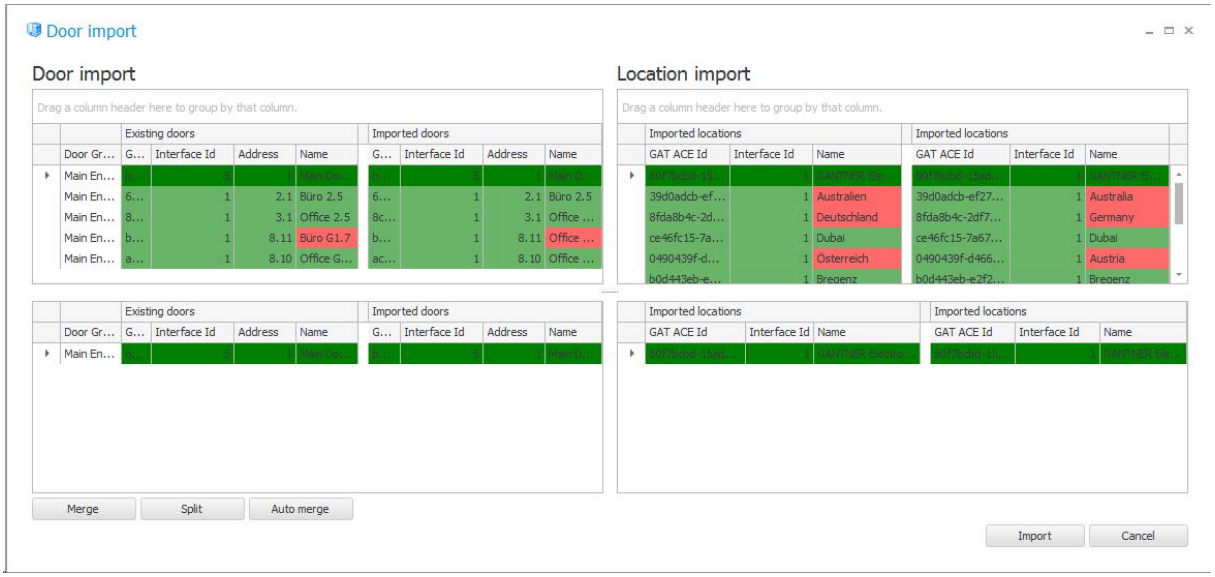


***Figure 5.14** – Location import*

On the right side of the window under "Location Import", you will see the existing locations in Matrix on the left and the locations to be imported from GAT ACE 7000 on the right. If locations have already been imported, locations already existing in Matrix are automatically assigned to the correct locations in GAT ACE. Correct assignments are displayed in green. If locations have changed in GAT ACE, e.g., new locations or name changes, these lines are highlighted in red. In the example above, the name of the location "Deutschland" in GAT ACE has been changed to "Germany".

► Here you can edit the assignment of the locations as described in the door import.

► If the assignments are correct, click on "Import".

You can access the list of locations via the "Locations" icon in the toolbar (see "6.2 Locations"). There you can assign a separate corporate calendar to each location.

5.4.3 Description text for doors

Additional text with any information can be entered for each door. This text is displayed when the mouse pointer is placed over the door name.

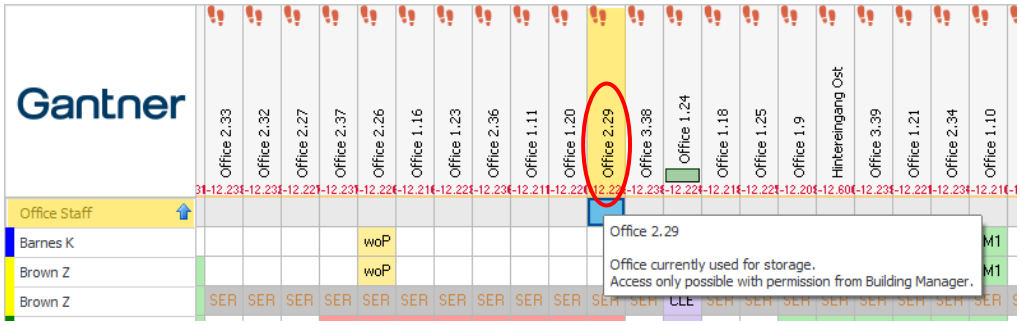


Figure 5.15 *- Door information for the "Office 2.29" door*

► To enter information for a door, double-click on a door in the matrix view.
  - The "Edit door" window opens with the settings for the door.

► Open the "Additional information" tab.

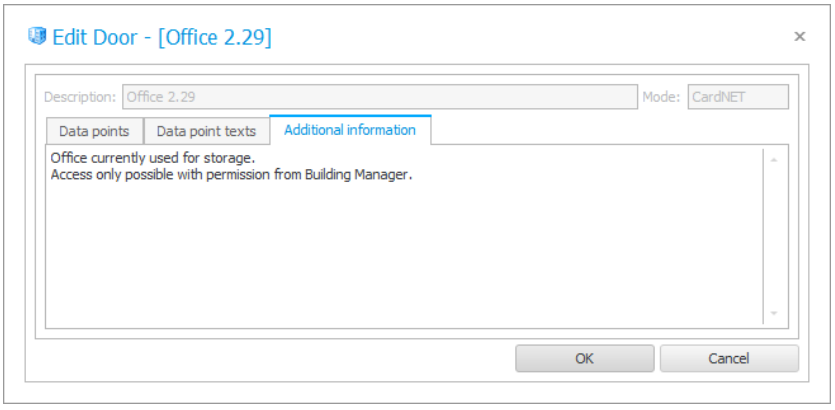


Figure 5.16 *- Enter additional door information*

  - You can enter any text for the door here.

► Confirm by clicking on "OK".

NOTE! The setting that defines which Matrix user may enter and display additional information can be specified in the user and role setting (ID 44, see "9 AUTHORIZATION MANAGEMENT").

5.4.4 Display of the battery-powered or wired GAT DL 73xx electronic locks

The battery-powered GAT DL 73xx electronic door locks from GANTNER are also imported from GAT ACE 7000 to Matrix and displayed in the upper door list.

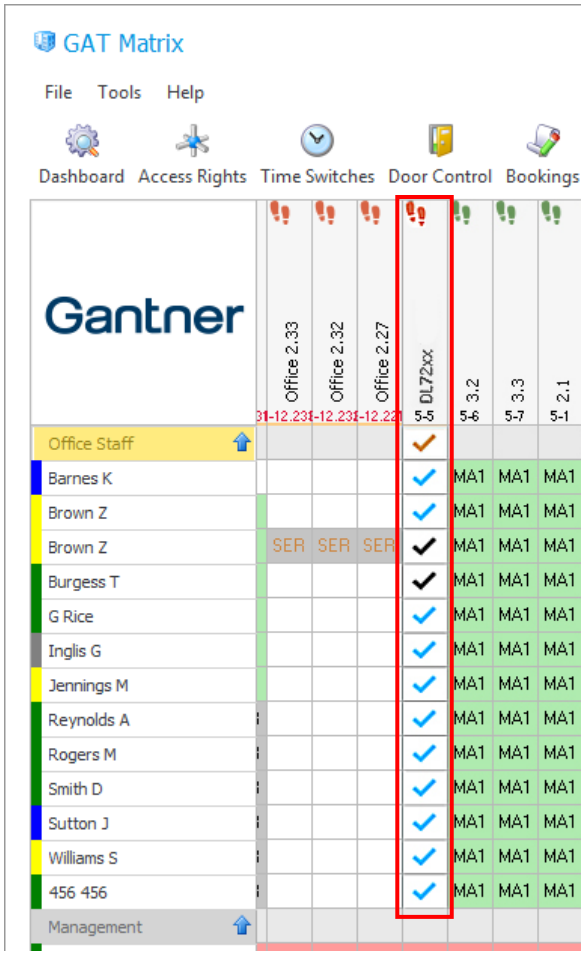


***Figure 5.17** – Display of the GAT DL 73xx door*

In contrast to the online doors, the following differences must be noted for the battery-powered GAT DL 73xx locks:

- An assigned personnel schedule is not shown with the abbreviation of the schedule but only with a tick symbol. The color of the tick corresponds to the normal inheritance rules (black -> directly assigned, yellow -> inherited from a group, blue -> inherited from a door and person group).
- No special authorizations can be assigned.
- No door schedules can be assigned.
- The settings for door control are not available.
- The bookings of these locks cannot be displayed via the context menu.
- In reports, the virtual schedule "0: Generic time plan for standalone devices" is displayed for these locks.

5.5 Importing doors and locations from SALTO ProAccess SPACE

To import the doors and locations from SALTO ProAccess SPACE, you can use ProAccess SPACE Synchronizer. This will help you to arrange the doors and locations in Matrix accordingly.

The locations in Matrix are called "partitions" in ProAccess SPACE. Locations are used to set different operating calendars for different devices or locations.

► For the import, select the "ProAccess Space Synchronization" menu item in the "Settings" menu.

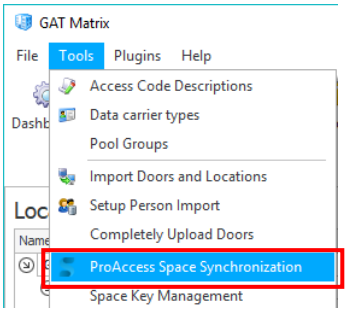


***Figure 5.18** - Option for importing doors and locations from ProAccess SPACE*

○ The SALTO ProAccess SPACE Synchronizer window opens.

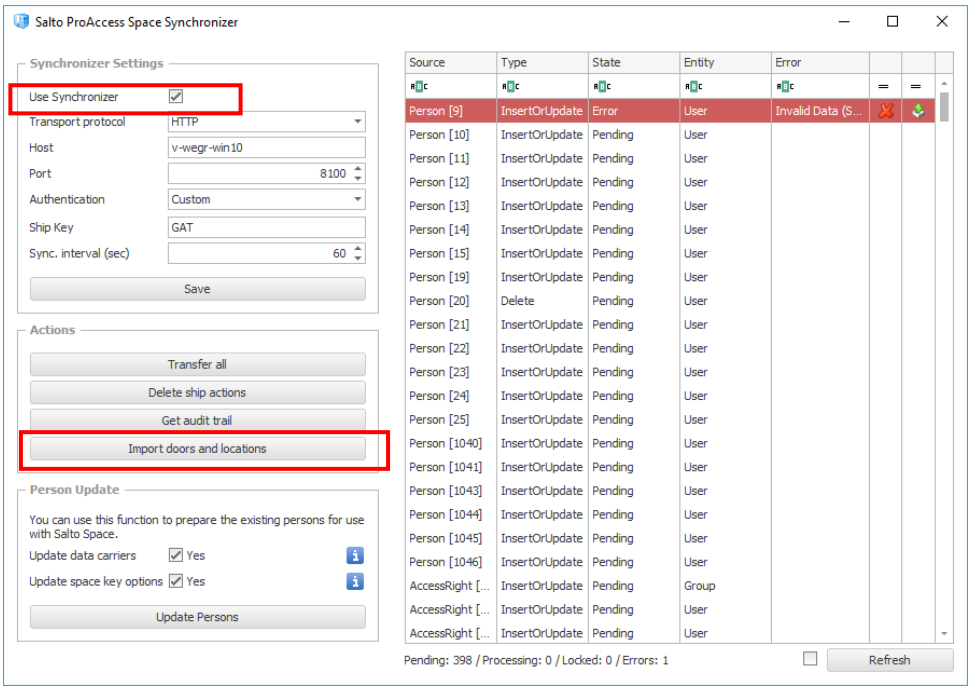


***Figure 5.19 –** SALTO ProAccess SPACE Synchronizer*

► The ProAccess SPACE Synchronizer must be enabled via the “Use Synchronizer” option.

NOTE! When the synchronizer is activated, the person names in Matrix are checked to ensure that they are unique as this is required for ProAccess SPACE. A note is displayed if the names are not unique.

○ If the ProAccess SPACE Synchronizer is activated, a window opens that asks whether Matrix should automatically convert the existing GANTNER time plans for SALTO systems. With "No", you can

proceed without converting the time plans. With "Yes", the time plans defined in the GANTNER system are converted to the time plans in a SALTO system.

For the personnel time plans, the functions are not converted into the SALTO functions, as these functions are defined via the door time plan in the SALTO system.

For the door time plans, the functions (e.g., office function, general open function) are converted to the corresponding SALTO functions.

Further information on the SALTO and GANTNER time plans and the conversion process can be found in the sections "5.11. Defining personnel time plans" and "5.12. Defining door time plans".

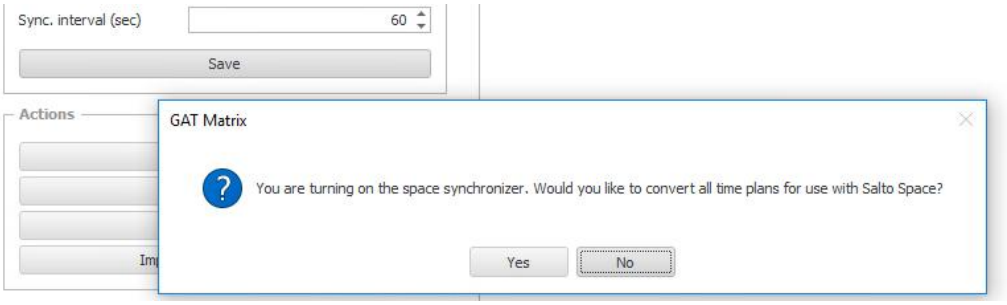


***Figure 5.20** – Query for automatic time plan conversion*

► To import the doors and locations, click the “Import doors and locations” button.

○ The window for selecting the door group opens.

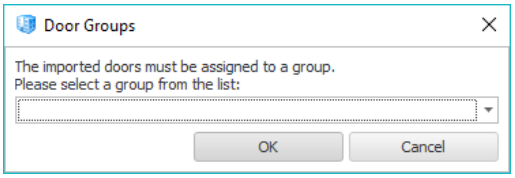


***Figure 5.21** – Selecting the import door group*

► Select the Matrix door group that you want to import the ProAccess SPACE doors to. This is used by default for newly imported doors but can be changed manually for the desired doors in the next step. Confirm with "OK".

○ The import window opens.

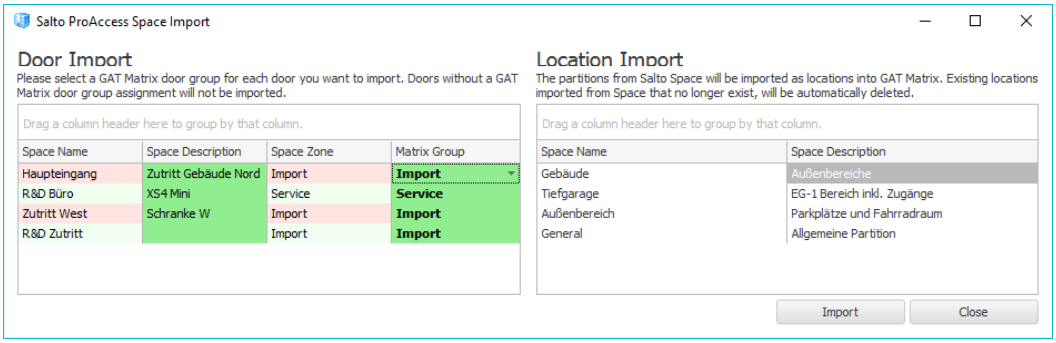


***Figure 5.22** – Import window for SALTO ProAccess SPACE software*

The doors and locations ("partitions") themselves are configured in ProAccess SPACE. The door names are also defined in ProAccess SPACE and loaded into Matrix.

NOTE! The addresses of the doors must always be unique in Matrix, i.e., no address may be duplicated. This is especially important when using one or more instances of GAT ACE. As ProAccess SPACE manages the addresses itself, this does not have to be observed with ProAccess SPACE.

In this window on the left side under "Door Import", you can see the SALTO doors that currently exist in Matrix (green) and the new doors that are yet to be imported (red). On the right side under "Location Import", the existing (white) and new locations to be imported (green) from SALTO ProAccess SPACE are displayed.

5.5.1 Configuring the import of doors and locations

In the "Door Import" list, all the doors defined in SALTO ProAccess SPACE are displayed. The doors that are already imported and present in Matrix are displayed in green with the door group that they are assigned to ("Matrix Group" column). The new doors that have not yet been imported into Matrix are displayed in red and the "Matrix Group" column contains the previously selected door group.

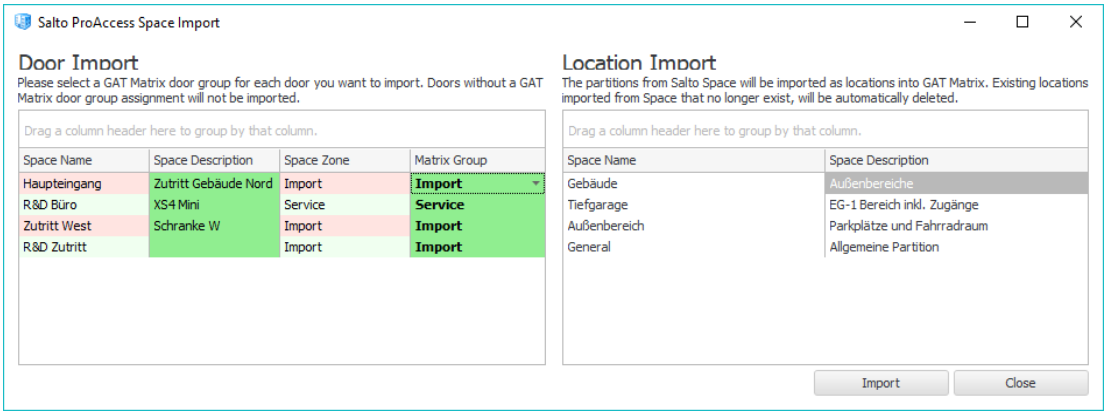
If data has changed for existing doors or the doors to be imported cannot be clearly assigned to the doors in Matrix, e.g., if the name of a door that has already been imported was subsequently changed in ProAccess SPACE, this is shown in red. Additionally, if, for example, the matrix group of a door already imported into Matrix has been changed in ProAccess SPACE, the group is displayed in red in the "Matrix Group" column.

► For each door, select the door group in the "Matrix Group" column that the door is to be imported into.

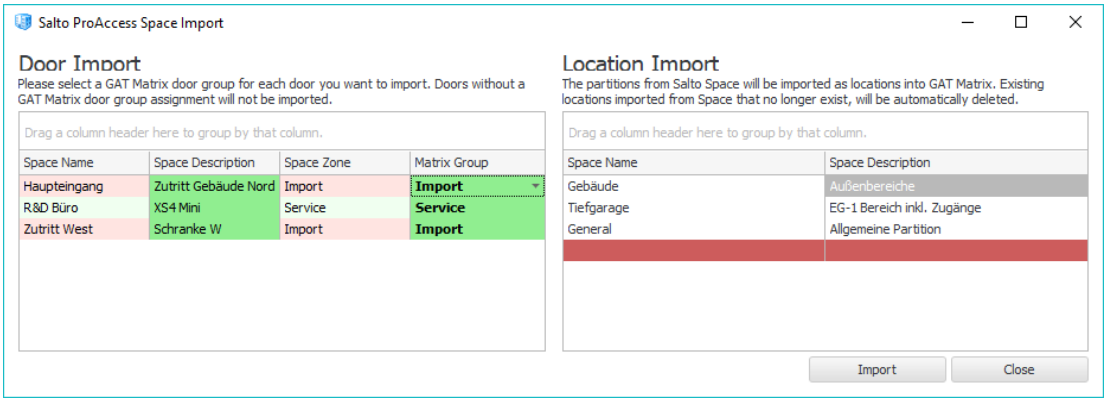
Notes: For instructions on how to create door groups, see "5.3 Person groups and door groups".
Doors that are not assigned to a matrix group (red) are not imported.

► Check the "Location import" list. Here you can see the locations defined in SALTO ProAccess SPACE and in Matrix. In ProAccess SPACE, these are called "Partitions".

- Lines marked in white are locations that have already been imported into Matrix with rows marked in green representing the new locations (partitions).



- Rows marked in red are locations that exist in Matrix but have been deleted in ProAccess SPACE. These locations will also be deleted in Matrix during the import.



► Click on "Import".

○ The imported doors are displayed for the selected group in the header of the matrix. For Salto doors, the blue text "Salto" is displayed below the door name.

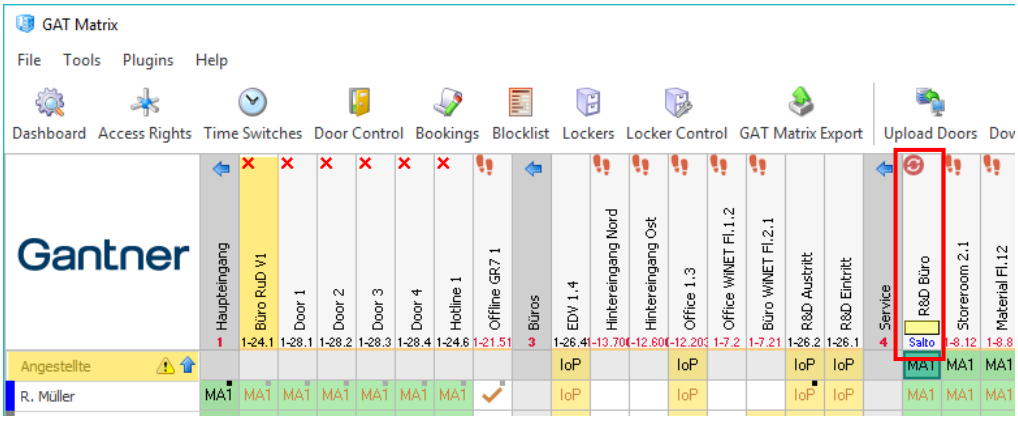


***Figure 5.23** - Imported SALTO doors in the main window*

The circle icon on an online or offline door indicates that this door needs to be reloaded.

For GANTNER offline doors, the feet icon ( ) is displayed if changes have been made to the door settings and related authorization data and these have not yet been loaded into the associated offline lock.
A red X symbol ( ) indicates that this door is set to inactive in GAT ACE or that the door has been deleted in GAT ACE.

Doors with a blue background still have commands open that have not yet been loaded from GAT ACE to the controllers.

Arranging doors in the groups
Doors can be moved to another position in a group. To do this, drag the door with the left mouse button to the desired position. To move several doors at the same time, you can use the "Move doors" function via the menu of the respective door groups (see "5.3.1. Moving persons or doors between groups ").

- The imported locations are displayed in the operational calendar view.

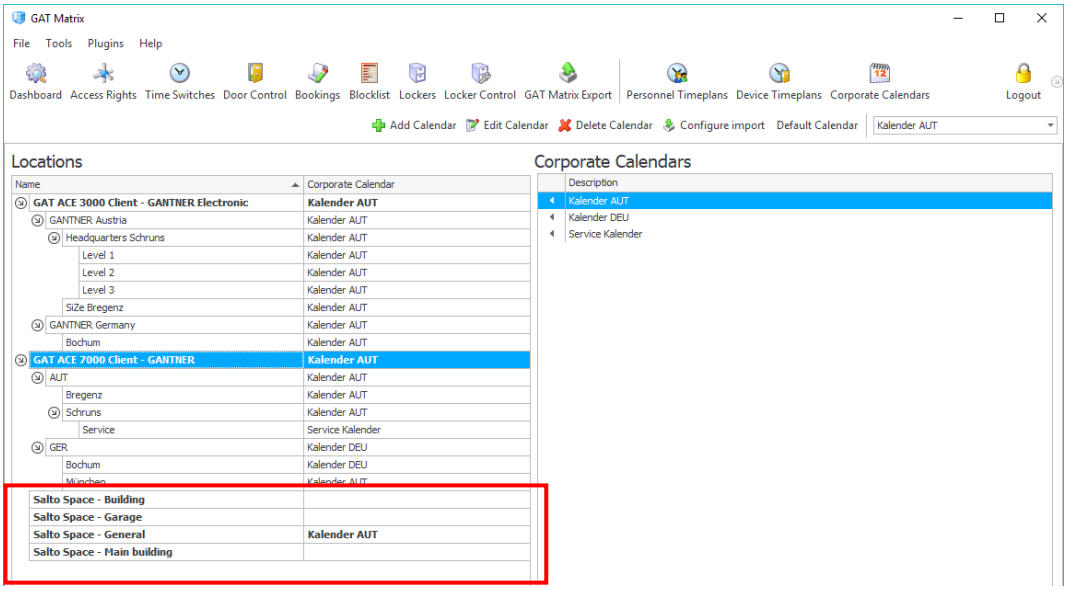


***Figure 5.24** – Imported SALTO partitions (locations) in the corporate calendar view*

5.5.2 Description text for doors

An additional text with any information can be entered for each door. This text is displayed when you hover the mouse pointer over the door name. This is also possible for SALTO doors. Note that this info text is not stored in SALTO ProAccess SPACE and is only displayed in Matrix.

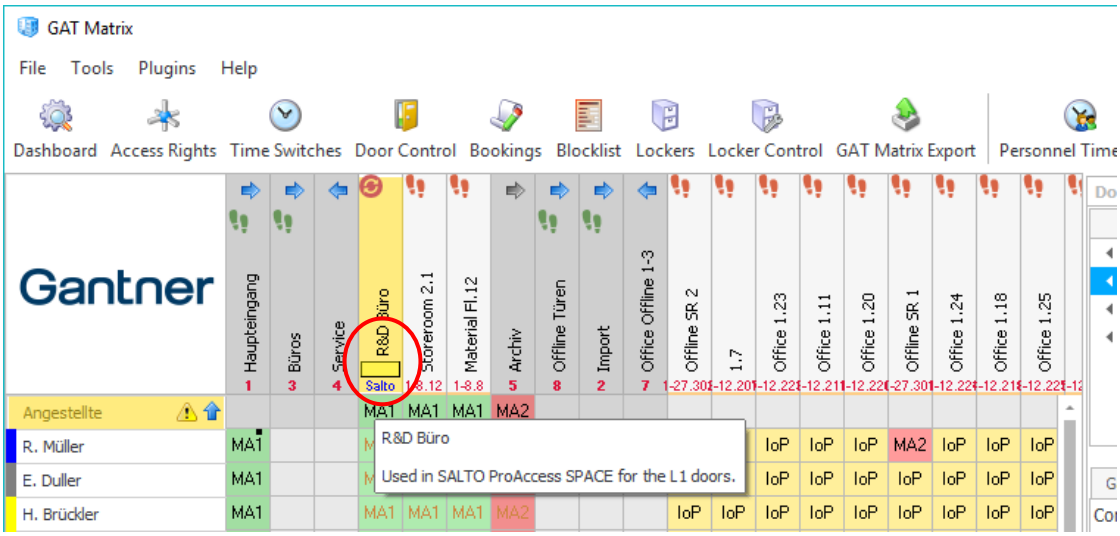


***Figure 5.25** - Door information for the SALTO "R&D" door*

► To enter the texts for doors, double-click on a door in the matrix view.
  ○ The "Edit Door" window opens with the settings for the door.
► Open the "Additional information" tab.

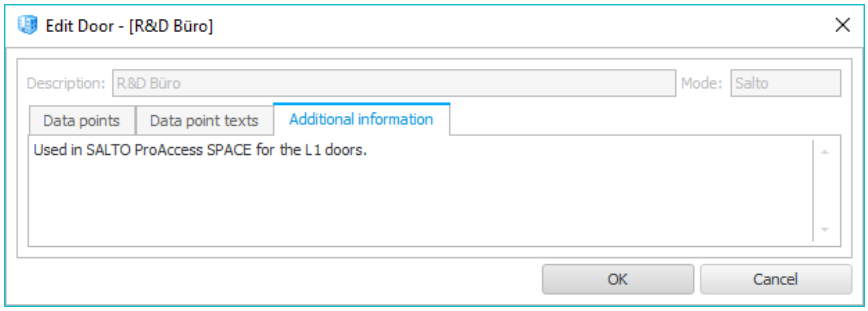


Figure 5.26 *- Entering door information*

  ○ Here you can enter any text for the door.
► Confirm by clicking on "OK".

NOTE! The setting that defines whether the matrix user is allowed to enter and display additional information is configured in the user and role settings (ID 44, see chapter "9 AUTHORIZATION MANAGEMENT").

For doors that are imported from ProAccess SPACE (see next page), a description text can be entered in the door definition.

► In Salto ProAccess SPACE, switch to the door display ("Access points" -> "Doors" -> Display door or add new door.
► The name of the door is entered in the "Name" field and the description text can be entered in the "Description" field next to it.
  ○ The description text is displayed in Matrix when you move the mouse over the door name in the header of the matrix.

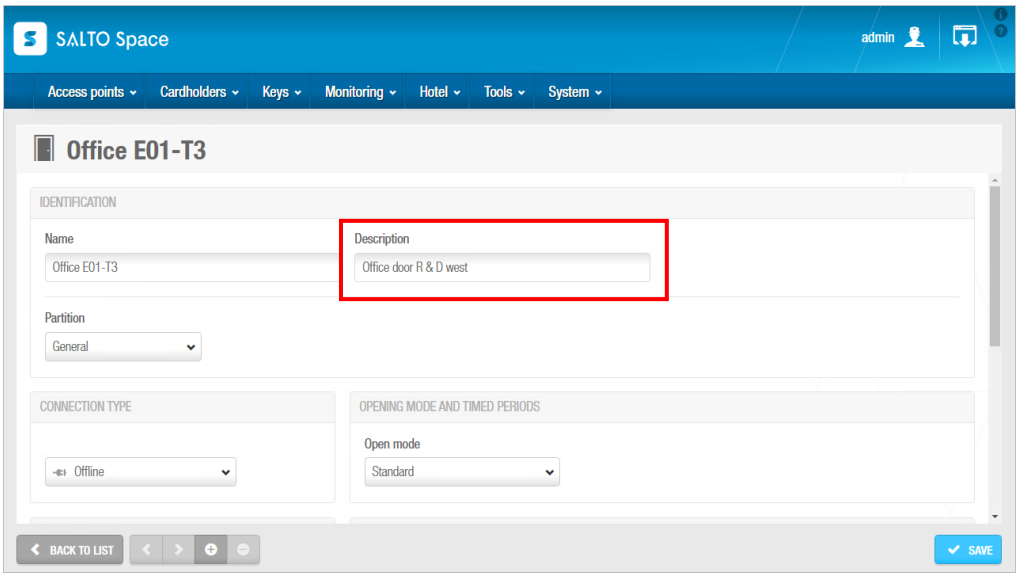


Figure 5.27 *- Entering door information in Salto ProAccess SPACE*

5.5.3 Display of SALTO locks and users (door import from ProAccess Space)

If locks or doors, which are configured and operated in the ProAccess Space software, are imported into Matrix, the assignment of authorizations can be completed in Matrix. The imported doors and authorizations are then displayed in Matrix as follows.

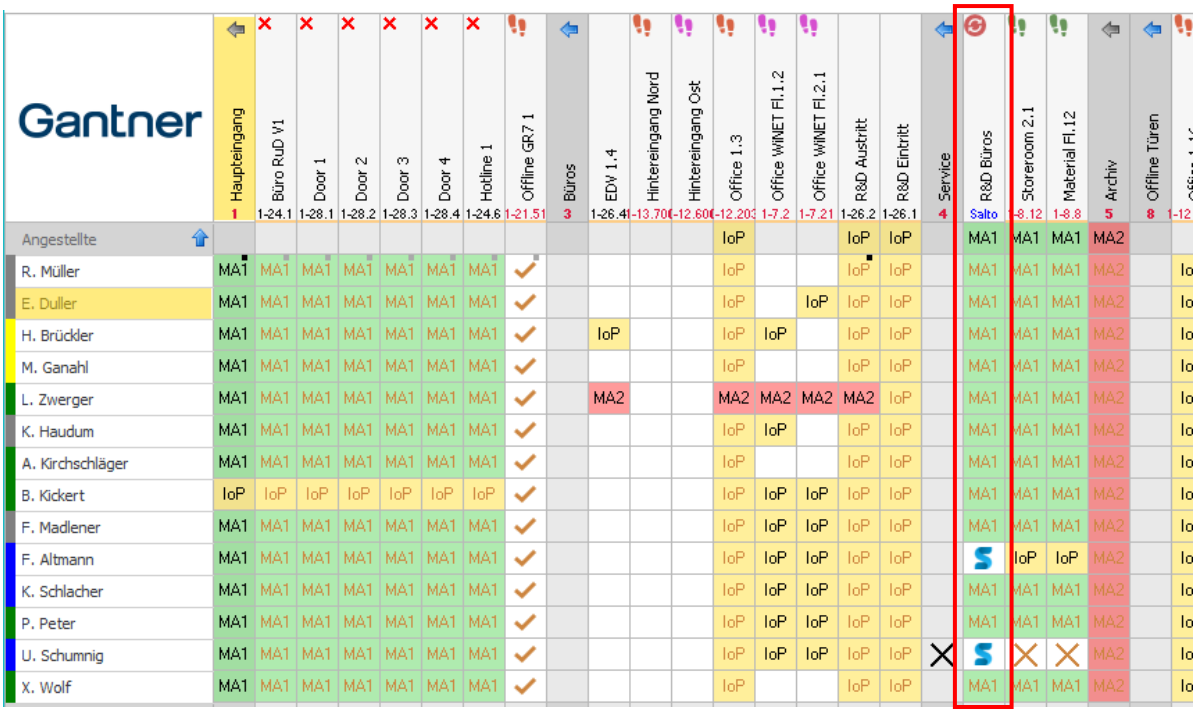


***Figure 5.28** - Display of doors and users from ProAccess Space*

Data such as doors imported from ProAccess Space are also indicated accordingly:

- For a door imported from ProAccess Space, "Salto" is displayed in blue font.
- A SALTO door cannot be used as a time switch.
- A Salto door can also be assigned more than one plan per person by inheriting permissions. The plans are added together. In this case, a blue "S" (S) is displayed and the resulting authorization is displayed to the right on the Salto tab.



Example: If a plan is assigned to a person group for a ProAccess SPACE door, this time plan is also inherited by all persons in the group (in the example, "MA1" for the "Employees" person group). If a different time plan is manually assigned to a person, this is indicated with a blue "S" symbol. The same applies if the time plan is assigned to the door group via inheritance.

5.6 Editing the master data of a person in the authorization matrix

- ► To add a new person to the authorization matrix, right-click on a person group in the left column of the matrix.
- ► Select "Add person" from the menu that is displayed.
  - ○ The following window is displayed. Figure 5.**29** provides an example with information filled in.

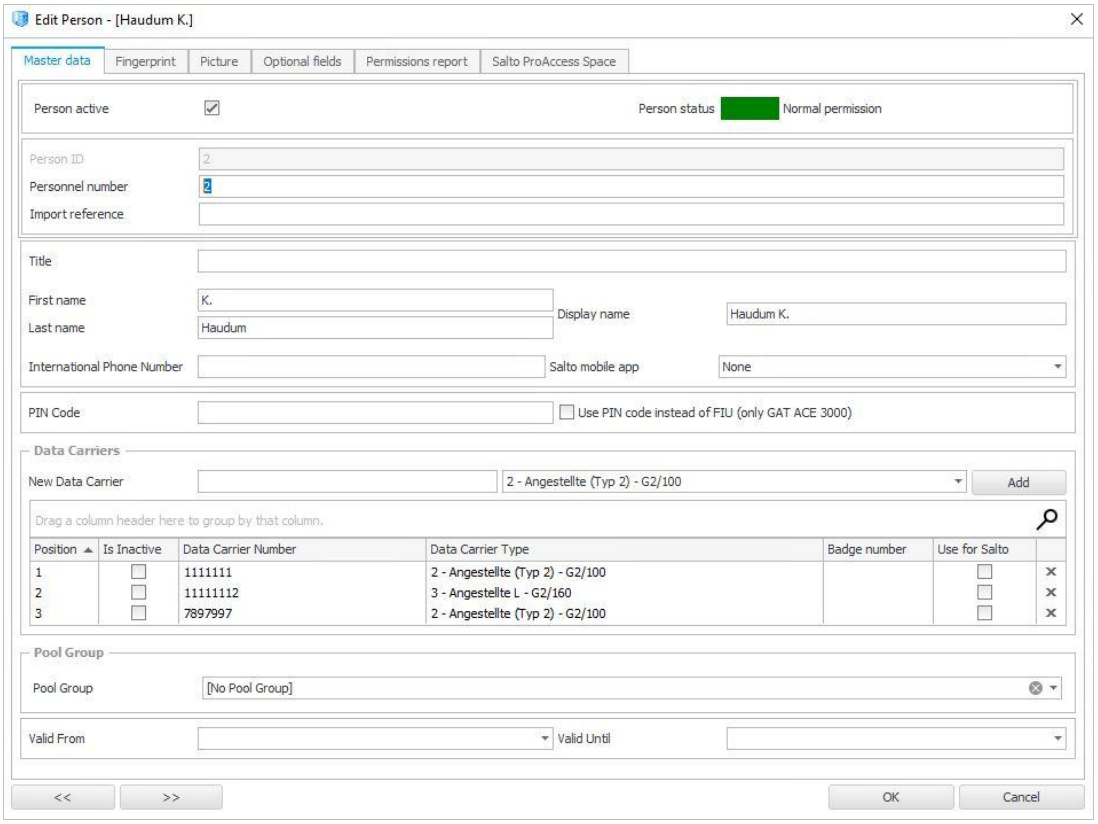


Figure 5.29 *- Defining personnel data*

The personnel data of the person is defined in this window. This process is described in the following pages.
The top-right "Person status" colored field displays the current status of the person (active or inactive, valid data carrier, valid validity period) in the defined color and as text. The status color is also displayed for each person in the matrix and the colors are configurable, see "4.10 Settings for person display" for more information.

The "Optional fields" tab is only displayed when at least one optional field is configured in the settings of Matrix (see "4.11 Optional fields for personnel data" and "5.6.10. Settings for license plate recognition").

An additional tab “TBS Biometrics” is also available in this window when the optional TBS biometric system has been configured in Matrix (see "5.6.8 TBS system (biometrics)").
The Salto ProAccess Space tab is only displayed when using the ProAccess Space software.

5.6.1 Defining personnel master data

The following information for each person can be defined in the input fields of the "Personnel Data" tab:

- Person active: When this option is selected, the person is activated and processed in Matrix. When this option is not selected, the person is inactive, i.e., their personnel data remains in Matrix, but they have no authorization in the access system. A deactivated person is displayed in the matrix by default with a gray bar in front of the name.

- Picture: A picture can be added for each person, which is displayed in the personnel data window. If there is no picture, this field is not displayed. The image is added via the “Picture” tab (see below).

- Person ID: This number is used by Matrix to identify the person and the number cannot be changed.

- Personnel Number: Enter an arbitrary number for the person, e.g., according to the internal personnel numbering system used in your company.
  NOTE! For systems using GAT ACE 3000, the personnel number in the system must be unique when anti-pass-back checks are made, or fingerprints are to be used for identification checks.

- Import Reference: Here you can enter information that will be used as reference on personnel import (see section "5.7 Import persons"). This field is only shown when this setting was defined in the global settings (see "4.8 Global settings").

- Title: The title of a person can be entered here, if available.

- First/Last Name: Enter the first name and last name of the person.
  NOTE! If the person is to be used with the SALTO ProAccess Space devices, then as of Matrix 5.0 the order of the first and last names in Matrix must be set correctly so that the persons are displayed and sorted correctly in the booking display (see "Display Name" below and "7.1 Sorting, grouping, & filtering bookings"). As of Matrix V 5.1, this is no longer necessary as the linking of persons between Matrix and ProAccess SPACE is done using the "Ext ID" number.
  If two persons have the same first and last names, the same names can be entered here for both persons, however, the "Display name" must be unique (see next setting).

- Display Name: This text is used to display the person in the authorization matrix. The display name is generated by Matrix from the entered first and first name of the person and the title (according to the setting in the general options, see “4.10 Settings for person display) and automatically entered here. The display name can be changed any time if desired.
  NOTE! If the automatically generated display name is changed manually and the title, first name or last name is changed again later, the display name will change back to the automatically generated name.

- International phone number / Salto mobile app:
  If Salto ProAccess SPACE is being used, the system users can also use a mobile app to identify themselves at the terminals. "None" in this field means that this function is not used. If you want to use a mobile app, enter the relevant mobile number in the left text field and select the appropriate interface or mobile app in the right field. "JustIN_Mobile" is used by default for the JustIN app.
  You can find more information on the JustIN mobile app under "5.23 Configuring the SALTO JustIN app for access control".

- PIN Code: With a time plan it is possible to define that access for a person at a terminal shall only be granted with valid PIN code input at the terminal. The PIN code for the person can be entered here. Use only numbers for the PIN code. If specified, the PIN code can have a length of 1 to 8 digits.
  When the "Use PIN code instead of FIU (only GAT ACE 3000)" option is enabled, the person can enter their PIN code for verification instead of the fingerprint. This is especially helpful for people with weak fingerprint patterns.
  NOTE! The PIN code is only displayed if you click in the field. If the cursor is in another field, only stars "*" are displayed. Click at any time in the PIN-code field to display the PIN code again.

- Data Carriers: Here all data carriers that are assigned to the person are listed. A data carrier type is assigned to each data carrier. This allows different reader or data carrier technologies to be used together in one system. The different data carriers can be physically separate data carriers or combi data carriers that combine several data carriers on one physical medium (e.g., card).

  Please read section "5.6.3 Authorizing and configuring data carriers for persons" for a detailed description of the data carriers and the available settings.

- Pool Group: In this field, you can assign the person to a pool group. For more information on pool groups, see "5.8 Pool groups".

- Valid From / Until: To define a certain validity period for the data carrier(s), enter the start or end points for the period in the format "dd.mm.yyyy hh:mm". The date and time can be selected from a calendar by pressing the arrow buttons to the right of the input fields. It is not possible to specify both start and end time points. Whether a validity period is planned, is active, or has expired is displayed in the matrix with a corresponding color before the name.

  F. Rainer .. Validity period is defined but has not started yet

  X. Franz .. Validity period is active, or no validity period has been defined

  F. Roland .. Validity period has expired

  NOTE! These colors are configurable in the software settings (see "4.10 Settings for person display").

  NOTE! Be aware that this feature only works in GAT ACE during the one-time loading of personnel data into the controller.

  NOTE! For offline doors with the Read Only function (or in GAT ACE 3000 also with CardNET), only the “Valid to” time of the validity period is written onto the data carrier. Therefore, the "Valid from" time must be in the past and not in the future. Offline conflicts for these doors are indicated by a yellow triangle with exclamation mark and a clock icon when the valid from date is set in the future (see "5.2 Main window").

- Tabs:
  - "Fingerprint": In this tab you can scan fingerprints for the person, which requires a fingerprint reader. With this fingerprint data, the person can identify themselves at suitable terminals using a fingerprint. More information about this tab is available in chapter "5.6.7 Scanning fingerprints".
  - "TBS Biometrics": This tab is only displayed if the use of biometric data via the TBS system is enabled. More information on this is available in chapter "5.6.8 TBS system (biometrics)".
  - "Picture": In this tab, an image of the person can be selected. This is then displayed in the personnel window on the first "Master data" tab. The tab is only displayed if the use of personal images is activated in the options (see "4.10 Settings for person display").

- "Optional fields": Additional personnel data can be entered in this tab. You can freely define these fields in the matrix (e.g., vehicle license plate, telephone number or address of the person). Instructions on how to create optional fields can be found in "4.11 Optional fields for personnel data".

- "Permissions report": Shown after opening this tab is an automatically generated report that lists all authorizations, schedules, and locker authorizations configured for the person (via the Relaxx software). You can save this report as a PDF or print it out.
In the options, you can set to generate the person reports automatically every hour or to create the reports manually (see "4.8 Global settings").

- "Salto ProAccess Space": This tab is only displayed when SALTO ProAccess Space software is used. In this tab, you can define the functions and validity period for the data carriers to be used for the doors in ProAccess Space. In addition, the data carriers that the persons are to use for the ProAccess Space doors can be read and coded here. For more information, see "5.6.11. Personnel settings for SALTO ProAccess Space".

The “OK & New Item” button makes it simple to define multiple persons in Matrix. Clicking this button saves the current person and immediately displays a new window to define the next person. The button can also be accessed by pressing the key combination “CTRL + ENTER”.

When an existing person is processed, you can use the buttons "<<" and ">>" to go directly to the previous or next person in the group, without having to close the person window.

5.6.2 Settings for persons in ProAccess SPACE

Persons defined in Matrix can also be used in the ProAccess SPACE software. As of Matrix version 5.1, people are linked or identified using a unique ID number (called "Ext ID" in ProAccess SPACE). It is important to configure the correct settings for personal identification in ProAccess SPACE.

► From the "System" menu, select the option "General options" and then open the "Users" tab.

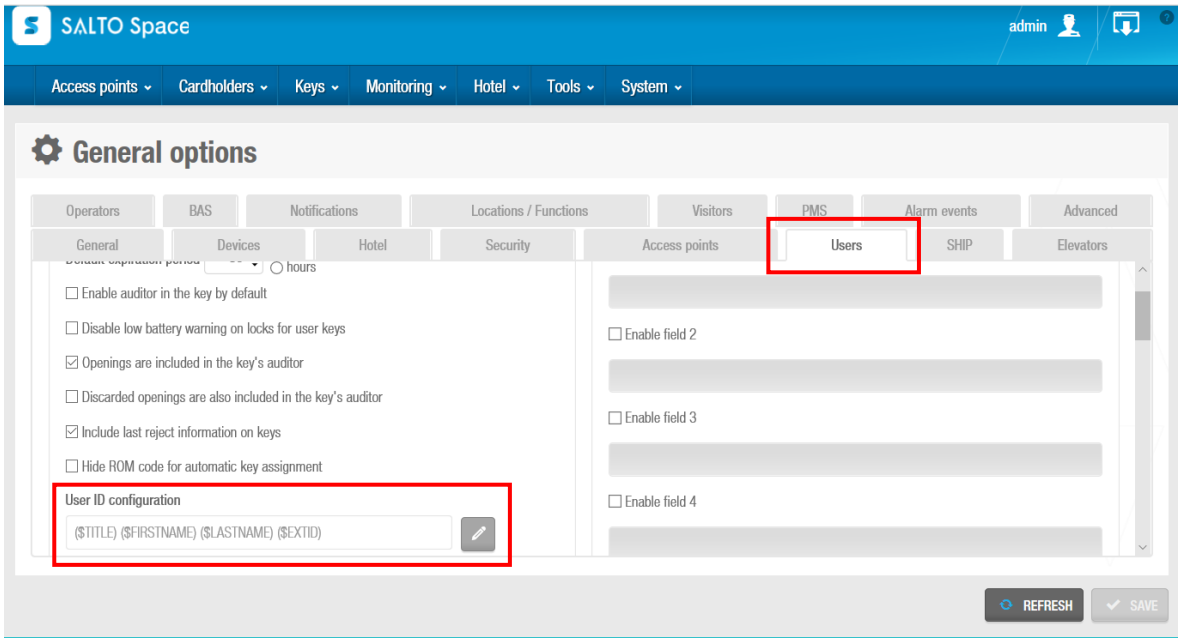


***Figure 5.30** - Defining the display name of persons with Ext ID*

► In the "User ID configuration" field, enter the desired name structure by defining the order of first name, last name, title etc. To do this, click on the edit icon and select the macros for the desired personnel data. Example: `($TITLE) ($FIRSTNAME) ($LASTNAME)` -> "Dr. John Doe"

► At the end of the macro, `($EXTID)` must be selected (see image above).

► Save the settings.

As of Matrix version 5.1, the identification of persons using Ext ID allows the names to be edited in Matrix at a later date (e.g. in the event of marriage) and for the persons to still remain linked to ProAccess SPACE using the Ext ID number.

The Ext ID number is generated automatically in ProAccess SPACE and shown in the personnel window (menu "Cardholders" -> "Users" -> double-click on a person).

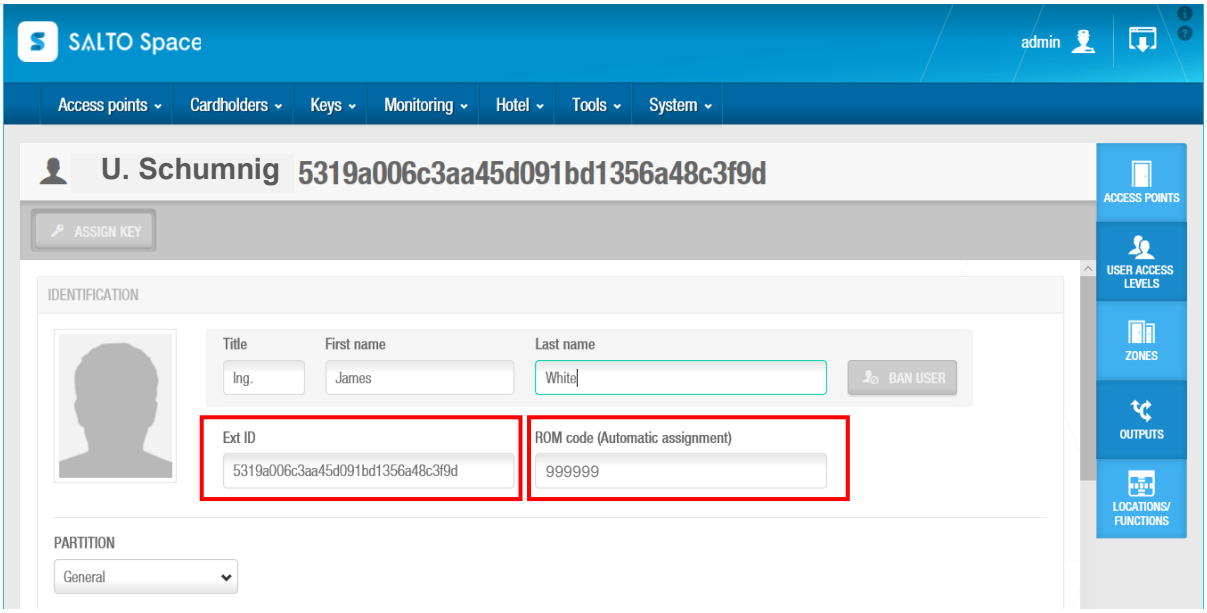


Figure 5.31 *- Personnel data in ProAccess SPACE*

The ROM code is also displayed in this window. This number corresponds to the data carrier numbers in Matrix and is only displayed if the data carrier is marked as "Use for Salto" in the personnel data in Matrix.

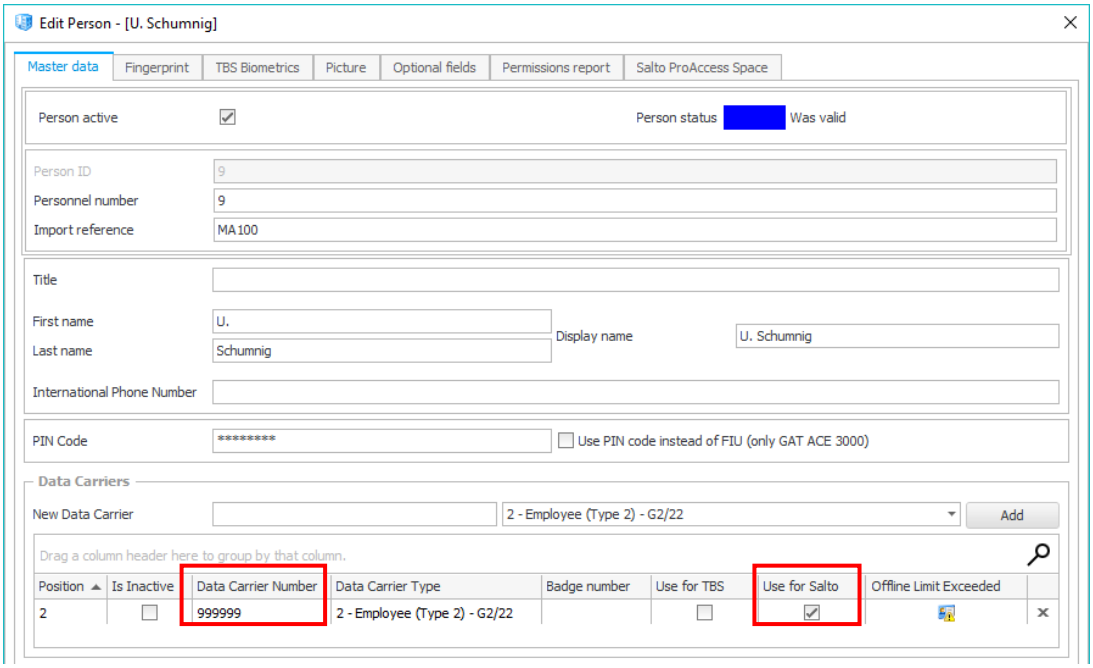


Figure 5.32 *- Personnel data in Matrix*

5.6.3 Authorizing and configuring data carriers for persons

At least one data carrier must be assigned to each person. The data carriers are used to identify the persons in the access system and are entered in the master data window.

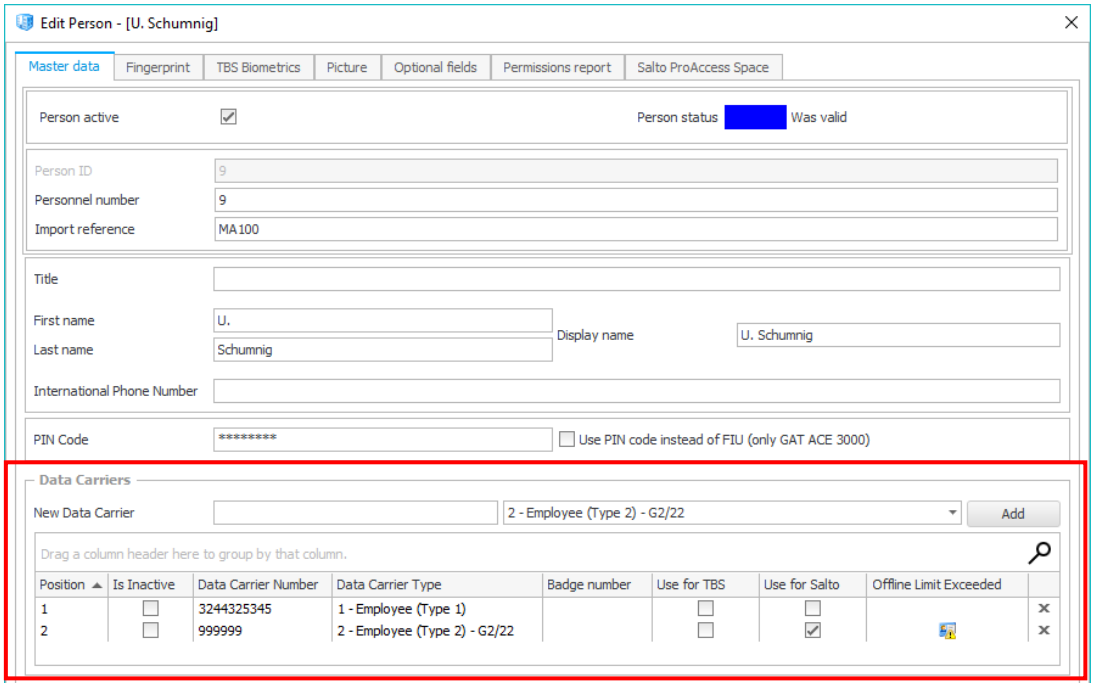


***Figure 5.33** - Define and assign data carriers for persons*

Every data carrier is assigned to a particular data carrier type. This allows different reader or data carrier technologies to be used together in one system. The different data carriers can be physically separate data carriers or combi data carriers that combine several data carriers on one physical medium (e.g., card).

► To assign a new data carrier, enter the data carrier number in the “New Data Carrier” field.

You can enter the data carrier numbers in decimal or hexadecimal format (e.g., dec: "1234" = hex: "4D2"). To enter the number in hexadecimal, first write "0x" followed by the number (up to 8 bytes). By pressing the enter key to confirm, the number is automatically converted to decimal format. Internally, Matrix always uses decimal format for the data carrier numbers.

► Select the type of data carrier from the menu to the right.

Data carrier types are defined via the “Data carrier types” option in the "Tools" menu (see "5.6.4 Defining data carrier types").

► Click on “Add” to finish.

► Alternatively, a read/write station (e.g., GAT Writer) can be used to read the data carrier number.

NOTE! For systems using GAT ACE 3000, a person may only use maximum one data carrier when an anti-pass-back check is to be made.

NOTE! For data carrier types that are used with GAT ACE 3000, the data carrier number must not be longer than 11 digits. For data carrier types for GAT ACE 7000, the data carrier number may also be longer.

It is possible to assign a data carrier directly from another person. For example, if a data carrier was assigned to a person and its validity period has expired, the data carrier is now "free" and can be reassigned to another person. Following assignment to the new person, the data carrier is automatically deleted when the previous person. Depending on the configuration in the general settings (see "4.10 Settings for person display"), this action is completed with or without a confirmation message.

► By selecting the options in the column ("Inactive"), the data carriers of a person can be activated or deactivated.

If a field is marked, the corresponding data carrier is temporarily disabled without deleting it completely. A person without an active data carrier has no access authorization as ID cannot be performed. People without active data carriers are displayed by default with a yellow bar in front of the person's name.

X. Franz .. Person with at least 1 active data carrier

K. Egon .. Person without active data carrier

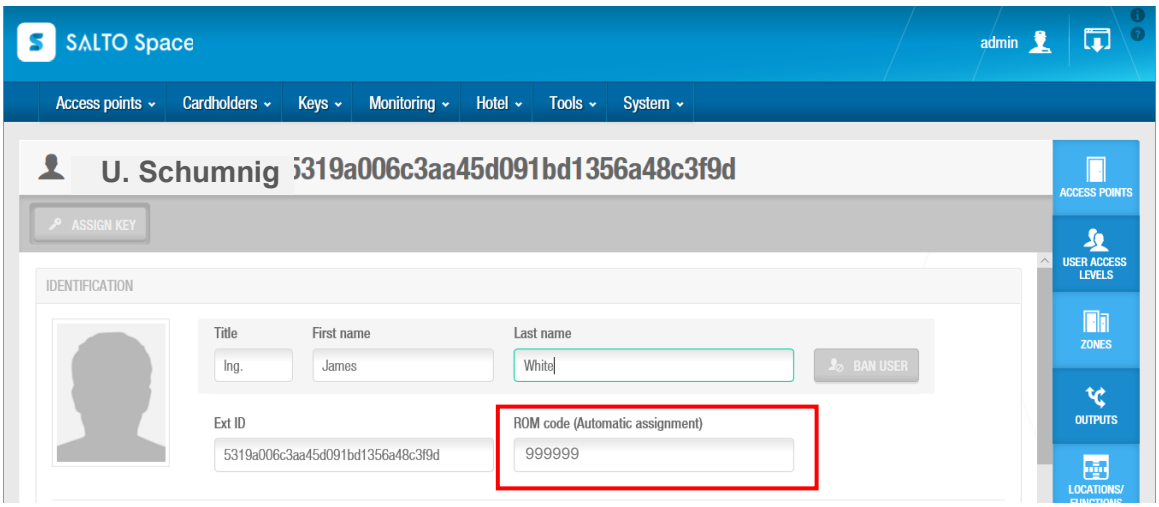
NOTE! These colors are configurable in software settings (see "4.10 Settings for person display").

► If the optional TBS biometrics system is installed, an additional "Use for TBS" column is displayed here (see "5.6.8 TBS system (biometrics)"). Here you can select the data carriers that are to be used with the TBS biometrics recognition system.

► If SALTO ProAccess SPACE is used, an additional column "Use for Salto" is displayed here (see "5.6.11.Personnel settings for SALTO ProAccess Space"). Here you can select the data carriers that are to be used in the ProAccess SPACE software.

Note: For existing data carriers, this selection can also be completed automatically (see "5.5 Importing doors and locations from SALTO ProAccess SPACE").

- After sending the updates of the personnel data from Matrix to SALTO ProAccess Space (see "5.5. Importing doors and locations from SALTO ProAccess SPACE"), each person who has the "Use for Salto" option enabled will have the data carrier number as ROM code entered.



NOTE! If a data carrier is used that has more permissions defined for offline doors than can be stored on it, a notification is displayed.

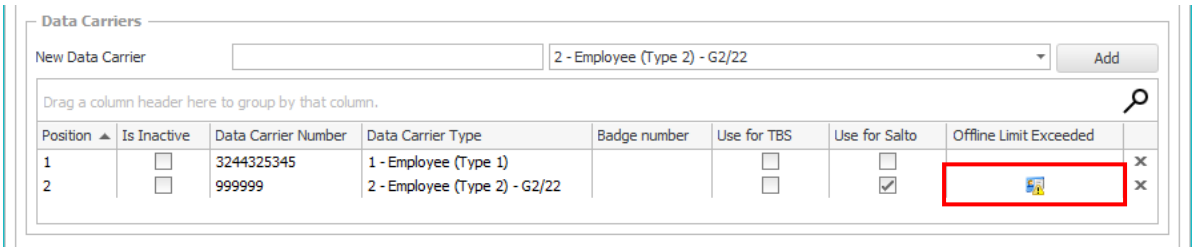


***Figure 5.34** - Exceeding the max. storable authorizations for offline doors*

Exceeding the offline limit (symbol shown in figure above) can be triggered by CardNET data for GANTNER products or SVN data for SALTO products.

The maximum number of CardNET and SVN permissions can be set when defining the data carrier types (see "5.6.4 Defining data carrier types").
If you delete a data carrier number, Matrix asks whether to automatically add the deleted data carrier to the blocklist. Selecting "Yes" adds the data carrier to the blocklist for all offline doors where the person had an access authorization. Selecting "No" only deletes the data carrier. See chapter “5.10 Data carrier blocklist” for information on the blocklist.

Automatic data carrier assignment

GANTNER uses coded ID numbers for the data carriers. These ID numbers can be used in the SALTO system to assign the data carriers to the persons.
For systems that have data carriers supplied by GANTNER with coding for GANTNER and SALTO, the settings required for this are as follows.

- ► In ProAccess SPACE, select “General options” from the “System” menu.
- ► Click on the “Users” tab.
- ► Scroll down to the "AUTOMATIC KEY ASSIGNMENT” section and select the “Automatic key assignment enabled" option.
- ► Enable the “SALTO user” option and the “#2” mode below it.
- ► Now enable the “CARD DATA” option.
  - This deactivates “CARD SERIAL NUMBER”, and other options are displayed.

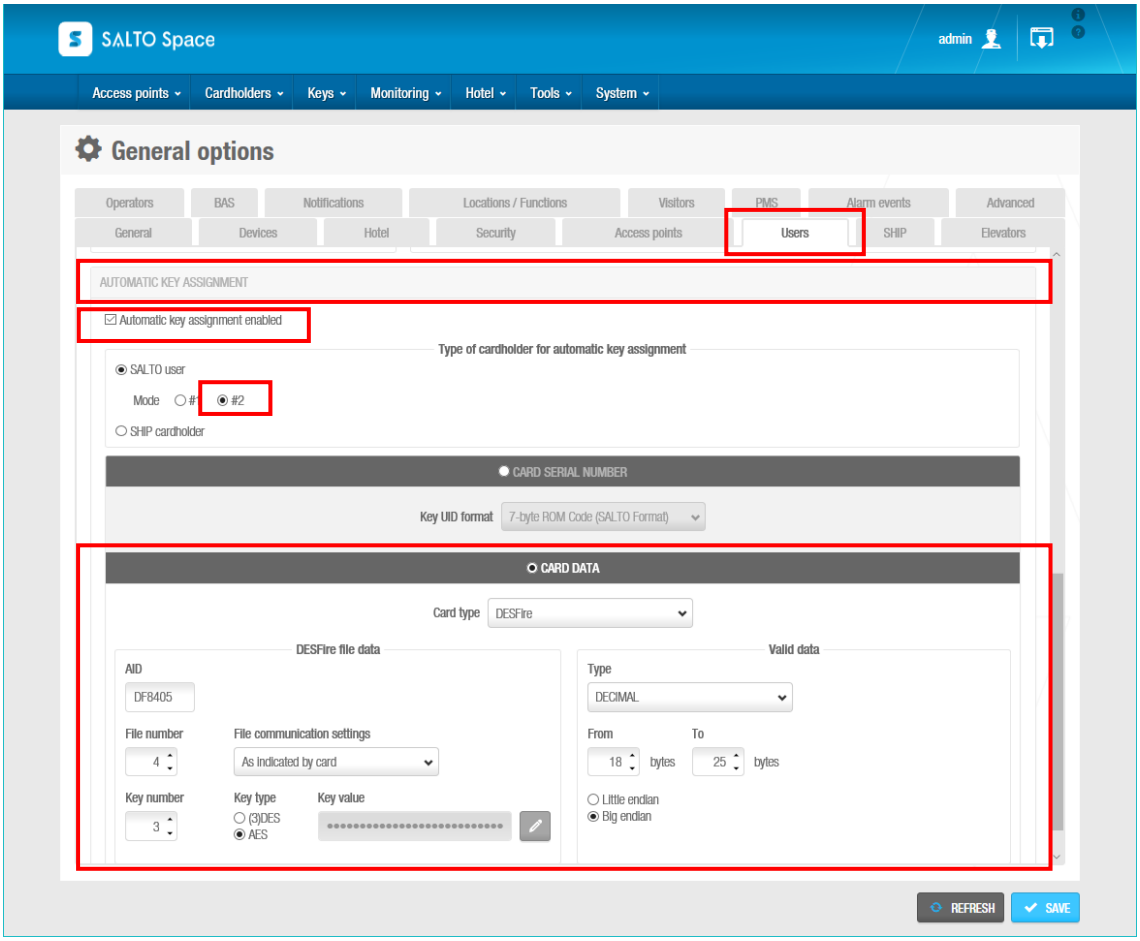


Figure 5.35 *- Settings for automatic data carrier allocation in SALTO ProAccess SPACE*

► Configure the options as shown in Figure 5.**35**.

The "Key value" that must be entered is specified by GANTNER under the term "FID Read Key". This key is system-dependent and must be suitable for the respective system to enable operation.

The following keys are valid for demo systems:

```
9999          67BB7698969CE15ED6707A81A5CA1F82
99999999      BC933AF2A1ABE668D06902D92D38BC06
```

Data carriers that were encoded before July 2022 were still encoded without the FID Read Key. For this reason, the automatic data carrier assignment can only be completed with restrictions. Please contact your GANTNER representative or GANTNER Support for assistance.

5.6.4 Defining data carrier types

Various types of RFID data carriers can be used in an access control system. These types are differentiated by, e.g., the RFID technology (LEGIC, MIFARE, etc.), the CardNET generation and type (CardNET G1, CardNET G2 with different memory sizes), and whether the data carrier type is enabled for use in ProAccess SPACE. Matrix allows different data carrier types to be used in a system. This ranges from simple systems with only one type of data carrier to complex systems that require a combination of data carrier technologies and CardNET types. Each user can use multiple data carrier types.

NOTE! GAT ACE 7000 must be installed to use multiple data carrier types. GAT ACE 3000 supports only one type.

See the terminology description "Read/write function (CardNET)" and "SALTO Virtual Network (SVN) and GANTNER SVN" for more information on the CardNET and SVN systems.

► Select "Data carrier types" menu item from the "Tools" menu.

○ The "Data Carrier Types" window opens. All defined data carrier types are listed.

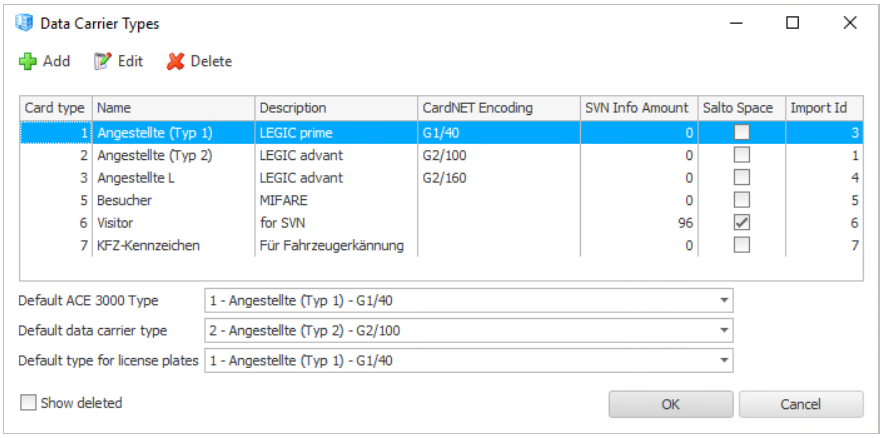


***Figure 5.36** - Defining data carrier types*

► Click on "Add" to define a new type of data carrier.

○ The following window opens.

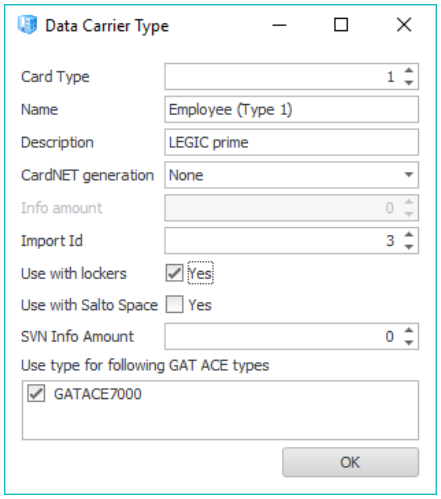


***Figure 5.37** - Defining a new data carrier type*

► Enter the following information for the new data carrier type:

- Card type: Define the number of the data carrier type in this field. For CardNET G1 data carriers, be aware that each data carrier must have a unique card type number.

  For CardNET G2 data carriers, multiple data carrier types with different settings that share the same card type number can be created. This allows you to create multiple CardNET G2 data carriers with different types of CardNET encoding to be used in a single facility. In Figure 5.36 for example, the “Employee card” with CardNET G2 encoding (G2/100) can be assigned to employees who are allowed to access a specific area of the facility only, and the “Employee large card” with CardNET G2 encoding (G2/160) can be assigned to employees who are allowed to access all areas of the facility, e.g., the Managing Director.

- Name: Enter the name of the data carrier type, e.g., Employee card.

- Description: Enter a brief description of the data carrier type, e.g., LEGIC advant.

- CardNET generation: Select the generation of CardNET encoding for the data carrier type. Select “G1” for LEGIC prime and LEGIC advant data carriers that use the previous CardNET G1 data structure. Select “G2” for LEGIC advant data carriers that use the new CardNET G2 data structure. Otherwise, select “None” for data carriers that are not using CardNET.

- Info amount: Define the quantity of data (groups, doors) that can be stored on the data carrier. For CardNET G1 data carriers, this value is fixed at 40 and cannot be changed. For CardNET G2 data carriers, a value to max. 200 can be defined here.

- Import ID: Every data carrier type must have a unique ID number, which is assigned automatically when defining a new data carrier. The Import ID number is used to distinguish between data carriers when importing into Matrix.

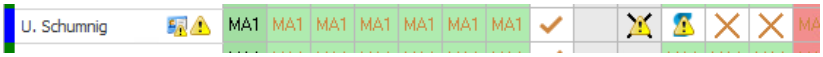
- Use with lockers: Select this option to enable the data carrier type for use in the locker matrix (see “5.18.6 Locker authorizations”).

- Use for Salto Space: When this setting is enabled, and a new data carrier of this type is created in the personnel data, the data carrier is enabled for use with SALTO ProAccess SPACE. For existing data carriers of this type, the setting is not changed.

- SVN Info Number: Here you can enter the maximum number of permissions that can be stored on a data carrier for the SVN application (see "SALTO Virtual Network (SVN) or GANTNER SVN" in the terminology chapter) for the SALTO ProAccess SPACE system. The default value is 96.

  A corresponding warning icon is displayed if the number of permissions defined for a person exceeds the data capacity.

  The max. number of SVN data depends not only on the coding but also on the number of plans, calendars, etc., that are used. The correct value must therefore be calculated for each system.



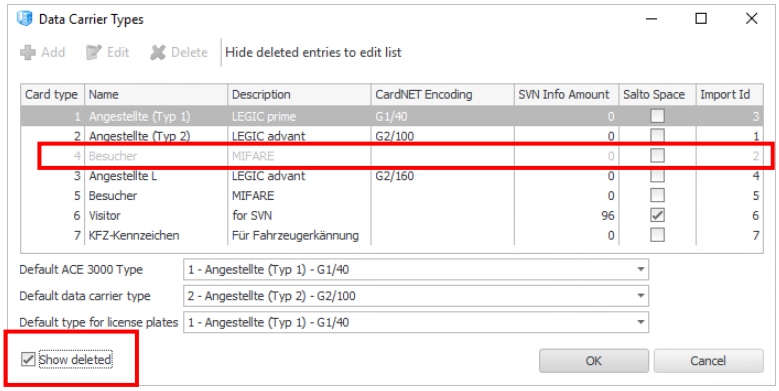
- Use type for following GAT ACE types:

  To use the data carrier type with GAT ACE 7000, select the "GATACE7000" option. When not selected, data carriers of this type are ignored by GAT ACE 7000.

► Click "OK" to add the new data carrier type.

Changing or deleting the data carrier type

- ► Click on "Edit" to change the details of a data carrier type in the list.
- ► Click on "Delete" to remove a data carrier type from the list. The data carrier type must not be used by any data carrier in Matrix or deletion is not possible.
- ► If the "Show deleted" option is enabled, all previously deleted data carrier types are displayed in gray.



- ► The list cannot be edited in this display mode. Disable the "Show deleted" option to edit the list again.

Defining the default data carrier types

- ► In the "Default ACE 3000 Type" field, select a data carrier type to use by default in GAT ACE 3000. Other data carrier types will not be recognized by GAT ACE 3000.
- ► In the “Default data carrier type” field, you can select the default types that are automatically preset in the person definition (see "5.6.1 Defining personnel master data").
- ► In the last field "Default type for license plates", you can select another data carrier type that is then used for the vehicle license plates defined in the system (see "5.6.10 Settings for license plate recognition").
  Note: A separate data carrier type that is not yet in use should always be used for the vehicle license plates.

5.6.5 Reading and deleting SALTO data carriers

You can read and delete the data carriers (also called "keys") used for SALTO doors. The corresponding hardware (encoding station) is required for this and must be created in ProAccess SPACE.

- ► Select "Space Key Management" from the "Tools" menu.
  - ○ The following window is displayed.

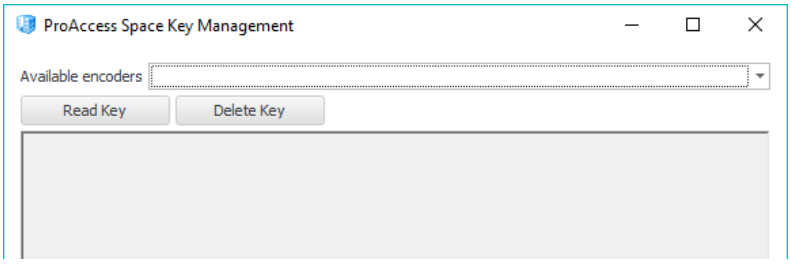


Figure 5.38 – SALTO Key Management

NOTE! If the LED flashes green at the encoding station after reading/writing a data carrier, the data carrier must be removed. If it remains on the encoding station, an error message is displayed in Matrix.

► In the "Available encoders" field, select the desired SALTO encoding station that is connected to the computer.

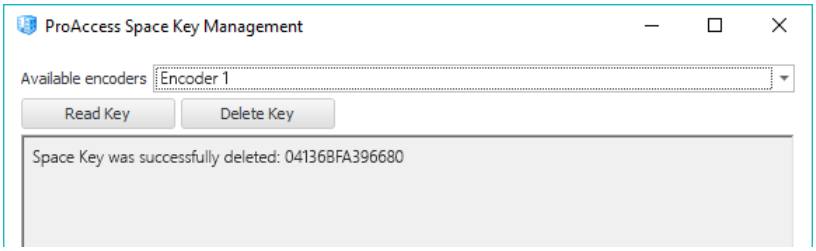
► Place the SALTO data carrier on the encoding station and click "Read Key".

- Information on whether the data carrier is assigned to a person or not is displayed.



► To delete a data carrier, place the SALTO data carrier on the encoding station and click "Delete Key". Deleting makes it possible to reassign the data carrier to another person later.

- Any existing authorizations saved on the data carrier are deleted and the assignment of the data carrier to other persons is possible again.



5.6.6 Automatically preparing existing persons for SALTO ProAccess SPACE

If, for example, you have defined persons for an existing Matrix system who are to be subsequently used for a SALTO ProAccess SPACE connection, you can automatically update the persons' data carriers for ProAccess SPACE. In doing so, one data carrier for each person can be selected for use with ProAccess SPACE and the SPACE data carrier options can be automatically set to the default values. To do so, proceed as follows.

► Select "ProAccess Space Synchronization" from the "Tools" menu.

- The following window is displayed.

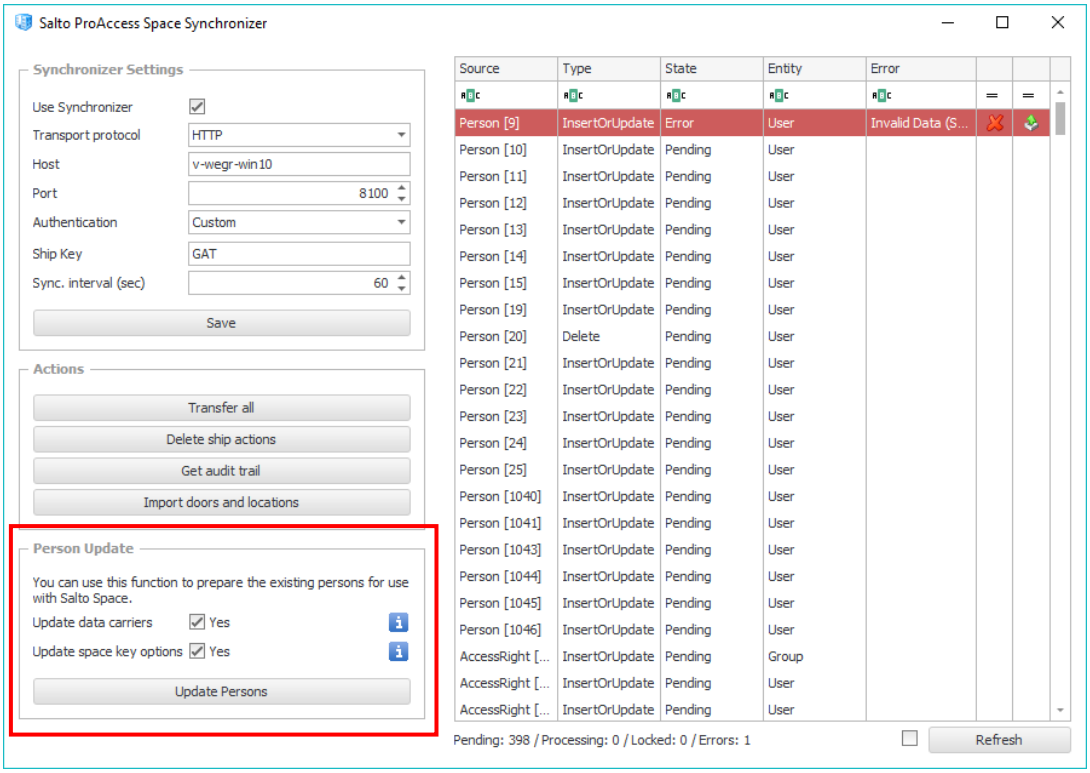


***Figure 5.39** – Person Update for SALTO ProAccess SPACE*

► In the “Person Update” area, select the desired function(s):

- Update data carriers: This option enables the first data carrier for use with ProAccess SPACE for all persons in general. The prerequisite for this is that this data carrier is also enabled for use with ProAccess SPACE (see "5.6.4 Defining data carrier types").

- Update space key options: This option applies the subsequently changed settings of the data carrier types to all previously assigned data carriers. This allows you to, for example, subsequently select a data carrier type for use with SALTO ProAccess SPACE and apply these settings to all persons that are already assigned to this type.

► Click on "Update Persons".

- The defined function(s) are executed.
- A notification about the executed functions is displayed. If a function could not be executed for persons, or if there are several data carriers per person for example, you can save the respective persons in a text file and then use this file to check the persons.

5.6.7 Scanning fingerprints

In the “Fingerprint” tab, up to four fingerprints (two for normal identification and two for triggering the threat alarm) can be scanned and saved.

NOTE! To scan fingerprints, a scanning device (e.g., GAT Fingerprint Reader FR010) must be connected to the PC. Furthermore, this function must be activated in the Global settings (menu "Tools" -> menu item "Options" -> register card "Global", see "4.8 Global settings").

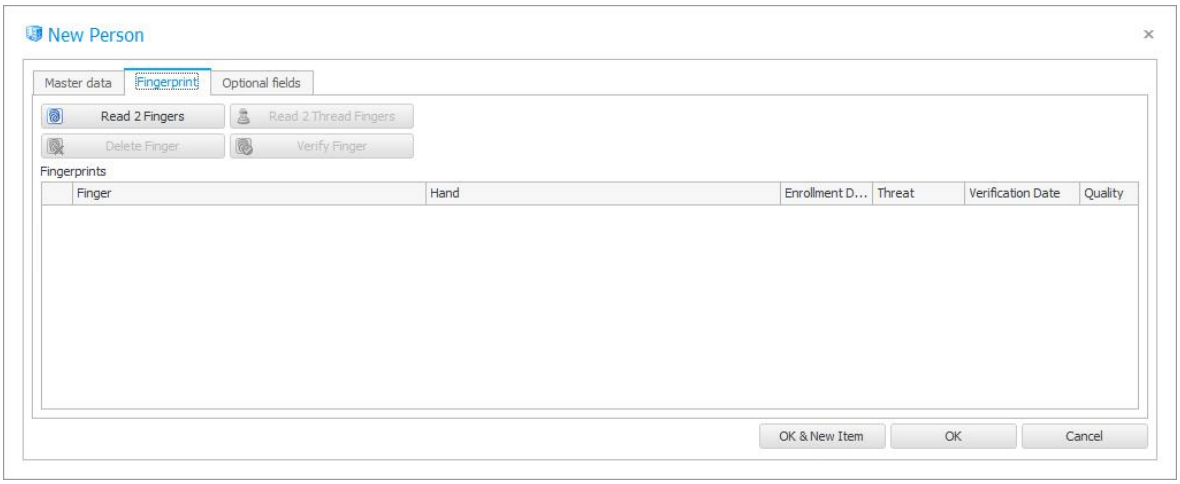


Figure 5.40 *- Fingerprint definition*

First, the fingers used for normal identification must be scanned after which the fingers used to activate the threat alarm can be scanned. The option to scan the threat fingers can be deactivated in the general settings (see "4.7. General settings").

If you mark the option "Voice instructions for fingerprint reading" in the general settings of Matrix (see "4.7. General settings*"), audible instructions are given along with the following instructions.*

Proceed with the following steps to scan fingerprints:

► Click on "Read 2 Fingers".

NOTE! The number "2" indicates how many fingers can be captured. When one finger has already been scanned, "Read 1 Finger" is shown on the button.

- The "Finger Selection" window opens.

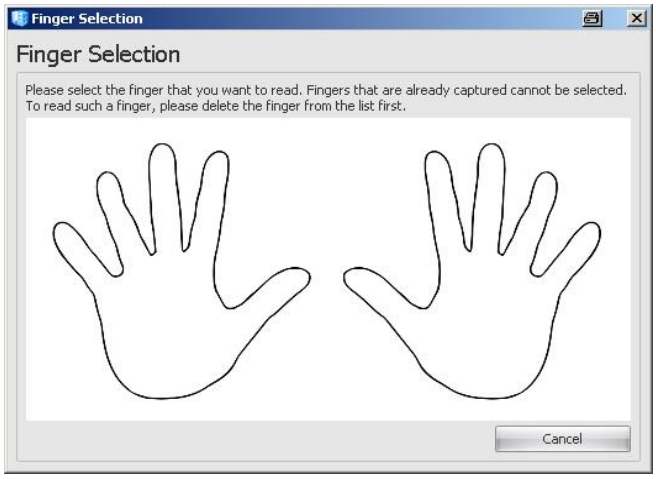


Figure 5.41 *- Selecting the finger*

► Select the first finger to be scanned by clicking on the finger in the picture.

When you select a finger that was already scanned, a message is displayed to confirm that the previous fingerprint data should be overwritten with the new fingerprint data.

- The finger is marked orange and the following window opens.

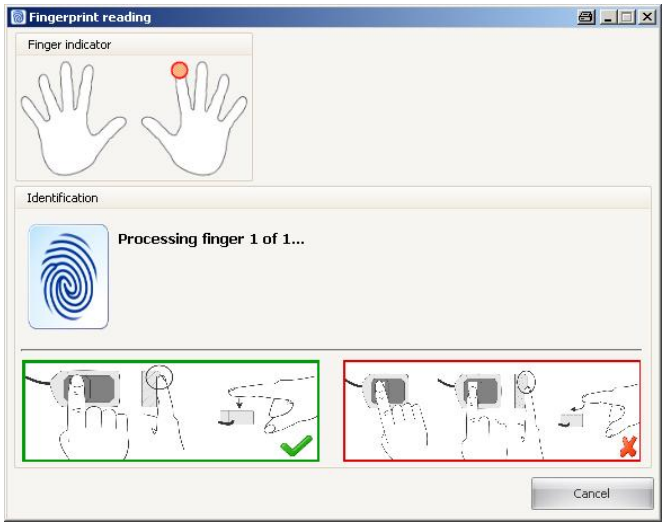


Figure 5.42 *- Scanning of fingerprints*

► The selected finger is shown again in the top-left picture. Now place the finger onto the sensor of the fingerprint reader. Be sure to place the finger vertically and gently onto the sensor.

- A message is displayed in the middle area of the window to inform whether the fingerprint was scanned successfully or not.

► When successful, scan the fingerprint again for verification.

- The personnel data window is shown again following the successful second scanning of the fingerprint. Figure 5.**43** shows a person who has successfully scanned all four possible fingerprints.

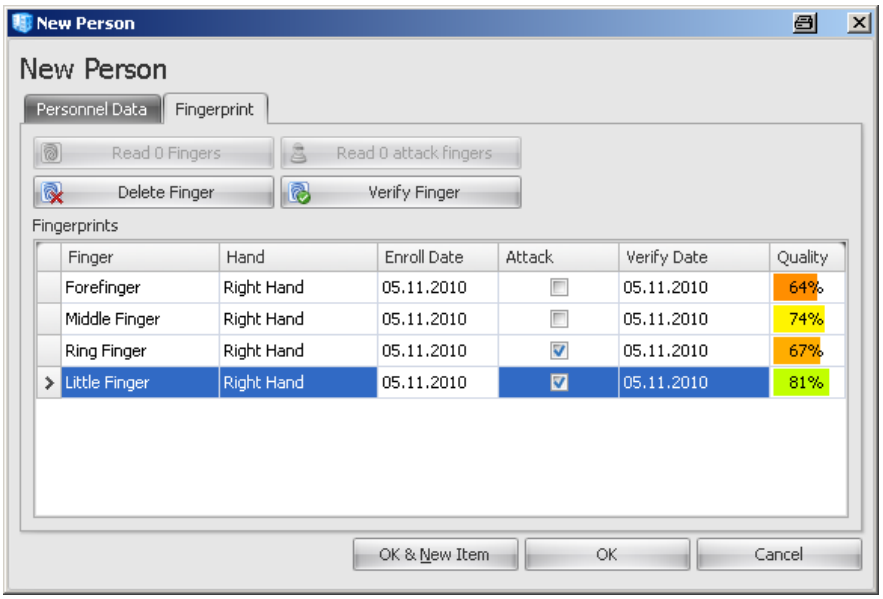


Figure 5.43 *- Definition of person - with fingerprints*

In the "Fingerprints" list each captured fingerprint is listed with the following information:

- Finger: Type of captured finger.
- Hand: Used hand (left or right).
- Enroll Date: Date when the fingerprint was scanned and saved. If, for example, a previously scanned finger is scanned again, the old fingerprint data is overwritten with the new one and the new capture date is shown here.
- Attack: If this field is marked with a tick, the corresponding finger is used for the threat alarm.
- Verify Date: Date on which the fingerprint was verified.
- Quality: Matrix analyses the fingerprint data and calculates how precisely the fingerprint can be verified. The quality of the fingerprint data is displayed in this column.

Deleting a fingerprint

► To delete fingerprint data, select the applicable finger from the list then click on "Delete Finger".

  ○ The fingerprint data is deleted from the terminals the next time they are uploaded after which the person can no longer use the finger for identification and access.

Verifying a fingerprint

► To test the quality of the fingerprint data, first select a finger from the list then click on the "Verify Finger" button.

  ○ The "Fingerprint validation" window opens.

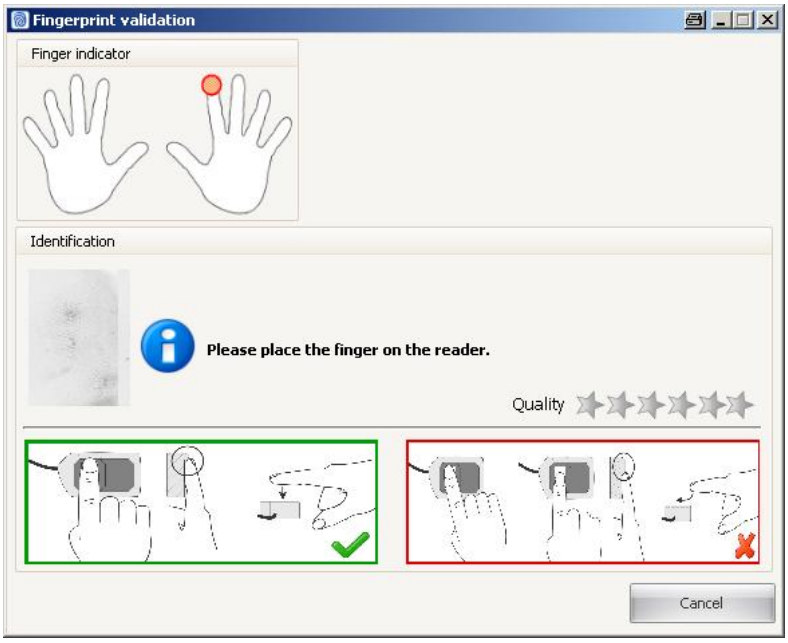


Figure 5.44 *- Verifying fingerprint data*

- ► Place the finger vertically and gently onto the sensor of the fingerprint reader.
  - ○ The fingerprint is read, and Matrix compares the scanned fingerprint to the saved fingerprint. The quality of the verification is shown via the stars and a message in the middle area of the window. It is possible to define a minimum value for quality. If this value is not reached during verification, the finger MUST be rescanned or another finger used instead.
- ► Close the window with the "Cancel" button.
- ► After entering all the information and saving the fingerprint data, save the settings via the "OK" button in the personnel window.
  - ○ The person is added to the selected group in the matrix.

To edit the personnel information of a person, click with the right mouse button onto the person and select "Edit person" from the menu.

NOTE! Ensure that the fingerprint reader is clean before scanning fingerprints. Use a soft, damp (not wet) cloth and no harsh detergents for cleaning. Also observe the cleaning instructions in the fingerprint reader manual.

5.6.8 TBS system (biometrics)

As an option for identification of the persons, biometric data (e.g., fingerprints) can also be captured using devices from TBS (Touchless Biometric Systems AG). When using this system, a TBS reader is required at each door where authentication via TBS biometric data is required. More information regarding TBS biometrics is available via their website.

To begin using the TBS system in Matrix, the following requirements must be met:

1. An expansion license (Matrix TBS Integration, Part No. 1103007) must be ordered from GANTNER and activated in Matrix. See chapter “10 LICENSE MANAGEMENT” for information on this process.
2. The “Enable TBS Synchronization” option must be selected in the Global settings tab (see “4.8 Global settings”), which is accessed via “Tools” > “Options” > “Global”.

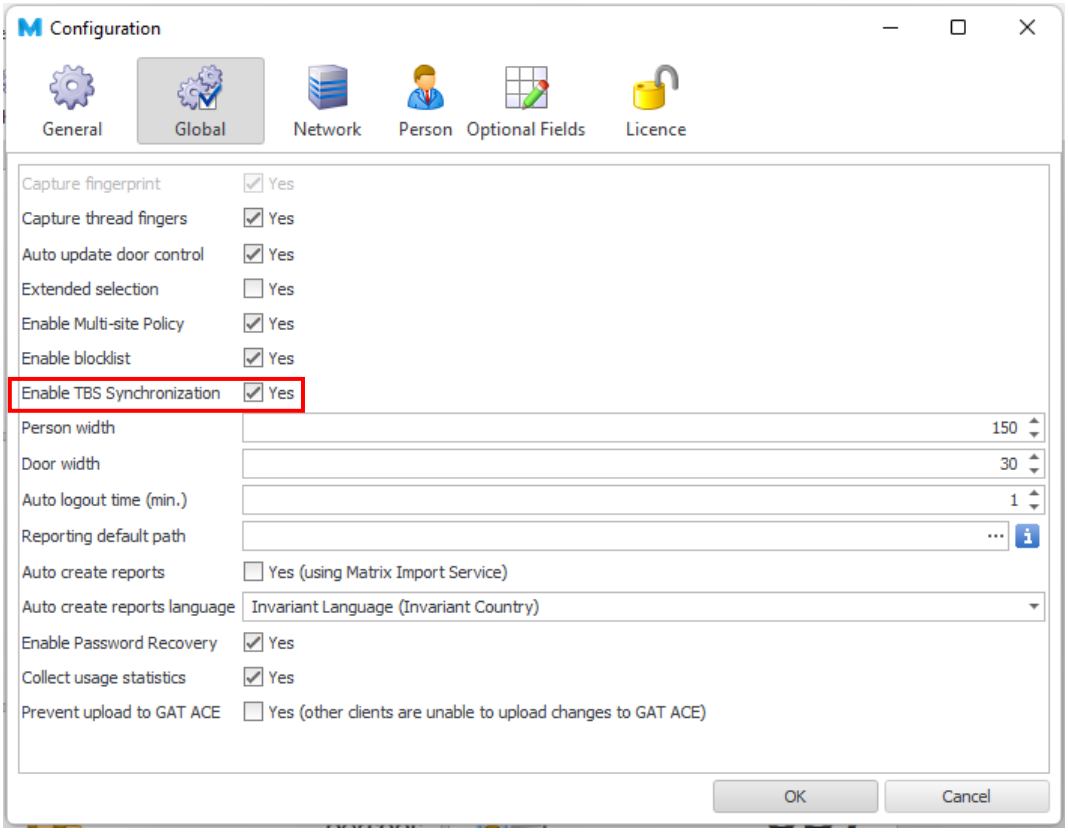


Figure 5.45 *- Setting for enabling TBS synchronization*

3. The following TBS software is required:
   - The software “TBS WebEdition” must be installed on a central server for communication with the TBS biometric devices.
   - The software “TBS .NET SDK” is needed to enroll the biometric data for Matrix and must be installed on every client that is to be used for enrolment. After enrolment, this software sends the biometric data to the “TBS WebEdition” software. The driver for the TBS biometric reader is also installed during the setup of this software.

TBS system setup

- The TBS software is included on the zip file that is delivered with the TBS biometric reader. Install the TBS software according to the included instructions, which are available via:
  `"TBS\WebEdition\_documentation"`.
- Go to the directory where the TBS software file is installed and open the path `"TBS\WebEdition\Core"`.
- Right-click onto `"web.config"` and select "Open with Editor".
  - Editor opens and displays the code from this file.
- Under `<appSettings>`, copy the `"auth RPKey"` value.
- In Matrix, go to "Tools" > "Options" > "Network" > "Network Services Configuration" > "TBS RemoteSync Interface", and paste the `"auth RPKey"` value into the `"TBS_AuthKeySetting"` field.

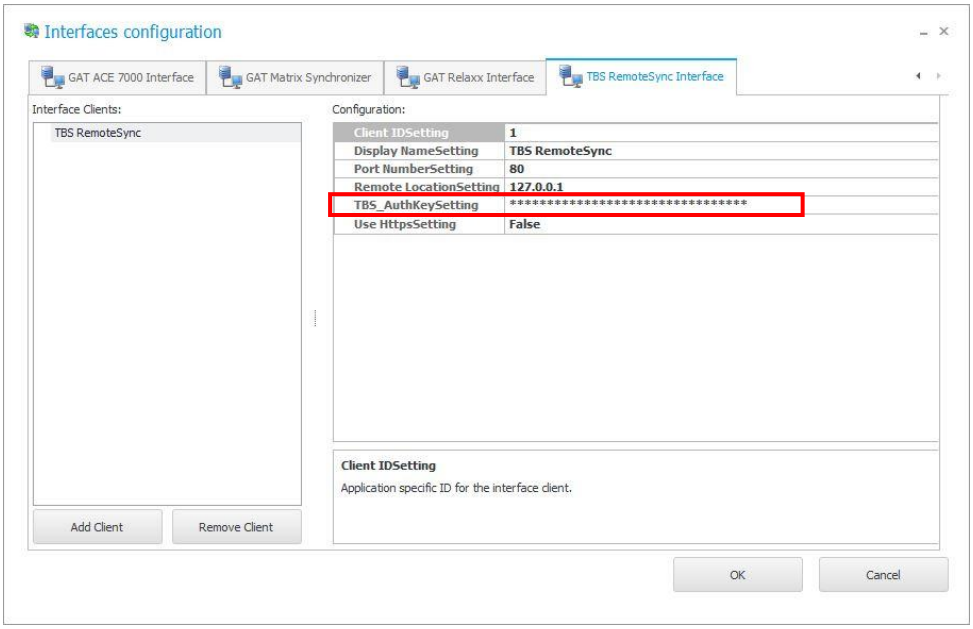


Figure 5.46 *- TBS RemoteSync Interface window*

- All other interface settings are set automatically according to the details of the local machine when installing Matrix.

See chapter "4.4.5 TBS RemoteSync interface" for a description of each setting.

- Click on "OK".

Scanning fingerprints with a TBS reading station

NOTE! Ensure that the fingerprint reader is clean before scanning fingerprints. Use a soft, damp (not wet) cloth and no harsh detergents for cleaning.

► Connect the TBS fingerprint reader to the computer via the USB cable.
  ○ The TBS Biometrics reader is now integrated with Matrix and ready to scan fingerprints.
► In the matrix display, click on the person whose fingerprints you want to scan.
  ○ The personnel data window opens.
► Open the “TBS Biometrics” tab in this window.

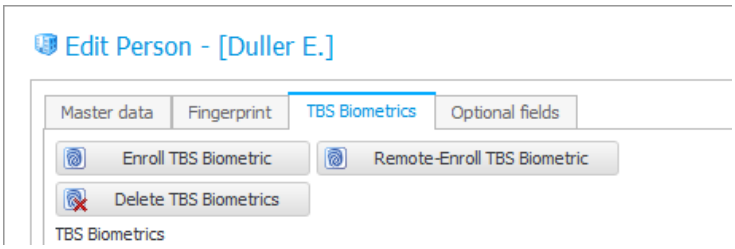


Figure 5.47 *- “TBS Biometrics” tab*

  ○ Here, the fingerprints that have already been recorded for the person are shown.

► Click on “Enroll TBS Biometric”.
  ○ The TBS Enrollment Wizard opens as shown in Figure 5.***48***.

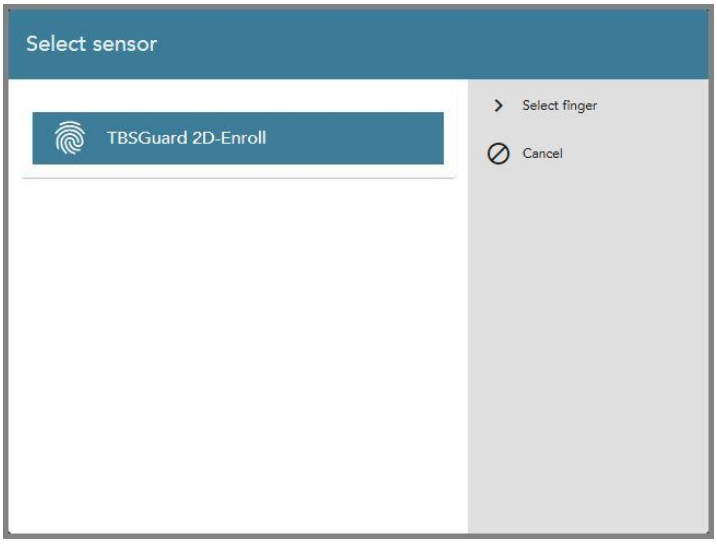


Figure 5.48 *- Capturing fingerprints via TBS – Step 1*

► Click on “Select finger” and select the first finger to scan by clicking on the finger in the picture.
  ○ The finger is marked blue.

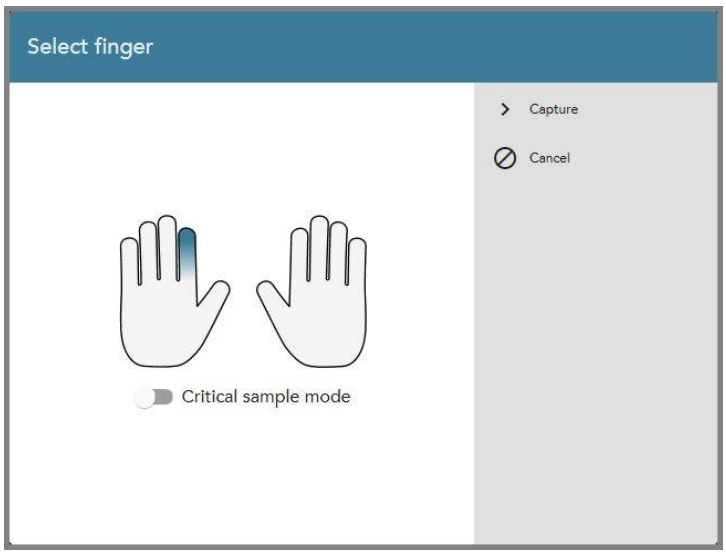


Figure 5.49 *- Capturing fingerprints via TBS – Step 2*

► Click on “Capture”.

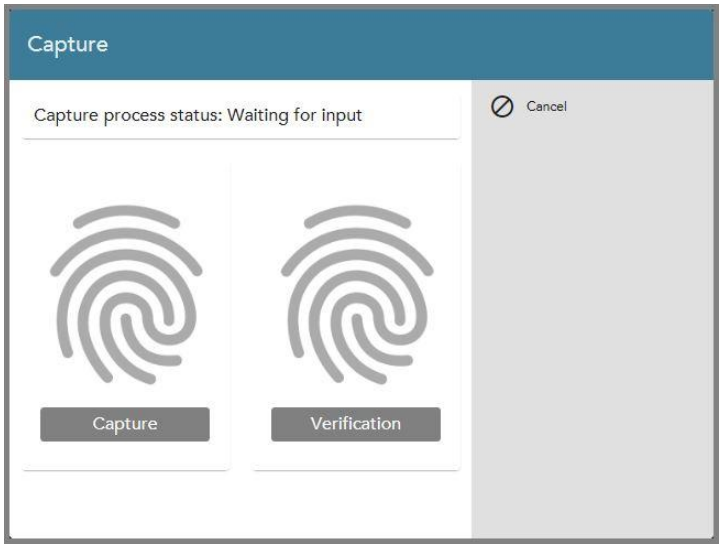


Figure 5.50 *- Capturing fingerprints via TBS – Step 3*

► Place the finger squarely onto the middle of the sensor.

- The fingerprint is automatically read, and the result of the scanned fingerprint is shown.

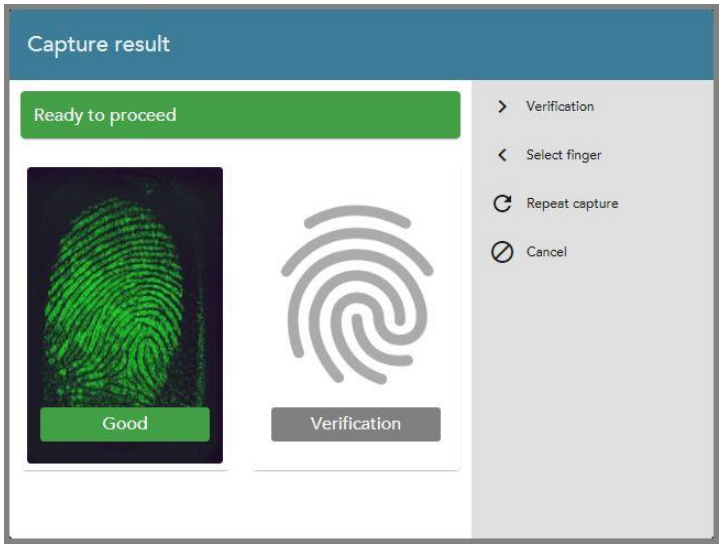


Figure 5.51 *- Capturing fingerprints via TBS – Step 4*

- “Good” should be shown for the scanned fingerprint.

► If “Poor” or "Low" is shown, repeat the process via the “Repeat capture” button.

► Some fingerprints may not ever produce a “Good” scan. All 10 fingerprints can be scanned so in this instance, select another finger.

► When “Good” is displayed for the fingerprint, click on “Verification”.

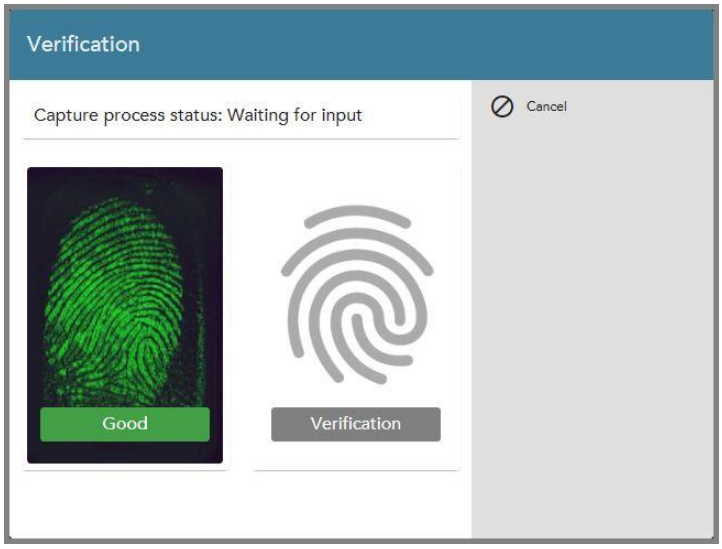


Figure 5.52 *- Capturing fingerprints via TBS – Step 5*

► Place the same finger onto the scanner.

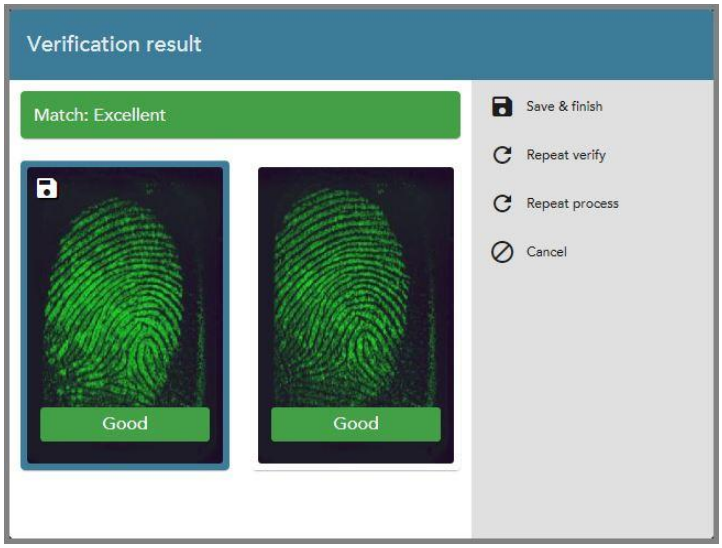


Figure 5.53 *- Capturing fingerprints via TBS – Step 6*

► “Good” must again be shown for the verified fingerprint. If not, repeat the process via the “Repeat verify” button.

► When two “Good” fingerprints are shown, click on “Save & Finish”.

- The details of the scanned fingerprint are displayed in the list.

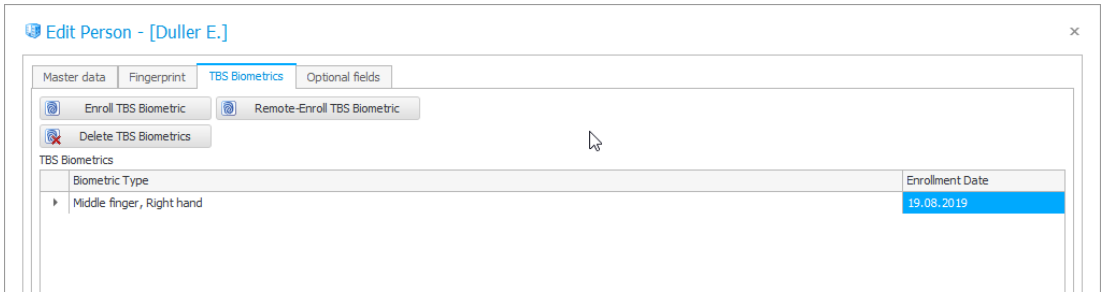


Figure 5.54 *- TBS Biometrics tab with scanned fingerprints shown*

Deleting fingerprint data

► To delete the TBS fingerprint data of a person, click on the "Delete TBS Biometrics" button.

- All TBS fingerprint data of the person is deleted from the terminals.

NOTE! It is not possible to delete the fingerprint data of an individual finger. This action deletes all TBS fingerprint data of the person and cannot be undone.

Using the TBS fingerprint data

- ► In the personnel data window, open the “Master data” tab.
- ► Under the “Data Carriers” area, the data carrier(s) assigned to the person can be enabled for use with the TBS fingerprint reader via the “Use for TBS” button.
- ► Click on “OK” to confirm the settings.

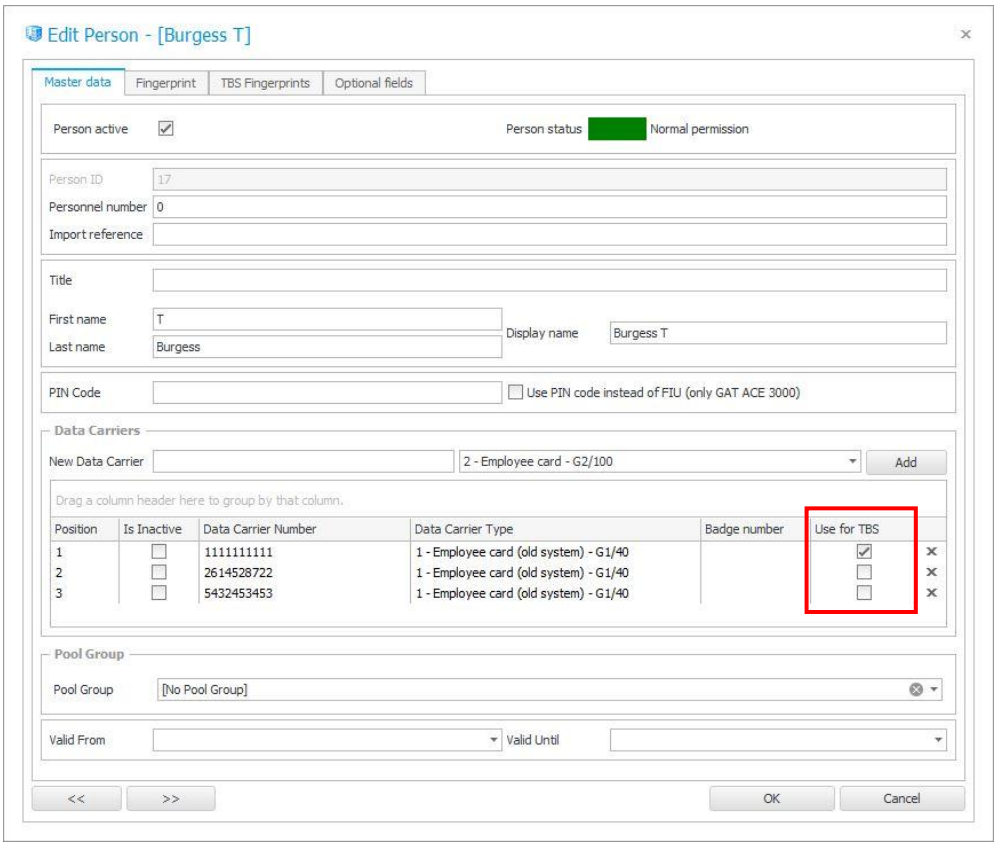


Figure 5.55 *- Assigning data carrier of a person for use with TBS fingerprint reader*

5.6.9 Inserting a picture for a person

On the “Picture” tab, an image or photo of a person can be selected that is then displayed in the personnel data on the first "Master data" tab.

The “Picture” tab is only displayed if the use of personal images is activated in the options (see "4.10 Settings for person display"). There you can also define how a picture should be inserted and saved. It is possible to save images directly in the database (which can increase the size of the database considerably) or to link to the images, which can then be saved in an accessible folder on the server.



Figure 5.56 *- Adding a picture for a person*

► Click on the “Choose Picture” button.

► Select a picture for the person.
The picture must be in bitmap format (JPG, PNG, GIF, ...) with a maximum size of 5 MB if the image is to be saved in the database. If the picture is only linked via a link, the picture can be of a larger size.

- If the option to insert the pictures using a link is selected, the path to the picture is displayed below the picture.
- If a picture that is linked is deleted or renamed, or if the folder with the pictures is not available (e.g., for a folder in the network), the picture is no longer displayed in the personnel data. However, the link is saved and as soon as the picture is available again with the correct name, the picture is displayed again.

► Confirm with "OK".

5.6.10 Settings for license plate recognition

As of Matrix version 5.2 together with GAT ACE 7000 version 2.2 and later, cameras for recognizing vehicle license plates are supported. The ID information and vehicle license plates of all people defined in Matrix are transferred from GAT ACE 7000 to the camera systems according to the camera settings defined in GAT ACE 7000. The GAT SR 950 camera available from GANTNER validates the read vehicle license plates and, if the validation is positive, transfers the ID number to the access controller via the Wiegand interface (e.g. GAT DC 7200). In this case, the GAT DC 7200 then checks whether a local decision is possible based on the stored authorizations or whether an online decision is required, e.g. if a pool management or anti-pass-back decision is required. With this system solution, all requirements can be mapped.
As of Matrix 5.3, it is also possible to use other camera systems for license plate recognition that communicate via Wiegand and support the SHA-1 26-bit standard. The SHA-1 hash algorithm is used to calculate check values from the license plates, which can be used to unambiguously check that the license plates match the personnel data without being able to draw conclusions about the license plate in plain text. For more information, refer to the documentation of the GAT DC 7200 controller, in which the cameras and the SHA-1 algorithms are configured.

NOTE: A separate license is required for license plate recognition (see "10 LICENSE MANAGEMENT"). If this is not available, the personnel data is sent to GAT ACE 7000 when the doors are loaded, but the license plates are ignored (not sent). An error message and a note are displayed in the error log.

In the Matrix software, one or more vehicle license plates per person can be inserted into the personnel data, which is done on the "Optional fields" tab.

NOTE: In the general settings, one field or multiple fields for license plate numbers must be defined once (see "4.11. Optional fields for personnel data").

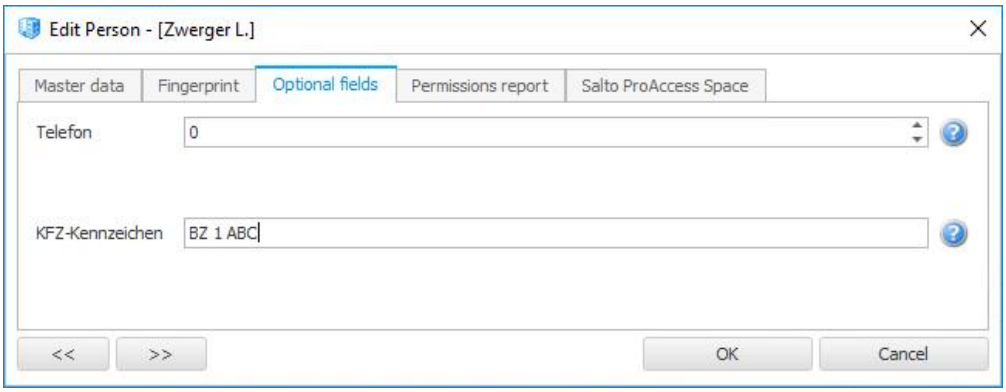
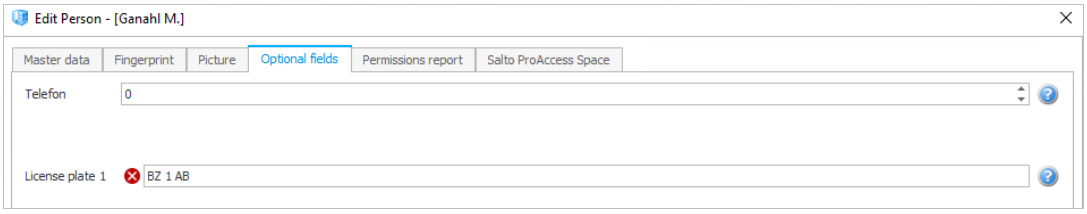


Figure 5.57 *- Personnel data, entering vehicle license plate data in the optional fields*

- ► Enter the license plate number in the field provided. The number can be entered with or without spaces. GAT ACE 7000 checks the entries for plausibility and corrects the entries accordingly if special characters or spaces are included.
- ► If multiple "License plate" fields have been defined, you can enter additional numbers, e.g., for a second car.
- ► Click on "OK" to save the entered data.
    - ○ If a license plate number is entered that is already being used by another person, a notification with red X symbol is displayed and saving is not possible. Another number must be entered in this case.



- For license plate recognition to work, a data carrier with a specific data carrier type must also be activated for each person for whom a license plate number is entered. This data carrier type must then be selected as "card type" in GAT ACE 7000 for the relevant cameras (see the information on camera configuration in the GAT ACE 7000 manual).
- To transfer the license plate information to the cameras, the data must be sent to GAT ACE 7000 ("Uploading doors").

  Note: GAT ACE 7000 always transfers all license plate information for all persons to all cameras simultaneously.

  Note: If you enter a license plate that has already been used for another person and then do not click on "OK" immediately but switch to another tab, the window cannot be closed by clicking on "OK". An error message is not displayed in this case. Open the "Optional fields" tab again and correct the entry.

5.6.11 Personnel settings for SALTO ProAccess Space

If SALTO ProAccess SPACE software is used and enabled in Matrix (see "5.5 Importing doors and locations from SALTO ProAccess SPACE"), an additional "Salto ProAccess Space" tab is displayed when editing personnel data.

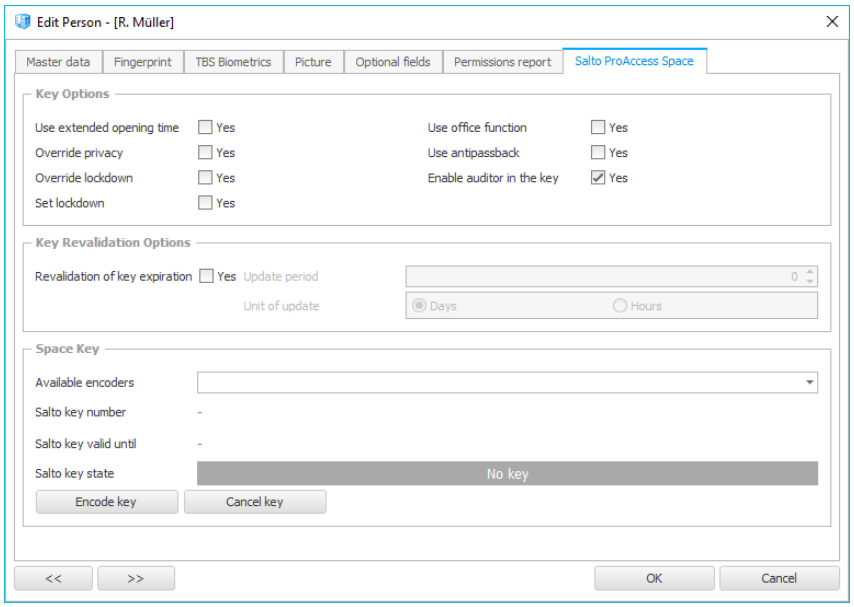


***Figure 5.58** – Personnel data, settings for SALTO ProAccess Space*

- In the "Key Options" area, enable the settings for the ProAccess Space data carriers. For more information, please refer to the ProAccess Space manual.
- In the "Key Revalidation Options" area, you can set the validity period for the person's data carrier.

► In the "Space Key" area, you can read from and also write to (encode) a data carrier using a SALTO encoding station connected to the PC. To do so, select the reading station in the "Available encoders" field and then click "Encode key" or "Cancel key".

NOTE! If the LED flashes green at the encoding station after reading/writing a data carrier, the data carrier must be removed. If it remains on the encoding station, an error message is displayed in Matrix

5.6.12 Assigning persons to groups

It is possible to drag persons to other locations in the authorization matrix, even to other groups, by holding down the SHIFT key while dragging the person to the new location with the left mouse button.

5.6.13 Reloading personnel data into a controller

After triggering the manipulation block or if there are problems with the authorization data of a person in a controller (e.g., if the person was not uploaded correctly), the authorization data of the person can be reloaded.

This function only operates with GAT ACE 3000 and not with GAT ACE 7000.

Right-click on the person in the matrix then select the "Reload person to doors" menu option.

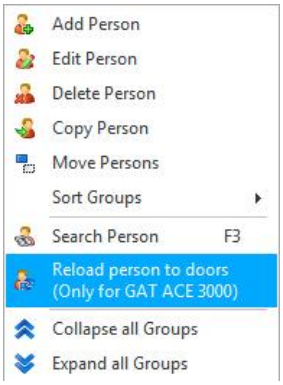


Figure 5.59 *- Reloading a single person*

GAT ACE automatically sends the personnel data to the applicable controller.

NOTE! When the multi-site policy is activated, a person that is selected to be loaded will only be uploaded to the terminals for which the person is authorized.

5.6.14 Copying a person

The “Copy Person” function can be used to make a copy of a person together with the access rights defined for this person. The copied person will be assigned to the same group as the person from which the copy was made. The access rights that will be copied contain only those who are directly assigned to the person (Person / Door or Person / Door Group). The data carriers and fingerprints of the person are not copied as they are unique for each person.

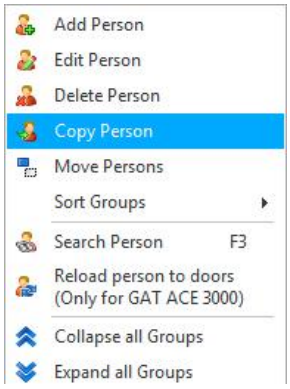


Figure 5.60 *- Copying a person*

After copying the person, the window for editing the personnel data opens.

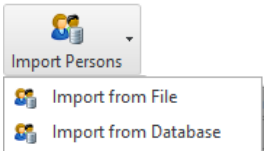
5.6.15 Deleting a person

When a person in Matrix is deleted, the data carriers assigned to the person are deleted, which means they do not have access authorization in the system. The person row with their assigned door authorizations is removed from the matrix.

- ► Right-click on the person to open the shortcut menu.
- ► Select "Delete Person".
  - ○ Depending on the configuration in the general settings (see "4.7. General settings"), the person is either deleted without notification or a notification is displayed to query whether the person should be deleted.
- ► Confirm "Yes" if a delete notification is displayed.
  - ○ If the blocklist is activated in the global settings (see "4.8 Global settings"), you are asked whether the data carrier(s) assigned to the person should be transferred to the blocklist.
- ► Select "Yes" if the data carrier has been lost or stolen. This will add the data carrier(s) to the blocklist. The offline doors will then need to be loaded using the programming device.
- ► Select "No" if the person has correctly returned the data carriers and it can be used for other persons. In this case, the offline doors do not need to be loaded using the programming device.
  - ○ The person is deleted from Matrix.

5.7 Import persons

Matrix offers the possibility to import persons from other applications via corresponding files or from another database. The import must be defined once. The same settings are then reused for further imports, and you must only click on the desired option under the "Import Persons" button in the toolbar.



“Import from File” starts importing via the configured CSV file and “Import from Database” starts importing via the configured database.
To configure the import persons settings, select the "Setup Person Import" option from the "Tools" menu. The following window opens.

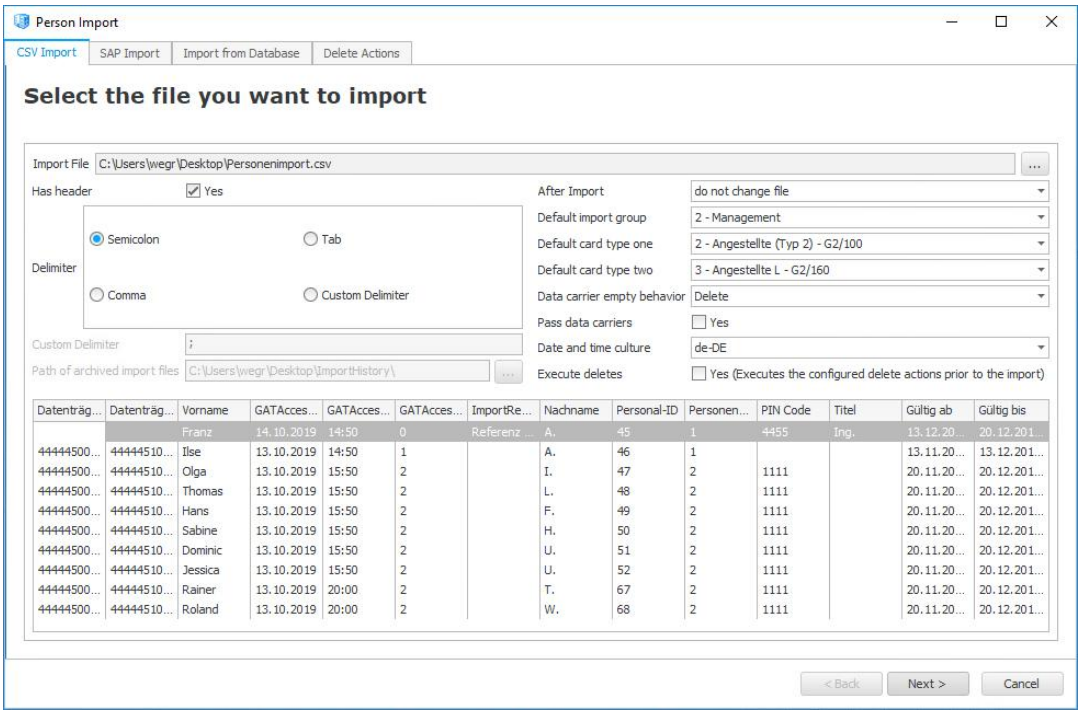


Figure 5.61 *- “Person Import” window*

NOTE! The following describes how to import persons via a CSV file. You can also import persons directly via SAP CC1 files ("SAP Import" tab - see “5.7.2 Importing via SAP” for more information) or from another database ("Import from Database" tab - see "5.7.3 Importing from database" for more information).

NOTE! If using SALTO ProAccess SPACE software, note that the names of all persons in Matrix must be unique for the import.

5.7.1 Importing via CSV file

On the "CSV Import" tab, click on the "..." button next to the “Import File” field to select the import file in which the persons to be imported are stored.

NOTE! The file must be a text file (CSV). For the exact format specifications of the import file see “Appendix D”.

The following settings can be defined for import of personnel data:

- Has header: If the first row in the import file is used for naming the rows in the file, you can mark this option. If the option is marked, the first line of the import file will not be imported.
- Delimiter: Select the symbol that is used in the import file for separation of the columns. In the input field "Custom Delimiter" right next to the "Delimiter field" you can also enter an own character to be used for the separation of columns. Therefore, the option with the same name must first be selected.
- After Import: In this field you can select what shall happen with the import file after successful import:
  - do not change file: The import file is neither changed nor deleted. Please think of deleting this file manually to free-up space on the disk.
  - remove file: After import, the import file is automatically deleted.
  - archive file: The import file is archived, which means that the file is copied to an archive directory and the import directory is deleted. The location of the archive directory can be entered below.
- Default import group: Select the default group in Matrix to which newly imported people, who are not already assigned to a group, are assigned to following importation. If the "No default group" option is selected, note that a group must be specified for each person in the import file. Persons not assigned to a group will not be imported.
- Default card type 1/2: If there are no data carrier types defined in the import file, select the default data carrier types to assign to the data carriers 1 and 2 of the imported persons. To define the data carrier types in the import file, the “Import ID” of the desired data carrier type must be defined (see "5.6.4 Defining data carrier types" for more information).
- Data carrier empty behavior:
  This option defines how the data carrier numbers of existing persons in Matrix should be handled during importation when no data carrier number(s) or "0" as the number(s) is/are defined:
  - "Delete": Only the data carriers that are assigned for importation (see next page) and have an empty import field or "0" in the import field are deleted. All unassigned data carriers remain.
  - "Ignore": The data carrier(s) of existing persons with an empty import field or "0" in the import field remain unchanged.
- Pass data carrier: If this option is enabled, a data carrier can be transferred from one person to another through the import process without the data carrier having to be deleted by a person first. If the option is not enabled, an error occurs when you try to assign a data carrier to a person and the data carrier is still assigned to another person. The assignment is not allowed in this case.
  Note: This function is only possible for invalid records, i.e., if the person’s validity date has not expired yet, the data carrier cannot be transferred. If the validity period has expired, the data carrier is removed from the person and assigned to the new person.
- Date and time culture: Select the format for the date and time data that is included in the import file. An example of each format is shown in the list next to the entry. This setting only affects the "Valid from" and "Valid until" fields. For the "GAT Access Date flag" and "GAT Access Time flag" fields, the "German" format is always used ("dd.MM.yyyy" and "HH: mm").
- Execute deletes: Select this option to execute the configured delete parameters (see “5.7.4 Delete actions”) prior to the import.

After selecting the file, a preview is shown in the bottom field of the window. When you selected the correct delimiter, you should see a table with each person in a separate row and each data field in a separate column of the table. An example is given in the following figure.

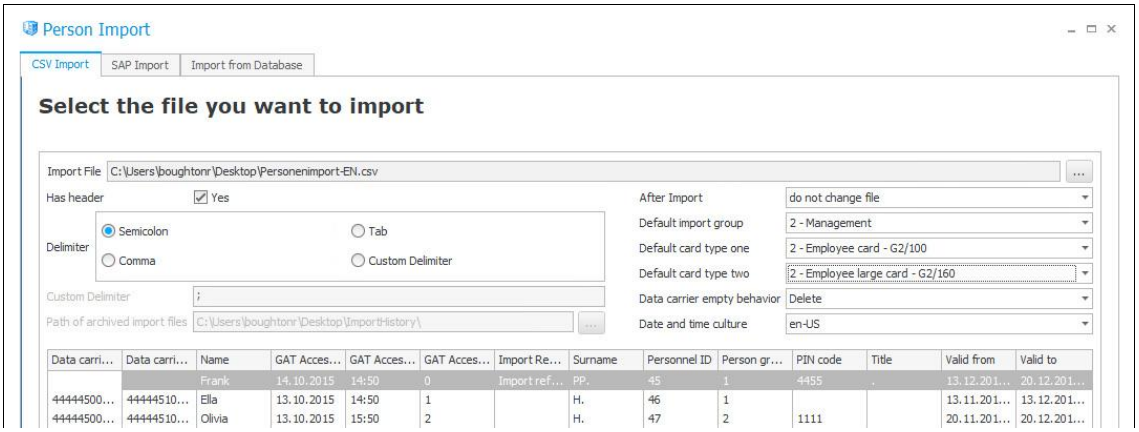


Figure 5.62 *- Person Import definition - Step 1*

NOTE! The first line of the import file is usually used for the naming of the different data columns. If the header file is shown in the first row of the table (as in the example below), mark the "Has Header" option in order to use this line as the header of the import table. The lines should no longer be displayed after selecting this option.

Data Carri...	Data Carri...	First Name	GAT Acces...	GAT Acces...	GAT Acces...	Import Ref...	Last Name	Personnel ID	Person Group	PIN Code	Title	Valid from	Valid to
		John	14.10.2015	14:50	0	Reference ...	Smith	45	1	4455	Ing.	13.12.201...	20.12.2015 2...
44444500001	44444510001	Jane	13.10.2015	14:50	1		Doe	46	1			13.11.201...	13.12.2015 2...
44444500002	44444510002	Jasper	13.10.2015	15:50	2		Nielsson	47	2	1111		20.11.201...	20.12.2015 2...

NOTE! When previewing the import file, it is not yet possible to check whether a person to be imported already exists in Matrix. Therefore, the selected standard import group is displayed for a person if no person group is specified in the import file. Only after import can assessment and appropriate processing take place.

If the preview is ok, press "Next". The following window is shown.

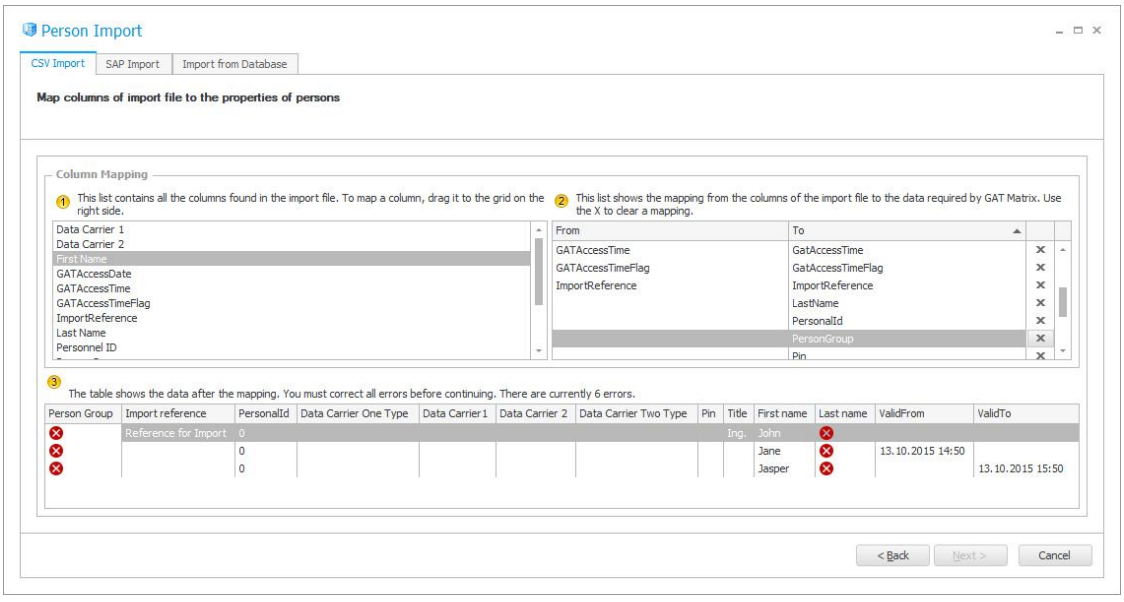


Figure 5.63 *- Person Import definition - Step 2 with incorrect mapping*

Here, you must define which columns (= data fields) of the import file to use for the data fields required by Matrix. Matrix attempts to assign the import fields as much as possible already with reference to the names of the columns. For columns where no match is found, you must assign the fields manually. The columns of the import file are shown in the top left field (1) and the data fields required by Matrix are shown in the column "To" in the top right field (2). In this field you can define the mapping from the import data fields to the data fields of Matrix by dragging a field from the top left field to the corresponding position in the column "From" in the top right field.

NOTE! If optional fields are defined in the personnel data (see "4.11. Optional fields for personnel data") they are also assigned here in the same way as the standard fields of Matrix. Pay attention that the imported values are of the same type as the corresponding data types of the optional fields. Otherwise, the person with a wrong data type cannot be imported or standard values are used (e.g., "01.01.0001" for the date). The behavior depends on the configured settings of the optional fields.

NOTE! Ensure that the data carrier number in the import file is always in decimal format (not in hexadecimal format).

The table at the bottom of the window (3) previews how Matrix will use the data from the import file. A red "X" icon displayed in this table means that the corresponding data field is not mapped correctly and must be checked.

If you want to use the "Valid from" and "Valid to" fields in the import file directly, but not the "GATAccessDate" GATAccessTime" and "GATAccessTimeFlag" fields from GAT Access, you must delete the assignments of these 3 GAT Access fields marked with the "X" icon. In addition, the previously defined date and time format is checked. If there are errors in the format, e.g., the date for the month or day is out of range (max. 12 or 31), or the "to" date is prior to the "from" date, an error symbol (red X) is displayed.

The next figure shows correct mapping.

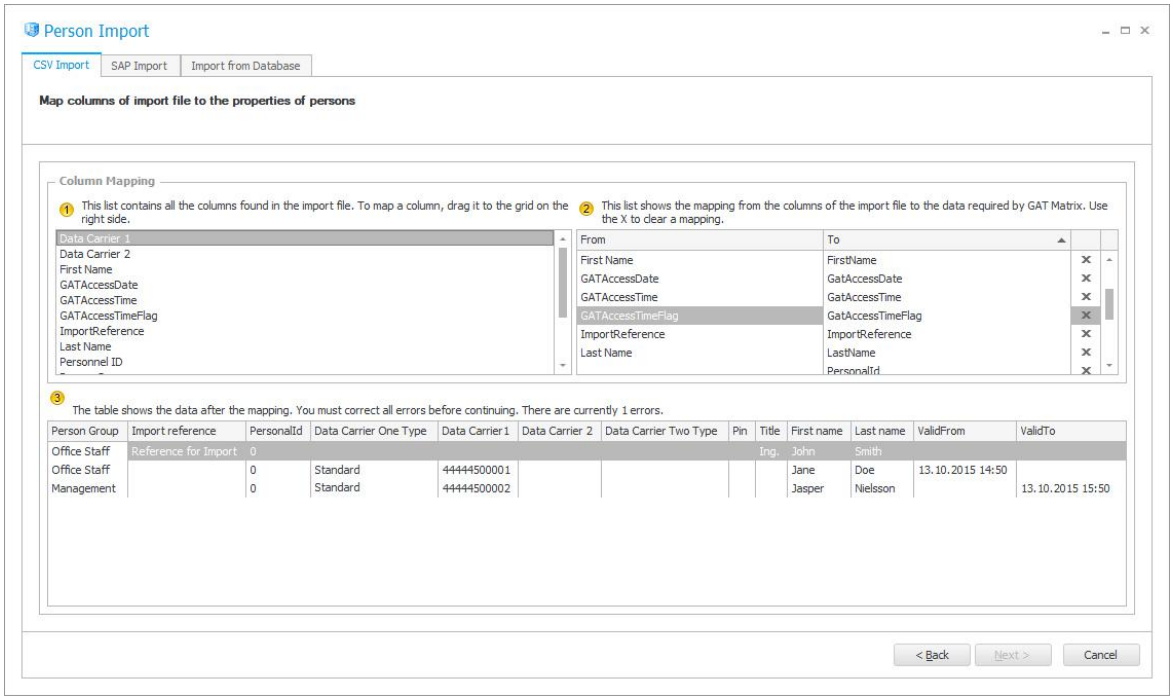


Figure 5.64 *- Person Import definition - Step 2 with correct mapping*

NOTE! The field "Import reference" in list (2) is only shown if the usage of an import reference was activated in the general settings (see chapter "4.8 Global settings").

Click on "Next" to proceed to the next step.

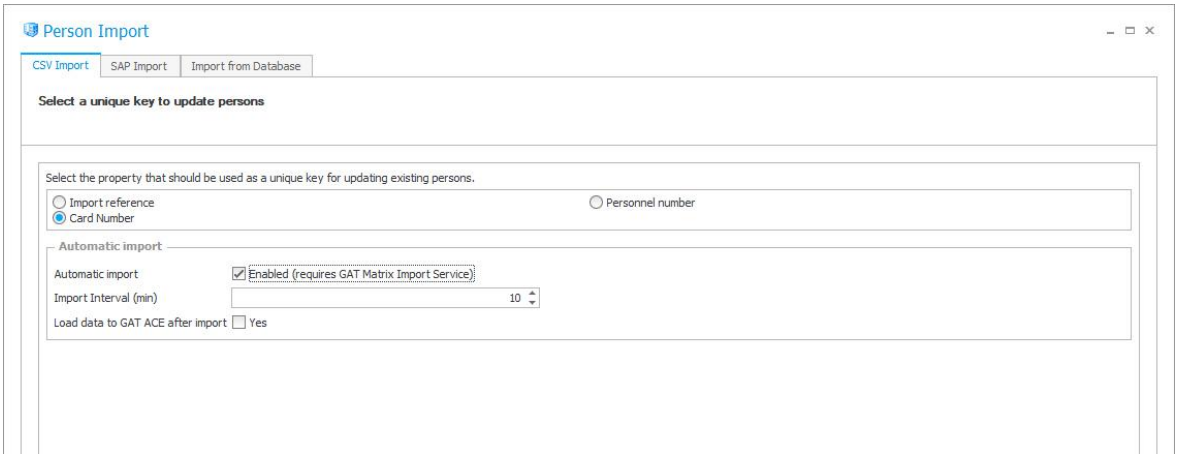


Figure 5.65 *- Person Import definition - Step 3*

If the import file contains persons who are already defined in Matrix, these persons will be updated with the information from the import file. Select which data shall be used for referencing the persons in Matrix with the imported person. "Import Reference" will use the field "Import Reference" of the personnel data, "Card Number" will use the "Data Carrier" field in the personnel settings and "Personnel Number" will use the "Personnel Number" field in the personnel settings for comparing the data.

NOTE! "Import Reference" can only be selected when this function was activated in the global settings (see "4.8 Global settings"). This allows to define an arbitrary value for the persons which will then be used for comparison on import.

Furthermore, you can define whether an automatic import should be executed at a predefined time interval. The import is carried out by the "Matrix - Person Import Service", which is available in the installation package and must be configured accordingly. Further information about the configuration of the import service can be found in chapter "11 PERSONS IMPORT SERVICE".

To activate the automatic import, the “Automatic Import” option must be enabled. The “Import Interval” option defines how often the import service will check the import file and import new persons. The “Load data to GAT ACE after Import” option allows you to upload the changes from Matrix to GAT ACE immediately after the import.

Click on "Next" and a new window will show if all information is correct.

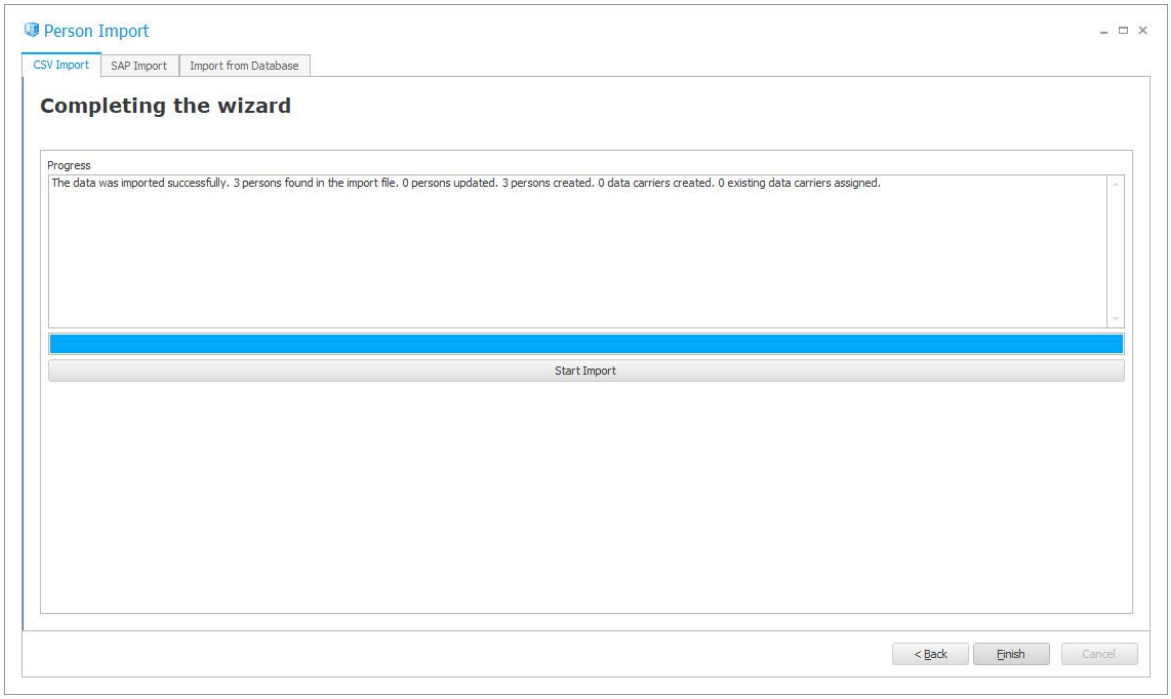


Figure 5.66 *- Person Import definition - Step 4*

You can start to import the persons by clicking on "Start Import". The status bar displays the import progress.

Finally, click on "Finish". The persons are added in the authorization matrix to the respective groups that were defined in the import data.

*If you want to edit or update the import file and import the same file again, you only need to click on the "Import Persons" button. The window from Figure 5.***66** *will open and you only need to click on "Start Import". To change settings, click on the "People Import" button at the top of the window to scroll back through the Import Wizard and make changes to the import settings.*

NOTE! Once the import is complete, the import file should be renamed or moved/deleted. If another import is performed later, the data that has been changed in Matrix in the meantime will be overwritten with the "old" data that is imported again.

5.7.2 Importing via SAP

To import persons from an SAP system or a comparable HR system via an SAP CC1 file, click on the "SAP Import" tab in the “Person Import” window ("Settings" menu, "Configure Person Import" menu item).

The import of persons can be done from an SAP system or a system that provides data compatible with the SAP CC1 format. Current SAP systems require a BAPI handler that creates the required format. The handler can be already installed by the customer for the SAP system or can be supplied by Gantner.

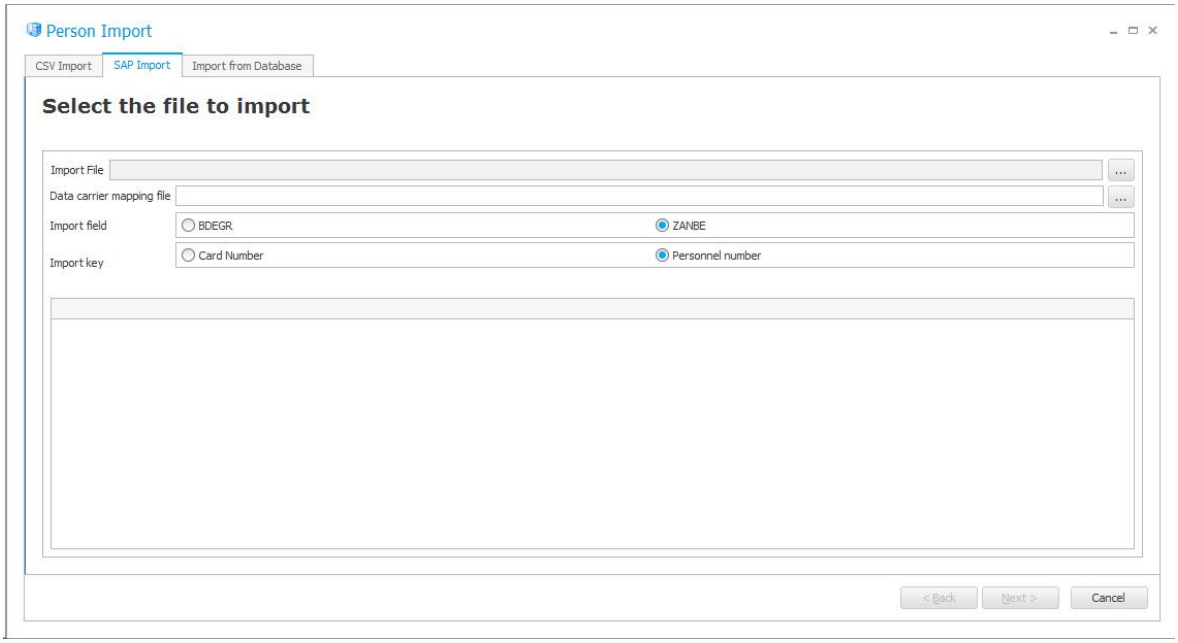


Figure 5.67 *– Person import via SAP*

The following settings are available for importing a personnel file:

- Import file: Click on the "..." button to select the file to be imported (format “.upd”). The default name of the file is "perso1.upd".
  See “Appendix D" for a description of the import file.
- Data carrier mapping file: In SAP CC1 format, the length of the data carrier numbers is limited. If longer data carrier numbers are used, this file can be used to recode the SAP data carrier number to the number actually used.
- Import field: Select in which SAP field the access authorizations are managed. The default option here is ZANBE. For more information, see “Appendix D”.
- Import key: Select which field should be used as the import key.

NOTE! If you are importing from an SAP CC1 file, map the "ACCESS_CONTROL_GROUP" field (previously named "ZANBE") to the person group number in Matrix. This field is a 2-digit, alphanumeric value in SAP.

NOTE! For the standard import group and the standard data carrier types, the information from the CSV import is used (see previous section). These must be set correctly on that window.

The rest of the import is similar to the import via CSV file.

5.7.3 Importing from database

With the import of persons from an external database you have the possibility to import personnel data from other programs into Matrix via a database. The import can be carried out manually or automatically. For an automatic import, the Matrix Import Service must be installed.

NOTE! Matrix and the Matrix Import Service do not clean up the import database tables. These must be self-cleaned by the remote terminal if desired.

The database import can also be used in parallel with the CSV and SAP imports. If an import is already running, any subsequent imports will wait until the first is finished.

► To configure the person, import from a database, click on the "Import from Database" tab.

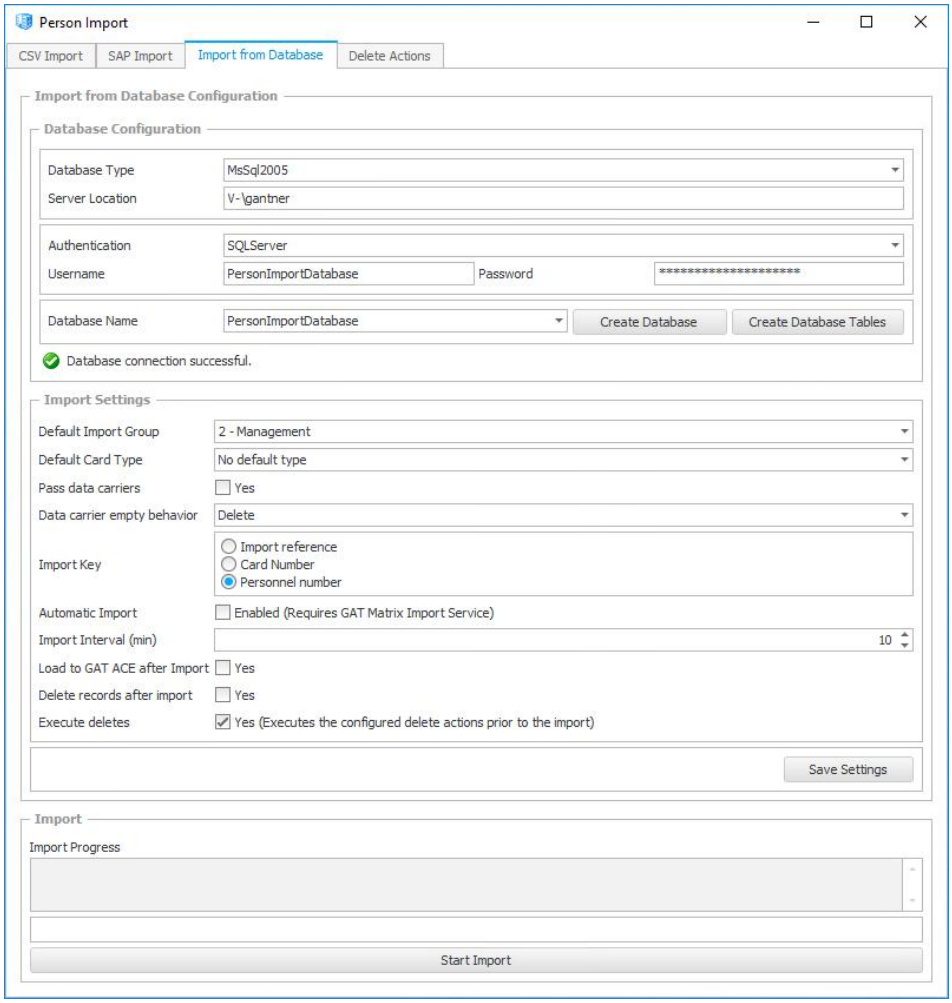


***Figure 5.68** – Person import from database*

► In the "Database Configuration" area, enter the details of the database that you want to import from.

The database can and should preferably be created from the Matrix import settings shown here. This ensures that all fields are created correctly.

- Database Type: Select the type of database ("MsSql2000" or "MsSql2005").
- Server Location: Enter the server name here (usually the computer name and the instance name of the database).
- Authentication: Select how Matrix should log into the database. This can be with SQL username and password or with Windows credentials. For SQL Server login, enter the username and password.
- Username/Password: For SQL Server login, enter the username and password here to connect to the database.

In the "Import settings" section, you can configure the import with the following fields.

- Default Import Group: Select here the default persons group in Matrix to which persons with no defined person group in the import file are to be assigned. When "No default group" is selected, a person group must be specified for each person in the import database. Persons without a specified person group are not imported.
- Default Card Type: Select here the default data carrier type that will be assigned to imported persons if a data carrier type is not already defined (see "5.6.4 Defining data carrier types" for information on card types).
- Pass data carrier: If this option is enabled, a data carrier can be transferred from one person to another through the import process without the data carrier having to be deleted by a person first. If the option is not enabled, an error occurs when you try to assign a data carrier to a person and the data carrier is still assigned to another person. The assignment is not allowed in this case.
  Note: This function is only possible for invalid records, i.e., if the person's validity date has not expired yet, the data carrier cannot be transferred. If the validity period has expired, the data carrier is removed from the +person and assigned to the new person.
- Field empty behavior: This option defines how the data carrier numbers of existing persons in Matrix should be handled during importation when no data carrier number(s) or "0" as the number(s) is/are defined:
  - "Delete": Only the data carriers that are assigned for importation (see next page) and have an empty import field or "0" in the import field are deleted. All unassigned data carriers remain.
  - "Ignore": The data carrier(s) of existing persons with an empty import field or "0" in the import field remain unchanged.
- Import Key: If the import file contains persons that are already defined in Matrix, these persons are updated with the data of the import file. Select here which information should be used to compare the persons in Matrix with persons in the import file. With the "Import reference" setting, the "Import reference" field is used for the transfer of persons. With the "Card Number" setting, the "Data carrier" field in the personnel data is used, and with the "Personnel number" setting the "Personnel number" field is used in the personal data.
  NOTE! The "Import reference" setting can only be selected here when the use of an import reference has been enabled in the general settings (see "4.8 Global settings"). This can be used to define any value for the persons used specifically for the import.
- Automatic Import: Select this option when you want to automatically import persons at defined intervals. The import is carried out by the "Matrix - Person Import Service", which is available in the installation package and must be configured accordingly (for details on configuring the import service, see chapter "11 PERSONS IMPORT SERVICE").
- Import Interval (min): This value defines at what intervals (specified in minutes) the import service will import persons when automatic import is activated. It should be noted that the interval begins to countdown after the completion of the import.
- Load to GAT ACE after Import:
  When this option is selected, the data is automatically loaded to GAT ACE after import.
- Delete records after import:

Select this option to delete the data records from the database after import and thus prevent multiple imports. Only successfully imported persons and their respective data sets (fingerprints and data carriers) are deleted.

- Execute deletes: Select this option to execute the configured delete parameters (see “5.7.4 Delete actions”) prior to the import.

► After you have configured the database import settings, save the changes by clicking on "Save Settings".

► In the lower "Import" section you can manually start the import, e.g., to check the entered data.

NOTE! When configuring the database, a file called “`personimport.hibernate.cfg.xml`” is created in the AppData folder for Matrix. This file, like the normal hibernate.cfg.xml, must be manually copied to the import service execution directory to allow the service to access the database (see "11 PERSONS IMPORT SERVICE").

If the “Delete actions” function is used with an SQL database, a file called "`delete.hibernate.cfg.xml`" is created in the AppData. This must also be copied to the execution directory, unless the “Use DB import settings” option is set to be used for the delete action. In that case, only the “`personimport.hibernate.cfg.xml`” is needed.

Overview of the database fields of a person:

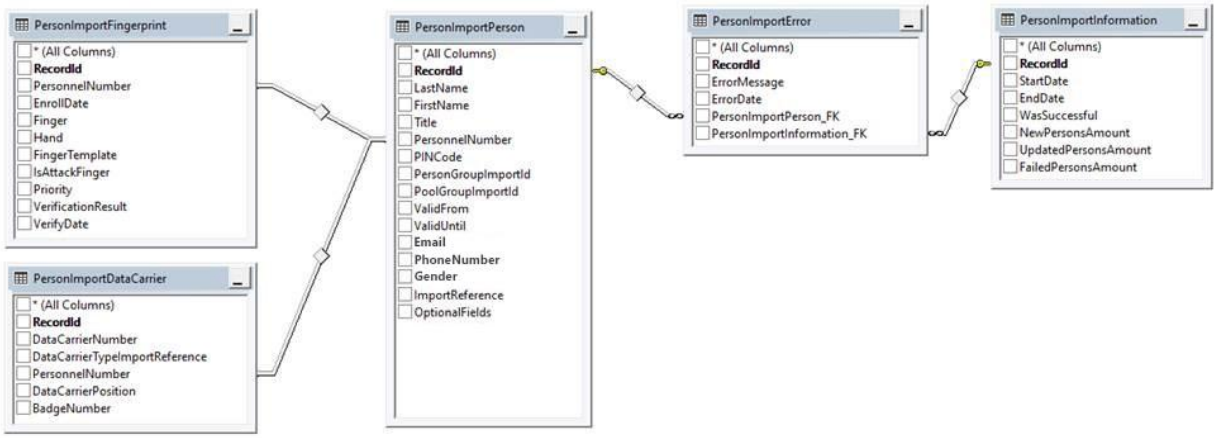


***Figure 5.69** – Database diagram of the import table*

- The "PersonImportPerson" table represents the person being imported.
- In the "PersonImportError" table, the Import Service writes any errors that occurred during an import. An error refers to the person and the import where the error occurred (i.e., in the PersonImportPerson and PersonImportInformation tables).
- The “PersonImportInformation” table represents a single person import that was run by the Import Service. Each time an import is performed, a new entry is written to this table.
- The "PersonImportDataCarrier" and "PersonImportFingerprint" tables on the left contain the data carriers and fingerprint data to be imported. A person from "PersonImportPerson" is linked to n data carriers in "PersonImportDataCarrier" and n fingerprints in "PersonImportFingerprint" via the "PersonnelNumber" field.
- There is only one default data carrier type for DB import.
- The data carriers in the "PersonImportDataCarrier" table are identified using the "PersonnelNumber" and "DataCarrierPosition" fields. This makes it possible for a person to re-import a data carrier with a number that has already been imported by using a different item number. To delete or overwrite a person's data carrier, the new data carrier number with the position of the data carrier to be deleted can be imported (e.g., data carrier 009 with position number 1 is overwritten by newly imported data carrier 010 with position number 1).

Table "PersonImportPerson"

Field	SQL data type	Comment	Mandatory field
RecordId	int	Primary key of the table	
LastName	nvarchar(100)	Surname	Yes
FirstName	nvarchar(100)	First name	No
Title	nvarchar(255)	Title of the person	No
PersonnelNumber	int	Employee number	Yes
PINCode	nvarchar(255)	PIN code of the person	No
PersonGroupImportedId	int	Import ID of the person group that the person will be imported to	Yes / No (2)
PoolGroupImportId	int	Import ID of the pool group to which the person is to be imported	No
ValidFrom	datetime	Start of the validity period of the person. ValidFrom must be before ValidUntil.	No
ValidUntil	datetime	End of the validity period of the person. ValidUntil must be after ValidFrom.	No
Email	nvarchar(255)	The person's email address. The string must be a valid email address.	No
PhoneNumber	nvarchar(255)	The person's phone number. The phone number begins with "+" and must be a valid number, e.g. "+43555233944".	No
Gender	Int	Information about the person's gender. The following four values are possible: 0: no information given 1: male 2: female 3: diverse If the field is empty or another value is given, "0" (no information given) will be used automatically.	No
ImportReference	nvarchar(255)	The defined import reference (if used)	Yes / No (1)

OptionalFields	nvarchar(MAX)	Format:
		`OptionalFields1Name|OptionalFields1Value;`
		`OptionalFields2Name|OptionalFields2Value;...`
		Name and value are separated by the character "|". Multiple fields are separated by a semicolon ";". The optional field definitions must exist in Matrix (see "5.6.1 Defining personnel master data")
			No

(1) *Depending on which criterion is imported.*

(2) *If no default import group is specified, the field is required. If the group does not exist with the ID provided, one will be created.*

***Table 5.1** – Fields of the "PersonImportPerson" table*

Table "PersonImportDataCarrier"

Field	SQL data type	Comment	Mandatory field
RecordId	int	Primary key of the table	
DataCarrierNumber	bigint(2)	Number of the data carrier	Yes/No (1)
DataCarrierTypeImportReference	int	Import reference of the data carrier type to be assigned to the data carrier	No
PersonnelNumber	int	Personnel number	Yes (3)
DataCarrierPosition	int	The position of the data carrier within the person's data carriers	Yes (4)
BadgeNumber	int	Number	Yes/No

(1) *Depending on which criterion is imported.*

(2) *If the associated data carrier type is used as the default for GAT ACE 3000, the data carrier number may only be max. 11 digits long. However, if the type is used for GAT ACE 7000, the data carrier number may be longer.*

(3) *Establishes the relationship to a person in the PersonImportPerson table.*

(4) *A person's data carrier is identified and updated exclusively via the PersonnelNumber and the DataCarrierPosition.*

***Table 5.2** – Fields of the "PersonImportDataCarrier" table*

Table "PersonImportFingerprint"

Field	SQL data type	Comment	Mandatory field
RecordId	int	Primary key of the table	
PersonnelNumber	int	Personnel number	Yes (1) (4)
EnrollDate	datetime	The enrollment date of the finger	No
Finger	int	The finger used	No (2) (4)
Hand	int	The hand used	No (3) (4)
FingerTemplate	Varbinary(MAX)	The fingerprint (template) of the finger	Yes
IsAttackFinger	bit	Indicates whether the finger is the duress finger	Yes
Priority	tinyint	The priority of the finger. The finger used most often should have the highest priority.	No
VerificationResult	int	An optional verification value that indicates how well a finger can be read	No
VerifyDate	datetime	The date of verification	No

(1) Establishes the relationship to a person in the "PersonImportPerson" table.

(2) 1 = thumb, 2 = index finger, 3 = middle finger, 4 = ring finger, 5 = little finger.

(3) 1 = left hand, 2 = right hand, 3 = unknown.

(4) A person's fingerprint is identified and updated using the PersonnelNumber, the hand, and the finger.

***Table 5.3** - Fields of the "PersonImportFingerprint" table*

Table "PersonImportError"

Field	SQL data type	Comment
RecordId	int	Primary key of the table
ErrorMessage	nvarchar(255)	The error that occurred
ErrorDate	datetime	The time when the error occurred
PersonImportPerson_FK	int	Reference to the "PersonImportPerson" table where the error occurred
PersonImportInformation_FK	int	Reference to the "PersonImportInformation" table where the error occurred

***Table 5.4** – Fields of the "PersonImportError" table*

Table "PersonImportInformation"

Field	SQL data type	Comment
RecordId	int	Primary key of the table
StartDate	datetime	Start date/time of the import
EndDate	datetime	End date/time of the import
WasSuccessful	Boolean	Indicates whether the import was successful
NewPersonsAmount	int	The number of new persons imported
UpdatedPersonsAmount	int	The number of persons who have been updated
FailedPersonsAmount	int	The number of persons who could not be imported

***Table 5.5** – Fields of the "PersonImportInformation" table*

5.7.4 Delete actions

In the “Delete Actions” tab, you have the possibility to delete personnel data from the Matrix database. The deletion can be carried out manually or automatically. A database or a CSV file can be used as the source for the delete actions.

► To configure a delete action, click on the "Delete Actions" tab.

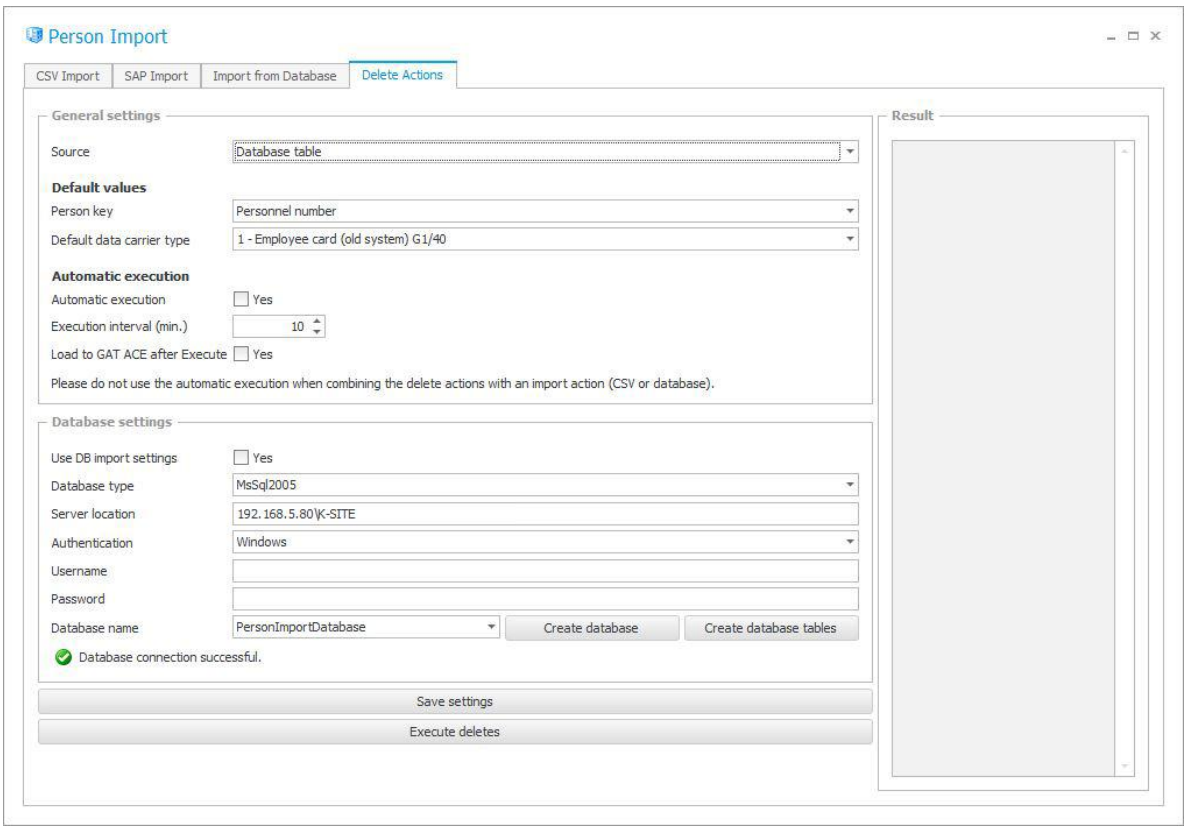


***Figure 5.70** – Deletion via database table*

► In the "General settings" area, enter the details of the database that you want to import from.

- Source: Select to delete data either via a CSV file or via a database table. The settings beneath the general settings change depending upon the source selection.
- Person key: If the delete file contains data that is already defined in Matrix, this data will be deleted according to the information in the delete file. Select here which information should be used to identify data in Matrix with data in the delete file. With the "Personnel number" setting, the "Personnel number" field is used to identify persons.
  With the "Import reference" setting, the "Import reference" field is used to identify persons. With the "Card Number" setting, the "Data carrier" field in the CSV or database table is used.
- Default data carrier type: Select the default data carrier type that will be used for identification during deletion if a data carrier type is not already defined in the data table (see "5.6.4 Defining data carrier types" for information on card types).

- Automatic execution: Select this option if you want to automatically execute the deletion at defined intervals.
- Execution interval (min): When the previous automatic execution setting has been selected, define here the intervals (in minutes) at which the action will automatically be executed. Note that the interval begins to countdown after the deletion is completed.
- Load to GAT ACE after Execute: When this option is selected, the data is automatically loaded to GAT ACE after execution.

► Depending on which source was selected (“CSV file” or “Database table”), configure the settings for the CSV file or database as required. A description of each setting is available in “5.7.1 Importing via CSV file” and “5.7.3 Importing from database”. For the database settings, select the “Use DB import settings” option to use the same settings as configured in the “Import from Database” tab.

► In addition, select what should be seen after deletion with the delete commands:

CSV – "After execution":

- Do not change file: The imported CSV file with the delete actions remains unchanged.
- Remove file: The CSV file is deleted. This setting is recommended to ensure the files that have already been deleted do not have to be edited again the next time they are deleted.
- Archive file: The CSV file is moved to a folder. You can select this in the "Path of archived files" field. The file name is assigned automatically according to the following format: "`gatmatrix_delete.archive.<Date><Time>`".

Database – "Delete records after execute":

- Yes: The successfully executed delete actions are deleted from the database. This setting is recommended so that these actions do not have to be edited again when you delete them again.

► After you have configured the settings, save the changes by clicking on "Save Settings".

► Alternatively, you can manually start the deletion by clicking on the "Execute deletes" button.

  ○ The results are displayed in the “Result” area to the right.

Overview of the database fields for delete actions with source "Database"

The "DeleteRecord" table serves as a source for the delete actions while data in the "DeleteRecordError" table is the results (errors & warnings) of these actions and filled in by Matrix.

Table "DeleteRecord"

Field	SQL data type	Comment	Mandatory
RecordId	int	Primary key of the table	
RecordType	nvarchar(255)	1 of 3 options available to set which data to delete: DP = delete person, DC = delete card, DF = delete fingerprint	Yes
PersonKey	nvarchar(255)	The number of the “Person key” setting defined in Matrix.	Yes / No (1)
DataCarrierNumber	nvarchar(255)	The number of the data carrier to be deleted.	Yes / No (2)
DataCarrierTypeImportId	int	The import ID number of the data carrier type.	Yes / No (2)
FingerprintHand	int	The hand number for fingerprint deletion. 1 = left, 2 = right, 3 = unknown	Yes / No (3)
FingerprintFinger	int	The fingerprint number for fingerprint deletion. 1 = thumb, 2 = index, 3 = middle, 4 = ring, 5 = pinky, 6 = unknown	Yes / No (3)

(1) *Only mandatory when deleting a person or a person’s fingerprints. Not mandatory for deleting a data carrier.*

(2) *Only mandatory when DC (delete card) is defined for RecordType.*

(3) *Only mandatory when DF (delete fingerprint) is defined for RecordType.*

***Table 5.6** – Fields of the "DeleteRecord" table*

Table "DeleteRecordError"

Field	SQL data type	Comment
RecordId	int	Primary key of the table
Severity	nvarchar(255)	The severity level for messages (“Warning” or “Error” are possible)
ErrorMessage	nvarchar(255)	The error that occurred
ErrorDate	datetime	The time when the error occurred
DeleteRecordId	int	Reference to the "PersonImportPerson" table where the error occurred

***Table 5.7** – Fields of the "DeleteRecordError" table*

Overview of the fields for the delete actions with source "CSV file"

The following table shows the fields in the CSV for the delete actions.

Delete fields in the CSV file

Field	SQL data type	Comment	Mandatory field
RecordType	string	1 of 3 options. Defines which data should be deleted: DP = person, DC = data carrier, DF = fingerprints	Yes
PersonKey	string	Personnel number of the person to be deleted.	Yes / No (1)
DataCarrierNumber	ulong	Number of the data carrier to be deleted.	Yes / No (2)
DataCarrierTypeImportId	int	ID number of the data carrier type.	Yes / No (3)
FingerprintHand	int	The hand from which fingerprints are to be deleted. 1 = left hand, 2 = right hand, 3 = unknown	Yes / No (4)
FingerprintFinger	int	Finger whose fingerprint is to be deleted. 1 = thumb, 2 = index finger, 3 = middle finger, 4 = ring finger, 5 = little finger, 6 = unknown	Yes / No (4)

(1) *Depending on the configuration under "Person key" / mandatory field if a person or a fingerprint is to be deleted. Not necessary to delete a data carrier.*

(2) *Mandatory field for RecordType "DC" (deletion of a data carrier).*

(3) *Mandatory field for RecordType "DC" (deletion of a data carrier). If not specified, the value from "Default data carrier type" is used*

(4) *Mandatory field for RecordType "DF" (deletion of a fingerprint).*

***Table 5.8 -** Delete fields in the CSV file*

If errors occur during the import, a file with the designation "`gatmatrix_delete.error.<Date><Time>`" is created in the same directory. A line with the following format is entered in this file for each error:

`Line: <LineNumber> - <Type> - < Description>`

The field `<Type>` can be "Error" or "Warning".

5.8 Pool groups

If you want to define access to an area where the number of persons who can access the area at one time is limited, you can use pool groups. An application example is the control of access to a parking lot that is used by several companies:

- Each company is assigned a certain number of parking spaces.
- For each company, a pool group is created.
- The employees of the companies are assigned to the relevant pool groups.
- When an employee enters the parking lot, they identify themselves using their data carrier. Before access is granted, it is checked whether there are still places left in the person's pool group. This requires the GAT ACE 7000 APB software.
- If the maximum number of employees for the pool group has already been reached, access is denied.

To configure the pool groups, complete the following steps.

► In the "Tools" menu, select the "Pool Groups" menu item.

○ The "Pool Groups" window opens where the existing pool groups are listed.

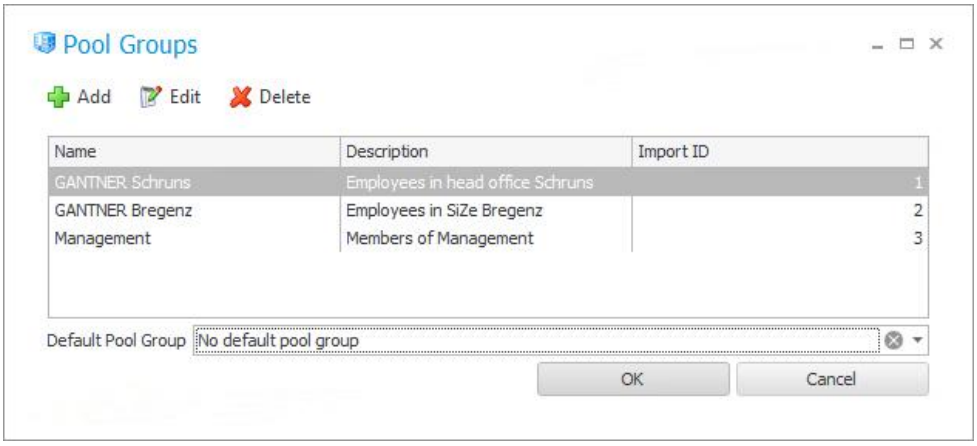


***Figure 5.71** – Pool groups window*

► To add a new pool group, click on "Add".

► To edit an existing pool group, select the group and click on "Edit".

○ In both cases, the "Pool Group" window opens.

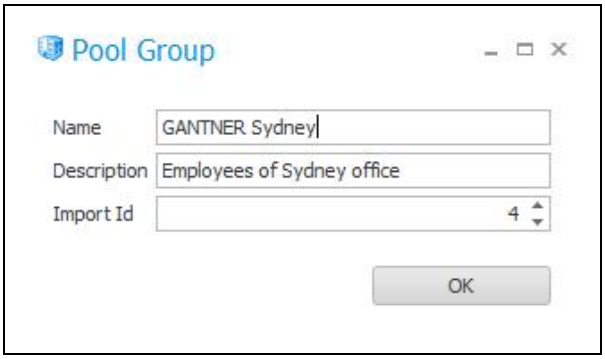


***Figure 5.72** – Defining a new pool group*

- ► Enter a name and, if desired, a description for the pool group.
- ► The Import ID is assigned automatically (next available) but can also be changed manually.
- ► Confirm with "OK".
    - ○ The pool group is displayed in the list of pool groups.
- ► You can now assign this pool group to the desired persons in Matrix, which occurs when defining the master data of a person (see "5.6.1 Defining personnel master data").
- ► In the “Default Pool Group” field, a pool group, which will be assigned to new persons by default, can be selected from the drop-down menu.

5.9 Multi-site policy

If the multi-site policy in Matrix is enabled and used, you can unlock individual person and door groups for each Matrix user. Users will then be able to see and edit only those groups unlocked for them. In addition, the use of several different corporate calendars for different locations (sites) is possible using the multi-site policy.

In conjunction with the multi-site function, which assigns a corporate calendar to each location imported from GAT ACE 7000 or GAT ACE 3000 (see "6.2 Locations"), it is possible to split a large location into multiple locations. Each location can only see the doors and persons of their location.

5.9.1 Enabling the multi-site policy

To use the multi-site policy, a special license is required that must be activated in the global settings (menu "Tools" -> menu item "Options").

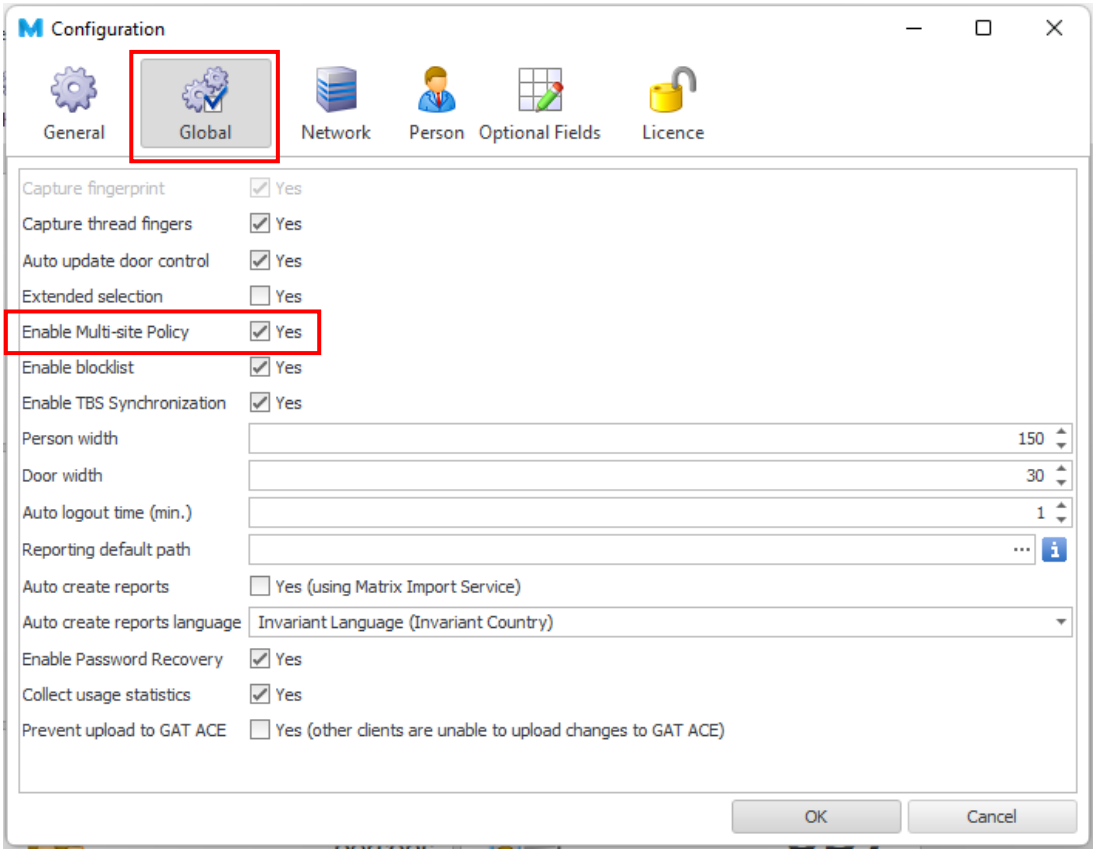


***Figure 5.73** – Global settings – Enabling the multi-site policy*

NOTE! If you change the multi-site policy setting (enabled to disabled or vice-versa), you must log out of Matrix and log in again for the change to take effect.

► To edit the multi-site policy settings, click on the menu item “Multi-site policy” in the "File" menu.
  ○ The following window is displayed. The window is divided into 3 tabs where you can assign the right for each user to see/edit the person groups, door groups, and corporate calendars.

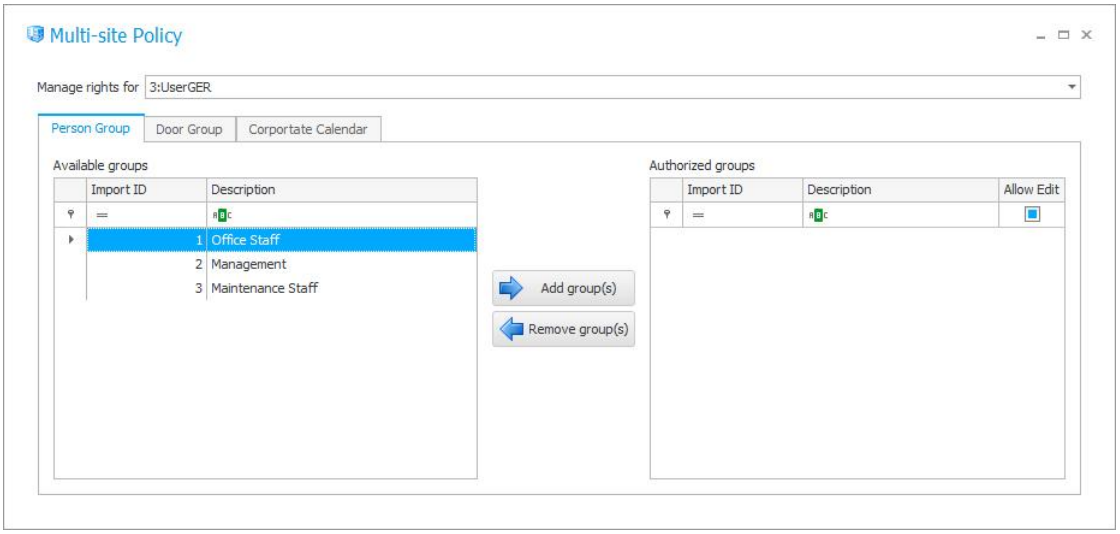


Figure 5.74 *- Assigning user rights - Person Group*

5.9.2 Assigning person groups

To assign person groups for a user, complete the following steps:

► Select the user in the "Manage rights for" field.

► Go to the "Person Group" tab.
  ○ The "Available groups" list on the left shows all the person groups available in Matrix (i.e., all the person groups that the currently logged-in user can see).
  ○ The "Authorized groups" list on the right shows all the person groups that are authorized for the selected user to see.

► Select one or more groups (with the UP or CTRL key) in the "Available groups" list then press "Add group(s)".
  ○ The selected groups are assigned to the "Authorized groups" list thereby granting permission for the user to see the groups.

► The “Allow Edit” option allows you to grant or deny permission for the user to edit (field is marked) or only see (field is not marked) the person group.

  NOTE! If the persons of a group are to be seen only, access authorizations can be assigned in this way without the master data of the persons having to be changed.

► To remove the assignment of a group, click on the group in the “Authorized groups" list then press "Remove group(s)".
  ○ The group is re-assigned to the "Available groups" list and is no longer authorized for the user.

5.9.3 Assigning door groups

To assign door groups for a user, complete the following steps:

► Select the user in the "Manage rights for" field.

► Go to the "Door Group" tab.

- The "Available groups" list on the left shows all the door groups available in Matrix (i.e., all the door groups that the currently logged-in user can see).
- The "Allocated groups" list on the right shows all the door groups that are authorized for the selected user to see.

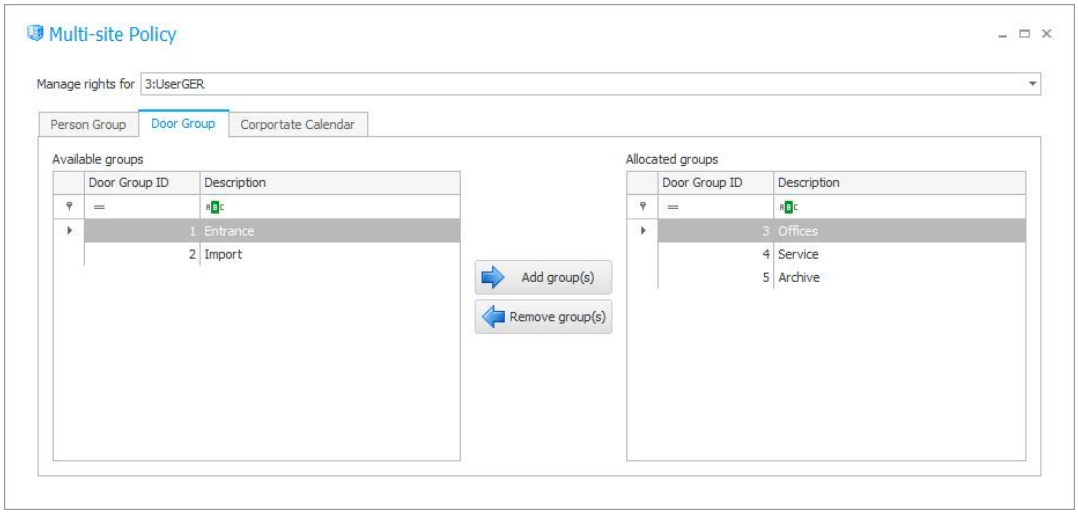


***Figure 5.75** - Assigning user rights - Door Group*

► Select one or more groups (with the UP or CTRL key) in the "Available groups" list then press "Add group(s)".

- The selected groups are assigned to the "Allocated groups" list thereby granting permission for the user to see/edit the groups.

► To remove the assignment of a group, click on the group in the “Allocated groups" list then press "Remove group(s)".

- The group is re-assigned to the "Available groups" list and is no longer authorized for the user.

5.9.4 Assigning corporate calendars

To assign corporate calendars for a user to edit, complete the following steps:

► Select the user in the "Manage rights for" field.

► Go to the "Corporate Calendar" tab.

- The "Available Calendars" list on the left shows all the corporate calendars available in Matrix (i.e., all the corporate calendars that the currently logged-in user can see).
- The "Allocated Calendars" list on the right shows all the corporate calendars that are authorized for the selected user to see.

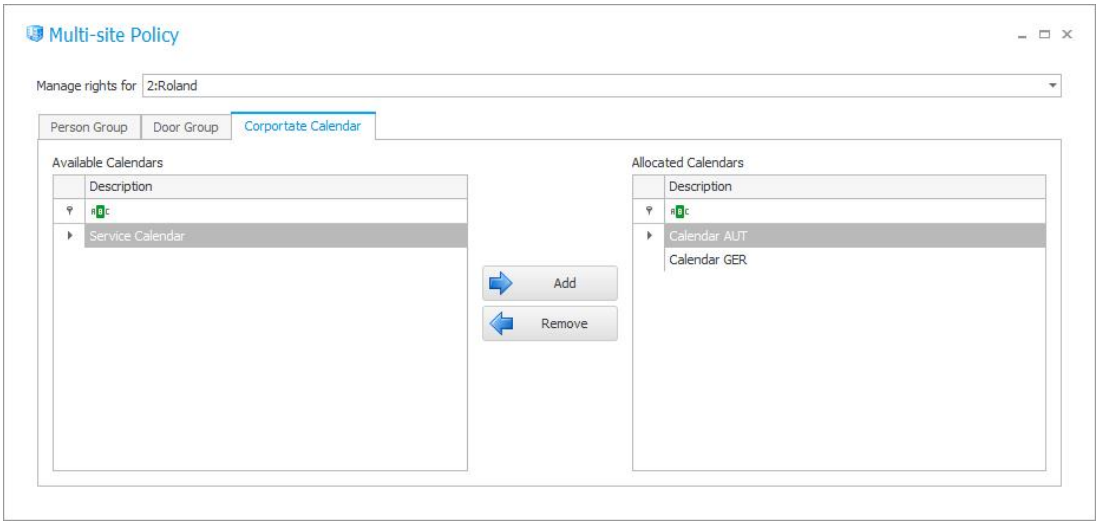


***Figure 5.76** - Assigning user rights – Corporate Calendar*

- ► Select one or more calendars (with the UP or CTRL key) in the "Available Calendars" list then press "Add group(s)".
    - The selected calendars are assigned to the "Allocated Calendars" list thereby granting permission for the user to see/edit the calendars.
- ► To remove the assignment of a calendar, click on the calendar in the “Allocated Calendars" list then press "Remove".
    - The calendar is re-assigned to the "Available Calendars" list and is no longer authorized for the user.

- ► You can select another user to assign groups and calendars to them.
- ► When you are finished configuring all the settings, close the window by clicking on the "X".

5.9.5 Enabling locker groups

If Matrix uses the Relaxx software and the electronic lockers from GANTNER, locker groups can be used for the control of lockers (see "5.19 Locker control"). To enable these locker groups for a system, complete the following steps:

- ► Select the client (user) in the "Manage rights for" field.
- ► Go to the "Locker group" tab.
    - In the list on the left, all locker groups available in Matrix are displayed, i.e., all the groups that the currently logged-in user is permitted to see.
    - In the list on the right under "Allocated groups", all the locker groups that are enabled for the selected user are displayed.

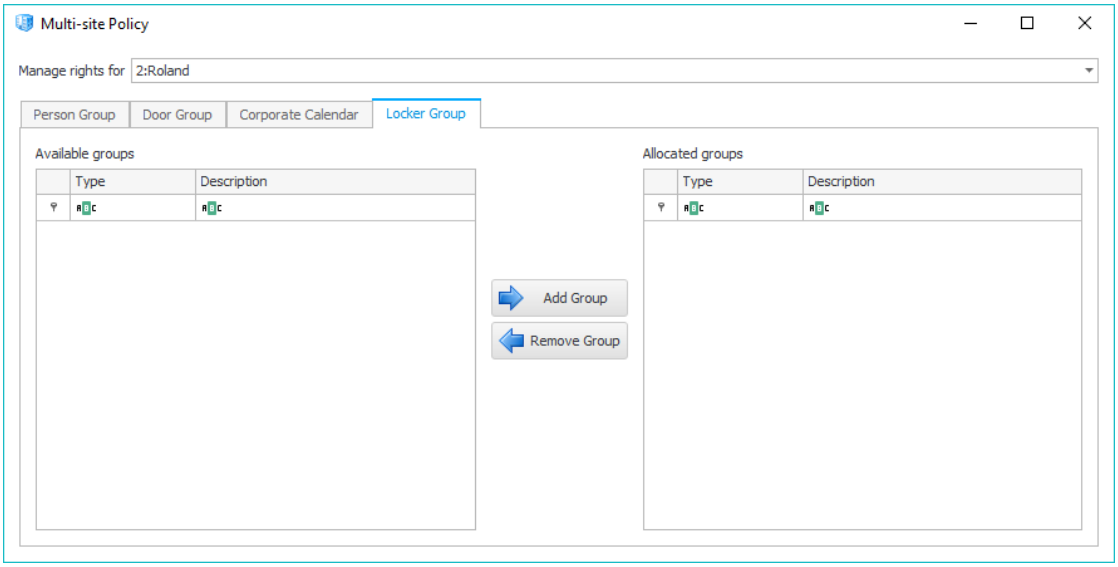


***Figure 5.77** - Define client rules - locker groups*

- ► Select one or more groups (using the shift or CTRL key) in the "Available groups" list and click "Add Group".
  - o The highlighted groups are transferred to the "Assigned groups" list thereby authorizing the groups for the user.
- ► To remove the assignment of a group, select the group in the right-hand list and click on "Remove Group".
  - o The group is transferred back to the "Available groups" list and is no longer authorized for the user.

5.9.6 Limitations of the multi-site policy

When using the multi-site policy, the following restrictions apply when editing persons and doors in Matrix.

Editing persons
The user can only edit a person (e.g., first name, last name, data carrier, etc.) when they have the right to see all access authorizations of the person.

Moving persons
The user can only move a person when they have the right to see all access authorizations of the person prior to being moved, and also only when the person does not receive access authorizations that the user is not allowed to see (e.g., through inheritance) after being moved.

Adding persons
A person may only be added if, after being added through inheritance, the person does not receive access authorizations that the user cannot see.

Deleting persons
The user can only delete a person when they have the right to see all access authorizations of the person.

Editing personnel time plans
The user can only modify, add, or delete a personnel time plan when they have the right to see all relevant person and door groups.

Editing door time plans
Door time plans may only be changed, added, or deleted if all relevant groups of person and door groups, for which the time plan is used, are visible to the user.

Editing corporate calendars
The user can only edit a corporate calendar when they have the right to see all the doors assigned to the calendar.

Import doors
To import doors, the user must have the right to see all person groups.

Loading doors
When loading doors, persons who are not visible to the user are ignored.

Complete initialization
A complete initialization is only possible for users who have the right to see all person and door groups.

NOTE! The multi-site policy does not affect the personnel time plans and personnel day plans. These apply to all users generally.

5.10 Data carrier blocklist

Using the blocklist, data carriers that are validated in the CardNET system can be temporarily invalidated. Data carriers added to the blocklist are invalid from when the change is transferred to the offline doors using the programming device.

The blocklist can only be used with offline doors where either the "CardNET" or "Hotel" operating mode is activated.
The blocklist can only be used for offline doors defined in GAT ACE 7000. For offline doors, defined in GAT ACE 3000, the blocklist has no function.
GAT Mobile Access Management does not use the blocklist function.

For the blocklist to be used, it must be enabled first.

► To enable the blocklist, select the "Options" menu item from the "Tools" menu.
  ○ The “Configuration” window opens.

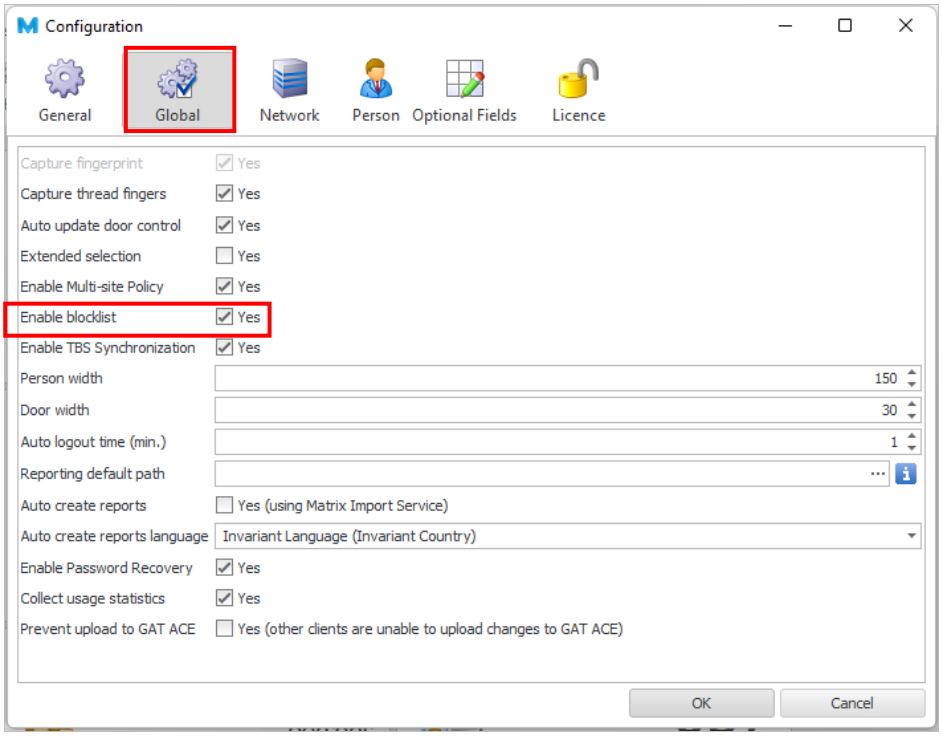


***Figure 5.78** – Enabling the blocklist*

► Go to the "Global" tab and select the "Enable blocklist" option.
  ○ The "Blocklist" icon is now displayed in the Matrix toolbar.

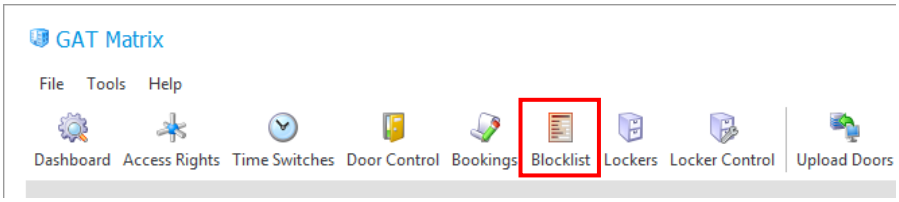


***Figure 5.79** – Blocklist icon*

► Click on the "Blocklist" icon.

○ The blocklist configuration page opens.

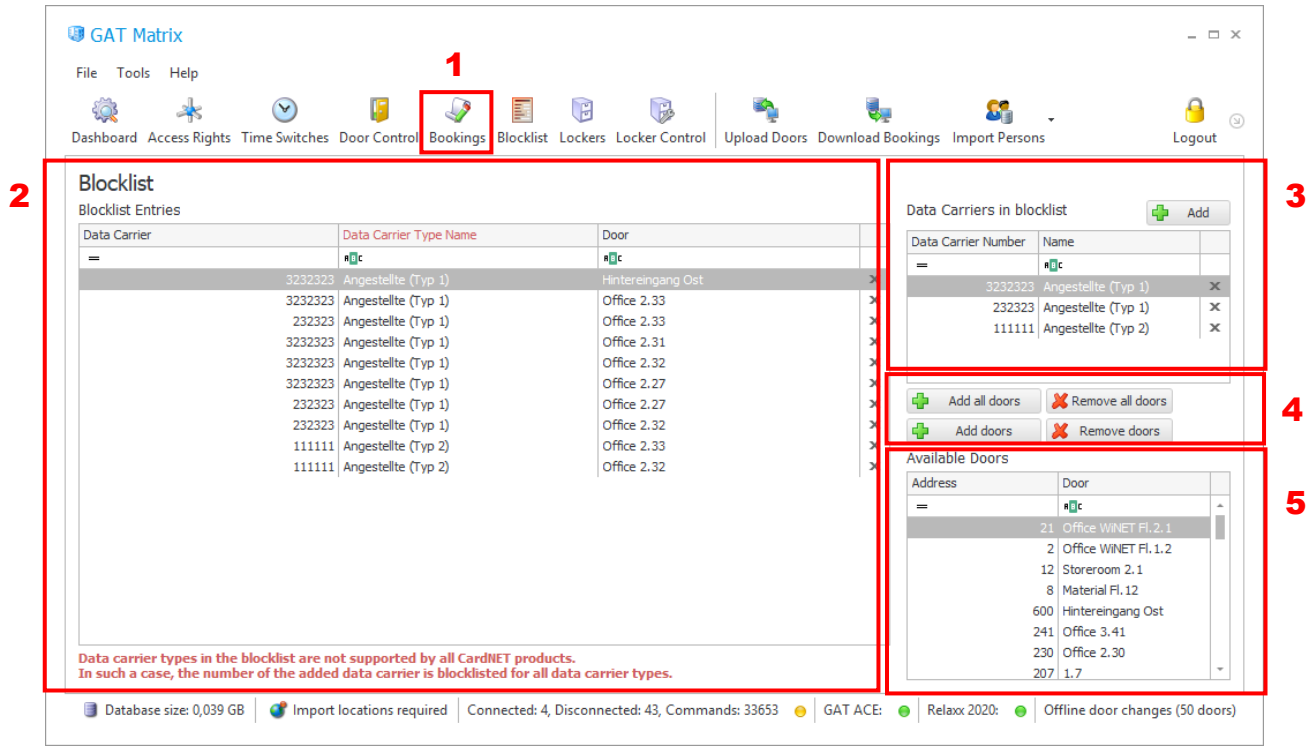


***Figure 5.80** - Blocklist*

The image shows an example with 7 data carriers in the blocklist. The window is divided into the following areas:

1 – Blocklist icon: Displays the blocklist in Matrix.

2 - Blocklist entries: Displayed here are all data carriers currently entered in the blocklist including the data carrier type and the doors to which the data carrier is assigned. To filter the display, enter the desired information in the header field of the table. For example, to display only a specific data carrier or door, enter the data carrier number or the door name in the relevant header field.

3 - Data carriers: Shown here are all data carriers that are assigned to the blocklist.

4 - Door assignment: Use these buttons to assign doors, where access is to be restricted, to the data carriers in the blocklist. You do not have to assign all doors to which a data carrier has authorization. Only assign those doors that are a security issue within the validity period of the data carrier.

5 - Door list: Listed here are all available offline doors, operating in CardNET or Hotel mode, which can be assigned to the data carriers in the blocklist. Doors operating in one of these modes are displayed with red ID numbers in the Matrix view.

5.10.1 Adding data carriers to the blocklist

When a person or data carrier is deleted in Matrix, a notification is displayed asking whether the data carrier should be automatically assigned to the blocklist (see "5.6.15. Deleting a person"). You can also manually enter data carriers into the blocklist.

► Click on “Add” in the data carrier list (3).

○ A window opens with all available data carriers in Matrix.

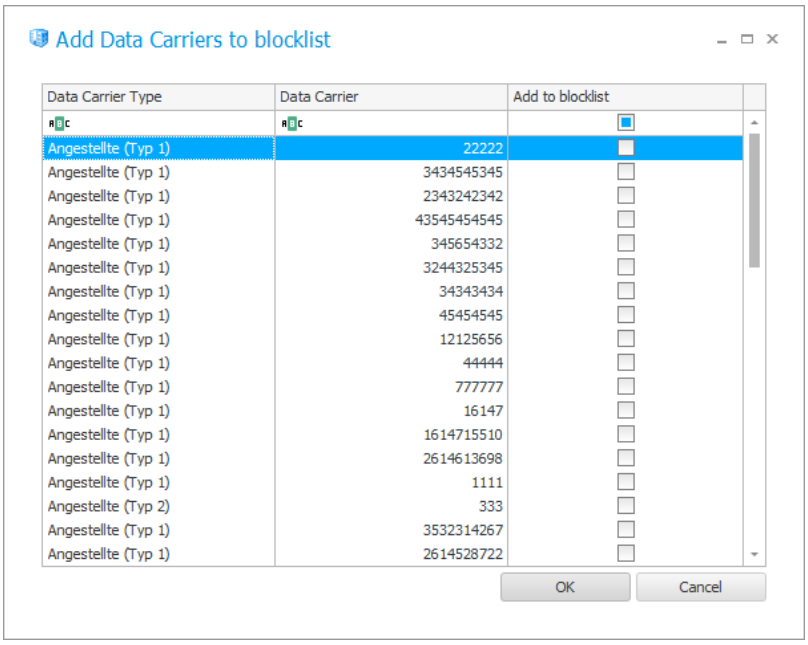


Figure 5.81 *- Available data carriers in Matrix*

► Select the data carrier(s) that you want to add to the blocklist.

► Click on "OK".

○ When a data carrier is transferred to the blocklist, the data carrier is deleted from the person to whom it was assigned. Matrix displays a corresponding message. Confirm with "Yes" or cancel with "No".

○ If you confirm with "Yes", the data carrier is added to the data carrier blocklist.

5.10.2 Assigning data carriers to doors

After a data carrier is added to the blocklist, it is not blocked from accessing all offline doors. You must first assign the relevant doors to it.

► Click on the desired data carrier in the list (3).

► To assign the data carrier to all available offline doors, click on "Add all doors".

► To assign the data carrier to specific offline doors, select the desired doors from the "Available Doors" (5) list. Use the “Ctrl” or “Shift” key to mark several doors here. Note that only those doors that the Matrix user is allowed to see according to the multi-site policy definition (if this function is used) are shown here.

► Click on "Add doors".

○ The data carrier and the assigned doors are entered into the blocklist.

Note that offline controllers can only store a blocklist with a limited number of data carriers. A warning is displayed in Matrix when too many data carriers are assigned to an offline door.

5.10.3 Deleting data carriers and door assignments from the blocklist

Data carriers that are entered into the blocklist cannot be assigned to persons. If you want to reuse a data carrier or remove it from the blocklist generally, proceed as follows.

- ► To delete the assignment of a data carrier from a single door, click on the "X" icon in the assignment line of the blocklist (2).
- ► To delete a data carrier from the blocklist, click on the "X" icon next to the data carrier in the list (3). Note that only users who see all the doors assigned to the data carrier (see "5.9 Multi-site policy") can delete the entry.
    - ○ A notification is displayed asking whether the data carrier is to be deleted. Click "Yes" to remove it from the blocklist or cancel with "No".
    - ○ A further notification is displayed asking whether the data carrier's door assignments should also be deleted from the blocklist. Click "Yes" to delete the assignments from the blocklist. Clicking "No" means that these assignments remain, and you do not have to redefine them should you need to re-insert the data carrier into the blocklist.
- ► To assign the data carrier to specific offline doors, select the desired doors in the "Available Doors" list (5). You can use the Ctrl or Shift key here to select multiple doors.
- ► Click on "Add doors".
    - ○ The data carrier with the assigned doors is added to the blocklist.

ATTENTION! Only delete a data carrier from the blocklist after it has been returned or after the data carrier authorization period has expired, i.e., the time of the last booking or the time of the blocklist entry + the updated authorization period, e.g., 7 days. This ensures that the data carrier no longer presents a security risk and can be deleted from the blocklist to make room for new entries.

5.10.4 Importing personnel data with blocklist

When data carriers are deleted after the import of personnel data, they are not automatically entered into the blocklist.
When a data carrier that has been entered into the blocklist is imported during the personnel data import, the entire associated import line is ignored, and a corresponding entry is created in the import log file.

5.11 Defining personnel time plans

To define a personnel time plan, click on the toolbar button "Personnel Time Plans" in the main window. The main window changes to the personnel time plan view.

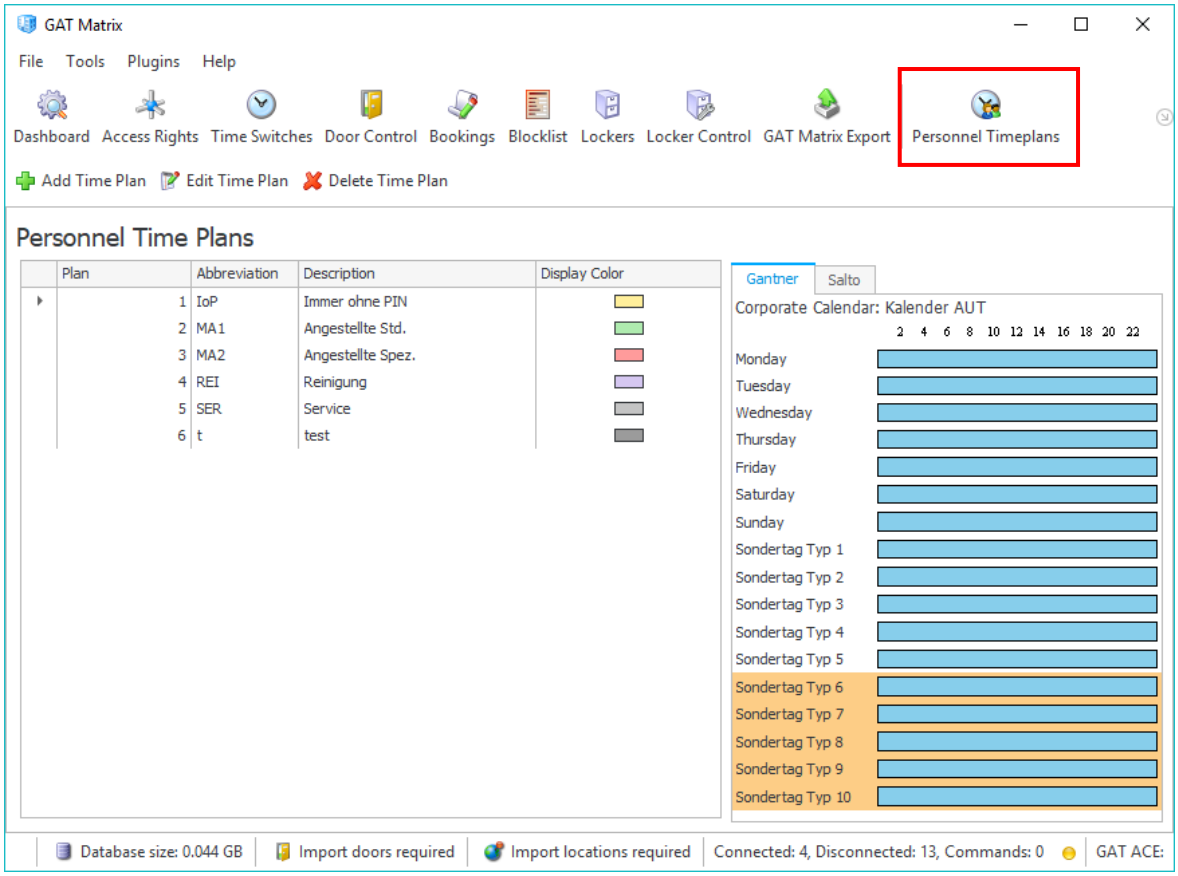


Figure 5.82 *- Personnel Time Plan definition*

The list on the left side shows the defined personnel time plans. By selecting a personnel time plan with the left mouse button, the plan will be shown graphically on the right side of the window. The colored bars represent the day plans assigned to the different days and the colors indicate the functions that are active during the corresponding time intervals. When the mouse pointer is positioned over a time interval the defined functions will be shown in clear text.
If ProAccess SPACE is being used, the display of day plans is divided into two tabs (for GANTNER and SALTO doors). You can display the desired day plan by selecting the tab at the top.

- ► To add a new personnel time plan, press the “Add Time Plan” button on the top of the personnel time plan list.
- ► To change the settings of an existing personnel time plan, double-click with the left mouse button onto the time plan.
    - In both cases the following window is shown.

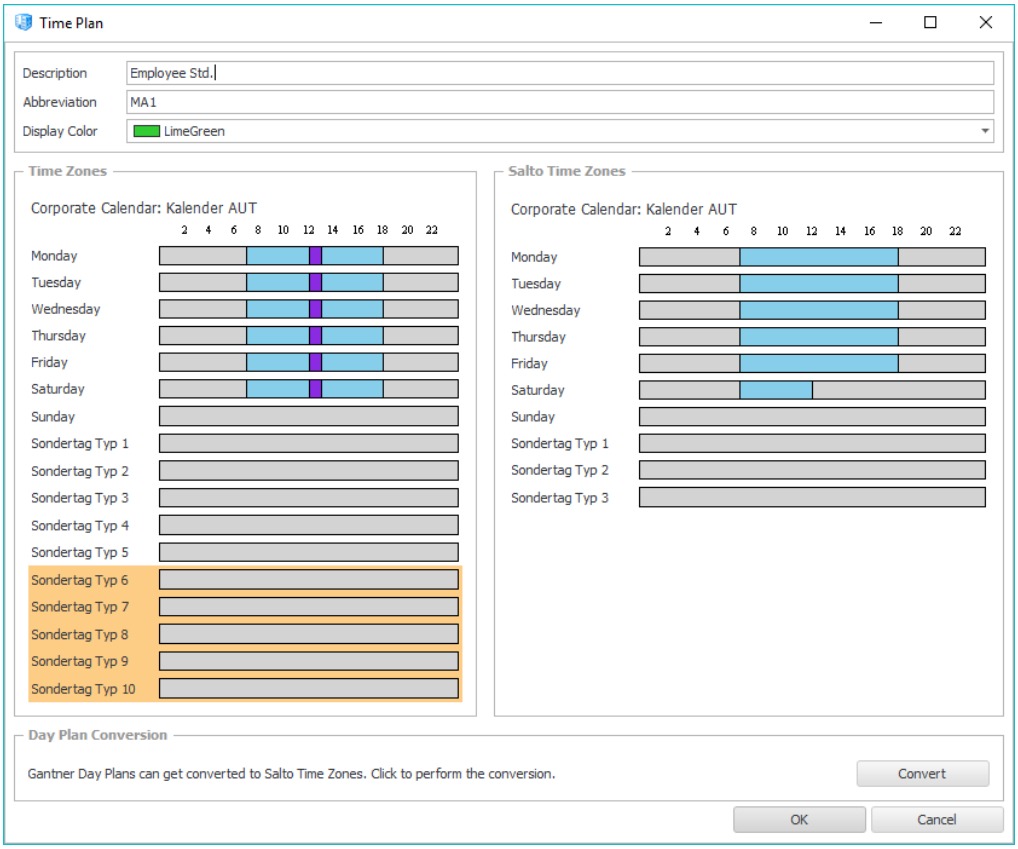


Figure 5.83 *- Settings of a Personnel Time Plan*

NOTE! GAT ACE 7000 only supports the special days 6 to 10 marked in orange. The colored markers are only displayed when GAT ACE 3000 is used.

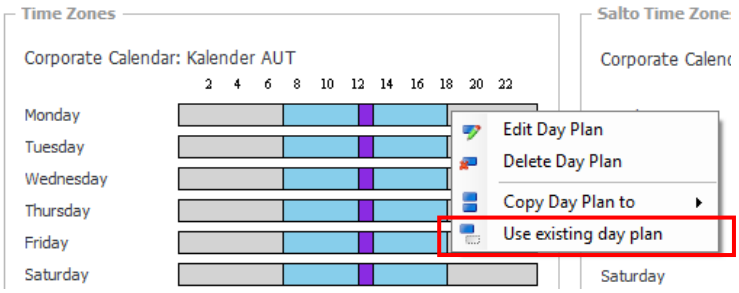
For a new personnel time plan this window is empty. For an existing personnel time plan, the assigned day plans are displayed for each day. For the GANTNER doors in a day plan, Matrix supports multiple time periods and different functions such as PIN code entry or special authorizations. For the doors imported from SALTO ProAccess SPACE, different functions are not possible for the time periods. Therefore, the display is separated into the time plans for the GANTNER doors (left "Time Zones" area) and the doors imported from SALTO ProAccess SPACE ("Salto Time Zones").

The following fields are used to configure the personnel time plan.

- Description: Enter a description for the personnel time plan.
- Abbreviation: Enter up to 3 alphanumerical letters or digits for the personnel time plan. These letters will be used in the authorization matrix to indicate the assigned personnel time plans.
- Display color: Select a color from the list box. This color will be used in the authorization matrix to indicate the assigned personnel time plan.
- Day fields: The day fields in the lower part of the window (17 fields on the left for GANTNER doors, 10 fields on the right for SALTO doors) show the day plans assigned to the employee schedule on individual days. It is possible to define a day plan for each individual day of the week and for up to 10 special days (GANTNER) or 3 special days (SALTO) (see "6. CORPORATE CALENDAR AND LOCATIONS"). The last 5 special days for GANTNER doors (marked orange) are only supported by GAT ACE 7000.

5.11.1 For GANTNER doors: assigning, changing, deleting day schedules

► To assign a day plan to a day, double-click on an empty day field in the left "Time Zones" area or right-click on a day field and select "Use existing day plan" from the menu.



○ The following window opens.

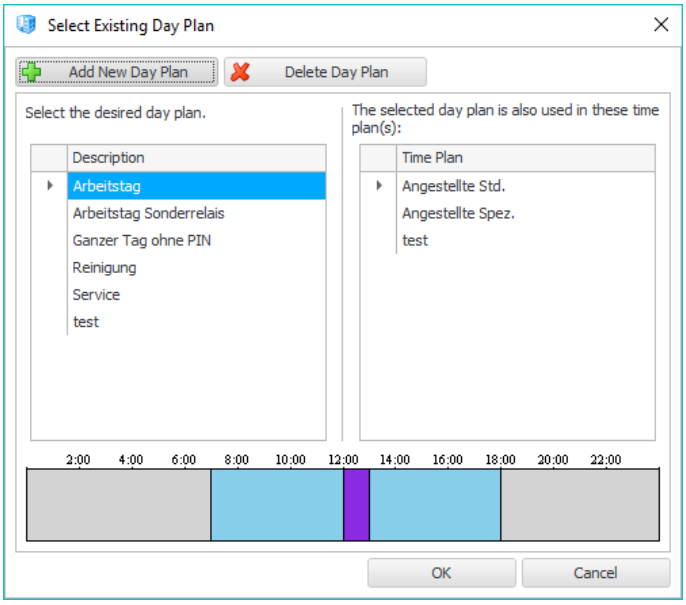


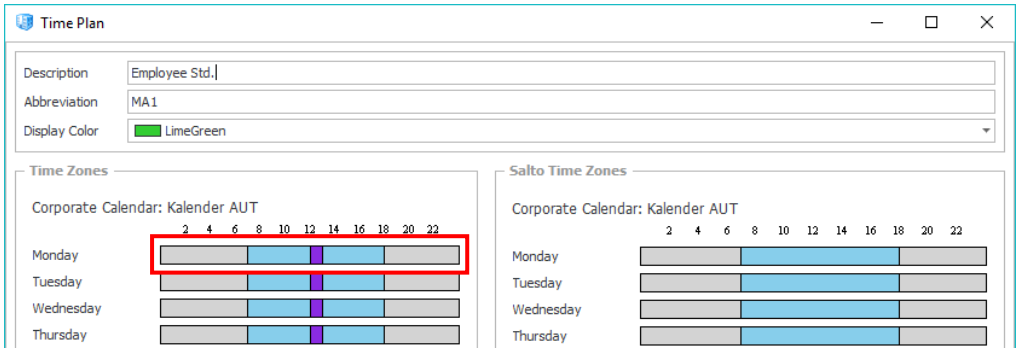
Figure 5.84 – *Assigning a day plan to a day*

The desired day plan can be selected in the left list. The right list displays the time plans that the selected day plan is already assigned to, and in the lower field a graphical representation of the day plan is shown. When you hover the mouse over this representation, the settings of the day plan are shown.

In this window you can add a new day plan by clicking on "Add New Day Plan". The settings window for the day plan will be opened (see "Figure 5.86").

► **Changing the settings of a day plan**

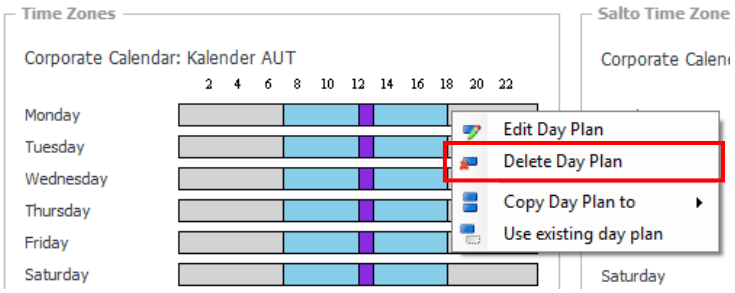
To change the settings of a day plan in a time plan window, double-click with the left mouse button on a day with an assigned day plan.



- The day plan window opens (see “5.11.2 For GANTNER personnel time plans: settings for day plans") where you can change the settings.

► **Deleting a day plan from a day**

To remove a day plan from a day, right click onto the day plan and select "Delete Day Plan" from the shown context menu.



- Depending on the general deletion setting (see "4.7. General settings"), either a confirmation window is displayed, or the day plan is deleted directly without additional confirmation. The day plan is only removed from the selected day but is not deleted completely.

► **Using a day plan with another day**

To use a previously assigned day plan for other days, simply drag & drop the day plan from one day to the other days.

Another option is to right click onto the day plan and select "Copy Day Plan to >" from the menu. Here you can select the day(s) where the day plan shall be copied to. With "WeekDays", "Workdays" or "SpecialDays" the day plan will be copied and assigned to all weekdays, workdays, or special days at once.

5.11.2 For GANTNER personnel time plans: settings for day plans

Day plans can be defined for **personnel time plans** and for **door time plans**. This section describes the day plans for personnel plans.

These settings apply to the day plans for the GANTNER doors and persons. For the SALTO doors and persons, only one time interval can be set (see next section).

A day plan for a personnel time plan defines the authorization functions for a person during a day. Up to 10 time intervals can be defined and during each of these time intervals different authorization functions can be set.

► **Defining a new day plan**
To define a new day plan, right-click onto an "empty" day plan field (on a day that has no day plan assigned) and select "New Day Plan" from the menu.

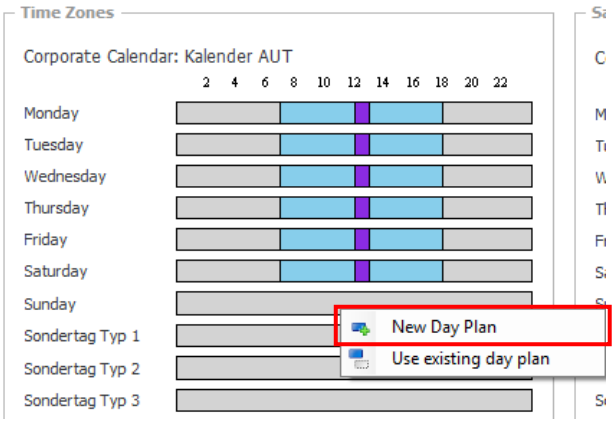
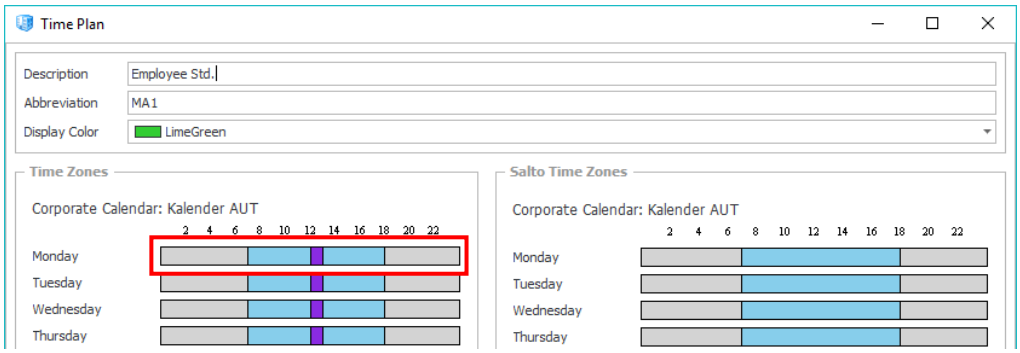


Figure 5.85 – *Adding a new day plan*

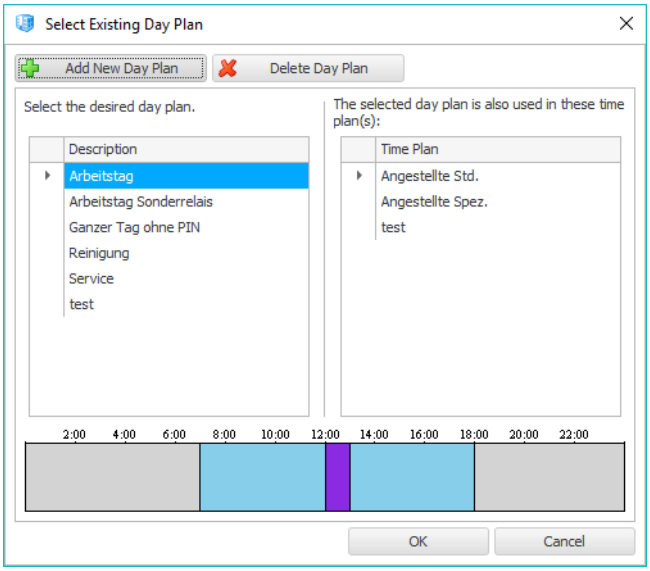
- The "Edit day plan" window opens (see Figure 5.**86**).

► **Changing the settings of an existing day plan**
To change the settings of an existing day plan, double-click onto the graphical representation of the day plan, where it is assigned to a day.

NOTE! When a day plan is changed, the changes are also applied to all other weekly plans that use this day plan.



You can also double-click on an empty day to open the "Select existing day plan" window, where all existing day plans are displayed.



- The "Edit day plan" window opens.

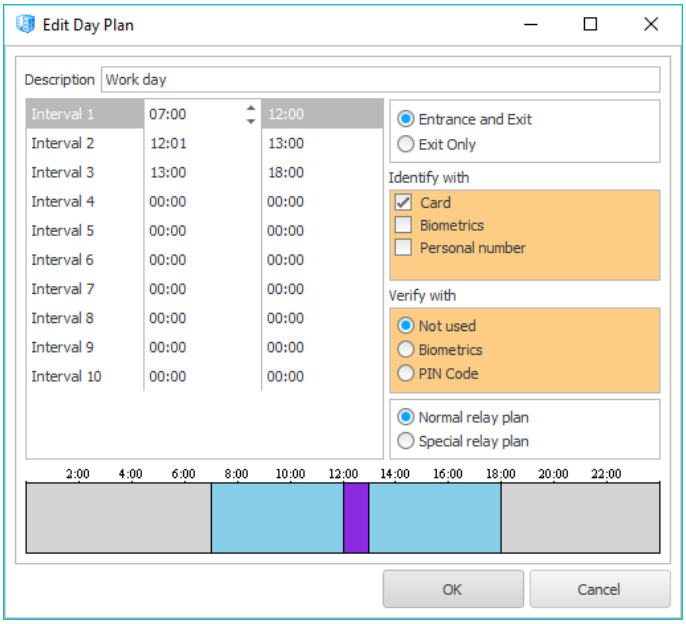


***Figure 5.86** – Day plan settings of a personnel plan*

NOTE! The functions marked in orange are only supported by GAT ACE 7000. GAT ACE 3000 only distinguishes between identification and/or verification but does not evaluate the details.
These colored markings are only displayed if a GAT ACE 3000 is also used.

In the window "Edit day plan", the following settings of a day plan can be defined:

- Description: Enter a description for the day plan in this field.
- Interval list: In the list on the left, select an interval and define the start and end time of the time interval.
- Functions: On the right side, select the functions that will be active during the selected time interval. The selected functions are indicated in color in the bar at the bottom of the window. The following functions are available:
  - "Entrance and Exit": Authorization for both entry and exit directions.
  - "Exit Only": The person is only allowed to exit at the door. The terminal at the door must be set to detect entry and exit correctly.
  - "Identify with": Select how users are identified. Identification via data carrier ("Card"), fingerprint ("Biometrics"), and/or PIN code is possible. Only applicable for GAT ACE 7000.
  - "Verify with": In addition to identification, you can activate an additional verification via fingerprint ("Biometrics") or PIN code. "Not used" means that identification alone is enough. Only applicable for GAT ACE 7000.
  - "Normal-/Special Relay Plan". Depending on the selection, the time window uses the normal or special relay plan (see "5.15 Relay time plans" for more information).

5.11.3 For SALTO doors: creating, changing, deleting time zones

Several time zones per day can be set for the doors that are imported from ProAccess SPACE. After assigning the time plan to a person and door, the authorization of the person is valid during the time zones, but invalid outside of the defined time zones.
The additional settings that are available for the GANTNER doors are unavailable for the time zones.

► **Adding a time zone**
To add a time zone to a day, right-click on an empty area of the day field and select "New Time Zone" from the menu.

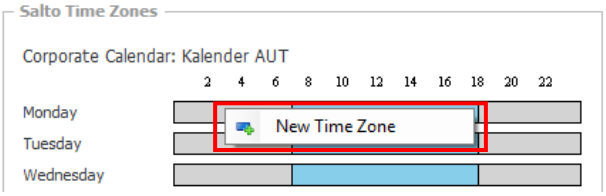


***Figure 5.87** – Salto Time Zones*

Note: For a day without a time zone, you can also double-click in the empty day field.

- ○ The following window opens for entering the time zone.

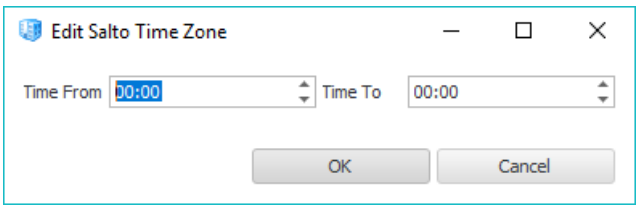
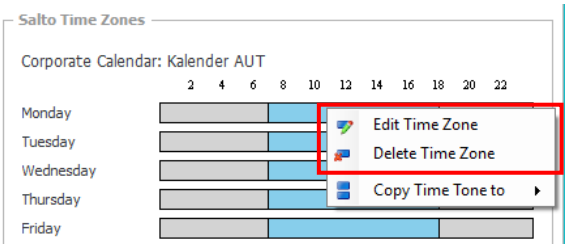


***Figure 5.88** - Time zone for a SALTO day plan*

► Enter the start and end time here and confirm with "OK".
- A time zone with the defined times is added to the SALTO personnel plan.
- If a person at a terminal is assigned to this plan, access is only possible during the time zone.

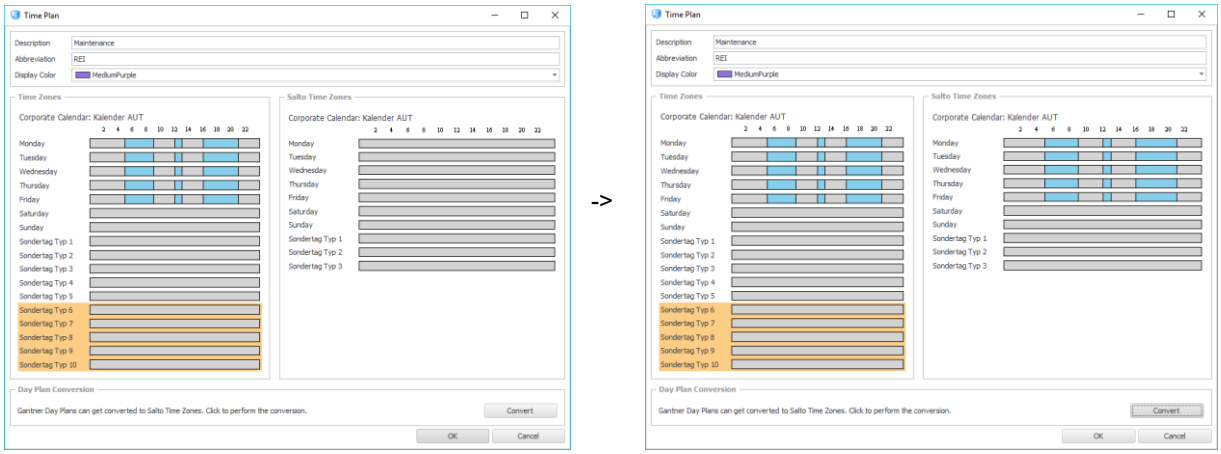
► **Editing or deleting a time zone**
To delete or edit an existing time zone, right-click on the zone and select the desired action from the menu.



► **Copying a time zone to another day**
If you want to use a defined time zone with another day, right click onto the time window and select the desired day from the "Copy Time Zone to" menu option.

5.11.4 Converting a GANTNER personnel plan to a SALTO personnel plan

It is possible to convert a day plan created within Matrix for GANTNER devices to SALTO time zones. In this case, the time zones defined for each day in the GANTNER plan are copied to the SALTO time plan page. The functions that have been configured in the GANTNER plan (e.g., with or without PIN code, entry or exit, etc.) are not copied because these are managed by the doors in the SALTO system rather than by the person. For this reason, it may be necessary to create door plans for SALTO doors in addition to the personnel plans in order to define functions for SALTO products that are comparable to GANTNER devices (see "5.12 Defining door time plans").



► To convert the GANTNER plan, click the "Convert" button.

- The time zones of the GANTNER plan (left side) are transferred to the corresponding days of the SALTO plan (right side) and displayed accordingly with colors for the different functions.
- The time zones in the special days 4 to 10 are ignored since the SALTO plans only support 3 special days.

► Then confirm by clicking on "Save".

When pressing "OK", Matrix checks if a conversion is required and possible. A message is shown allowing you to decide whether to carry out the conversion.

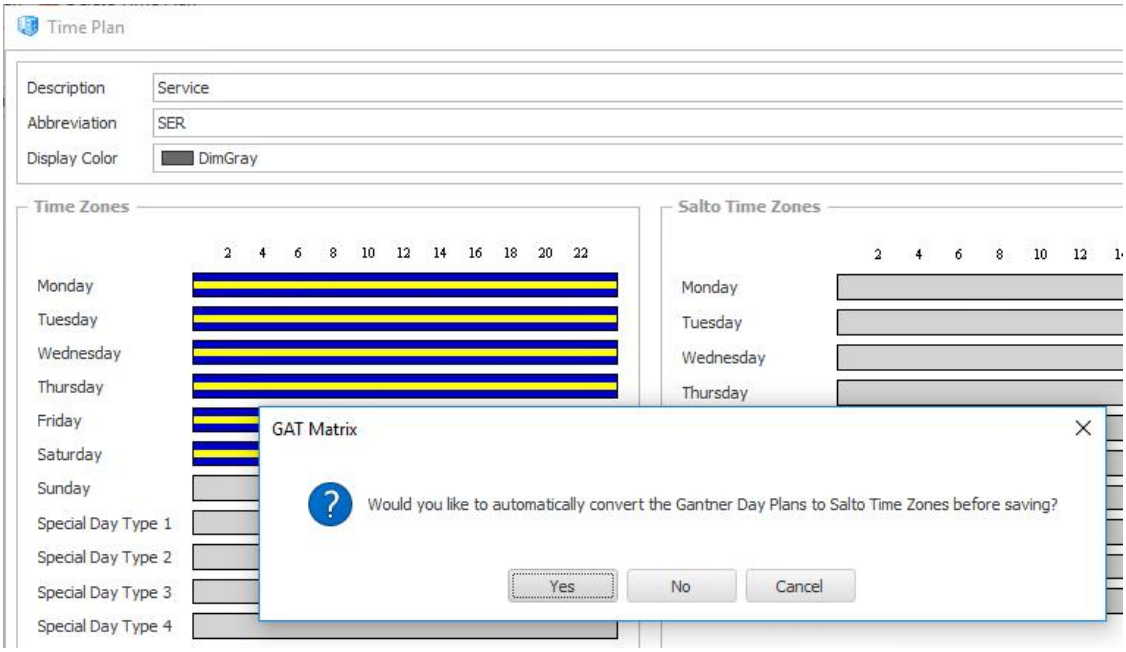


Figure 5.89 *– Query whether to carry out the conversion of the door time plans for ProAccess SPACE*

5.12 Defining door time plans

A door time plan can be assigned to a door to determine the door functions that will be active during certain time intervals of a day. With a door time plan it is possible to unlock a door generally for a certain time period, to activate the office function, to check only the company ID of data carriers or to suppress certain alarms.

Door plans can also be created and assigned in Matrix for doors imported from SALTO ProAccess SPACE.

► To define a door time plan, click on the toolbar button "Device Time Plans" in the main window.
  - The main window changes to the door time plan view.

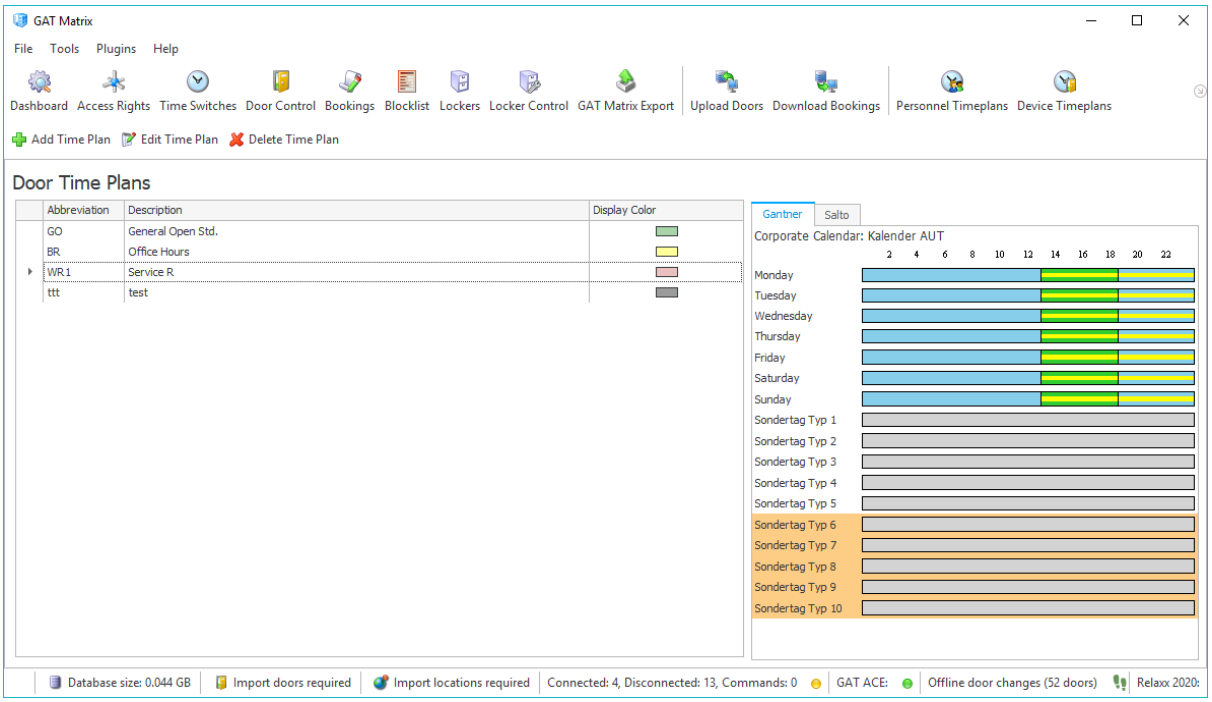


Figure 5.90 *- Door Time Plan definition*

Working with door time plans is similar to with personnel time plans. The only difference is how door time plans are used and which functions can be set via day plans. For the day plan description of door time plans, see "5.12.2 For GANTNER door plans: settings for day plans".

The list on the left side shows all defined door time plans. By selecting a door time plan with the left mouse button, the plan will be shown graphically on the right side of the window. The colored bars are day plans assigned to the days and the colors show the functions that are active during the corresponding time intervals. When the mouse pointer is positioned over a time interval the functions of that time interval will be shown in clear text.
If ProAccess SPACE is used, the display of day plans is separated into 2 tabs (for GANTNER and SALTO doors). You can view the desired day plans by selecting the tab at the top.

► To add a new door time plan, press the “Add Time Plan” button on the top of the door time plan list.

► To change the settings of an existing door time plan, double-click with the left mouse button onto the time plan.
  - In both cases, the following window opens.

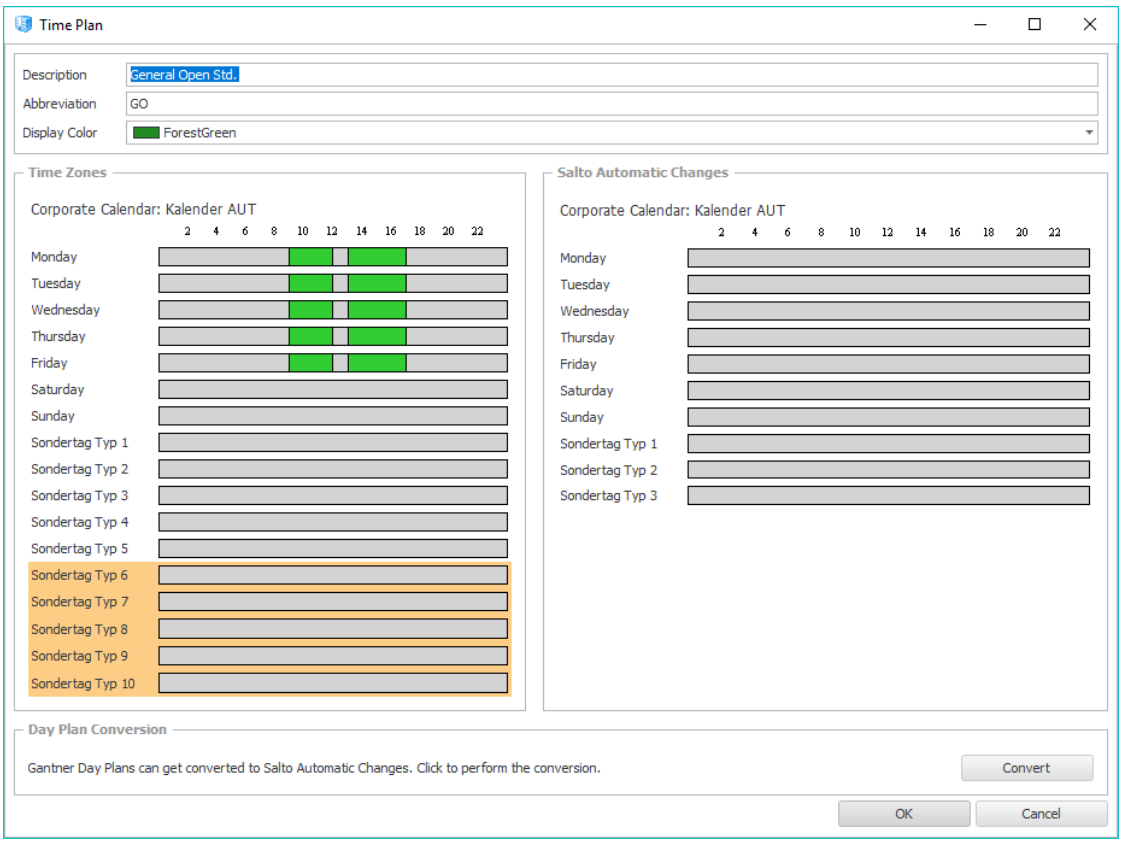


Figure 5.91 *- Settings of a door time plan*

NOTE! The special days 6 to 10 marked orange are only supported by GAT ACE 7000. These colored markers are only displayed when GAT ACE 3000 is used.

For a new door time plan, this window is empty. For an existing door time plan, the previously defined day plans are shown. For the GANTNER doors in each day plan, Matrix supports multiple time zones and different functions such as the general open function or office function. For doors imported from SALTO ProAccess SPACE, multiple time zones are possible per day, but the functionality is different from the GANTNER doors. Therefore, the display is divided into the plans for the GANTNER doors (left field "Time Zones"), and the doors imported from SALTO ProAccess SPACE (right field "Salto Automatic Changes").

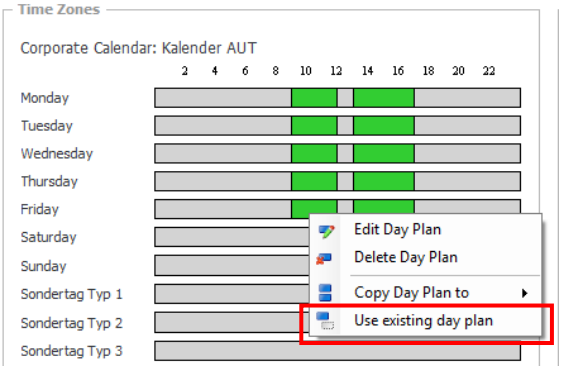
The following fields are used to configure the door time plan.

- Description: Enter a description for the door time plan.
- Abbreviation: Enter up to 3 alphanumerical letters or digits for the door time plan. These letters will be used in the authorization matrix to indicate the assigned door time plans.
- Display color: Select a color from the list box. This color will be used in the authorization matrix to indicate the assigned door time plan.
- Day fields: The day fields in the lower part of the window (17 fields on the left for GANTNER doors, 10 fields on the right for SALTO doors) show the day plans assigned to the staff schedule on individual days.

It is possible to define a day plan for each individual day of the week and for up to 10 special days (GANTNER) or 3 special days (SALTO) (see "6. CORPORATE CALENDAR AND LOCATIONS"). The last 5 special days for GANTNER doors (marked orange) are only supported by GAT ACE 7000.

5.12.1 For GANTNER doors: assigning, changing, deleting day plans

► In order to assign a day plan to a day, double-click on the empty day plan field in the left "Time Zones" area or right-click on a day field and select "Use existing day plan" from the menu.



○ The following window opens.

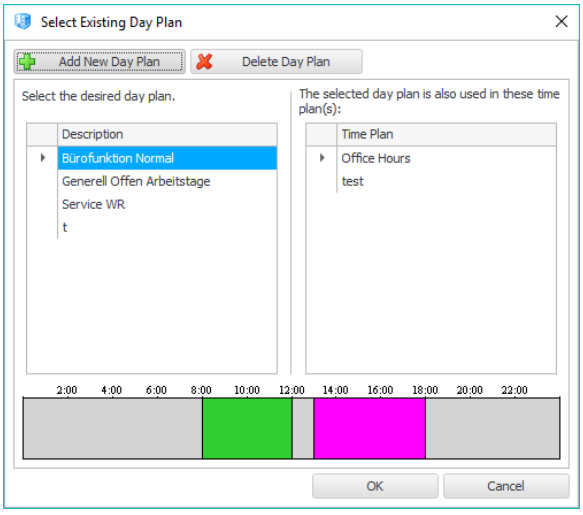


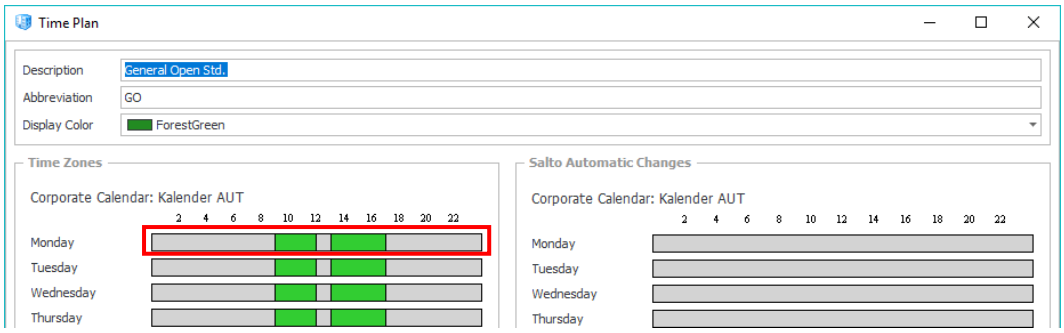
Figure 5.92 *- Assigning a day plan to a day*

The day plan can be selected in the left list. The right list will show in which door time plans the selected day plan is also used and in the lower field you see a graphical representation of the day plan. When you hover the mouse over this representation the settings of this day plan will be shown.

In this window you can add a new day plan by clicking on "Add New Day Plan". The settings window for the day plan opens (see “5.12.2 For GANTNER door plans: settings for day plans”).

► **Changing the settings of a day plan**

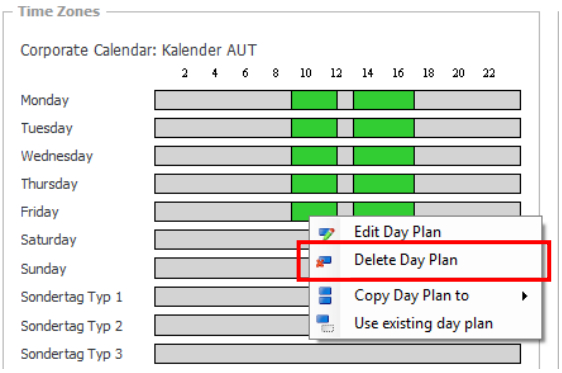
To change the settings of a day plan in the time plan window, double-click with the left mouse button in the “Time plan” window onto a day with the assigned day plan.



- The day plan window opens (see "5.12.2 For GANTNER door plans: settings for day plans") where you can change the settings.

► **Deleting a day plan from a day**

To remove a day plan from a day, right-click onto the day plan and select "Delete Day Plan" from the menu.



- Depending on the general deleting confirmation setting (see "4.7. General settings"), either a window will open where the deletion must be confirmed, or the day plan will be deleted directly without additional confirmation. The day plan will only be removed from the selected day but will not be deleted completely.

► **Using a day plan with another day**

To use a previously assigned day plan for other days, simply drag & drop the day plan from one day to the other day(s).

Another option is to right click onto the day plan and select "Copy Day Plan to >" from the menu. Here you can select the day(s) where the day plan shall be copied to. With "WeekDays", "Workdays" or "SpecialDays" the day plan will be copied and assigned to all weekdays, workdays, or special days at once.

5.12.2 For GANTNER door plans: settings for day plans

Day plans can be defined for **personnel time plans** and for **door time plans**. This section describes the day plans for door time plans.

These settings apply to the day plans for the GANTNER doors and persons. Different settings are possible for the SALTO doors and persons (see next section).

A day plan for a door time plan defines the behavior of a terminal during a day. Up to 10 time intervals can be defined and during each of these time intervals other functions can be set.

► **Defining a new day plan**

To define a new day plan, click with the right mouse button onto an "empty" day plan field (at a day that has not yet a day plan assigned) and select "New Day Plan" from the menu.

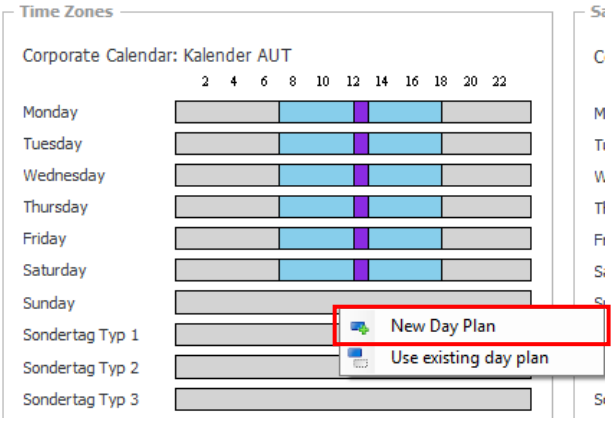
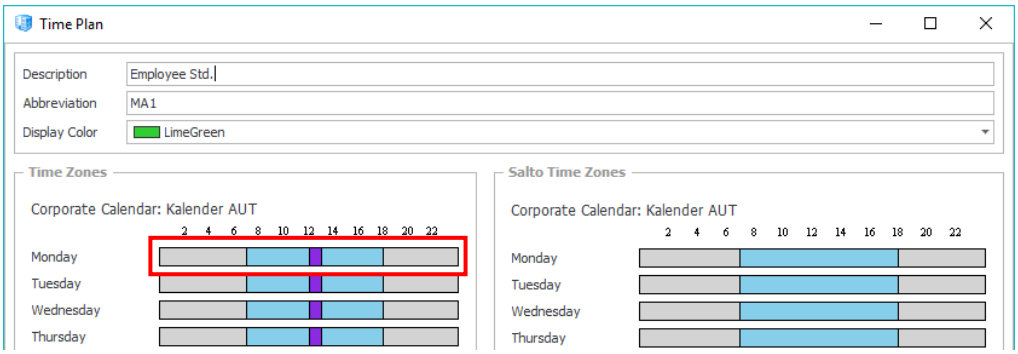


***Figure 5.93** – Adding a new day plan*

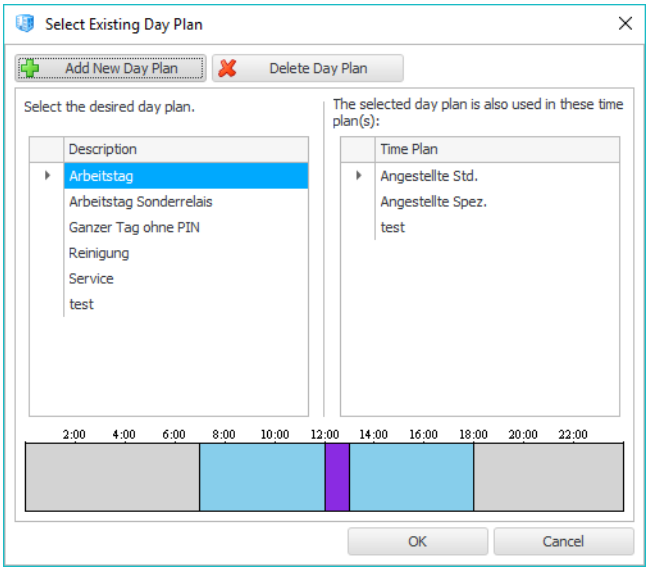
- The window "Edit Day Plan" opens (see Figure 5.***94***).

► **Changing the settings of an existing day plan**

To change the settings of an existing day plan, double-click onto the graphical representation of the day plan, where it is assigned to a day.



You can also double-click onto an "empty" day plan field to open the "Select Existing Day Plan" window, where all defined day plans are listed.



- The "Edit Day Plan" window opens (see Figure 5.***94***).

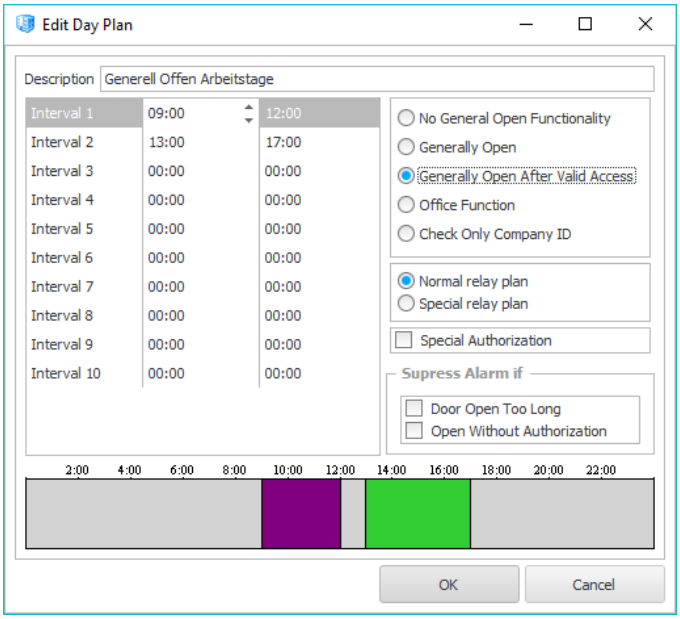


Figure 5.94 *- Day plan settings for a door time plan*

Here, the following settings can be defined:

- Description: Enter a description for the day plan in this field.
- Interval list: In the list on the left of the window select an interval and define the start and end time of that time interval.

- Functions: On the right side select the functions which shall be active during the selected time interval. The selected functions will be indicated in color in the bar at the bottom of the window. The following functions are available:
  - No General Open Functionality:
    The door will not be generally unlocked during the time interval. This setting is used to specify alarm suppression during certain time intervals.
  - Generally Open: When this function is active the door is permanently unlocked by the terminal during the time interval and access is possible without identification. This is used for example during office hours to allow access for persons. After the time interval the door will be locked again (depending on the possible function of the following time interval).
  - Generally Open After Valid Access:
    For a time interval with this function set, the door is initially locked and then permanently unlocked after the first valid identification at the terminal until the end of the time interval and then locked again (depending on the function of the next time interval).
  - Office Function: When this option is enabled, the door will be unlocked after the first valid identification in the time interval. The door will remain unlocked until the end of the time interval or until another valid identification at the terminal. In this case the door will be locked again. With repeated valid identifications this unlocking and locking functionality can be repeated during the entire time interval.
  - Check Only Company ID:
    With this function, only the company ID number on the data carriers is checked by the terminal for access authorization. Access is possible with any data carrier which company ID matches one of the company IDs defined for the terminal (in GAT Manager or GAT ACE).
  - Normal-/Special relay plan:
    Depending on the selection, the time window uses the normal or special relay plan (for information about the relay plans see "5.15 Relay time plans").
  - Special Authorization: This function is used by terminals with the FLEX protocol (e.g., GAT Terminal 3100 and older) to control special authorizations parallel to standard unlocking functions. In addition to the standard access functions, this allows doors, gates, etc., to be unlocked at the configured time for valid authorizations or with the general open function.
    This function is no longer provided with Generation 7 controllers (e.g., GAT DC 7200) as here these applications can be realized on 2 or more doors.
  - Suppress Alarm if "Door Open Too Long":
    Mark this function to suppress the "Door open too long" alarm. Without suppression this alarm will be activated if after a valid identification at a terminal the corresponding door is opened longer than the "Maximum Door Open Time" (defined in GAT Manager or GAT ACE).
  - Suppress Alarm if "Open Without Authorization":
    Mark this function to suppress the "Open without authorization" alarm. Without suppression this alarm will be activated if a door is opened without valid authorization at the terminal (for example maintenance tasks at the door, manipulations or break-in).

Define all required intervals and functions and confirm your settings with "OK". The day plan will be updated or added respectively to the door time plan list.

5.12.3 For SALTO doors: creating, changing, deleting time zones

Several time zones per day can be defined for the doors imported from ProAccess SPACE. After assigning the plan to a door, the time zones in the plan determine the function of the door (e.g., when the office function is active).

The configuration of time zones is similar to the GANTNER doors. However, day plans cannot be defined for SALTO doors.

► **Adding a time interval**
To add a time interval to a day, right-click on an empty area of the day field and select "New Time Interval" from the menu.

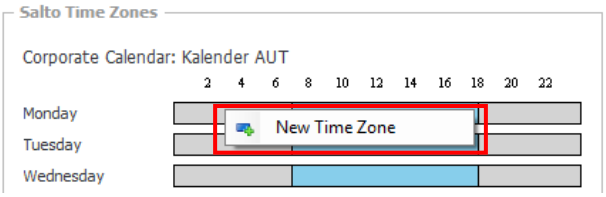


***Figure 5.95** – Salto Time Intervals*

Note: For a day without a defined time zone, you can also double-click in the empty day field.

- The following window opens for configuring the time zones and functions.

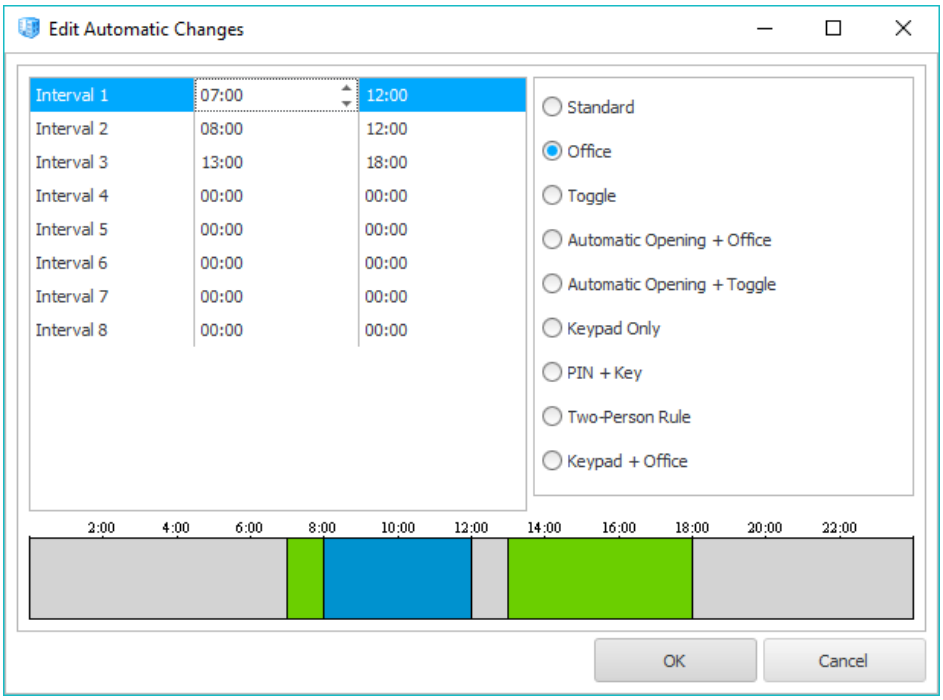
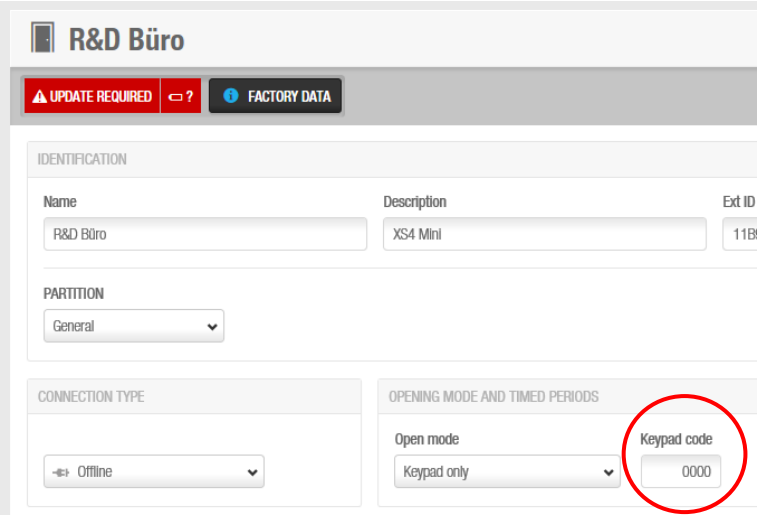


***Figure 5.96** - Time zone for a SALTO day plan for doors*

► You can define 8 time zones here. To do this, enter the start and end time for an interval and while the line of the interval is still highlighted, select the function for the interval on the right.
  - In the time bar at the bottom of the window, each time zone with the defined function is displayed. The color indicates the function.

- The following functions are possible:

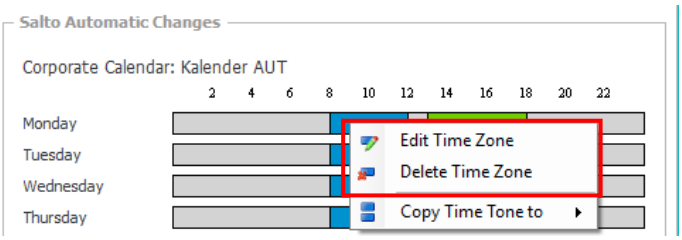
- Standard: Authorization valid for both entry and exit at the door.
- Office function: The lock can be set to continuously open/unlocked by any person whose person profile has the "Office" option selected and has access authorization for the door. For more information, see the data carrier settings. To activate Office mode, hold the data carrier in front of the lock while pressing the inside handle of the door. To deactivate Office mode, repeat the procedure.
- Toggle: The lock can be set to continuously open/unlocked by any authorized person who reads an access-authorized data carrier at the lock. The inside handle on the door does not have to be held down. The next authorized data carrier read by the lock locks the door again. This (data carrier-controlled) toggling continues with each reading of an authorized data carrier.
- Automatic opening + Office: The lock is in office mode (office function). If the door is closed, the lock opens automatically at specified times and remains open for a specified period (e.g., from 08:00 to 18:00). At the end of each period, the lock locks again (if the door is unlocked) and remains in office mode (Office).
- Automatic opening + Toggle: The lock is in data carrier-controlled mode (see previous option). If the door is closed, the lock opens automatically at specified times and remains open for a specified period (e.g., from 08:00 to 18:00). At the end of each period, the lock locks again (if the door is open) and remains in data carrier-controlled mode.
- Keypad Only: The lock can be opened at any time by entering a valid door code into the keypad. The door code must be one to eight digits long and is valid for all persons. Select the “Keypad only” option in SALTO ProAccess SPACE and enter a code into the “Keypad code” field. The lock can also be opened with a valid data carrier.



- PIN + Key:	The lock can only be opened with a valid data carrier in combination with the entry of a valid PIN code via the keypad. This measure increases the security. If the PIN code is incorrect, access is denied. The PIN code is defined in the user profile. For more information, see PIN codes.
- Two-Person Rule:	In this mode, two persons must each read a valid data carrier at the lock in order to open the door.
- Keypad + Office:	The lock is in keypad mode. When the door is closed, the lock automatically unlocks at specified times and the door remains open for a specified period (e.g., from 08:00 to 18:00). At the end of each period, the lock locks again (if the door was open) and remains in keypad mode.

► When all time zones have been defined for the day, confirm with "OK".

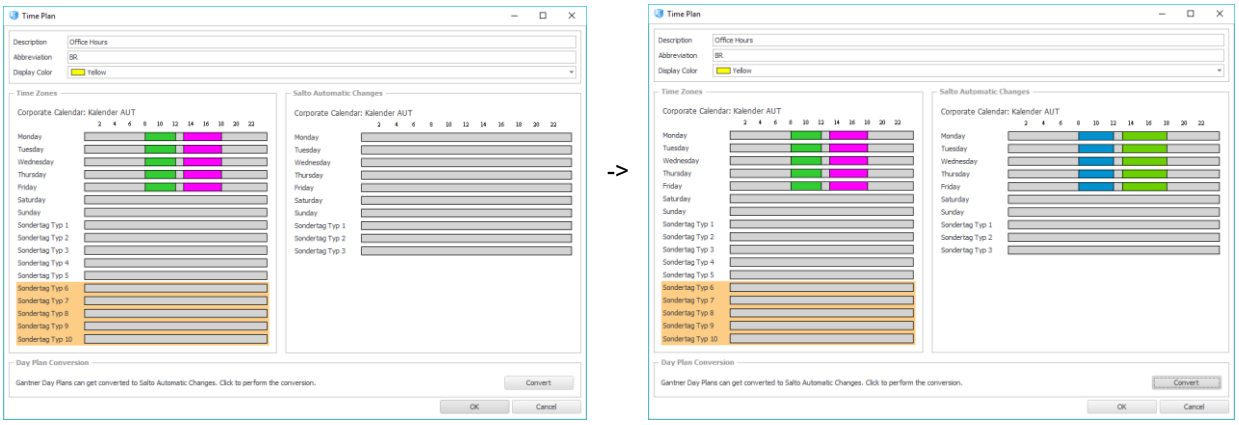
► **Edit time interval or delete from a day**
To delete or edit an existing time zone, right-click on the zone and select the desired action from the menu.



► **Copy a time interval to another day**
If you want to use a defined time zone with another day, right click onto the time window and select the desired day from the "Copy Time Zone to" menu option.

5.12.4 Converting a GANTNER door plan to SALTO time zones

It is possible to convert a day plan created within Matrix for GANTNER devices to SALTO time zones. In this case, the time zones defined for each day in the GANTNER plan are copied to the SALTO time plan page. The functions that have been configured in the GANTNER plan (e.g., office function, general open) are adopted and transferred to the SALTO functions.



► To convert the GANTNER time plan, click the "Convert" button.

- The time zones of the GANTNER plan (left side) are transferred to the corresponding days of the SALTO plan (right side) and displayed accordingly with colors for the different functions.
- The time zones in the special days 4 to 10 are ignored since the SALTO plans only support 3 special days.

► Confirm by clicking on "Save".

When pressing "OK", Matrix checks if a conversion is required and possible. A message is shown allowing you to decide whether to carry out the conversion.

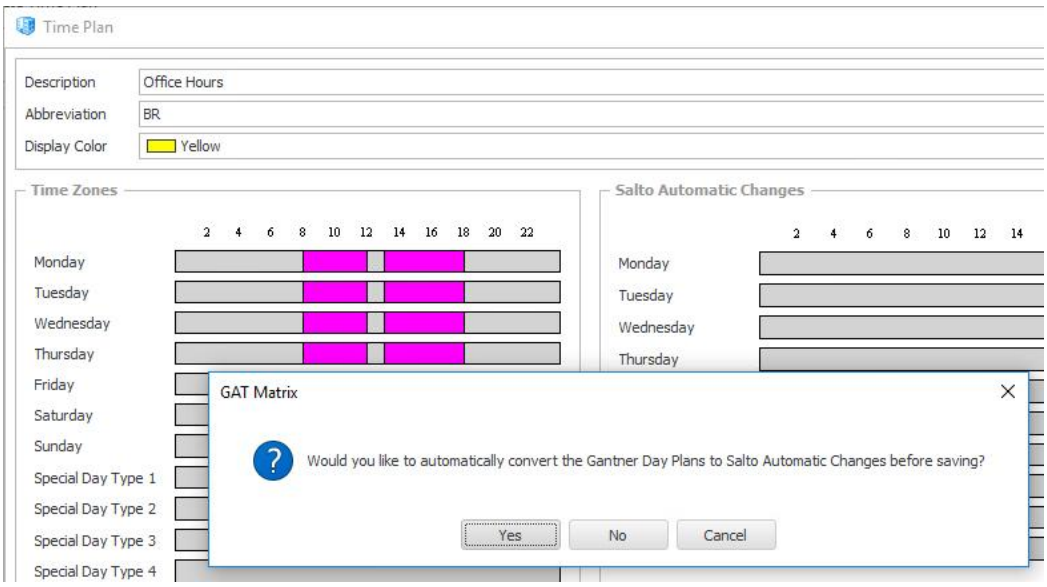


***Figure 5.97** – Query whether to carry out the conversion of the door time plans for ProAccess SPACE*

5.13 Assigning door time plans to the doors

A certain door time plan can be assigned to a terminal via drag and drop or manually. Perform the following steps:

1. Select the door in the matrix left clicking on the door name.
2. On the right side of the main window the defined door time plans will be shown.
3. Click on the arrow on the left of the door time plan column (see red mark in the figure below) to assign the door time plan.

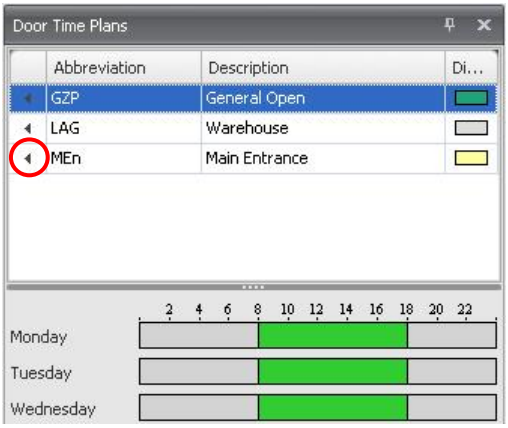


Figure 5.98 *- Assigning a door time plan*

4. At the selected terminal, a colored field is displayed to indicate the assigned door time plan.

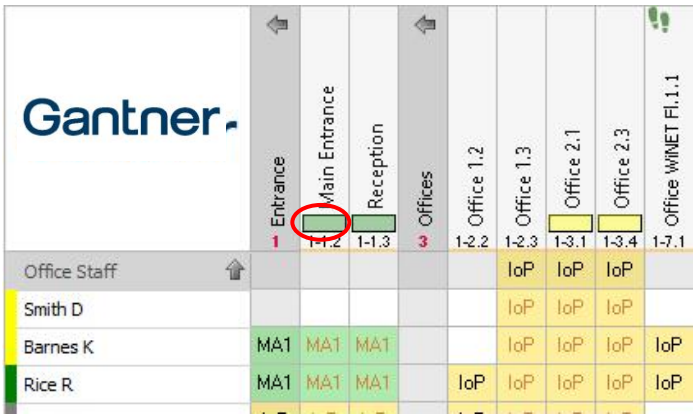


Figure 5.99 *- Indication of an assigned door time plan*

For SALTO doors, the procedure for assigning a door plan is identical to that of GANTNER doors.

It is also possible to assign a door time plan to several doors at once. In this case, first select all the doors by left clicking and dragging then proceed with step 2 from the instructions above.

Another option is to assign a door time plan via drag & drop. You can directly drag a time plan from the list on the right onto a terminal in the matrix.

If door time plans are deleted, it may take several minutes for the changes to take effect on SALTO online doors.

5.14 Defining authorizations of persons in the authorization matrix

In the authorization matrix personnel time plans are assigned to the matrix fields and this will then define the type of authorization for the person at the corresponding terminal.



If the authorization matrix is not displayed, e.g., after editing a personnel or door time plan, you can click on the "Access Rights" toolbar button to display the matrix again.

To assign a personnel time plan to a person at a door select the corresponding field in the matrix. The available personnel time plans will be shown on the right. Click on the black arrow of a personnel time plan to assign that time plan to the selected matrix field. It is also possible to assign a personnel time plan via drag & drop by dragging a personnel time plan from the list directly onto the corresponding field in the matrix.

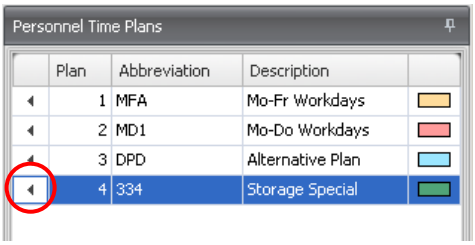


Figure 5.100 *- Assign a personnel time plan*

5.14.1 Symbols and color indications used in the authorization matrix

The following figure shows an example of an authorization matrix.

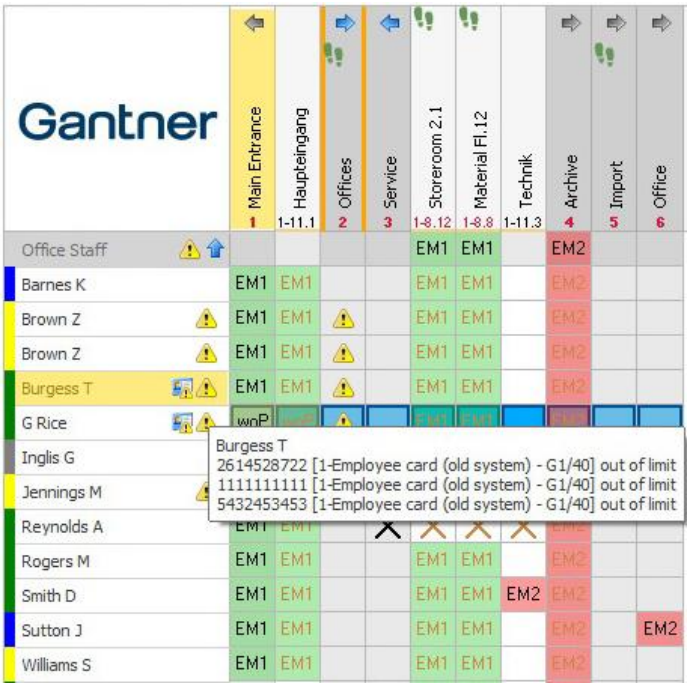
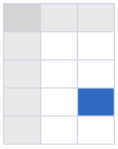


Figure 5.101 *- Example of an authorization matrix*

To indicate certain information in the authorization matrix, the following symbols and colors are used:



… If no time plan is assigned or inherited, .. the cells have a white background.
.. the cells of groups are light grey.
.. the cells where groups cross are dark gray.
In this case, the corresponding person(s) have no access authorization at the corresponding door(s).



… The color of the field and the abbreviation in the field match the description and the color of the assigned time plan. In this example the personnel time plan called "Storage Special" is assigned.

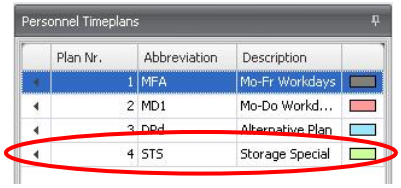


Figure 5.102 *- Time plan list*



… If the abbreviation in a matrix field is black, the personnel time plan was assigned directly to that field.



… If the abbreviation in a matrix field is orange, the personnel time plan is inherited from a group. Inherited plans can be overridden by explicitly assigning a time plan.



… If a black dot is shown in a matrix field, special rights are assigned to the person at the door (see "5.14.2 Assigning special rights").



… A matrix field with this icon is displayed in SALTO doors if more than one plan is assigned to the respective person for this matrix field. The plans are displayed on the right side on the "Salto" tab.



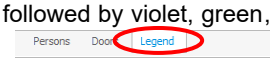
… This symbol is shown for offline doors and persons for which/whom the intended access rights cannot be assigned anymore (i.e., those persons do not have access rights at those doors). The symbol is also displayed for person groups that contain such conflicts. Conflicts in collapsed groups are also easily recognized and the group can be expanded by double-clicking on the exclamation mark symbol.
If the warning symbol is displayed for a person who has more than one card assigned or the max. number of offline permissions for the person has been exceeded, a card symbol is also displayed (). Move your mouse over the symbol to see which data carrier is affected.
Info: For offline doors, the authorization data is written onto the data carriers of the persons. A data carrier has space for 10 doors and 30 door groups. If these amounts are exceeded, the authorization data cannot be written anymore, which means the person does not have access rights for those doors. In this case please try to group offline doors to door groups (see "5.18.2 Uploading offline doors").



…… For offline doors with the Read Only function (or in GAT ACE 3000 also with CardNET), only the “Valid to” time of the validity period is written onto the data carrier. Therefore, the "Valid from" time must be in the past and not in the future. Offline conflicts for these doors are indicated by a yellow triangle with exclamation mark and a clock icon when the valid from date is set in the future (see "5.2 Main window").



.. A footstep symbol for an offline door indicates whether there are changes that need to be loaded to the offline door using the transport device. If the symbol is displayed in orange, loading is in progress. The remaining colors indicate which data is not up to date in the terminal in order of priority. If there are several colors, the one with the highest priority is displayed. Red has the highest priority, followed by violet, green, and blue. The exact meaning of each color is provided in the legend tab.



… The colored displays in front of the persons indicate their status. Further information can be found by double-clicking on the personal data (see "5.6.1 Defining personnel master data").

… If a black X is indicated in a matrix field, the corresponding person does not have any access authorization at this door. Access can be denied for a person at a door by pressing the right mouse button onto the matrix field and selecting "Deny access" from the context menu that appears.

… Similar to the inheritance of time plans, the denial of an access right can also be inherited. This is marked by an orange X.

… This symbol on doors indicates that GAT ACE 7000 is still processing authorization data, which is then sent to the appropriate controller (indicated by a blue bar).

… A battery symbol next to a door indicates that the main power supply to the controller for this door has failed and the controller is currently being supplied by an emergency power supply (UPS).

5.14.2 Assigning special rights

Special rights can be assigned to any person for single or multiple doors provided the controllers that control these doors are also configured for the special rights option. Certain special functions are then activated for these persons. For persons with special rights, the "special rights output" of the controller is activated in addition to the normal unlocking operation.

Special rights have no function for SALTO doors. They only affect GANTNER doors.

To assign special door rights for a person, right-click in the corresponding matrix field. The following menu opens.

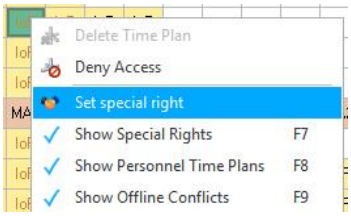
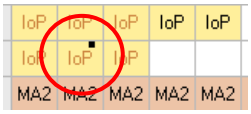


***Figure 5.103** – Setting special rights*

Special rights for persons are indicated in the matrix with a black dot in the field of the respective terminal.



Similar to time plans, you can also assign special rights to person groups and door groups. In this case, the special right is inherited by all persons in the person group or by all terminals in the door group. Inherited special rights are indicated with grey dots instead of black dots in the corresponding matrix fields. Figure 5.104 shows an example of how special rights can be inherited.



***Figure 5.104** – Inheritance of special rights*

In addition to setting special rights for persons, special rights can also be configured for doors in the door plans (see "5.12.2 For GANTNER door plans: settings for day plans"). The differences are:
- When assigning a special right to a person, the selected special function or special relay is active only for this person at the controller. Other persons do not have the same special function.
- When assigning a special right in the daily schedule to a door time plan, the special relay is activated for each valid identification of a person regardless of whether the individual has been assigned the special relay function.

In order to set the special rights, the following window opens in which the desired special rights can be specifically configured or deleted.

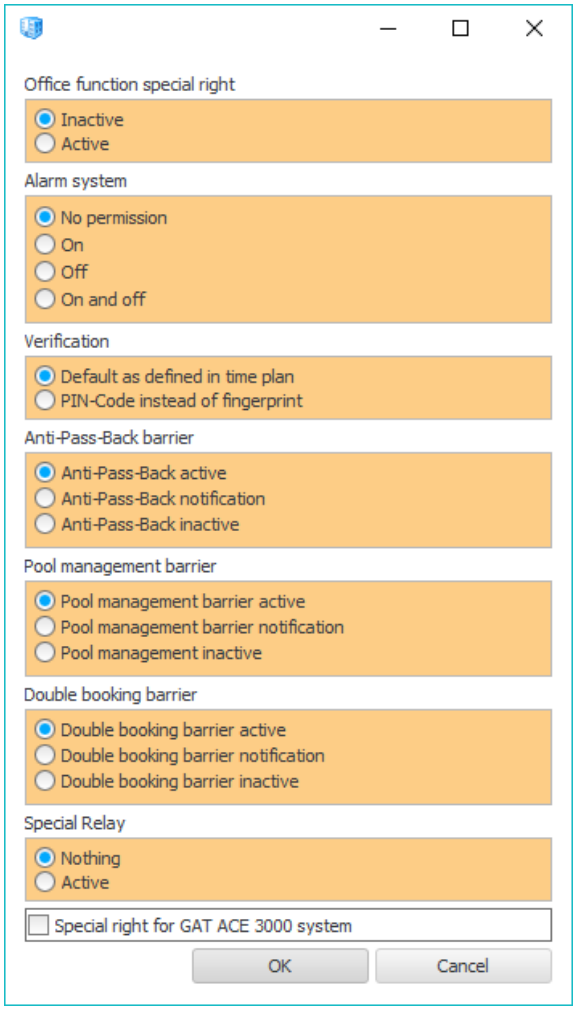


Figure 5.105 – *Defining special rights*

GAT ACE 7000 is required to enable or disable (orange markings) the various special rights individually. GAT ACE 3000 uses only one special right and does not differentiate between the different types of special rights. Therefore, the "special rights for GAT ACE 3000 system" field is automatically selected in this window when at least one special right for GAT ACE 7000 is defined.
The orange markings, which identify the GAT ACE 7000 options, and the "Special right for GAT ACE 3000 Systems" option are only displayed when GAT ACE 3000 is used.

The following special rights are listed in the window:

- Office function special right: If the office function is activated, the door is permanently unlocked after an identification with valid authorization until a new identification cancels this and sets the door to the mode defined according to the schedule (e.g. "Open by means of valid identification"). This function must also be configured at the corresponding GAT DC 7200 controller.
- Alarm system: For certain controllers and readers, persons can control an alarm via their data carrier and by pressing a button. You can specify whether the selected person can only activate the alarm, only deactivate the alarm, or both activate and deactivate.
- Verification: This setting overrides the verification settings of a personnel time plan. If you select "Default time plan" the verification settings according to the personnel time plan are used (see “5.11.2 For GANTNER personnel time plans: settings for day plans"). However, if the “Verification with biometrics” option is selected in a personnel time plan, and the “PIN code instead of fingerprint” special right is activated, then a PIN code is used to verify the person instead of a fingerprint (e.g., helpful if the person has trouble scanning their fingerprint).
- Anti-pass-back barrier: For certain person groups, for whom the anti-pass-back function presents problems, the anti-pass-back lock can be disabled. This can be used e.g., for service technicians who are inhibited by the anti-pass-back function and find themselves locked out of a room they wish to re-enter after exiting through a service door. With the "notification" setting, access is still granted when an anti-pass-back lock is activated, however, a corresponding message is displayed to the user.
- Pool management barrier: The pool management barrier allows only a certain number of people to access a specific area/room at the same time. For certain people, this function can be deactivated so that they can also gain access according to pool management when the max. number of people is reached. With the "notification" setting, access is still granted when a pool management barrier is activated, however, a corresponding message is displayed to the user.
- Double booking barrier: The double-booking barrier prevents a data carrier from being used twice within a definable period, e.g., 10 minutes. This function can be disabled for certain people with special functions. With the "notification" setting, access is still granted when a double-booking barrier is activated, however, a corresponding message is displayed to the user.
- Special relay: For GAT controllers, a relay output can be configured as a "special relay". When a person, who is set to "use" for the special relay, accesses the respective door, the special relay is also activated. This is useful, e.g., if an entrance gate in addition to the door needs to be opened for certain individuals.

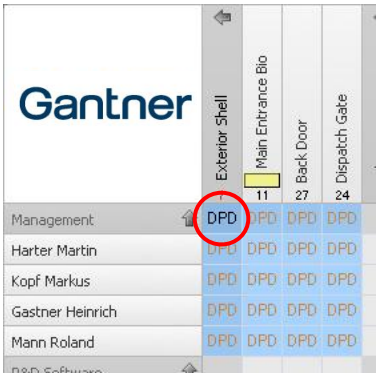
To remove a special right from a person, open the menu in the corresponding matrix field and deactivate the special right in the special rights window.

5.14.3 Assignment possibilities

There are different ways to assign personnel time plans to persons. A personnel time plan can be assigned directly to a certain person at a certain door or indirectly by assigning the personnel time plan to a person or door group which means that all persons/doors inside the assigned group(s) will inherit the personnel time plan.

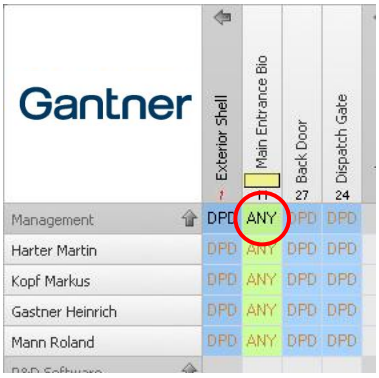
Example for inheritance of personnel time plans:

By assigning a personnel time plan to a door or person group the personnel time plan will get inherited to all doors/persons in the door/person group.
If a person has multiple personnel time plans assigned at a door (via direct assignment and/or inheritance), a directly assigned time plan will override the inherited time plans. The following figures show how inherited time plans can be overridden by setting a more specific personnel time plan.



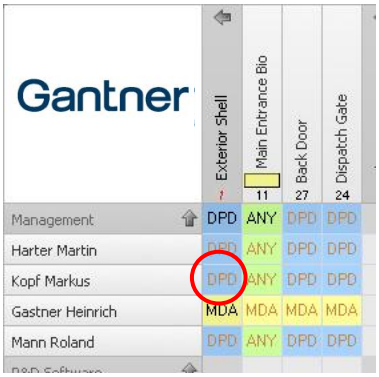
The personnel time plan "**DPD**" is assigned to the person group "Management" for the door group "Exterior Shell".

-> All persons in the "Management" group will inherit the personnel time plan "DPD" at all doors in the door group "Exterior Shell".



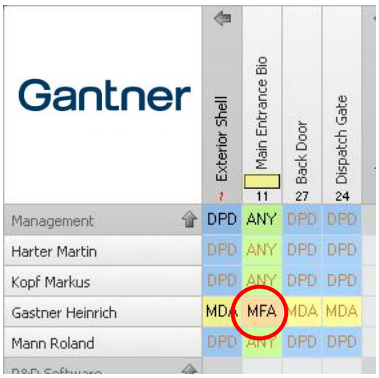
At the door "Main Entrance Bio" the personnel time plan "**ANY**" is assigned to the person group "Management".

-> All persons in the person group "Management" inherit the time plan "ANY" at the door "Main Entrance Bio". This time plan will override the previously assigned personnel time plan "DPD".



The personnel time plan "**MDA**" is assigned to the person "Gastner Heinrich" for the door group "Exterior Shell".

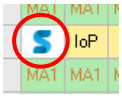
➔ The person "Gastner Heinrich" inherits the personnel time plan "MDA" at all doors in the door group "Exterior Shell". Because the assignment of a personnel time plan to a person at a door group is higher priority than the assignment of a personnel time plan to a door at a person group, the personnel time plan "MDA" will be active for "Gastner Heinrich" at the door "Main Entrance Bio". It does not matter if "MDA" or "ANY" is assigned first.

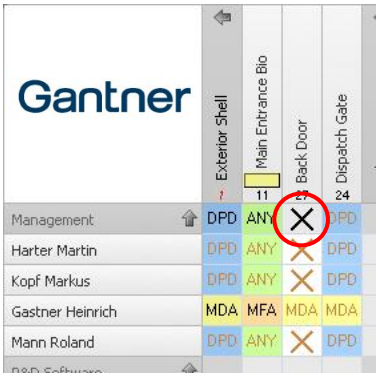


The personnel time plan "**MFA**" is assigned to the person "Gastner Heinrich" for the door "Main Entrance Bio".

➔ "Gastner Heinrich" will have the personnel time plan "MFA" active at the door "Main Entrance Bio" because the direct assignment of a personnel time plan to a single person at a certain door has highest priority over the other assignments and inheritances.

Note: If the door is a SALTO door, a blue "S" is displayed in this case instead of MFA. This indicates that the person has more than one time plan for this door (e.g., by inheritance).





At the "Back Door" the **access is denied** for the person group "Management" by selecting "Deny Access" from the context menu.

➔ Denying an access follows the same rules as assigning a personnel time plan. In the example all persons in the group "Management" will inherit "Deny Access" for the door "Back Door" except for the person "Gastner Heinrich", for whom the personnel time plan "MDA" is still active because this time plan was assigned to the person and this assignment has higher priority.

5.14.4 Deleting an assigned personnel time plan from a person

In order to delete the assignment of a personnel time plan, right-click into the matrix and select "Delete Time Plan". Only the assignment of the time plan will be deleted. The time plan itself is not deleted.

A time plan can only be deleted from where it was assigned. The "Delete Time Plan" menu item is only available when right-clicking on a black abbreviation in the matrix where the personnel time plan has been assigned.

5.15 Relay time plans

For certain controller types, so-called relay expanders can be connected. These are peripherals with up to 32 relays that can be additionally activated during a normal relay unlocking provided the terminal has a valid identification. This makes it possible to realize applications such as e.g., lift controls, where additional specific levels are released after valid authorization at the controller.

A relay plan clearly determines which relay of the relay expander should be activated. By assignment of the relay plans to doors and persons, the behavior of the doors can be controlled for each person. In this case, for each person at every door with the appropriate type of controller, a relay plan can be assigned in one step to individuals or to a whole group of persons.

Furthermore, you have to differentiate between "Normal Relay Plans" and "Special Relay Plans". A Normal- as well as a Special Relay plan can be assigned for a person at a controller. Which of the two relay plans is then used at what times is defined in the Personnel Time Plan and Door Time Plan.



The relay plans are defined in a separate matrix and assigned to the doors and persons. For processing and assignment of relay plans, select the icon "Relay Plans". The relay plan overview opens in the main area of Matrix.

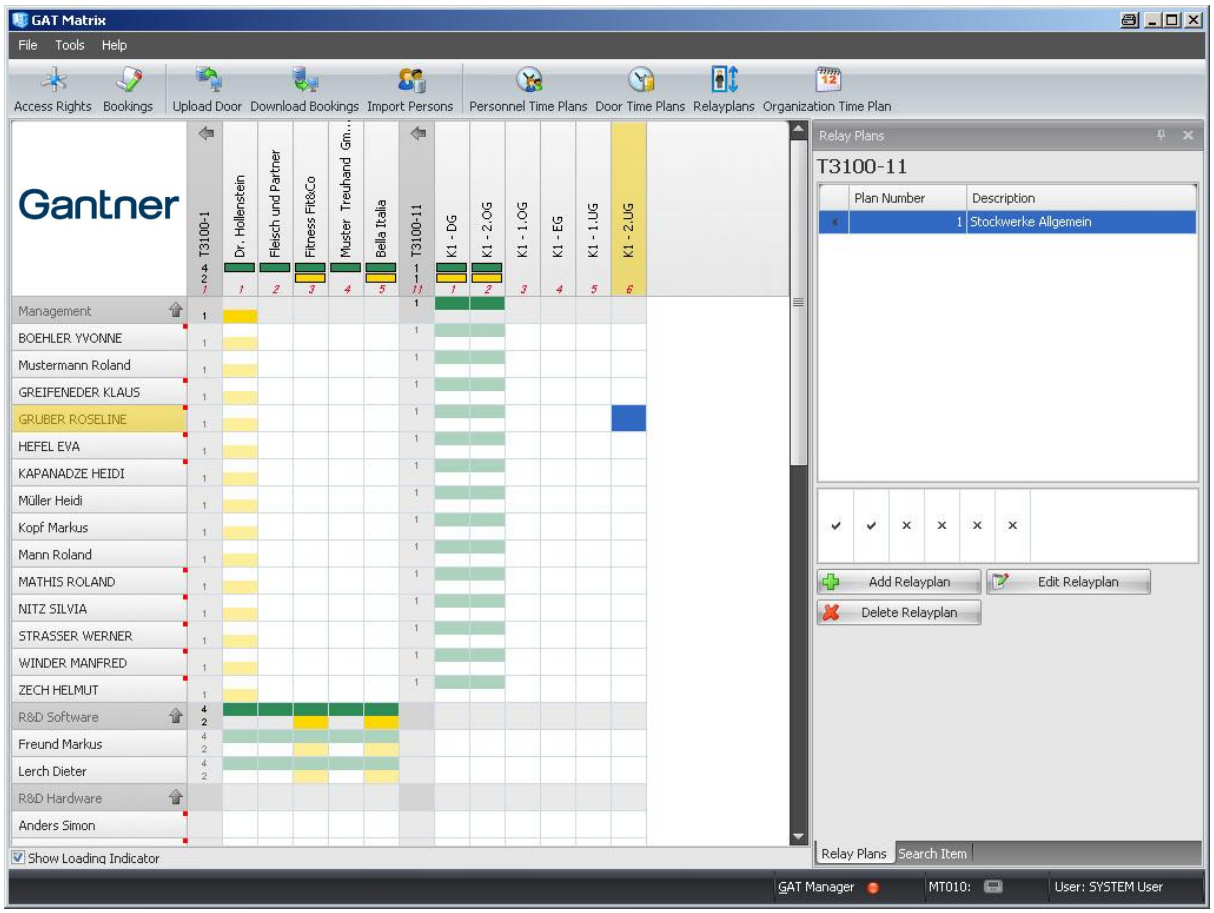


Figure 5.106 *– Relay plan overview*

The controller relays that are used with relay expanders are defined in GAT ACE 3000 or GAT ACE 7000 in the GAT DC 7xxx door controller settings and imported from there. In these definitions, you can specify the names of the doors/controllers and relays.

This window is similarly arranged to the access authorization window (see section "5.2 Main window"). Persons are listed in the left column of the matrix as usual. The doors that have relay expanders are shown in the top row of the matrix. Doors without relay expanders, i.e., where no relay plan can be assigned, are not shown. Unlike the access authorization matrix, doors in groups are not compiled here. Each door is displayed like a group with the relays, which are controlled by the terminal, listed alongside.

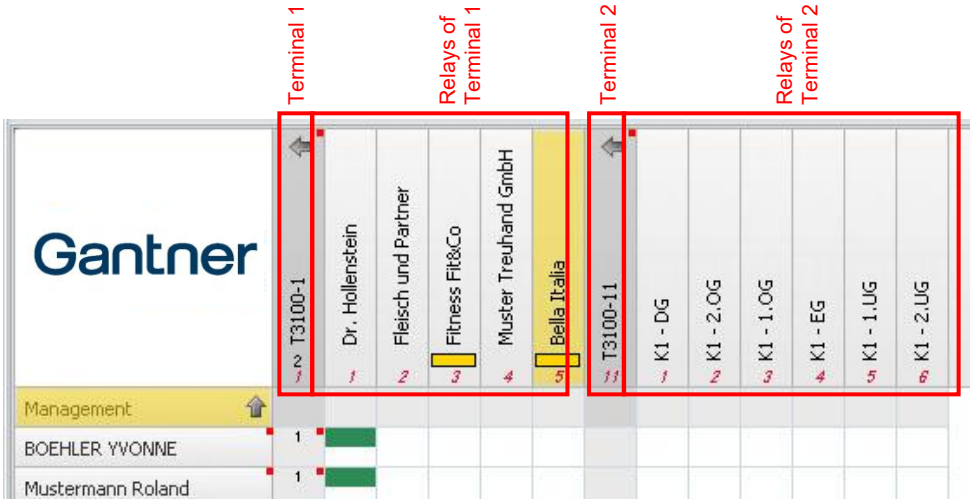


Figure 5.107 *– Doors and relays*

If a person is assigned to a relay plan, the used relays in the relay plan will be shown in color in the matrix. A Normal Relay plan will be shown green in the upper half of the person line and a Special Relay Plan will be shown yellow in the lower half of the person line. The number of the relay plan is in the terminal column.

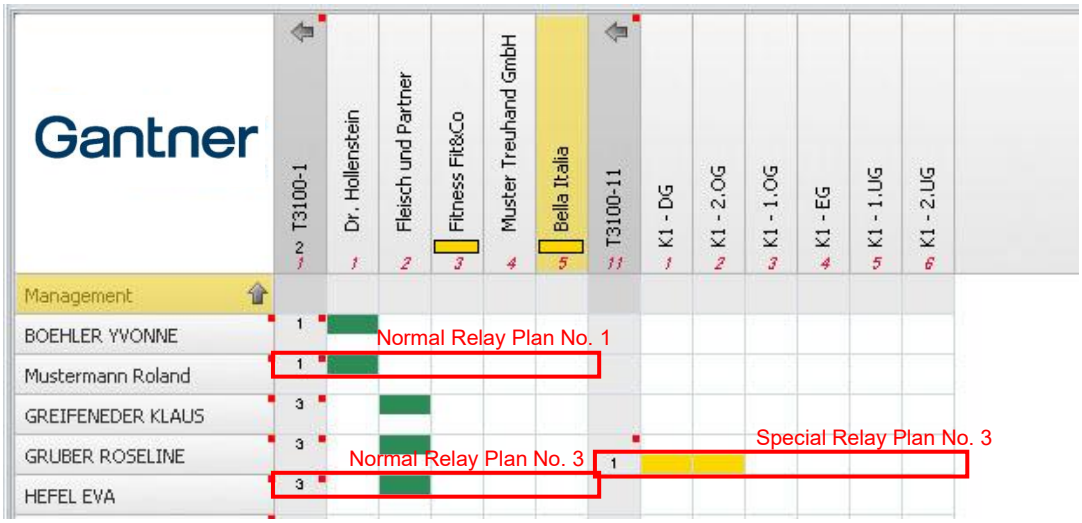


Figure 5.108 *– Presentation of relay plans*

In the Relay Plan Matrix, only relay plans can be managed and assigned. It is not possible to change persons, move groups, etc.

5.15.1 Creating, editing, & deleting relay plans

On the right beside the relay plan overview, the relay plans of the doors are administrated. In order to create and edit the relay plan of a door, click on a matrix field of the door or one of its relays. Thereby, the previously defined relay plans for this door are shown.

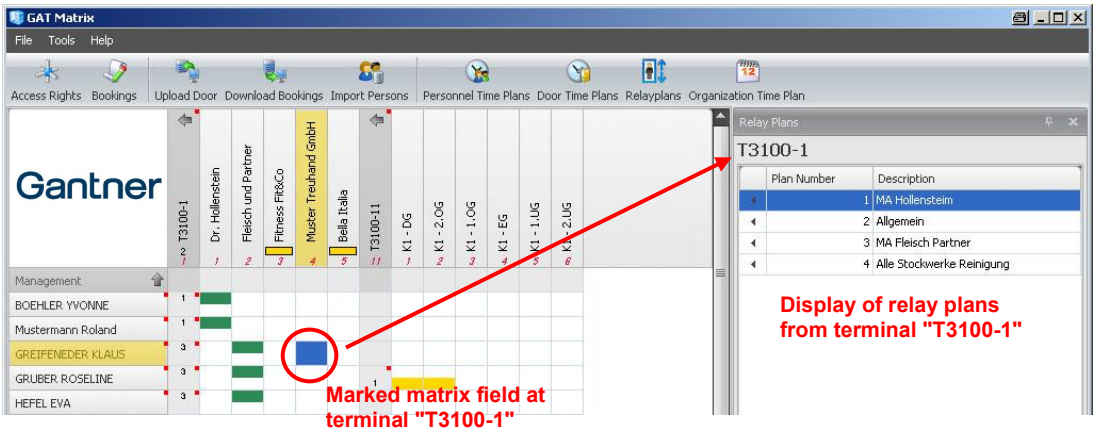


Figure 5.109 *– Edit Relay Plans*

If a relay plan will be selected in the list, you can see below the list an overview of the relays, which will be used in this relay plan. In the following example, the relay plan "MA Hollensteim" only used 1 relay (indicated by a tick). The remaining 4 relays are not used.

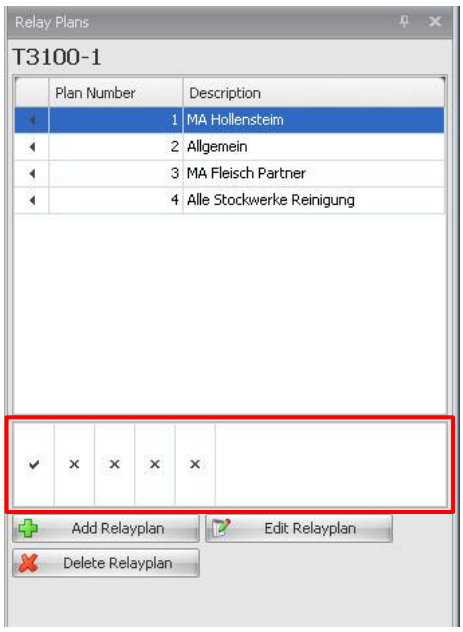


Figure 5.110 *– Relay Plan List*

In order to edit the relay plan of a door, select the door from the list and then click on the appropriate button below the relay plan list.

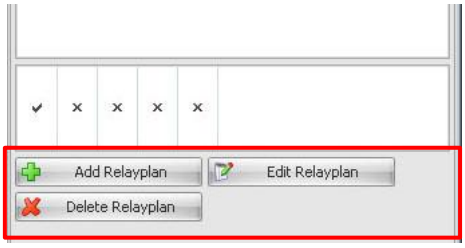


Figure 5.111 *– Relay Plan List*

With "Add Relay Plan", a new relay plan will be inserted and with "Edit Relay Plan", an existing relay plan can be changed. In both cases, the following window opens:

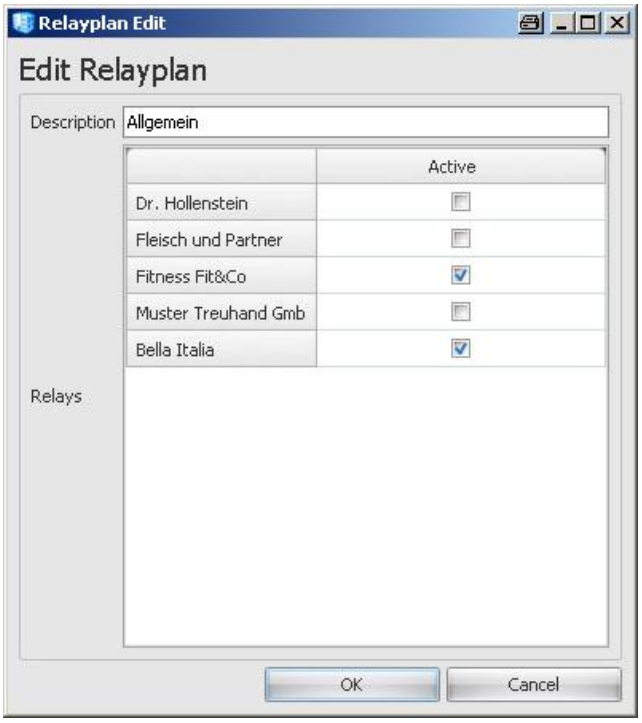


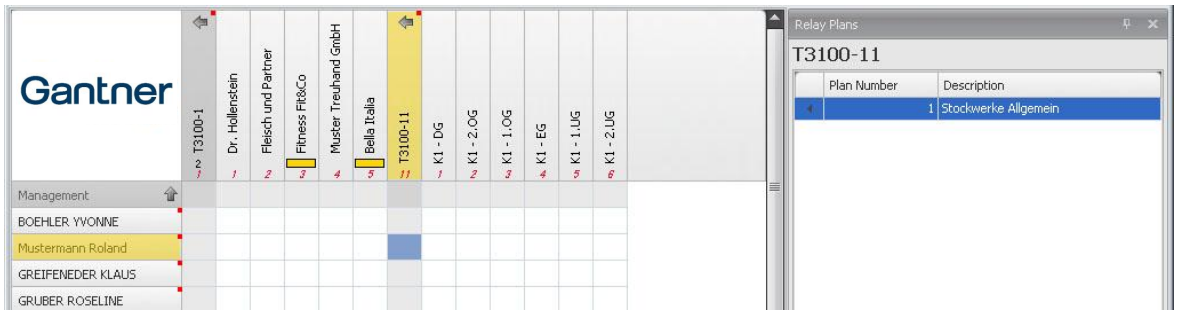
Figure 5.112 *– Add / Edit Relay Plan*

All relays, which are activated for the selected door in GAT ACE 3000 and the GAT DC 7xxx controllers, are shown in this window. Enter in "Description" a name for the relay plan and mark the relays which you want to use.

With the button "Cancel" below the relay plan list, a marked relay plan can be deleted. This will then be deleted in the relay plan matrix. The persons, who were assigned to this relay plan, can no longer use the relay of the connected relay expander.

5.15.2 Assigning a relay plan to a person

To assign the relay plan of a door to a person, select the row of the person for the applicable door in the matrix. For this purpose, you can click on the door column or on a relay column within the door group. In the following example, the person "Mustermann Roland" will be assigned to the relay schedule of the door "T3100-11".



Or:



Figure 5.113 *– Selection for Relay Plan Assignments*

Now click on the relay plan, to which the person should be assigned, via the arrow icon in the first column. A pop-up menu is displayed where you can define the relay plan as a normal relay plan or special relay plan.

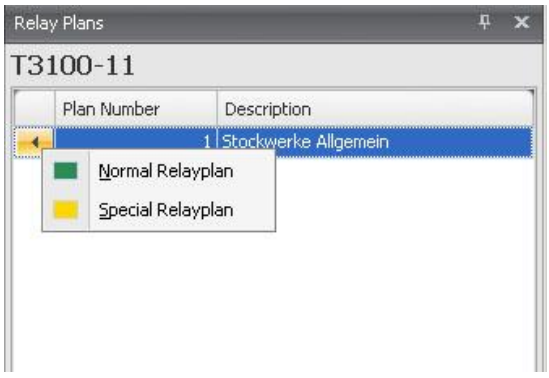


Figure 5.114 *– Assigning a relay plan as a normal or special relay plan*

After selecting the desired option, the relay plan is assigned to the matrix and the relay field, which is used in the relay plan, displayed with the appropriate color.



Figure 5.115 *– Display of the Relay of the Relay Plan*

In the shown example, the Person "GREIFENEDER KLAUS" has been assigned at the Terminal "T3100-11" of the relay plan "Stockwerke Allgemein" as normal relay plan (green).

5.15.3 Assigning a relay plan to multiple persons or a group of persons (inheritance)

In order to assign a relay plan to several persons, you can mark the fields of the desired persons simultaneously via SHIFT- or CTRL-key at the desired controller.

A relay plan also can be assigned to a group of persons. For this, mark an appropriate terminal field in the line of the persons group in the matrix and then assign the relay plan. The relay plan will be inherited on all persons in the group "inherited". An inherited relay plan will be shown with a brighter color (light green or light orange).



Figure 5.116 *– Inherited Relay Plan for groups of persons "Management"*

If a person will be specifically assigned to another relay plan, this relay plan will be used, instead of the inherited relay plans, if they are the same relay plan types (normal or special relay plan).



Figure 5.117 *–Directly assigned relay plan overwrites an inherited relay plan*

5.15.4 Denying the relay plan of a person

In order to not use explicitly the relay plan of a person, the relay plan can be denied. This is useful, for example, when a relay plan of all persons in a group, with the exception of a special person, should be applied. The relay plan then can be assigned to a group, thereby all persons of a group deny a relay plan. The relay plan will be denied to the desired person. In order to deny the relay plan at a person, click on a matrix field for the person at the appropriate door or door relay. Select from the pop-menu either "Deny Normal Relay Plan" or "Deny Special Relay Plan". A denied normal relay plan will be shown with a black "X" in the upper part of the appropriate matrix field and with a denied special relay plan, these "X" will be shown in the lower half of the line.

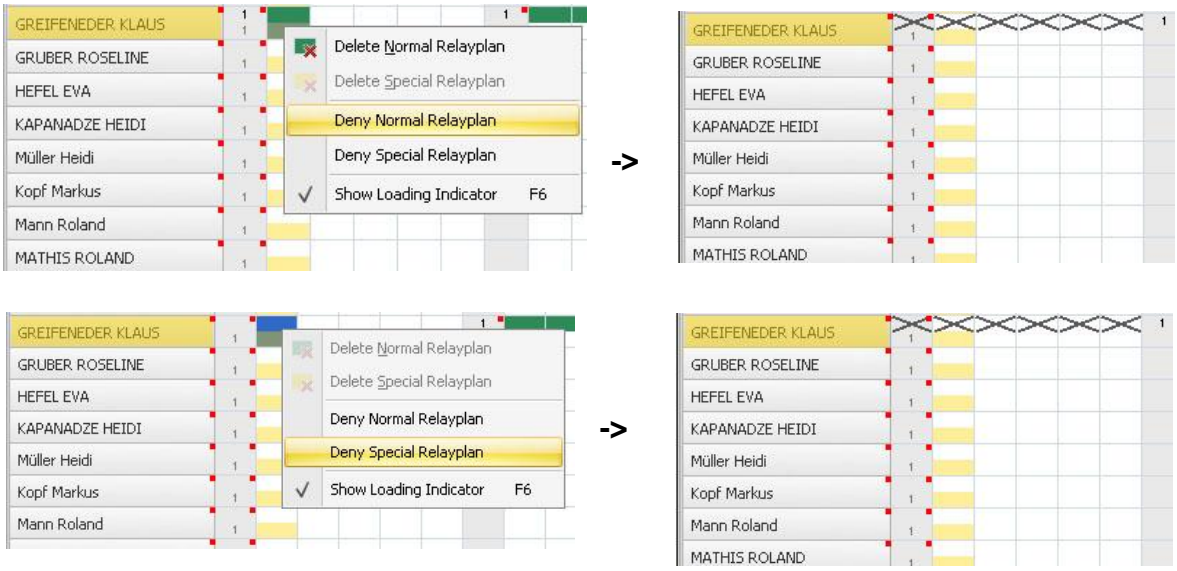


Figure 5.118 *–Deny relay plan*

5.15.5 Deleting a relay plan assignment

In order to delete a relay plan assignment, click on the relay plan, which should be deleted, of the desired person with the right mouse button. In the pop-up menu item, select either "Delete Normal Relay Plan" or "Delete Special Relay Plan".

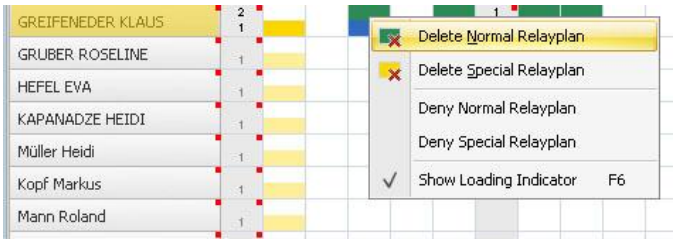


Figure 5.119 *–Delete the assigned Relay Plan*

The selected relay plan (Normal- or Special relay plan) will be deleted for the person at the door. The relays are no longer used for the identification process of a person.

5.15.6 Assigning a relay plan to a door (for general open plans)

A relay plan also can be assigned directly at the door. The defined relays of the relay plan are tightened every time whenever, according to the General Open Plan of the door, the normal unlocking relays are activated

The assignment of a relay plan to a door is similar to the assignment of a person. First, mark the door directly in the headline of the matrix and then assign the relay plan as "Normal Relay Plan" or "Special Relay Plan" by clicking on the arrow icon in the first column in the relay plan list.

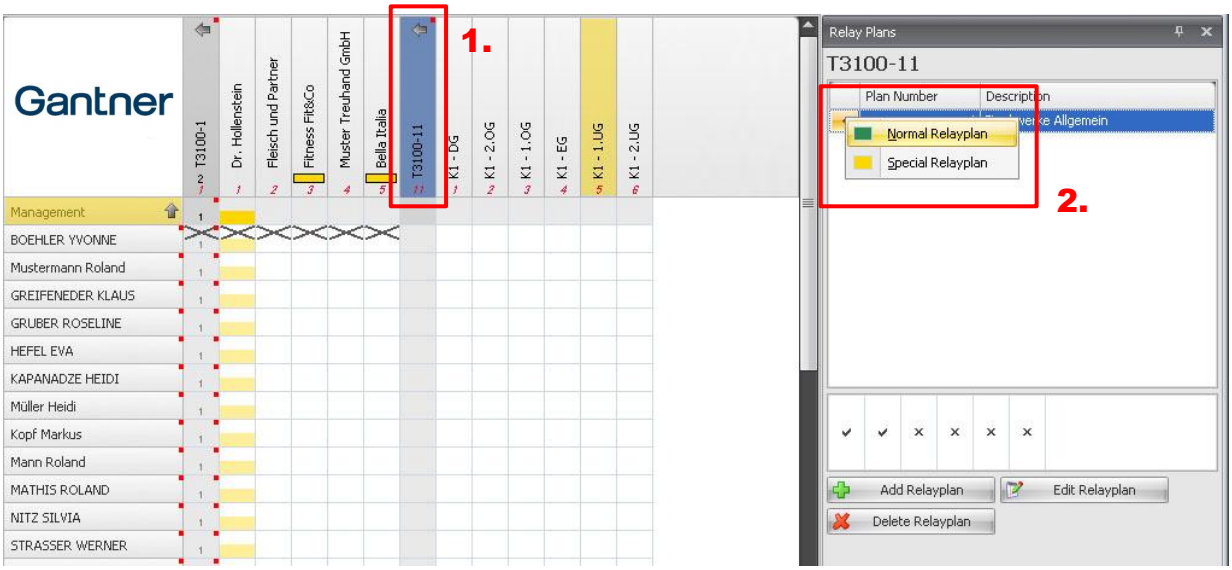


Figure 5.120 *– Assign a relay plan to a door*

If a relay plan is assigned to a door, the recommended relays with the defined color (green = Normal Relay plan, yellow = Special Relay plan) are assigned and the relay plan number is shown in a black number at the door.

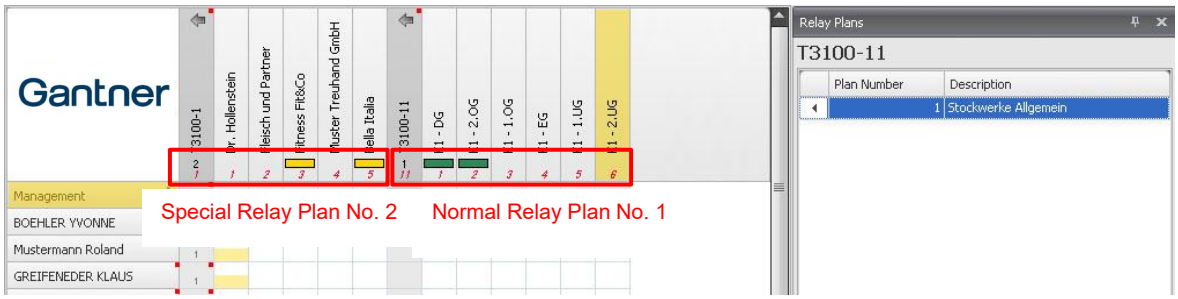


Figure 5.121 *–Door with assigned Normal- or Special Relay plan*

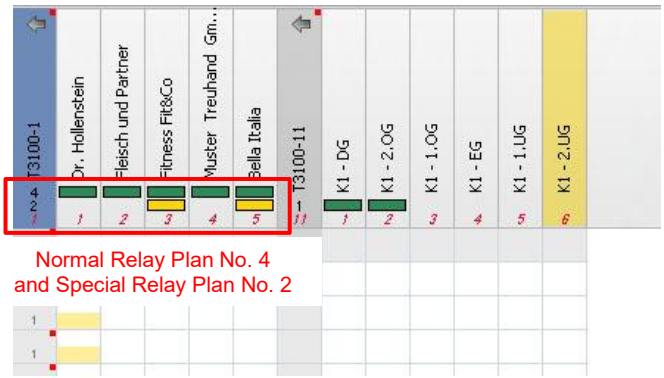


Figure 5.122 *– Door with assigned normal or special relay plan*

In order to delete the relay plan again, right-click on the door and select "Delete Normal Relay plan" or "Delete Special Relay Plan".

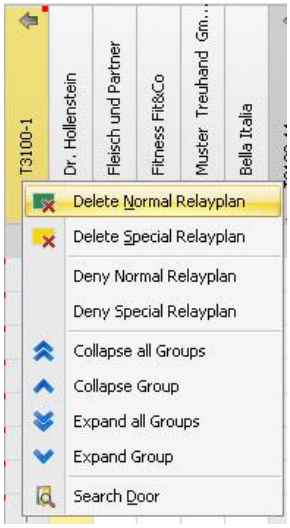


Figure 5.123 *– Delete relay plan from a door*

5.16 Time switches

For doors, the "Time Switches" function can be activated. This function does not use the door to identify persons, rather it will automatically control access based on an assigned door schedule. This allows, e.g., entrance gates to open autonomously, without having to carry out an identification, on working days at working times and the rest of the time to be closed.

A door with the time switch function activated does not require a license. This means that any number of doors in addition to the maximum number of doors determined by the license can use the time switch function. The time switches are not displayed in the matrix view of the access authorizations, but in the "Time Switches" overview.

The time switch function is not possible for doors imported from SALTO ProAccess SPACE.

NOTE! Note that before importing a door, the maximum number of doors (determined by the license) must not yet be reached, otherwise a new door cannot be imported. Even if the new door is to be used as a time switch, a door license must still be available for the import. Only after the time switch function has been activated does the position used for this door become available again.

All doors that are defined as time switches are displayed in the "Time Switches" overview.

► Click on the "Time Switches" icon.

○ The overview of all doors used as time switches is displayed.

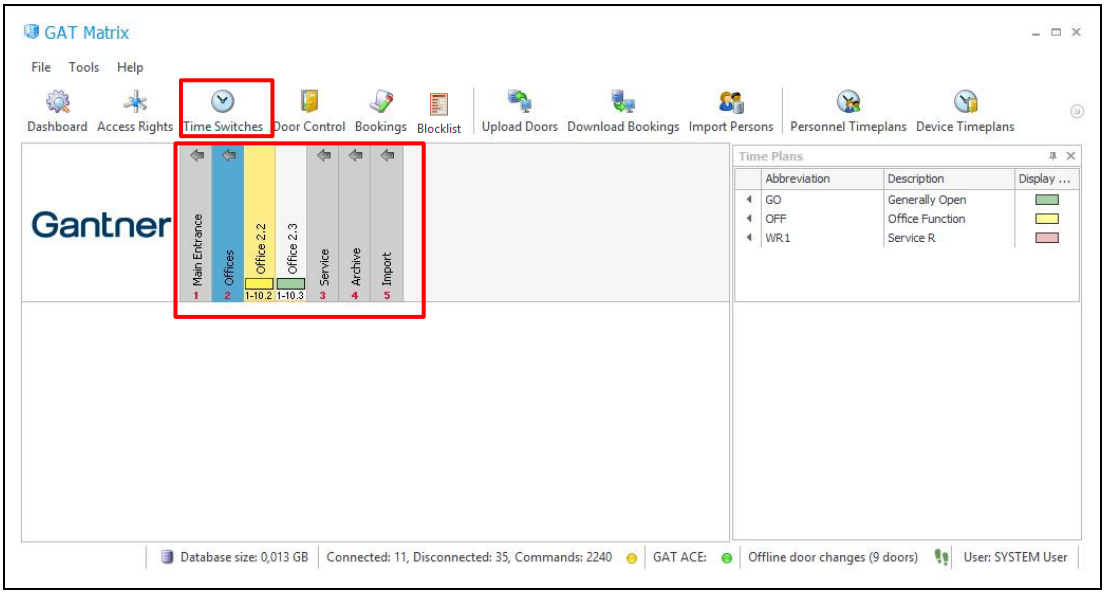


Figure 5.124 – *Time Switches overview*

► To define a door as a time switch, double-click on the name of the door in the access authorization matrix.

○ The window "Edit door - *[door name]*" opens.

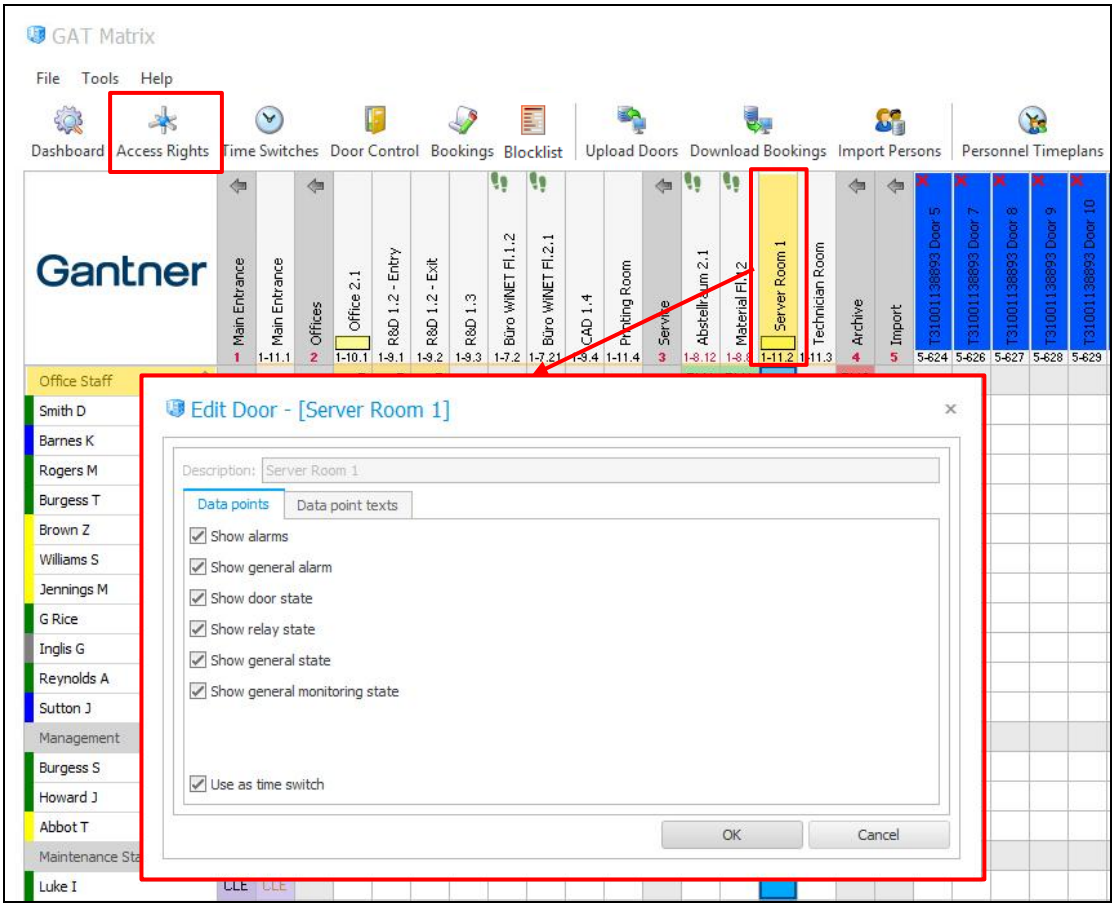


***Figure 5.125** – Activating the time switch function for a door*

► Select the "Use as time switch" option and confirm with "OK".

○ The door is hidden in the access authorization matrix and displayed in the time switches overview.

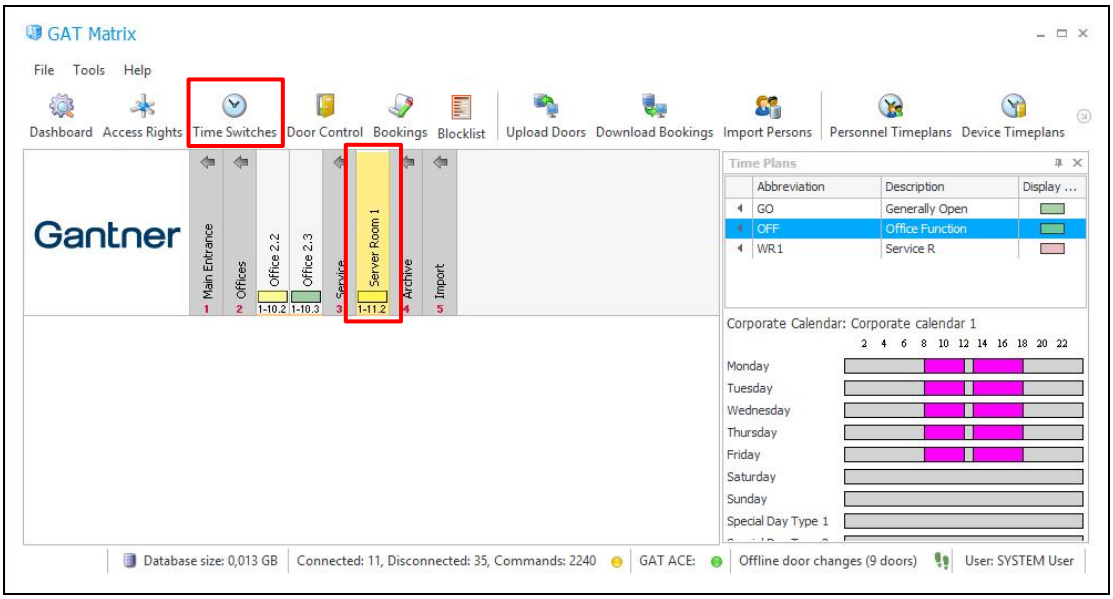


***Figure 5.126** – Door added as a time switch*

► Select the new door in the overview and then click on the arrow symbol of a door schedule to assign this door schedule to the selected door.

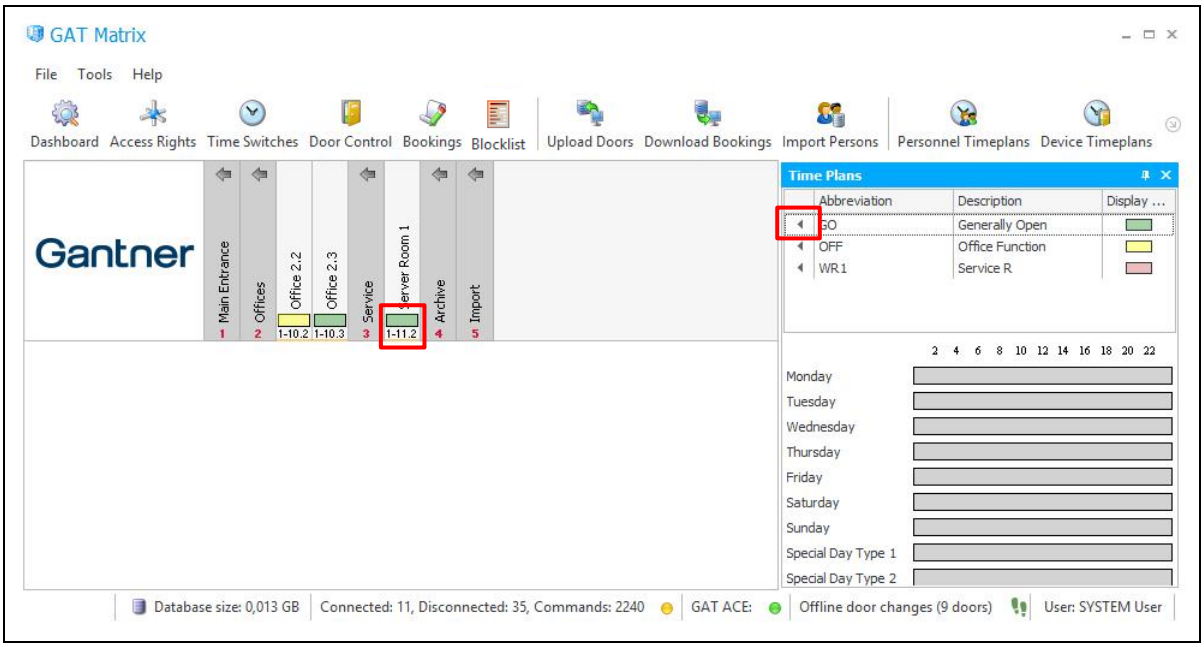


***Figure 5.127** – Assigning a door schedule to a door*

- The door schedule is displayed with a colored box near the door.
- The assigned door schedule now determines which functions the door automatically performs at which times.

5.17 Door control

Door control is an additional function in Matrix that must be activated via a separate license (see “10. LICENSE MANAGEMENT”). Door control provides a separate overview in Matrix of the current status messages and alarm messages of the doors with activated alarms displayed. In addition, you can remotely control the doors (i.e., unlock or lock) directly in Matrix.

The door control function is also possible for doors imported from SALTO ProAccess SPACE. This is completed in the same way as for the GANTNER doors.

► Check whether a license code has been entered for the door control function in Matrix (menu "Help" -> "License Information" -> "License details") and that the "Valid until" date has not yet expired.

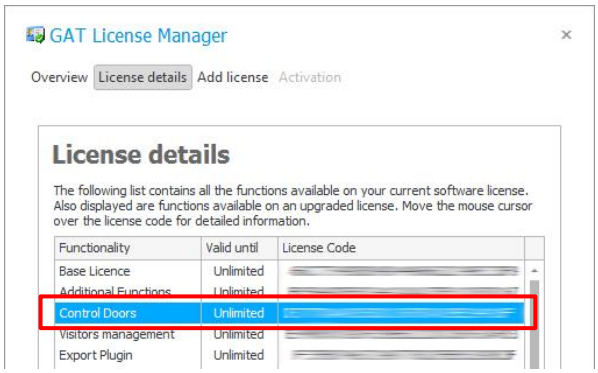


***Figure 5.128** – License detail – Control Doors*

► Click on the "Door Control" icon in the Matrix toolbar.

- The "Door Control" overview is displayed.

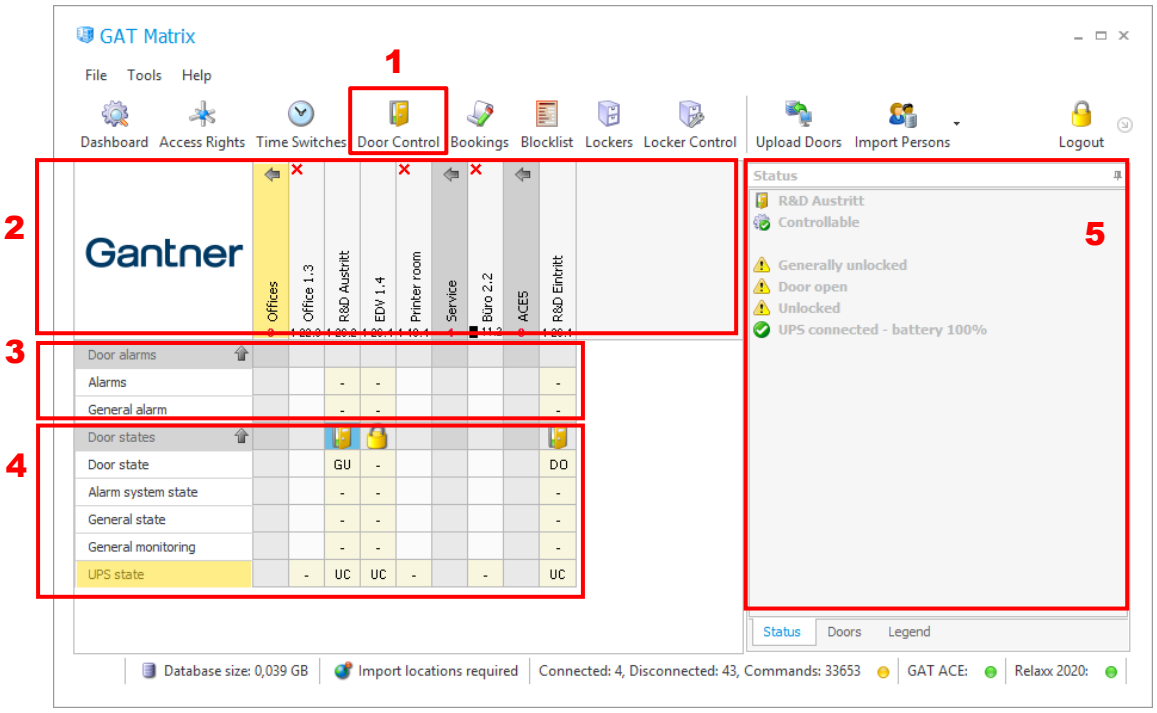


***Figure 5.129** – Door Control user interface*

1 - "Door Control" icon: Click on this icon to open the door control overview.

2 – Door list: Displayed here are all the doors that are enabled for door control.

3 - "Door alarms" group: If activated, the alarms that have occurred are displayed here (see below). For each door, it is possible to select which specific information should be displayed. The yellow fields are activated data points and are displayed. Fields with a light gray background are not used.

4 - "Door states" group: If activated, the state information for each door is displayed here. The yellow fields are activated data points (see next section) that are displayed. White fields are inactive. In the group heading row, the door state is indicated via a symbol with a code written in the following line. A "?" symbol means that the state cannot be determined (door offline or no status input defined).

- E … Door has been unlocked via Matrix control or on site for single access. After unlocking, the door is locked again.
- DF … The door is permanently open via a permanent release in the door control or via an active general open plan.
- TO … Door is open.
- BL … The door is locked and cannot be unlocked (e.g., via an input used to lock the door or by blocking it via the door control).

5 – Status field: Displayed here is detailed information about the selected state field, e.g., the type of alarms or door states that have occurred.

5.17.1 Activating door control for a door

► To activate door control for a door, return to the authorization matrix by clicking on the "Access Rights" icon in the toolbar.

► Double-click on the desired door in the header of the authorization matrix.

○ The "Edit door - *[door name]*" window opens.

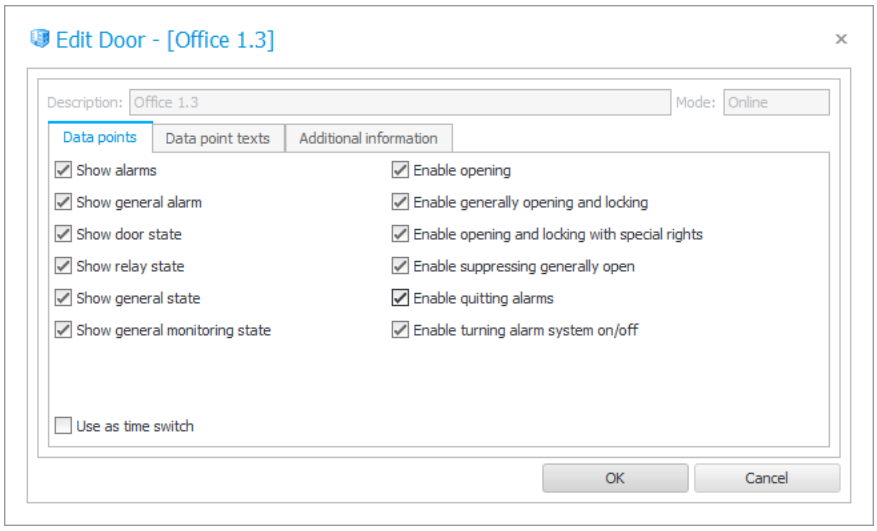


Figure 5.130 *– Data points for door control of a door*

► On the left side, select the data points that should be displayed in the door control.

- Show alarms: If an alarm occurs, it will be shown in the door control display with a symbol and a shortcut.
- Show general alarm: If a general alarm occurs, it will be displayed in the overview.
- Show door state: An icon indicates whether the door is open, closed, or blocked.
- Show relay state: Shows the state of the switching relays, which are used to switch alarm systems.
- Show general state: Shows the state of the input that is defined to acquire a General Status.
- Show general monitoring state: Shows the state of the input defined for the General Monitoring function.

Note: Not all of these control commands and status information can be used with SALTO doors.

► On the right side, select the control functions that you want to enable for the door.

NOTE: The options marked here also determine which control commands are available in the "GAT Mobile Access Management" mobile app.

► Confirm with "OK".

► Click on the "Door Control" icon in the toolbar.

○ The "Door Control" overview opens, and the newly activated door is displayed.

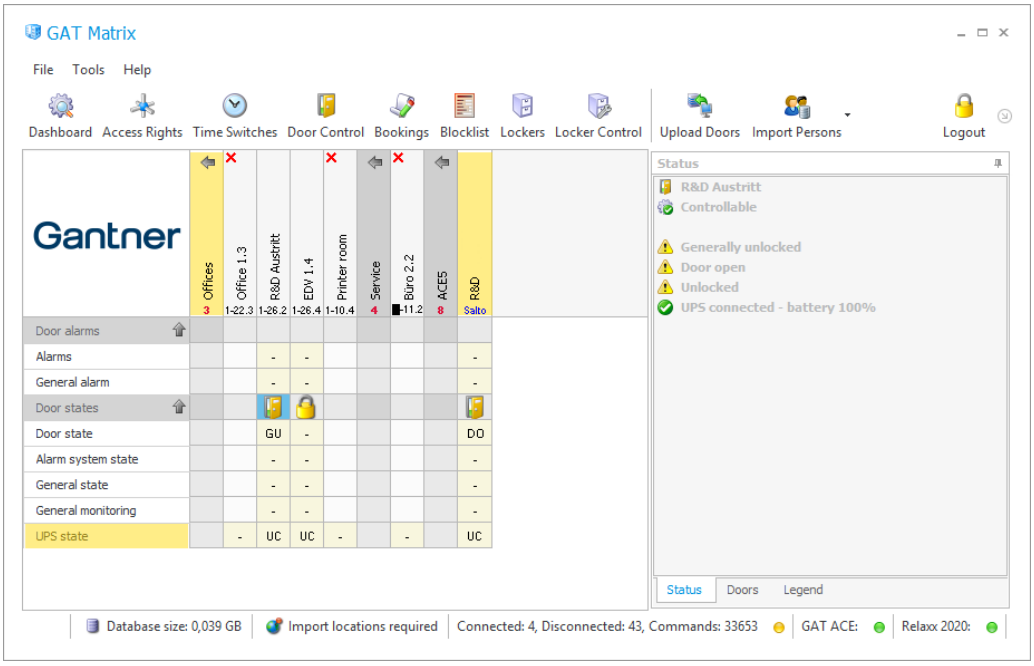


***Figure 5.131** – Door Control overview*

NOTE! If command control for a door connected to GAT ACE 3000 is not possible, please check whether the control is enabled in the terminal. Only then is control possible. For controllers in GAT ACE 7000, this does not have to be enabled first.

NOTE! Doors from SALTO ProAccess SPACE ("R&D" in the figure) have restricted functions. The restrictions are displayed in detail on the "Door control" window.

NOTE! The door control of SALTO doors is not currently supported in the GAT MobileAcces app.

5.17.2 Displaying and acknowledging alarms

If an alarm has occurred, this is indicated in the upper lines of the "Door alarm" group by means of symbols and, if the data points "Show alarms" or "Show general alarm" are activated, also with abbreviations in the door control overview. The following figure shows a door open timeout alarm (DOT) and a manipulation alarm (MAN).

*To acknowledge door alarms, the data point "Enable quitting alarms" must be selected for the door (see Figure 5.***130***)*

► If an alarm has occurred, always check the reason for the alarm first.

► Resolve the problem that triggered the alarm.

► Acknowledge the alarm by right-clicking and selecting the corresponding option in the pop-up menu.

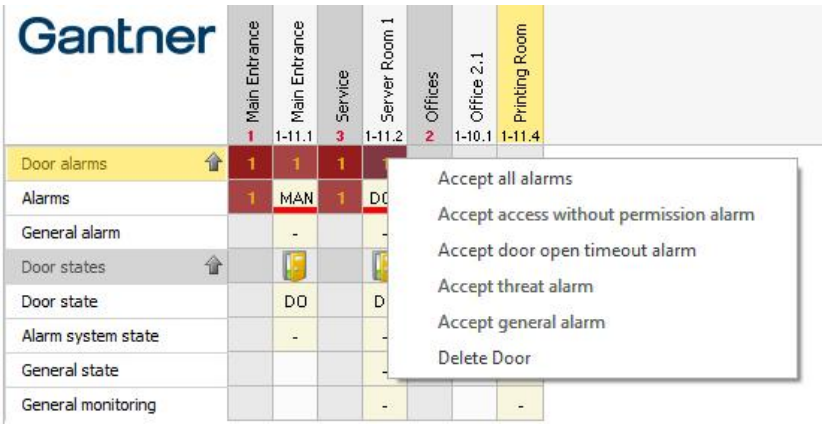


Figure 5.132 *– Alarm acknowledgement*

- Accept all alarms: With this option, you acknowledge (cancel) all alarms that affect the selected field. For example, a manipulation alarm and a too-long-open alarm can be generated simultaneously at a door. In this case, both alarms will be cancelled.
- Accept specific alarm: With this option, you can select a specific alarm to be acknowledged. Only the selected alarm will be cancelled, and the rest will remain.

5.17.3 Controlling the doors

The control functions can be activated individually for each door by enabling the respective data points (right column in Figure 5.130).

Different options can be selected for the door control. Generally, a distinction can be made between the control of the door state and the control of the alarm system.

Door state

► Right-click on a controllable field in the "Door states" column (yellow background).

- A pop-up menu opens in which you can select the following options:

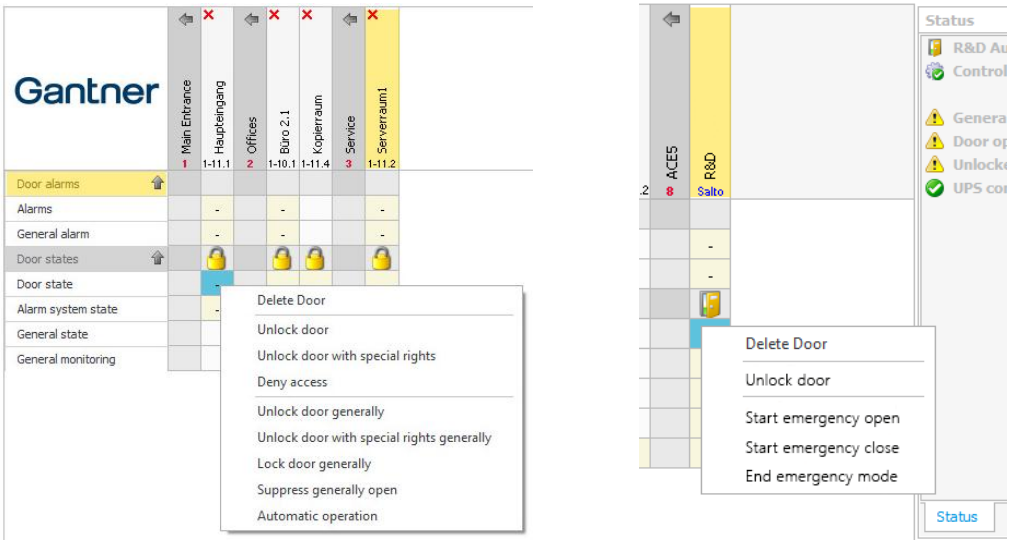


Figure 5.133 *– Door control options for GANTNER (ACE) doors and... ... for SALTO doors*

► Select one of the following options:

- Unlock door: The door is unlocked for the configured unlocking time. The abbreviation “E” is displayed.
- Unlock door w. special rights: The door is unlocked for the configured unlocking time and the special rights activated.
- Deny access: Access is blocked.
- Unlock door generally: The door is permanently unlocked. The abbreviation "DF" is displayed.
- Unlock door w. special rights generally: The door is permanently unlocked using the special relay plan. The abbreviation "DF" is displayed.
- Lock door generally: The door is locked and cannot be opened even with valid identification. If a general open plan or a permanent release is active, these will be overridden, and the door will remain locked. The abbreviation "BL" is displayed.
- Suppress generally open: An active generally open time plan at the door gets deactivated. The door operates autonomously according to the stored authorization data, i.e., the door is locked and can be unlocked with an authorized data carrier. The abbreviation “GOS” is displayed.
- Automatic operation: The door control is transferred again to the door controller and checked according to the stored authorization data and schedules. For example, if a general open plan is active at the door, but the door has been blocked in the door control, the blocking is lifted again, and the door unlocked according to the general open plan.
- Start emergency open: If emergency opening is started via this option (e.g., in the event of an emergency), access to the door is possible for all persons generally, regardless of their authorization.
- Start emergency close: With an emergency closing, the door is locked for all persons generally, e.g. in the event of an emergency. The restricted access also applies to persons who are otherwise authorized to use the door.
- End emergency mode: Returns the door from emergency mode to the normal operating state.

Alarm system state

In this row you can turn the alarm system on and off. It functions by switching the relay on and off, which activates or deactivates the alarm system provided that the wiring is correct.
To be able to use the function, the alarm system function ("EMA control and block lock function ...") must first be activated in the controller (see manual of the controller).

► Right-click onto a controllable field in the "Alarm system state" line (yellow background).

- A pop-up menu opens in which you can select the following options:

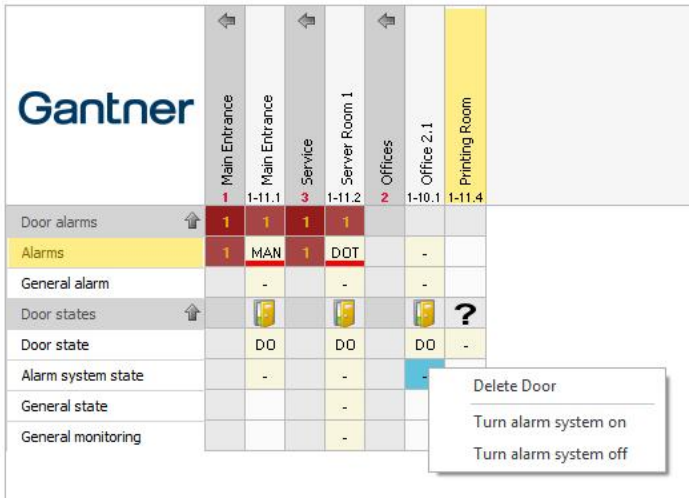


***Figure 5.134** – Turning the alarm system on/off*

► Select one of the following options (only possible for GANTNER doors, not available for SALTO doors):

- Turn alarm system on: When the alarm system is turned on:
  - the abbreviation "ON" is displayed in the "Alarm system state" line, and,
  - the door is blocked (abbreviation "BL" and lock symbol in "Door state" line)

  The activation of the alarm system is only possible with the door closed. If you select the menu item with the door open, corresponding information is displayed.

- Turn alarm system off: The alarm system is deactivated. The abbreviation "ON" and the lock symbol with "BL" abbreviation are deleted.

5.17.4 Deleting doors and general control

A "Delete Door" option is available in every popup window. With this option, the door is deleted from Matrix (also from the authorization matrix).

If you right-click on a door in the header, you will see all the control options (alarms and states) and can select them here. You do not have to click on a field in the matrix.

5.18 Upload doors

After the creation of persons, assigning of time plans, etc., all changes must be uploaded to the door controllers so that these changes take effect. For this process, there is a distinction between online and offline doors.

5.18.1 Uploading online doors

In order to upload these changes in the Online Terminals (doors), press the “Upload Door” toolbar button in Matrix and wait for the operation to complete.

When this task is successful, GAT ACE will now start to process the commands and send the required data to the devices.

The status bar shows the number of commands that still need to be processed (19 commands in the following example). The LED symbol next to "Commands:" is displayed in red or orange so long as there are commands that have not been sent to GAT ACE.

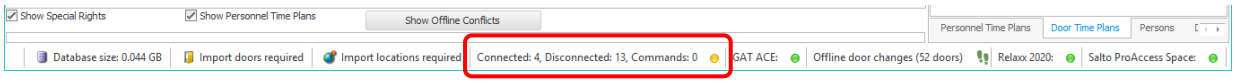


Figure 5.135 *– Status bar information*

When all commands have been successfully sent to all GAT ACE clients, "Disconnected: 0" is displayed and the LED icon is green. The value after "Commands:" shows how many commands have been sent. In addition, the following message indicates that the transfer of authorizations to GAT ACE was successful.

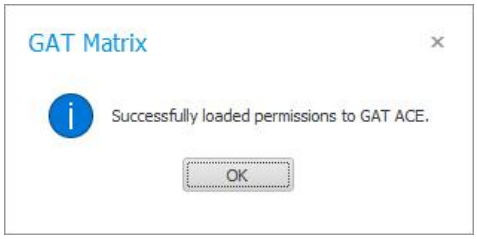


Figure 5.136 *– All commands with permissions have been transferred to GAT ACE*

Please note that this message does not mean that the data was also sent to the terminals since there can be inactive communication channels or terminals in GAT ACE. Before uploading data, Matrix will show a warning if there are inactive terminals or communication channels. It is your responsibility to activate the terminals or communication channels again in GAT ACE. Matrix does not automatically complete this process.

NOTE! The connection to GAT ACE and the controllers is shown by an LED symbol next to “GAT ACE” with various colors displayed according to the current status. For more information see "5.22 GAT ACE status".

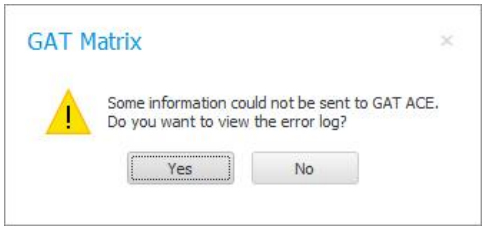


Figure 5.137 – *Warning message about inactive controllers or communication channels*

If errors have occurred during loading, these are indicated by a message. If you press the "Yes" button in this message window, the corresponding log file opens with a record of the errors.

```
1  Error Formatting Terminal Memory of Door [3:001 / 3]
2  Error Formatting Terminal Memory of Door [5:Terminal 4]
3  Error Formatting Terminal Memory of Door [13:Back Door]
4  Error Formatting Terminal Memory of Door [21:Main Entrance]
5  Error Formatting Terminal Memory of Door [23:Terminal 2]
6  Error Formatting Terminal Memory of Door [25:Warehouse Door 1]
7  Error Formatting Terminal Memory of Door [34:Dispatch Outside Left]
8  Error Formatting Terminal Memory of Door [10:T3100 Plus]
9  Error Loading Configuration of Door [2:001 / 2] with TimePlan [0:]
10 Error Loading Configuration of Door [3:001 / 3] with TimePlan [0:]
11 Error Loading Configuration of Door [4:001 / 4] with TimePlan [99:Warehouse]
12 Error Loading TimePlan [99:Warehouse] at Door [4:001 / 4]
13 Error Loading Configuration of Door [5:Terminal 4] with TimePlan [0:]
14 Error Loading Configuration of Door [12:Terminal 1] with TimePlan [0:]
15 Error Loading Configuration of Door [13:Back Door] with TimePlan [0:]
16 Error Loading Configuration of Door [14:Terminal 3] with TimePlan [0:]
17 Error Loading Configuration of Door [21:Main Entrance] with TimePlan [99:Main Entrance]
18 Error Loading TimePlan [99:Main Entrance] at Door [21:Main Entrance]
19 Error Loading Configuration of Door [22:Dispatch Office] with TimePlan [99:Main Entrance]
20 Error Loading TimePlan [99:Main Entrance] at Door [22:Dispatch Office]
21 Error Loading Configuration of Door [23:Terminal 2] with TimePlan [0:]
22 Error Loading Configuration of Door [24:Terminal 3] with TimePlan [99:Warehouse]
```

Figure 5.138 *– The log-data file records any errors when loading doors*

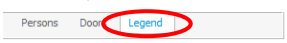
NOTE! If Matrix is closed before uploading changes to the controllers, you will be asked if the changes shall now be uploaded.

5.18.2 Uploading offline doors

For offline doors, the controllers are not directly connected via network to Matrix and GAT ACE respectively. For the configuration of these offline locks, the difference between the CardNET and WiNET functions must be clarified.

- For offline doors with CardNET function, configuration, data transmission, and the uploading of booking data are performed on-site using either the GAT MT 010 handheld programmer, via RF with GAT Config Manager and the GAT DL 090 / 092, or via GAT ACE 7000 and the GAT DL 092. The authorization of data carriers occurs at certain online controllers that support the read / write mode (CardNET mode). By reading a data carrier at one of those devices, the data carrier is coded accordingly.
- For offline doors with WiNET function, communication via a wireless transmitter is possible:
  GAT DL 090 for GAT DL 32x, 34x, 350, and 360
  GAT DL 092 for GAT DL 32x, 34x, 350, 360, and GAT DL 370

When changes have been made to the settings of offline doors (except for offline doors with WiNET), a green footsteps symbol is displayed in the status bar of Matrix. This indicates that the offline doors must updated with the changed settings, e.g., using the GAT MT 010 on site. You can also see how many offline doors need to be loaded in the dashboard area of Matrix.
With the “Upload Door” button in the symbol bar of Matrix all changes to the authorization data are sent to GAT ACE and, if used, Relaxx. To activate those changes in the access control system, all offline locks with CardNET function (not WiNET) must be uploaded onsite using the GAT MT 010 or via RF with the GAT DL 090 / 092. For CardNET systems, the data carriers of the persons must also be read ONCE at a controller with CardNET functionality in order to be coded accordingly.

If not all data can be updated when loading the offline locks, this is shown with the corresponding colors of the footsteps symbols. The colors are arranged by priority (from red to violet, green, and blue). If there are several colors at the same time, the color with the highest priority is displayed. The meaning of each color is described in the "Legend" 

tab to the right of the matrix.

Requirements for using offline doors:
Matrix from version 3.1.0 supports devices with read-only mode as well as read/write mode.

Notes about offline door groups:
All doors within a door group also automatically form an offline door group. The addresses of the offline doors and the ID numbers of the offline door groups are indicated as red numbers in front of the door names or group names respectively. For online doors, this number is displayed in black color. The ID numbers of the groups are calculated automatically on creation of a group.

Example of usage
As GANTNER data carriers can only store 10 offline locks and 30 offline door groups, the offline locks, which have the same access rights (time plans), should be grouped together in one door group. Therefore, only one authorization for the entire group is written onto the data carrier rather than a single authorization for each door. Figure 5.139 shows an example where the doors "Engineering Fl.1" and "Material Fl.1" both have the same time plan "MA2" assigned. Because both doors are members of the same group (ID number "4"), only one access right for group ID 4 will be written onto the data carriers of the corresponding persons and not the rights for each door separately.

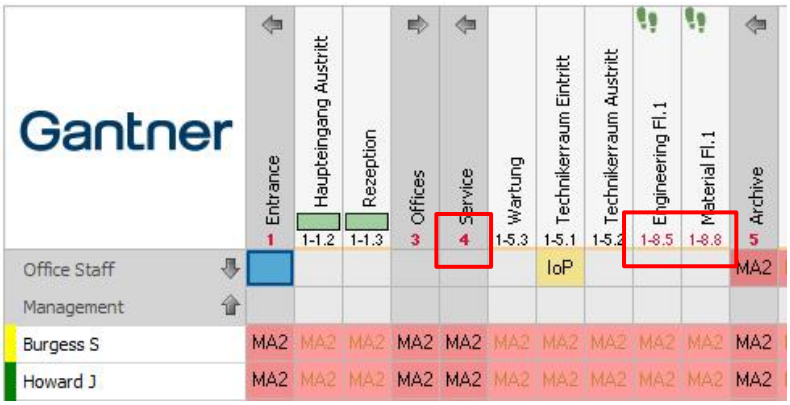


Figure 5.139 *– Indication of the offline doors and offline door group IDs*

However, should a different schedule be assigned to one of the offline doors in the example shown, then individual authorizations are written for ALL offline doors in group 7.
By clicking on the "Show offline file conflicts" button, Matrix automatically calculates whether the offline data can be written to the required data carriers. This calculation is done as a background process. The progress of this calculation is shown as a green bar below the matrix (see "5.2 Main window"). If, for example, it is not possible anymore to write all offline rights of a person onto its data carrier, as much access rights will be written onto the data carrier as possible and for the remaining fields in the matrix a yellow exclamation symbol is shown . This means that this person does not have any access right at those doors. The offline doors must then be collected to one new offline door group.
NOTE! The exclamation symbol is not only displayed for doors and people but also for persons groups that have one or more similar conflicts. You can quickly identify conflicts even when the groups are collapsed. In this case, click on the symbol to automatically expand all door groups that contain an exclamation symbol.
Note that each person marked with an exclamation symbol must be manually selected and loaded via the "Reload person to doors" menu item.

NOTE! After pressing "Upload Door" you must wait until GAT ACE has processed all commands from Matrix before the data can be transferred to the offline terminals. All commands are processed when "GAT ACE (0)" is displayed in the status line of Matrix.

5.18.3 Loading online doors from SALTO

The changes made to the ProAccess SPACE doors are loaded to the controllers and locks separately from the GANTNER doors. This is not done via the GAT ACE software but via the Salto ProAccess SPACE Synchronizer and the ProAccess SPACE software.

Displayed in the status bar is information about the connections of Matrix to the external applications such as GAT ACE and SALTO ProAccess SPACE (green = connection OK). The number of data packets yet to be loaded is also displayed there. The number of changes yet to be applied to the SALTO doors is shown next to "Pending Salto changes".

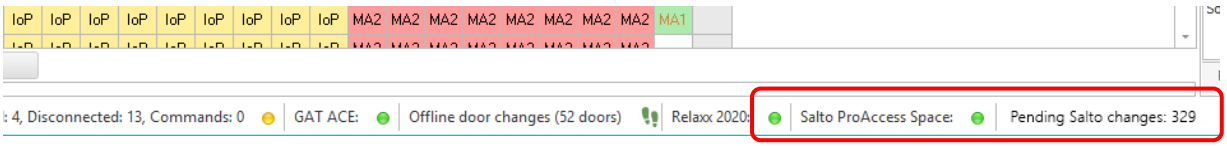


Figure 5.140 *– Information in the status bar*

► Select "ProAccess Space Synchronization" from the “Tools” menu or double-click on the text "Pending Salto changes" in the status bar.

○ The following window is displayed.

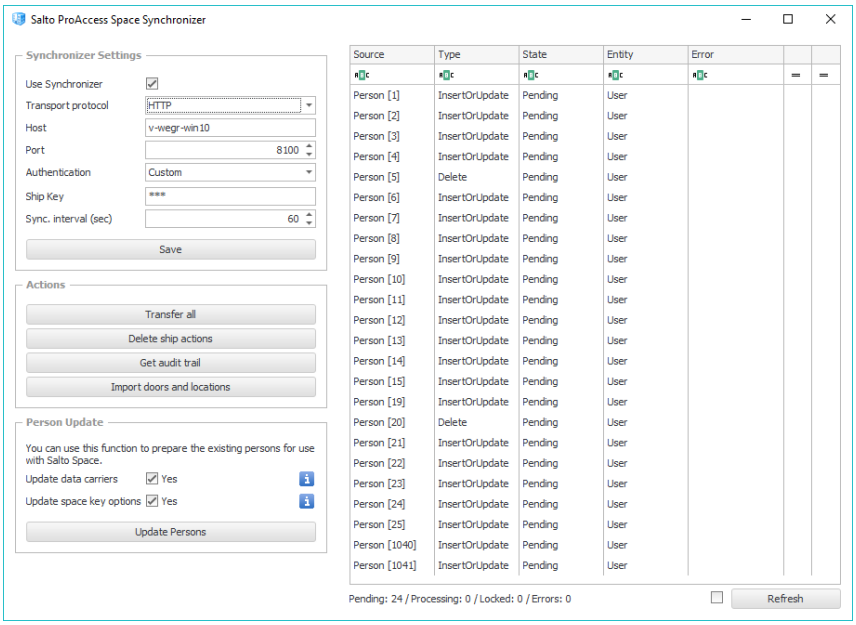


Figure 5.141 *– Configuration and communication of SALTO ProAccess SPACE Synchronizer*

On the left side, the connection settings for ProAccess SPACE Synchronizer are configured. The list on the right displays the commands that are to be sent from Matrix to ProAccess SPACE.

The following connection settings are available:

- Use Synchronizer: Enable this option to send the commands to ProAccess SPACE.
  Note: When the Synchronizer is enabled, Matrix is checked for unique records (personnel names, etc.). Unique records are required for ProAccess SPACE and can cause problems if not used, so the feature cannot be enabled for non-unique records.

- Transport protocol: Select the desired transfer protocol here (default = http).
- Host / Port: The computer name or IP address of the computer and the port used for communication to ProAccess SPACE (default = 8100).
- Authentication: Here you select how Matrix should identify itself to the ProAccess SPACE software. Default is "Custom". Depending on the selected setting, enter the data for the identification below.
- Sync Interval (sec): Defines the time in seconds that ProAccess SPACE Synchronizer waits for before checking whether changes are available for processing. If there are no changes, the synchronizer remains inactive during the interval.

► To load the authorization data (persons, plans, etc.) to ProAccess SPACE, click on "Transfer all" and confirm with "OK".

- The data is written as ship actions to the transfer table on the right and automatically sent to the GAT ProAccess Space Synchronizer, which then transfers them to the ProAccess SPACE software.
- If a problem occurred during a ship action, the row is highlighted in red.
- By double-clicking on a line, you can display more detailed information about the ship action. This helps, for example, when searching for errors ("Exception" response).

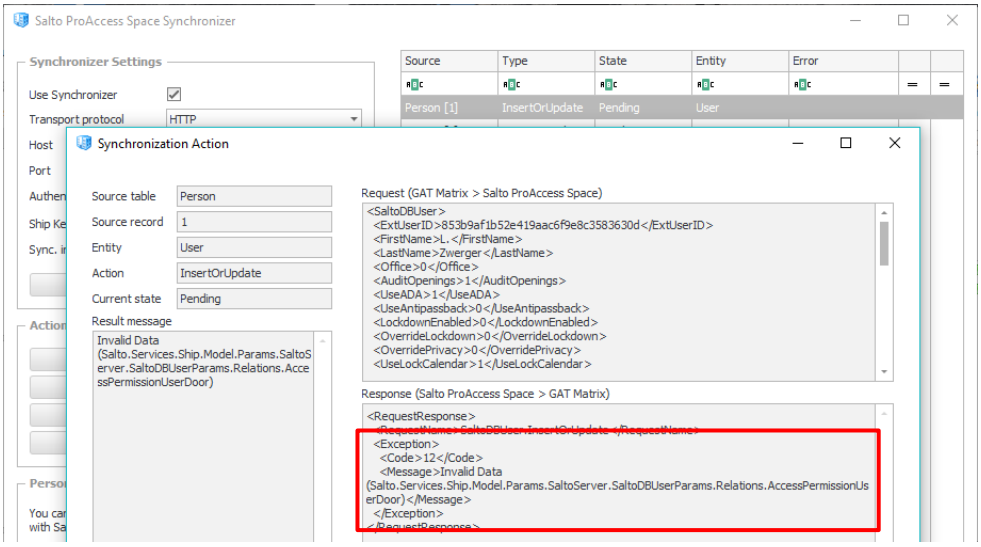


Figure 5.142 *– Information about a ship action for SALTO ProAccess SPACE Synchronizer*

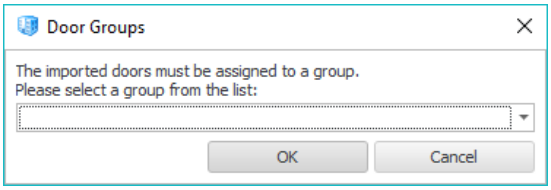
► To update the table, click on "Refresh" below the table. Alternatively, you can enable the option next to the "Refresh" button so that the table is updated automatically on an ongoing basis.

► With "Delete ship actions", you can delete the actions listed in the table. In this case, no more actions will be sent to ProAccess SPACE. You must then restart loading to send the configurations from Matrix to ProAccess SPACE.

► Bookings (audit trails) are usually transferred automatically from ProAccess SPACE to Matrix. If this is not the case, the transfer can be started via the "Get audit trail" button.

► The "Import doors and locations" button can be used to import the doors and locations from ProAccess SPACE to Matrix.

- The following window opens.



► Select the door group to which the doors are to be imported here. All door groups defined in Matrix are displayed. Then click "OK".

○ The following window opens.

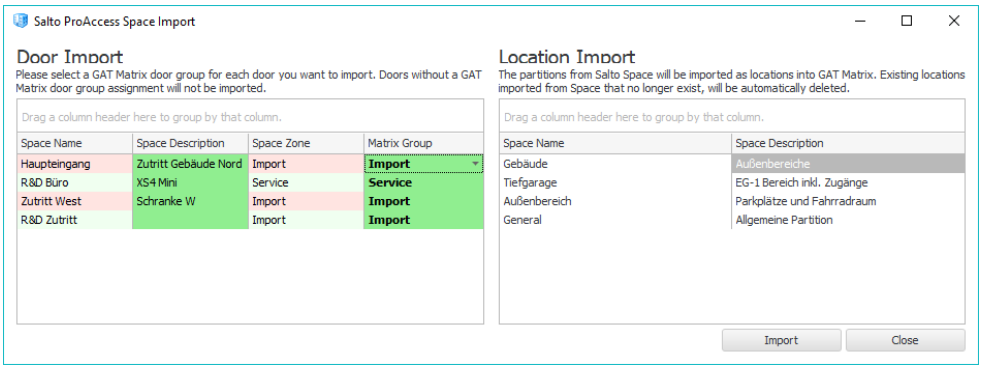


***Figure 5.143** – Importing doors and locations from SALTO ProAccess SPACE*

○ The doors to be imported are displayed on the left. On the right, the locations (called "partitions" in ProAccess SPACE) are displayed. For more information about the import function, see "5.5 Importing doors and locations from SALTO ProAccess SPACE".

5.18.4 Loading offline doors from SALTO via programming device (PPD)

The authorization data for the offline doors defined in the SALTO ProAccess SPACE software can be transferred via a handheld programming device. Communication takes place using a SALTO coding station connected to the computer or network. The programmer is placed on the station and the data is transmitted wirelessly. Proceed as follows:

► Select "Space PPD Management" from the “Tools” menu.

○ The following window is displayed. All SALTO doors are listed here.

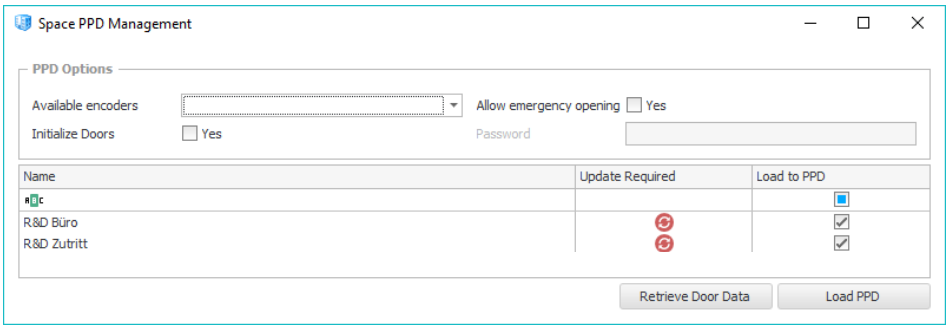


***Figure 5.144** – Transfer of data via PPD programming device*

- ► Select the SALTO encoding station to be used from the "Available encoders" field. The encoder must be connected to the computer.
- ► Select "Initialize Doors" if you also want to initialize the doors in addition to transferring the authorization data. Initialization is required when commissioning a SALTO door for the first time.
- ► In the "Load to PPD" column, select the doors that you want to transfer data from. By default, all doors that require an update are selected.
- ► Click on "Retrieve Door Data" to import the door data stored on the programming device (e.g., battery charge states) into Matrix.

5.18.5 Reloading a single door

Matrix provides the possibility to reload a single door.

NOTE! This function is only applicable for doors in GAT ACE 3000.

This function is accessed using the context menu of a door and is useful, for example, when a controller is being replaced and the access rights must be loaded to the new controller afterwards.

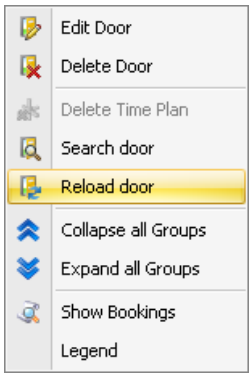


***Figure 5.145** – Reload a single door*

NOTE! If the "Multi-site policy" is activated (see "5.9 Multi-site policy"), only the persons at this door who are visible to the currently logged-in user will be reloaded.

5.18.6 Locker authorizations

For GANTNER's range of electronic locker locks, e.g., the GAT NET.Lock 7020, GANTNER provides Relaxx software for managing the electronic locker system. From Matrix V4.3.0, it is possible to integrate Relaxx with Matrix thereby allowing you to assign persons the authorization to use a locker or group of lockers directly in Matrix.

The main tasks of configuring the locker system hardware as well as the creation of locker areas and groups is completed in Relaxx. For detailed information on the installation and operation of Relaxx and the GAT NET.Lock system, see the documentation of the respective product. The following instructions describe how to use the "Lockers" function in Matrix.

The following requirements must be met in order to use the "Lockers" function in Matrix:

1. Relaxx Enterprise Edition, min. V 5.1.2, must be installed on the same computer or accessible via the network interface. For information on configuring the settings for the GAT Relaxx interface, see "4.4.4 Relaxx interface". A green dot next to "Relaxx 2020" in the status bar indicates that the connection to Relaxx 2020 is operating. A red dot indicates that the connection is not operating.

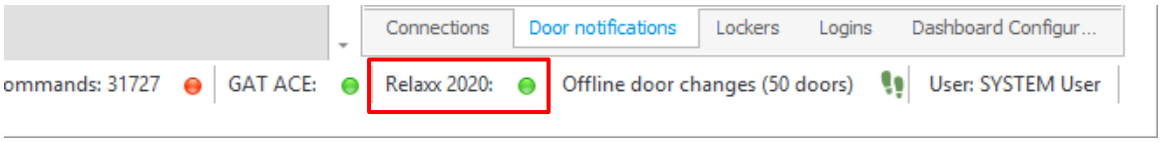


Figure 5.146 *– Connection to Relaxx shown in the status bar*

2. In the user management settings (menu "File" > "User Management"), the "Manage lockers" permission must be set for every user who is going to use the locker control system.

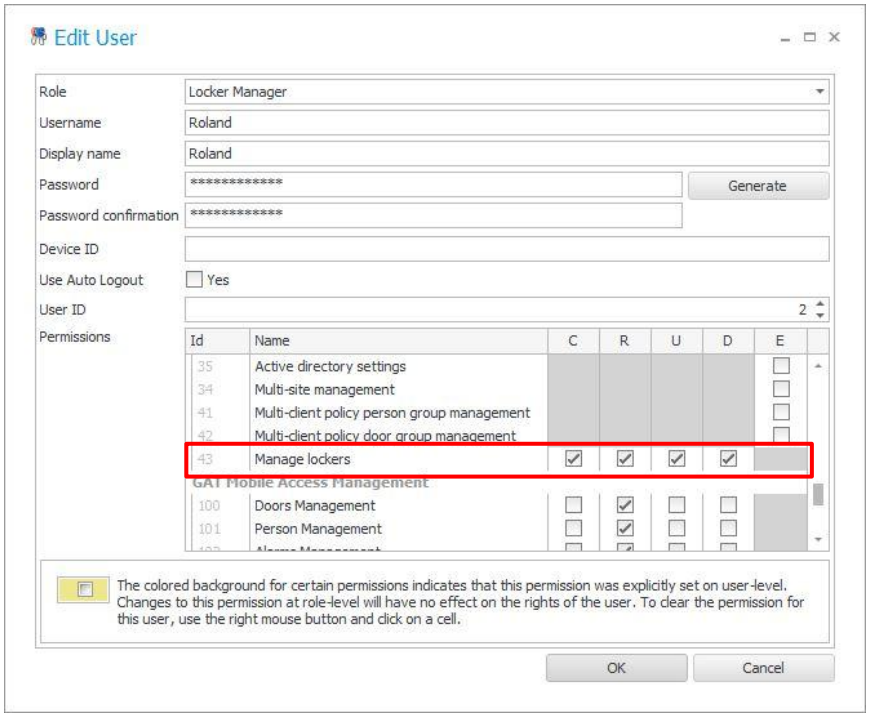


Figure 5.147 *– The "Manage locker" permissions*

See chapter "9 AUTHORIZATION MANAGEMENT" for information on creating roles and users.

3. If the multi-site policy is activated in the Global settings ("Tools" > "Options" > "Global" > "Enable

Multi-site policy"), the locker groups that the user is allowed to view must be assigned to them in the “Allocated groups” area (available via “File” > “Multi-site Policy” > “Locker Group” tab):

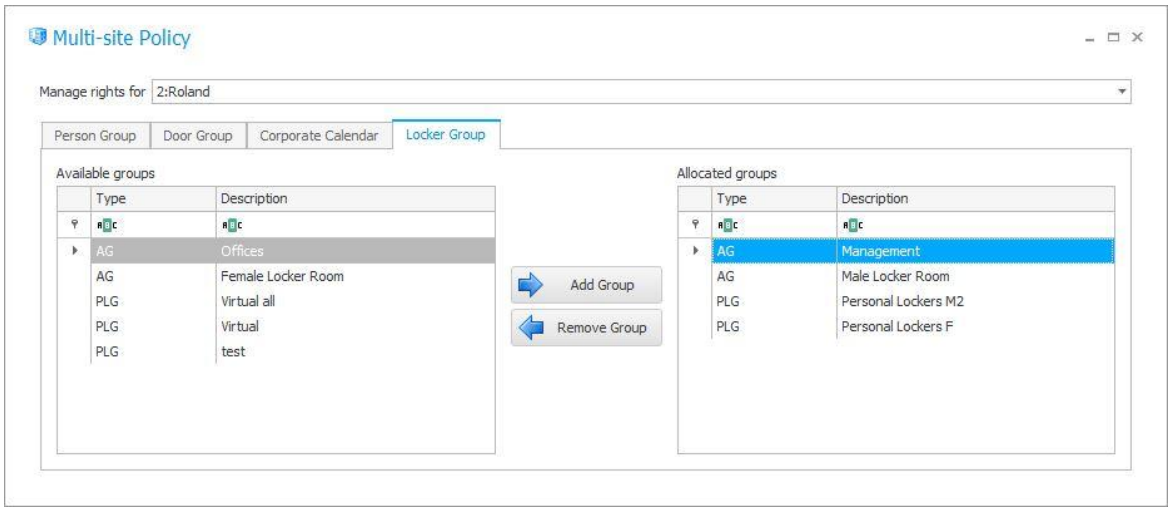
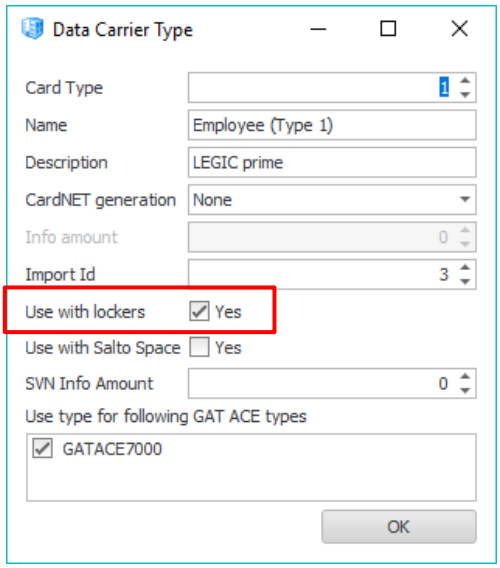


Figure 5.148 *– Allocating locker groups for the user*

This defines which locker groups the user is allowed to view in the locker matrix. In the example above, 4 groups are set for the user “Roland”. When “Roland” logs in, only those 4 groups are displayed.

4. In the “Data Carrier Type” window (“Tools” > “Data Carrier Types” > “Data Carrier Type”), the “Use with lockers“ option must be selected for each data carrier type to allow that data carrier type to be assigned to lockers in the locker matrix.



NOTE! The lockers cannot use multiple different data carrier technologies or encodings simultaneously!

Figure 5.149 *– “Use with lockers” option for the data carrier type*

5.18.7 Locker matrix



You can view the locker matrix by clicking on "Lockers" in the toolbar.

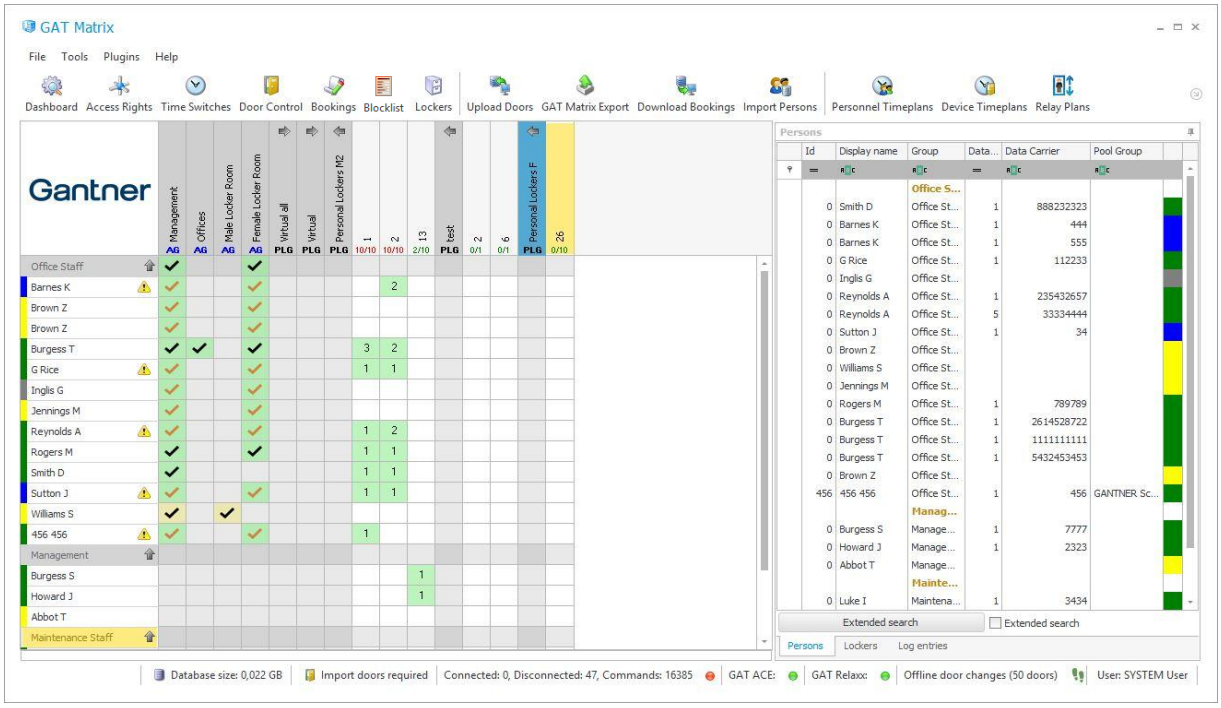
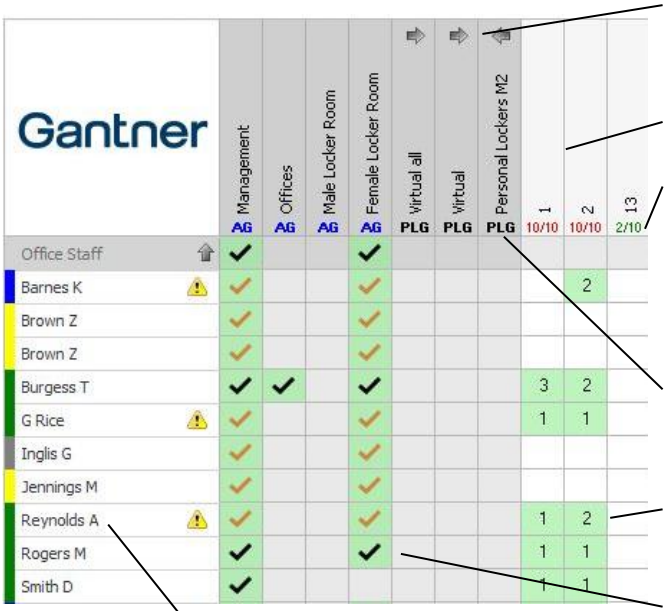


Figure 5.150 *– Locker matrix*

The locker matrix is used to assign or remove the authorization of persons to use the lockers. The layout of the locker matrix is similar to the authorization matrix.



Each locker belongs to a **locker group**, which is defined in Relaxx. Click on the arrow to show/hide the lockers within the group.

The **lockers** are shown here next to the group.

The **numbers** under each locker number indicate the number of data carriers already assigned to the locker followed by the maximum number of data carriers that can be assigned. If you want to change the maximum number, this is done in Relaxx via the controller settings.

These **letters** indicate the type of group:
PLG = personal locker group (personal lockers)
AG = authorization group (free lockers)

This **number** is the amount of data carriers from the person assigned to use the locker.

A **black tick** indicates that the authorization was directly assigned to the group. An **orange tick** indicates that the authorization was inherited from a group.

The **persons** are listed in groups in the left column of the matrix.

The area to the right of the locker matrix displays information depending on whether the “Persons”, “Lockers”, or “Log entries” tab is selected.

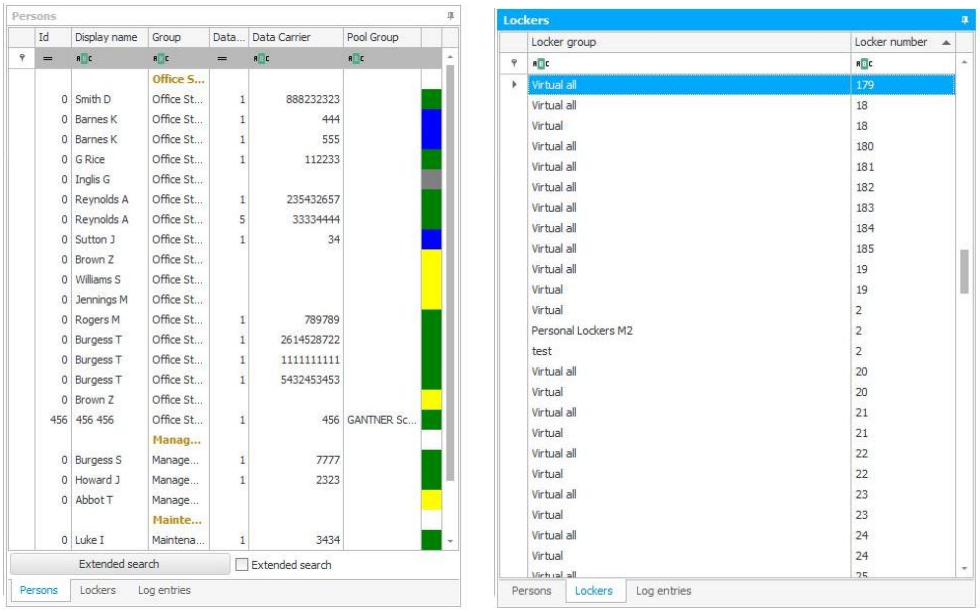
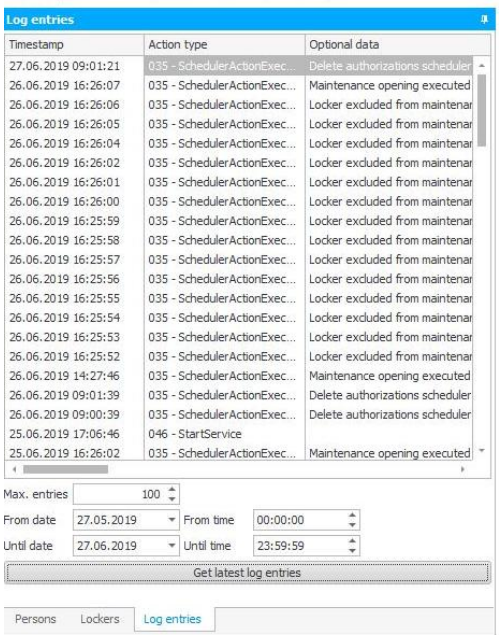


Figure 5.151 *– “Persons” and “Lockers” tabs*

To search for a specific person or locker, enter the search term into the respective column of the top row. An extended search function is available at the bottom of the tab "Persons" to fine-tune a search. Alternatively, you can sort the list by clicking onto the “ABC” symbol at the top of the respective column and selecting a sorting option from the menu.



The log entries function in a similar way as in the authorization matrix. Click onto the “Get latest log entries” button at the bottom, which will load and display the latest log data from Relaxx.

Figure 5.152 *– “Log entries” tab*

5.18.8 Assigning locker authorizations

The two types of groups - personal locker groups (PLG) and authorization groups (AG) – as well as the authorization list must first be defined in Relaxx. The instructions for assigning persons to these locker groups are explained in the following chapters.

Each time an authorization is assigned/unassigned in Matrix, a new authorization group is automatically created, or an existing group updated, in Relaxx. Changes made to the settings in one software occur instantly in the locker system without having to click an additional button; however, the changes may take a few moments to be seen in Matrix or Relaxx.

Press F5 in Matrix to refresh the data when changes are not immediately displayed.

5.18.9 Locker authorizations for free locker selection

When a person is assigned to an authorization group in the locker system, they may use any unoccupied locker (“free locker”) in that group. Other persons assigned to the group may also use any unoccupied locker in the group.

Authorization groups are indicated via the acronym “AG” underneath the locker group name.

In the following example, three persons in the “Management” group are assigned to use the lockers in the “Management” authorization group.



Figure 5.153 *– Assignments to authorization groups indicated via a tick symbol in the matrix*

► To assign a person to an authorization group, right-click onto the desired person and authorization group square in the matrix and select “Edit group assignment”.

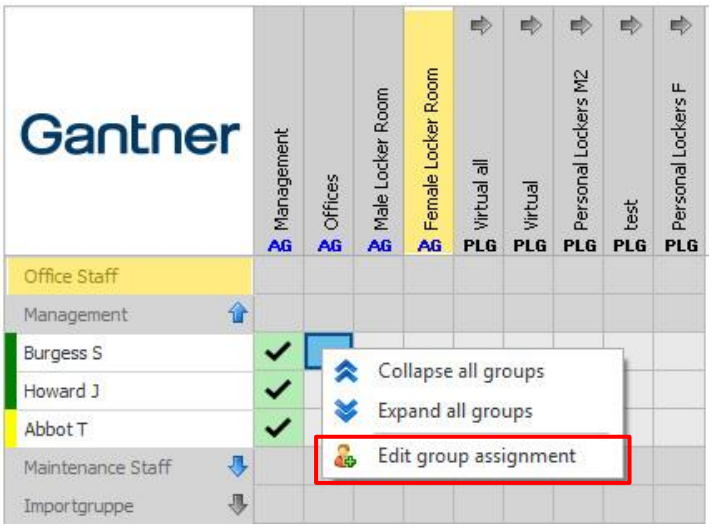


Figure 5.154 *– "Edit group assignment" option*

- The "Authorization Group" window opens.

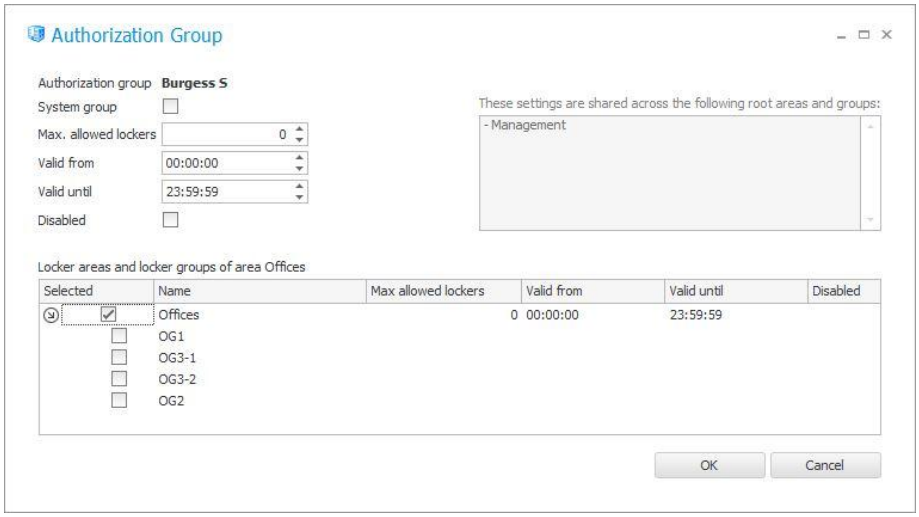


Figure 5.155 *– Authorization Group window*

► Edit the following settings:

- System group: When this option is selected, the authorization group type "System" from Relaxx will be used.

  Notice: A third group type "Maintenance" also exists in Relaxx; however, this type cannot be used in Matrix.

- Max. allowed lockers: Enter the maximum number of lockers that the person is allowed to use in the group at the same time.

- Valid from / Valid until: Define a validity period for the day during which the person is allowed to use the lockers in the authorization group. The default validity period (as shown in Figure 5.155) indicates that the person can use the lockers for the whole day.

- Disabled: This setting can be used to temporarily prevent the person from using lockers in the authorization group.
- Locker areas and locker groups of area:

  This area shows all the locker groups and sub-groups (as configured in Relaxx) of the selected authorization group. Select the groups and sub-groups to which the person will be assigned. In Figure 5.155, “Burgess S” is being assigned to the “Offices” area, which includes authorization to use all the lockers included in the 4 sub-groups (OG1, OG2, etc.).

► Click on “OK” to save the settings.

  ○ The assignment is indicated via a black tick.

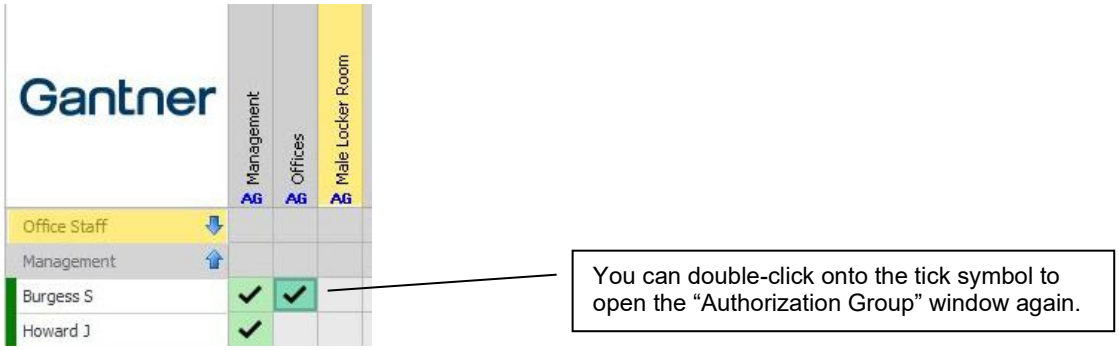


Figure 5.156 *– Indication of direct authorization group assignment*

► To remove the assignment, open the “Authorization Group” window again and deselect the groups to which the person is assigned. Click on “OK” to save the settings.

► The previous instructions can also be used to assign/remove all persons in a person group to/from an authorization group. Select the desired person group and authorization group square in the matrix and mark or unmark the groups as required.

  ○ A black tick at the person group and orange ticks at each person in the group is shown in the matrix to indicate the inherited assignment of the persons to the authorization group. An inherited authorization can be overridden by explicitly assigning or removing authorization.



Figure 5.157 *– Indication of inherited authorization group assignment*

5.18.10 Locker authorizations for personal lockers and shared lockers

Personal locker groups are used to assign persons to individual lockers that only they may use. Other persons can also be assigned to use the same locker, e.g., a department locker where all employees of a department share a single locker. It is possible for two persons who are assigned to the same personal locker to lock and unlock the locker using their data carriers simultaneously.

A personal locker group is indicated via the acronym "PLG" under the group name.

NOTE! The validity date set in the "Edit Person" window in Matrix is used for the locker system and overrides any validity date set in Relaxx.

Assigning a specific locker to a person

► Right-click onto the desired person and locker square in the matrix and select "Add personal locker: xxx". If more than 1 data carrier is shown, select the desired data carrier to use for assignment. In the following example, data carrier number "444" from "Barnes K." is being assigned to locker 1 in the "Personal Lockers M2" group.

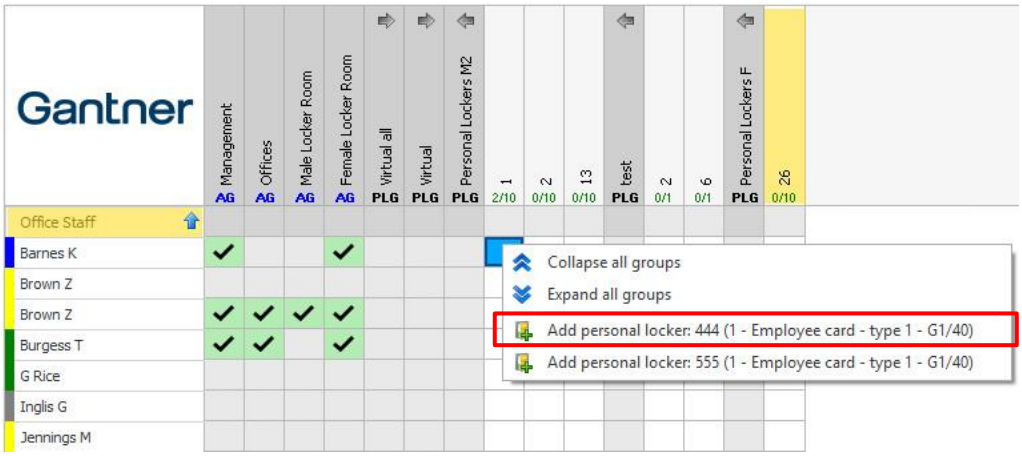


Figure 5.158 *– Assigning a person to a personal locker*

○ It is possible to assign multiple data carriers to use the locker. The number in the matrix square indicates the number of data carriers from the person that have been assigned to the locker.

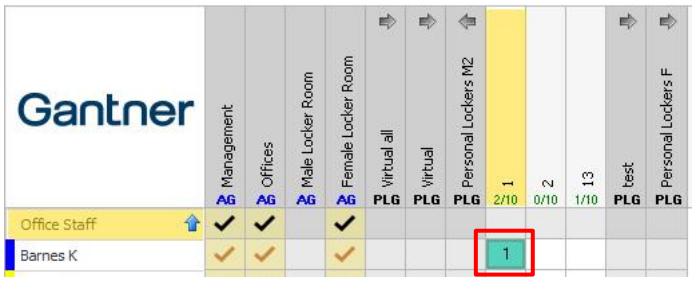


Figure 5.159 *– Indication of how many data carriers the person has assigned to the personal locker*

Automatically assign the first available locker of a locker group to a person

► Right-click on the desired person and locker group square in the matrix and select “Find personal locker: xxx”. In the following example, data carrier “1” from “Barnes K” is being assigned to the next available locker in the “Personal Lockers M2” group. If more than 1 data carrier is shown, select the desired data carrier to use for assignment.

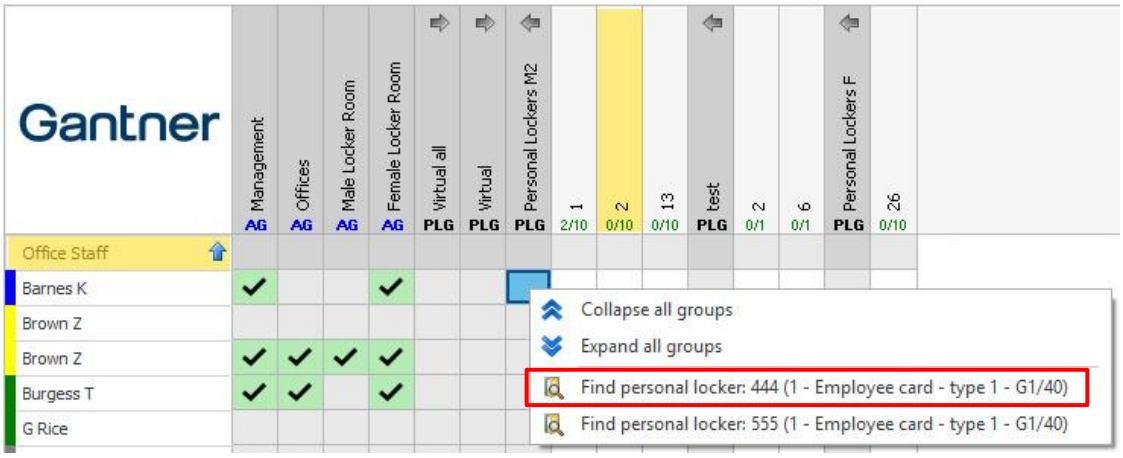


Figure 5.160 *– Automatically assigning a person to a personal locker*

Assigning a specific locker to all persons in a person group

► Right-click on the desired person group and locker group square in the matrix and select "Add personal lockers" from the menu. In the following example, locker 13 is being assigned to all persons in the “Office Staff” group. If a person has multiple data carriers, the locker is assigned to each data carrier.

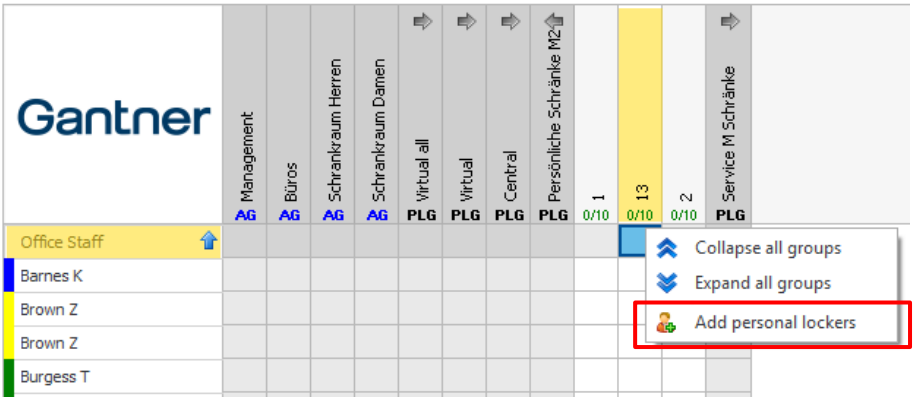


Figure 5.161 *– Automatic assignment of all persons in a person group to an available personal locker*

- If there are not enough personal lockers in the locker group to assign all data carriers to the persons, a message is displayed showing which data carriers could not be assigned.

When assigning authorizations automatically, note the following requirements:

- For each locker, only the max. number of data carriers, which have been defined for the locker in Relaxx as the max. value (an assignment is already reserved for group assignment), can be assigned to a locker. The assigned data carriers and the max. possible numbers are displayed for each locker (in the previous example, locker "13" currently has 0 data carriers assigned from a possible maximum of 10 -> 0/10).
- Only the data carrier types that have the setting "Use with lockers" enabled can be assigned (see "5.6.4 Defining data carrier types").

Deactivated person data carriers are also assigned. The display 2+1 indicates that 2 active and 1 inactive data carriers have been assigned.

Assign the next available locker in a locker group to all persons in a person group

► To automatically assign all persons in a group to the next available lockers in personal locker group, right-click onto the desired person group and locker group square in the matrix and select “Find personal lockers for all persons”. In the following example, the persons in the “Office Staff” group are being assigned to the next available lockers in the “Personal Lockers M2” group.

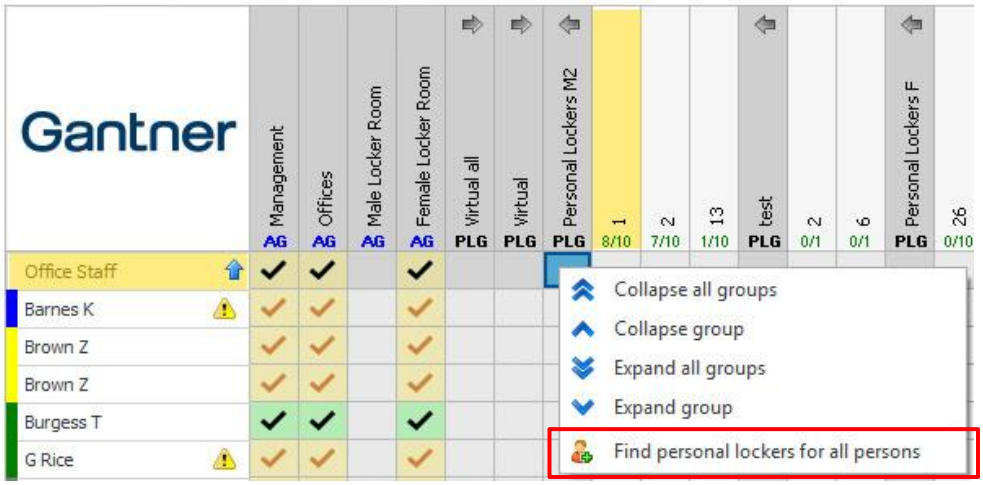


Figure 5.162 *– Automatically assigning all persons of a person group to personal lockers*

- If there are not enough personal lockers in the group for assignment, a message is shown displaying the persons who were not assigned to a locker.

When assigning authorizations automatically, note the following requirements:

- For each locker, only the max. number of data carriers, which have been defined for the locker in Relaxx as the max. value (an assignment is already reserved for group assignment), can be assigned to a locker. The assigned data carriers and the max. possible numbers are displayed for each locker (in the previous example, locker "13" currently has 1 data carrier assigned from a possible maximum of 10 -> 1/10).
- Only the data carrier types that have the setting "Use with lockers" enabled can be assigned (see "5.6.4 Defining data carrier types").

- Deactivated person data carriers are also assigned. The display 2+1 indicates that 2 active and 1 inactive data carriers have been assigned.
- For the assignment of authorizations, only the lockers to which no other data carrier has yet been assigned are used, even if the max. number of assignments has not yet been reached. For example, a locker with 4/10 (4 current authorizations from possible maximum of 10) will not be used. This prevents unintentionally authorizing data carriers for a locker that is already in use.

Assign several available lockers to several persons

► By marking an area of several persons and lockers and right-clicking on the area, all data carriers of the selected persons can be assigned (authorized) to the lockers contained in the area in one step. To do this, select "Add personal lockers for selection" from the menu.

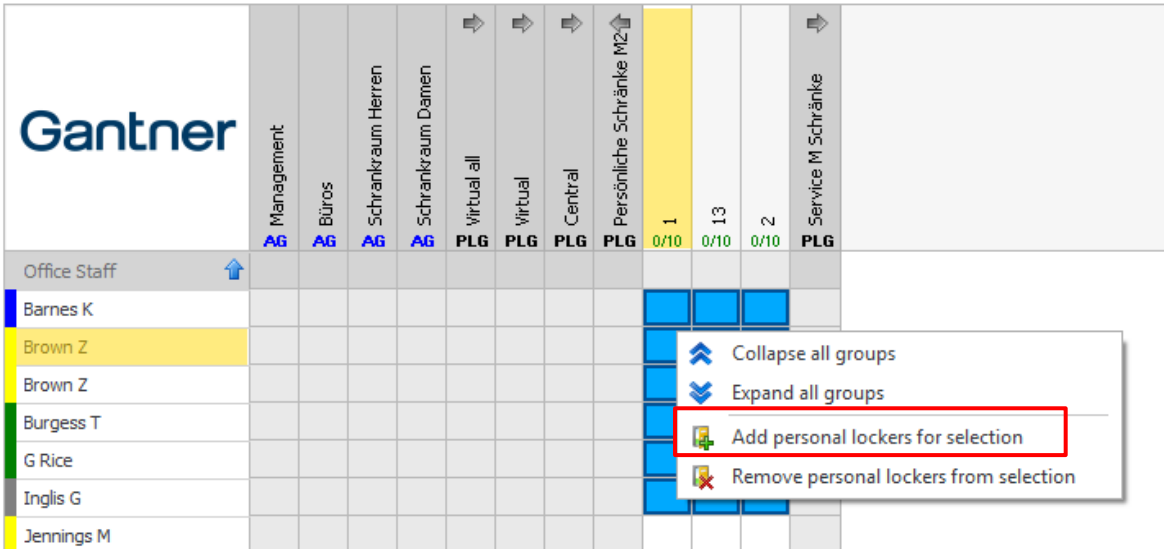


Figure 5.163 *– Automatic assignment of certain people to available personal lockers*

- If there are not enough personal lockers available in the selection to assign to all of the persons' data carriers, a message is displayed to inform which data carriers could not be assigned.

Deleting data carrier authorizations

► To remove the assignment of a data carrier, right-click onto the desired person and locker square in the matrix and select “Remove personal locker: xxx”

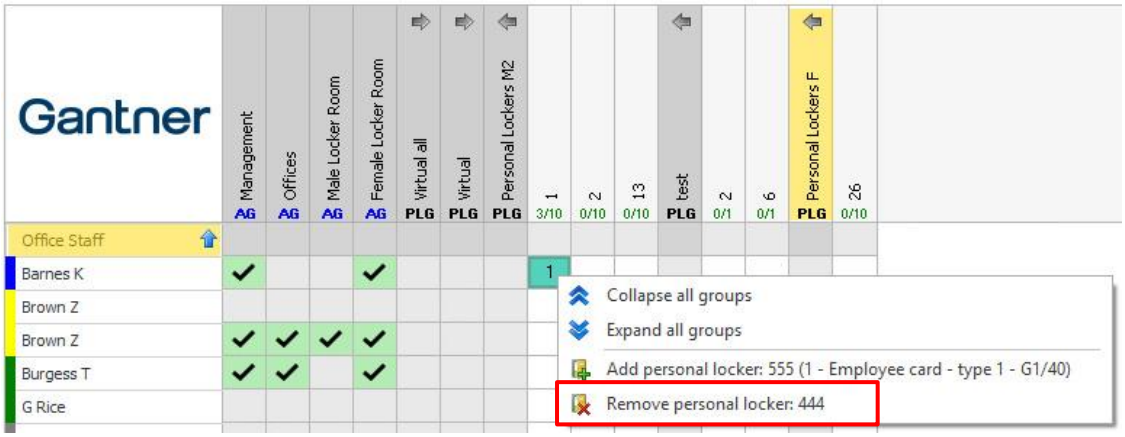


Figure 5.164 *– Removing a personal locker assignment*

5.19 Locker control

The control of the GANTNER electronic locker locks, e.g., the GAT NET.Lock 7020, can be done directly in Matrix. A connection to the Relaxx software is required.
In addition, similar to the way the locker authorizations are assigned, the following conditions must be met.

For a more detailed description of the requirements listed below, please read the detailed description in chapter "5.18.6 Locker authorizations".

1. GAT Relaxx Enterprise Edition, min. V 5.1.2, must either be installed on the same computer or an installation on another computer must be accessible via the network.

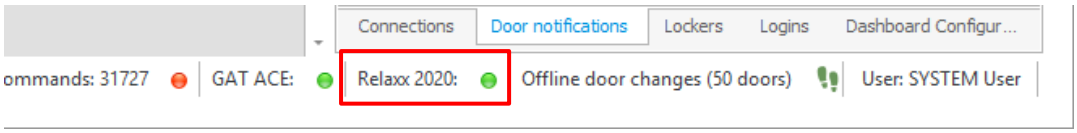


Figure 5.165 *– Connection to Relaxx shown in the status bar*

2. In the user management settings (menu "File" > "User Management"), the "Manage lockers" permission must be set for every user who is going to use the locker control system.

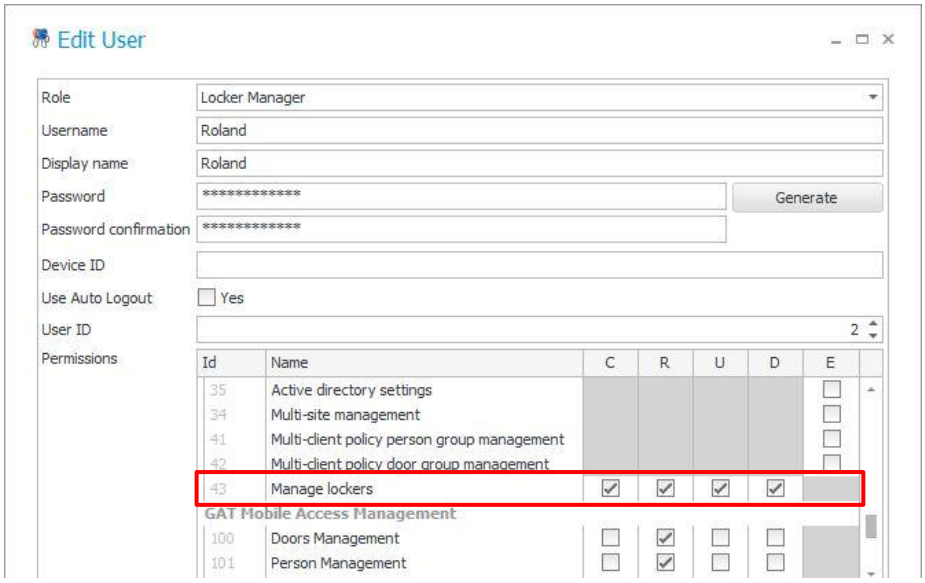


Figure 5.166 *– The "Manage locker" permissions*

See chapter "9 AUTHORIZATION MANAGEMENT" for information on creating roles and users.

3. The client rules must be set accordingly.

4. The "Door management" license must be activated.

5. Min. Relaxx Enterprise license required.

6. In order to display changes to the locker status in the matrix, the option "Notify third-party software of locker events" must also be activated in the general software settings (see Figure 5.*167*).

7. In these settings, the option "Use ASCII command coding" must also be enabled.
Note: After an update to Relaxx 7.x or later, this option is disabled and must be manually enabled.

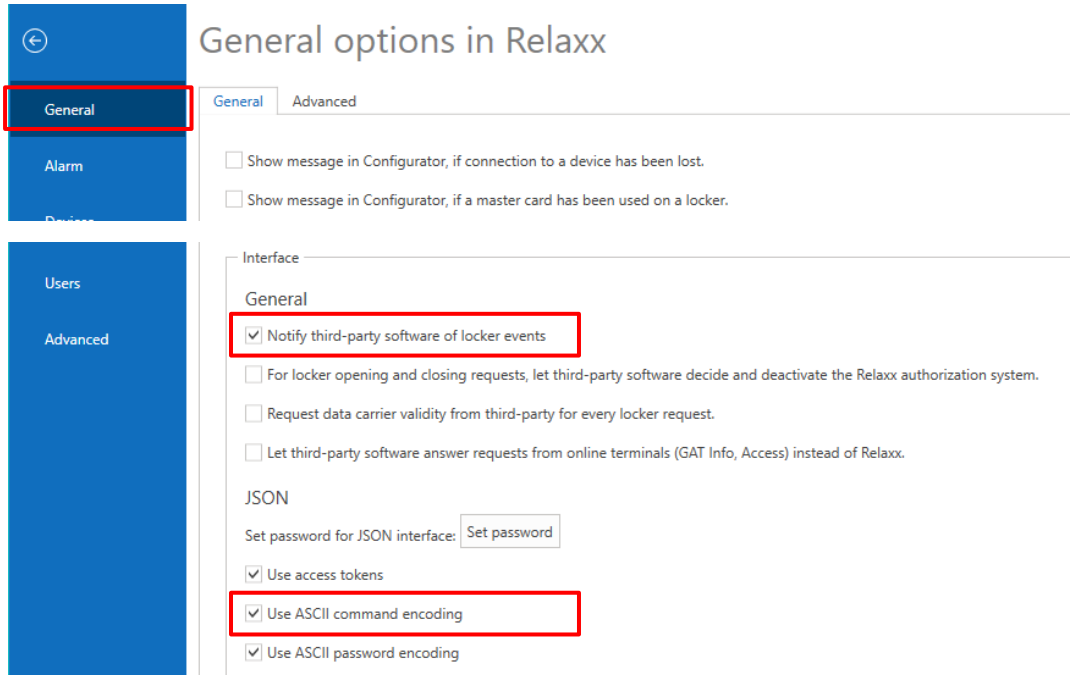


Figure 5.167 *- General settings in Relaxx*

5.19.1 Matrix display for locker control



Click on this icon to open the locker matrix display.

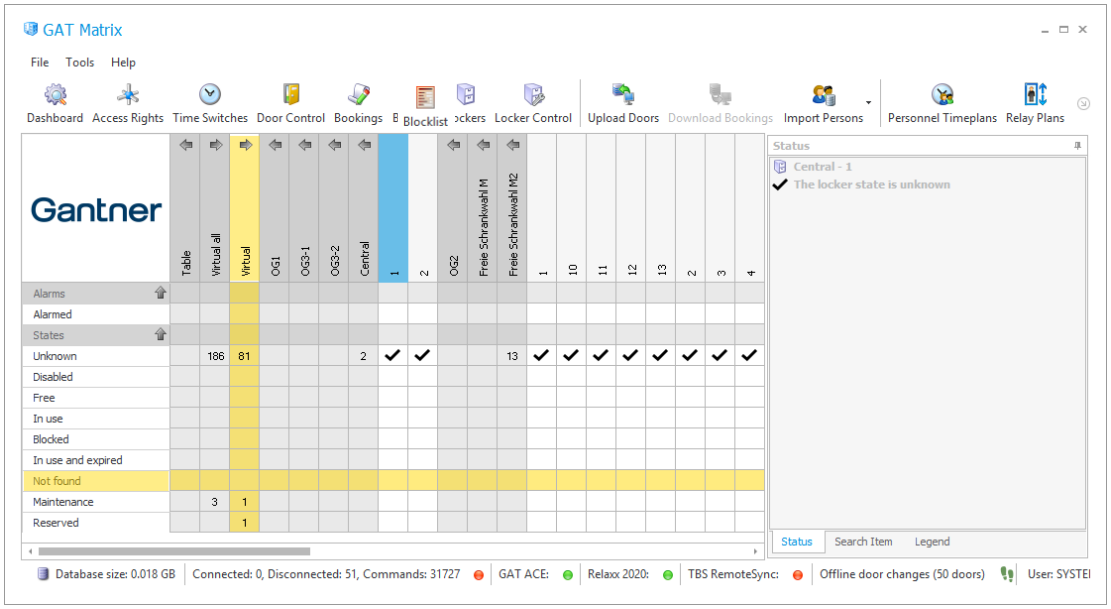


Figure 5.168 *– Locker matrix*

Shown in the top row of the locker matrix are all the lockers that have been imported by the Relaxx software. The various alarms and statuses are listed in the left column. The ticks indicate the current status of each locker. The following status information is displayed:

- Unknown: The status of the locker is unknown. The connection to the locker may be interrupted or the controller that controls the locker cannot be reached.
- Disabled: The locker has been deactivated in Relaxx. It is out of order and cannot be used currently.
- Free: A tick means that the locker is unoccupied and can be locked by an authorized user (see authorization assignment).
- In use: If a locker is locked by a user, a tick is displayed here.
- Blocked: The locker has been blocked in Relaxx, i.e., it cannot be used currently.
- In use and expired: The locker has been locked by a user, but the defined usage period has expired, and the locker has not yet been opened again.
- Not found: The locker has not been created in Relaxx.
- Maintenance: The locker is in maintenance mode and cannot be used currently. For example, this mode can be automatically activated after an alarm or reservation to check the locker before further use.
- Reserved: The locker is a personal locker and has been reserved for one person.

The numbers shown in a locker group column indicate how many lockers have the respective status.

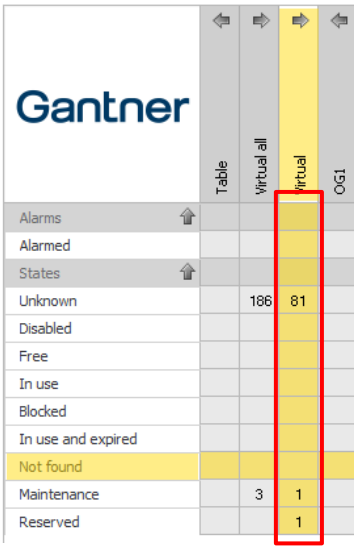


Figure 5.169 *– Total number of statuses in a locker group*

The area to the right of the locker matrix contains three tabs that are used to display further information about the locker currently selected in the matrix. The "Status" tab displays the information, the “Search Item” tab is used to search for a locker, and a description of the status messages is provided in the "Legend" tab.

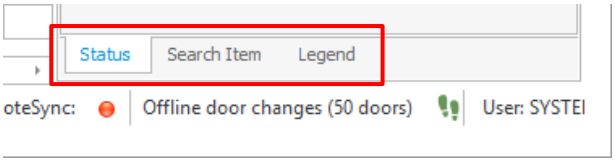


Figure 5.170 *– Information display*

5.19.2 Controlling the lockers

The lockers can be controlled directly in the matrix view by selecting the desired functions as follows.

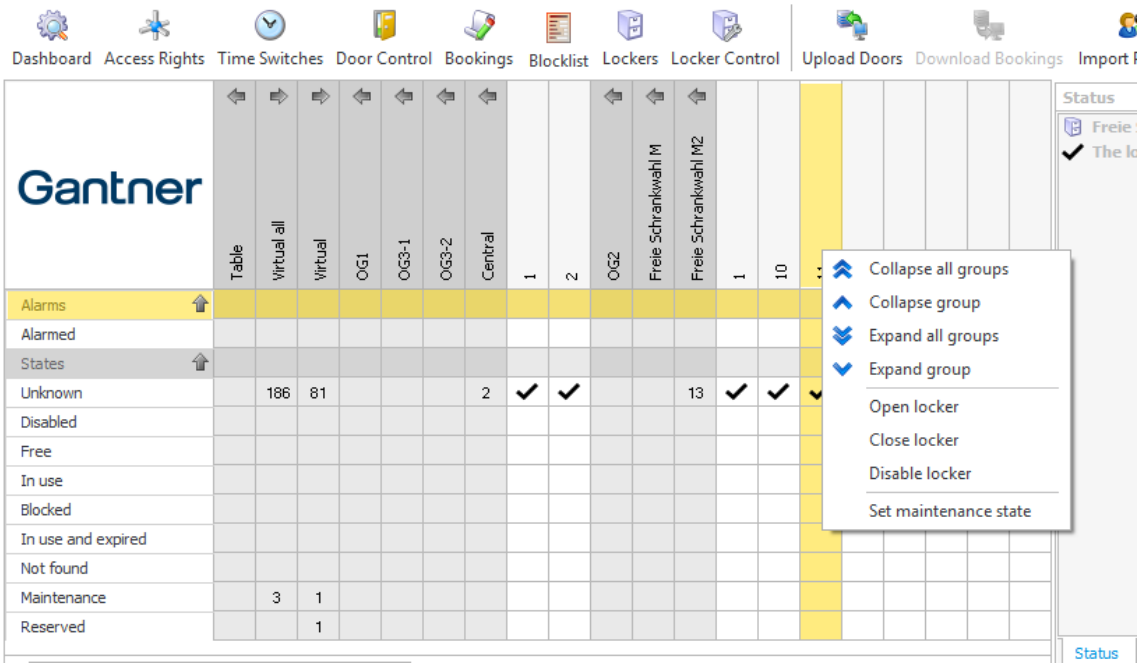


***Figure 5.171** – Locker control options*

- ► Right-click onto a locker; it does not matter where you click in the column.
  - o A pop-up menu with the available functions is displayed.
- ► Select "Open locker" to unlock the locker.
- ► Select "Close locker" to lock the locker.
- ► With "Disable locker", the locker can be deactivated, which means that operation is not possible. The menu option "Enable locker" is then displayed via which the locker can be put into operation again.
- ► With "Set maintenance state", the locker can be put into maintenance mode. It can then no longer be used by a user until it is reactivated via the "Cancel maintenance state" command.

  Note: Maintenance mode can also be activated automatically (e.g., after a reservation has expired).

5.20 Search function

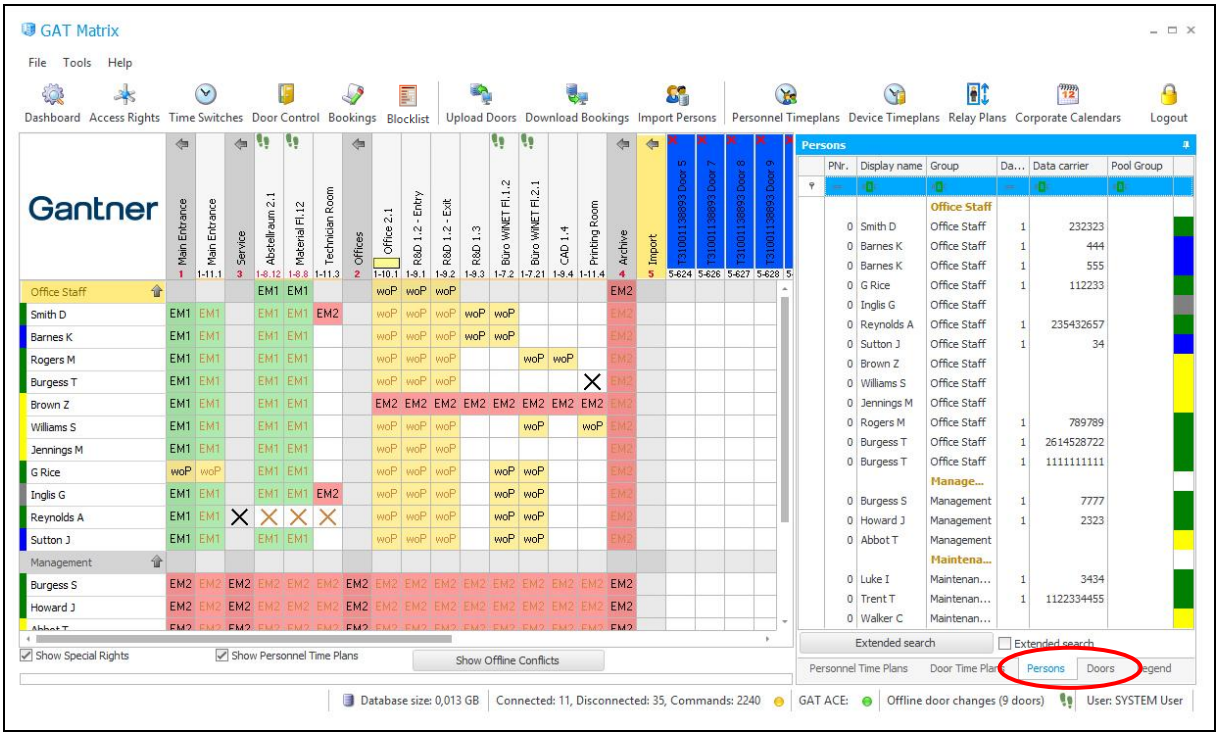


Figure 5.172 *- Search function for persons and doors (controller)*

To search for a person, door (controller), or a particular group, click on the "Persons" or "Doors" tab on the right side of the main window or press the keyboard button "F3" or "F4". A list of all defined persons or doors is shown, depending on the selected tab.

Persons and doors are displayed in black color in this list and person or door groups respectively are displayed in yellow-brown color and bold font.

You can search for persons by entering either the ID number, part of the display name (can be any part of the name), group name, data carrier type, data carrier number, or pool group at the top of the person list. To search for a door, enter the address of the relevant controller, a door description, or the door group at the top of the door list. It is sufficient to enter only part of the search term. The list is filtered and only the results that match the search term are displayed.

The displayed items can be sorted alphabetically up or downwards by pressing repeatedly on the top of the corresponding column header.

When a person or door is found, double click with the left mouse button onto the person or door in the list. The person or door will be highlighted in the authorization matrix. If only one exact match is found for the entered search term the result will automatically be highlighted in the authorization matrix.

Extended search

By clicking on the "Extended search" option, you can search for a person using information in the optional fields. The following window opens.

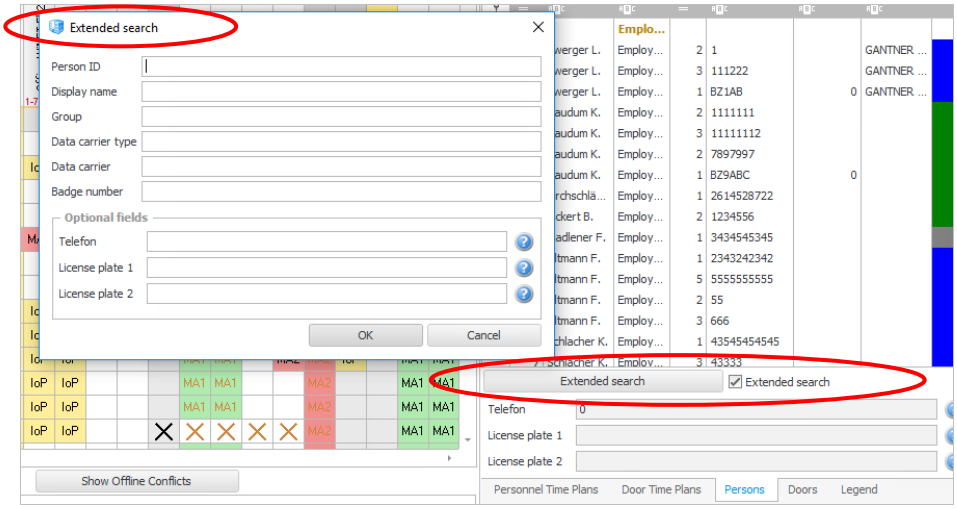


Figure 5.173 *- Advanced search function for persons*

Note: When using several license plate fields, make sure that you enter the license plate that you are looking for into the correct field. For example, if a license plate is entered in the optional field "License plate 2" for a person but you are searching for it in the "License plate 1" field, it will not be found. The spelling must also be correct ("BZ 999 ED" will not be found if you search for "BZ-999 ED").

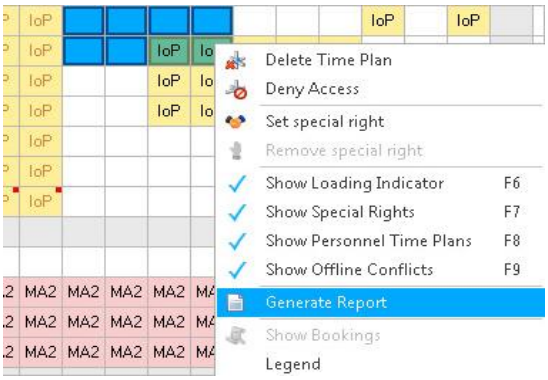
5.21 Creating access authorization reports

Matrix allows the creation of reports resp. the interpretation via the assigned access authorizations. These reports contain information about which persons have which access authorizations on which doors.

In order to create a report, follow these steps:

► Mark the appropriate cells in the access matrix for which a report should be created. You can either mark the desired area with the left mouse button or select the desired field with the STRG-key and the left mouse button.

► Within the marked area, right-click and select the "Generate Report" menu item.



- The "Reports" window opens as shown in Figure 5.174 - Generate reports window (Blocklist).

If you select the crossing point of the groups (Persons- and Door groups), the report will be completed for all persons and doors within the groups. You can create a report for all access authorizations by collapsing all groups, selecting all cells, and then selecting the "Generate Report" menu option.

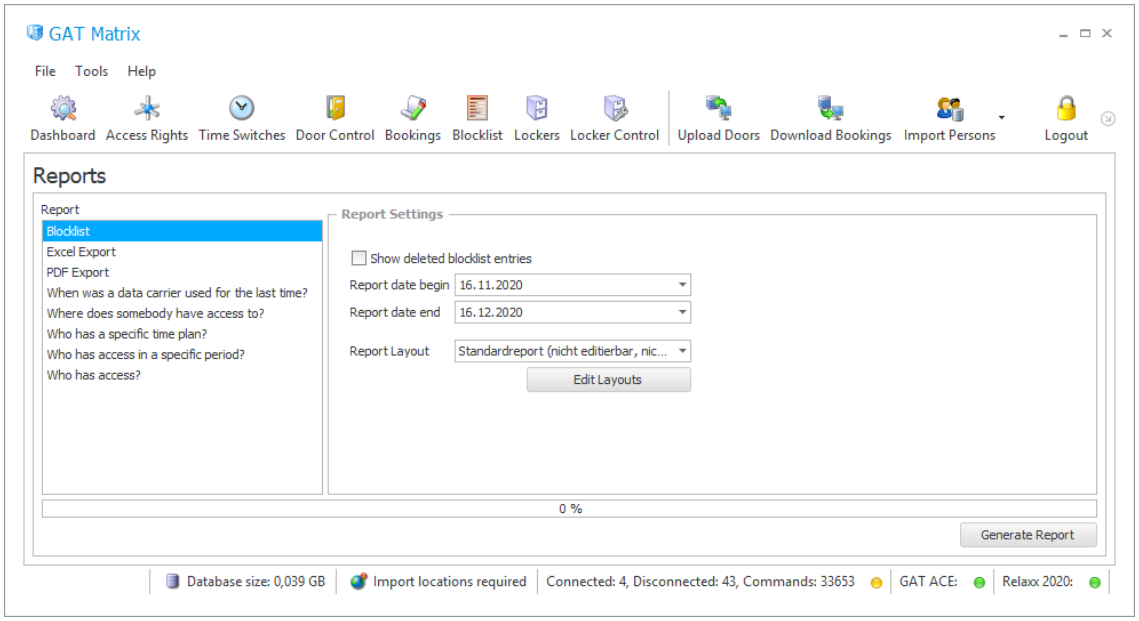


***Figure 5.174** - Generate reports window (Blocklist)*

► Select the type of report from the list to the left then define the applicable settings in the area to the right. Next, click on the button "Generate Report."

There are different types of reports available, which are described on the following pages.

5.21.1 Blocklist

This report type generates an overview of the blocklist entries (see "5.10 Data carrier blocklist"). Different data can be included in the report with the following settings available for this purpose.

- Show deleted blocklist entries: If this field is marked, the blocklist entries that have been deleted are also displayed with a corresponding note. If the field is not selected, the report only shows the entries currently in the blocklist.
- Report date begin / end: Here you can define the period during which the blocklist entries are considered.
- Report Layout: Select the type of layout for the report.

After entering the desired settings, click on "Generate Report". A window opens that displays the report and here you can print the report or save it to a file.

5.21.2 Excel export

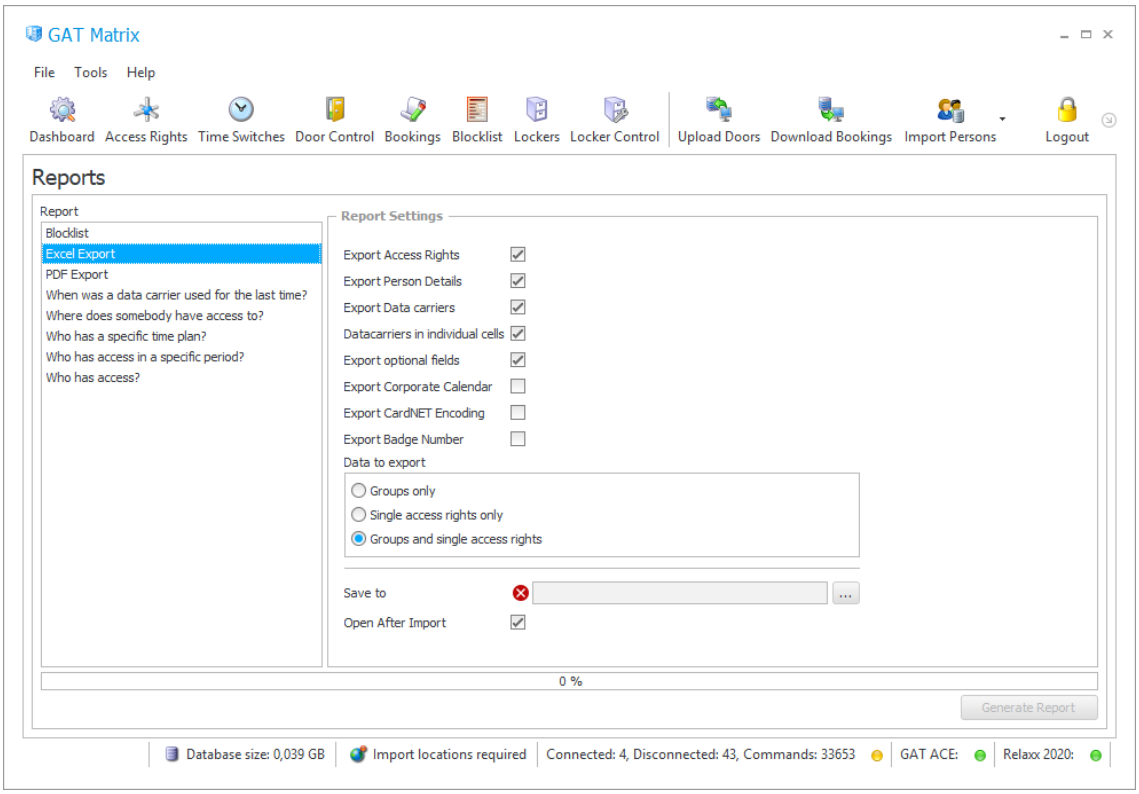


Figure 5.175 *- Generate reports window (Excel)*

This report type generates an overview of access authorizations (time plans) of the persons and the terminals in the matrix form. The result will be stored in a data file in Microsoft Excel-format (.csv) and can be opened up to Microsoft Excel 2003.
Different data can be defined for the report. The following settings are possible:

- Export access rights: If this field is marked, the access rights of the selected person are specified for the marked doors in the export. The specification is similar to Matrix with symbols and colors.
  If this option is not marked, only persons are listed in the report and not doors.
- Export person details: With this field, in addition to the display name, the Personal-IDs and Personal numbers of the persons and further details (title, first / last name, PIN-code) of the persons will be exported.
- Export data carriers: If this field is marked, the number of the data carrier (two data carriers are possible per person) will be exported for each person.
- Data carriers in individual cells: If this field is marked, a separate column is used for each person's data carrier. Otherwise several data carriers from one person are entered in the same column.
- Export optional fields: If this option is marked, the optional fields of persons will be exported (see "4.11. Optional fields for personnel data").
- Export Corporate Calendar: If this option is marked, the name of the corporate calendar assigned to each terminal will be exported in the Excel export.
- Export CardNET encoding: If this option is marked, the type of CardNET encoding is included in the Excel export.

- Export Badge Number: If this option is marked, the ID numbers of the data carriers are also exported in the Excel export.
- Data to export:
  - Groups Only: Only persons and door groups are exported and not the individual persons and doors.
  - Single access rights only: All marked persons and doors with assigned time plans will be exported, but without group classifications.
  - Groups and single access rights: With this setting, all marked persons and doors with time plans and inclusive the group classification will be exported. This view corresponds to the display in the Matrix.
- Save to: You can specify the storage location and the name of the export data file. By clicking on the field "…", you can select the folder via Windows-window.
- Open after import: If this field is marked, the exported file will open automatically after the report is generated.

► After marking all settings, click on the button "Generate Report".

  ○ All marked information will be exported and written in the .csv data file.

5.21.3 PDF export of persons

In this report type, all previously marked persons with their personal data (title, first / last name, personnel number, and card numbers) will be exported in a PDF-data file. To each person, all assigned time plans (for the marked doors) will be listed. If you select the type PDF Export, the following window is displayed.

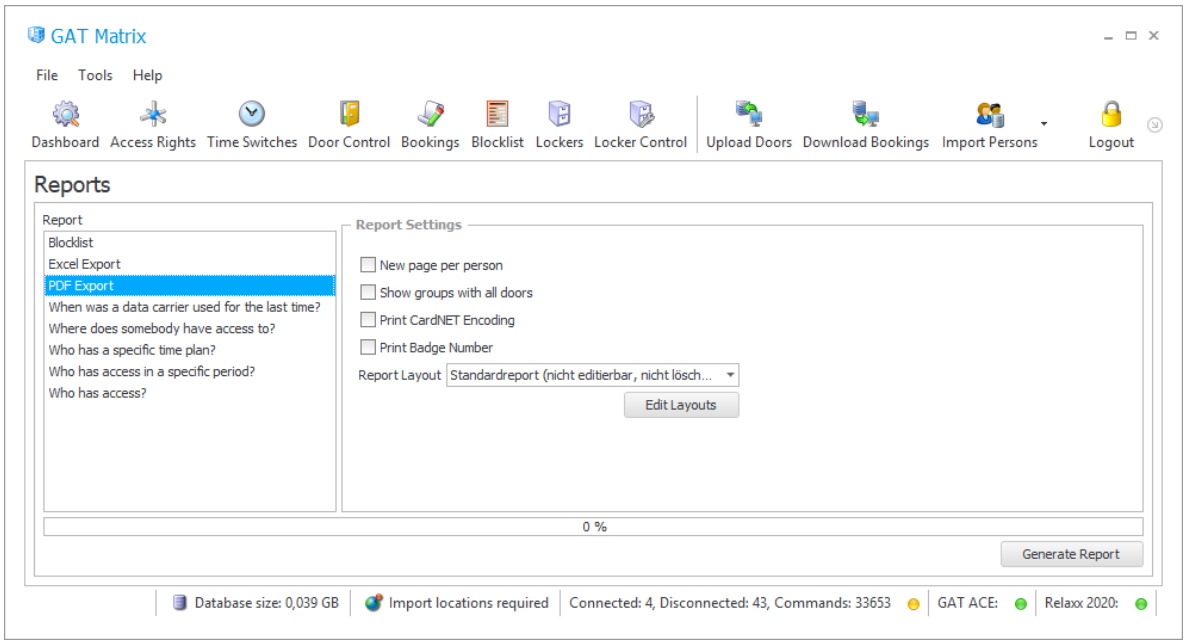


***Figure 5.176** - Generate reports window (PDF)*

The following settings are available:

- New page per person: If this option is marked, a new PDF page is generated for each person.
- Show groups with all doors: If this option is marked, the doors in each group are displayed in the report next to the groups. Without this option marked, only the groups but no doors are shown.
- Print CardNET encoding: If this field is marked, the type of CardNET encoding (if used) is included in the export.
- Print badge number: If this field is marked, the badge number (if used) is included in the export.
- Report layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If your license includes the Report Designer (see "10. LICENSE MANAGEMENT"), you can create a new layout via the "Edit Layouts" button.

► Finally, click on "Generate Report".

  - The report opens in a new preview window.

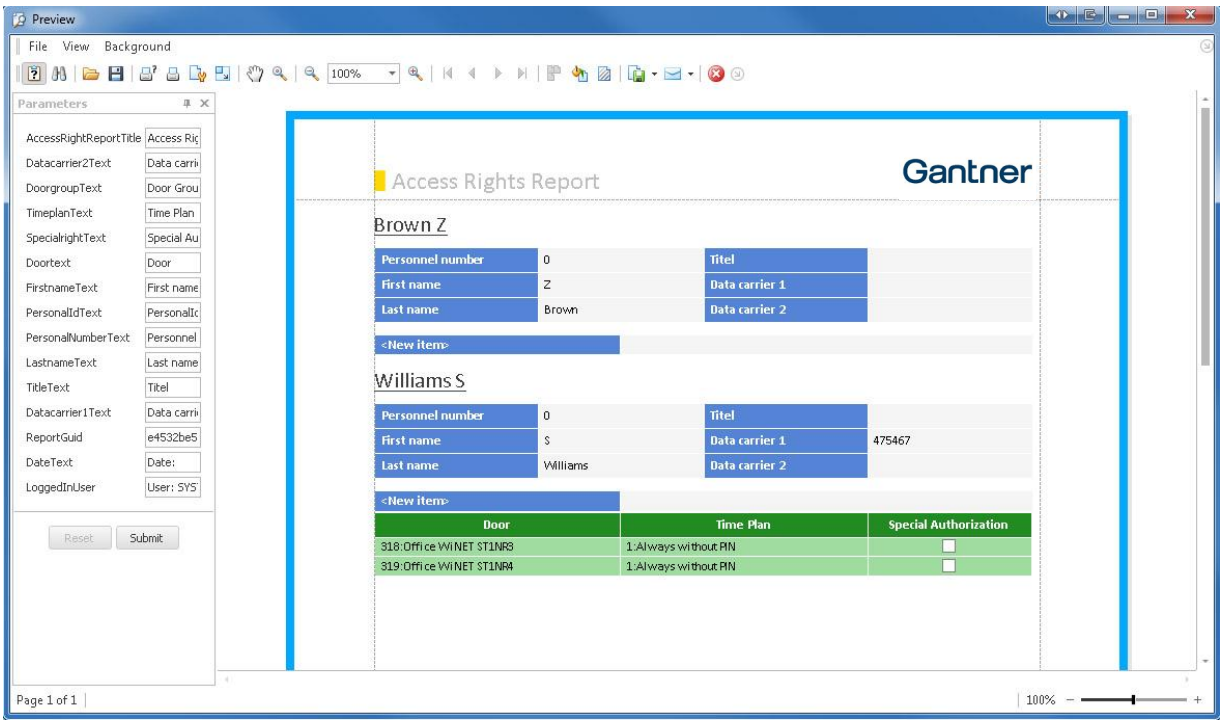


Figure 5.177 *- Preview of a PDF report*

Using the icons in the title bar, some layout settings can be adjusted, e.g., page margins inserted or the background color and also the watermarks changed.

Shown in the standard report for each person are their personal information and respective time plans. The display is structured as follows:

- Orange (Door Groups): Only time plans that are assigned for the person to a door group (directly at the person or inherited from the person group) are shown. In the first column is the door group with appropriate offline-group number and in the second column is the number and the designation of the time plan. If the person has a special authorization for a door group, this is shown in the last column.
  If the person is assigned to a single door, i.e., within the door group, another time plan as the door group is assigned. This time plan overwrites the group time plan for the single door and is marked with a gray line. In the shown example, the person is assigned to another time plan within the door group "2: Production" at the door "35: Production Main Door" as the group.
- Green (Single doors): The doors will be listed where the person is directly assigned to a time plan, also not via a group of doors. In the first column, the door will be shown with the terminal address and door designation. In the second column is the number and the designation of the time plan and in the last column is marked whether the person has assigned a special authorization at the door.

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

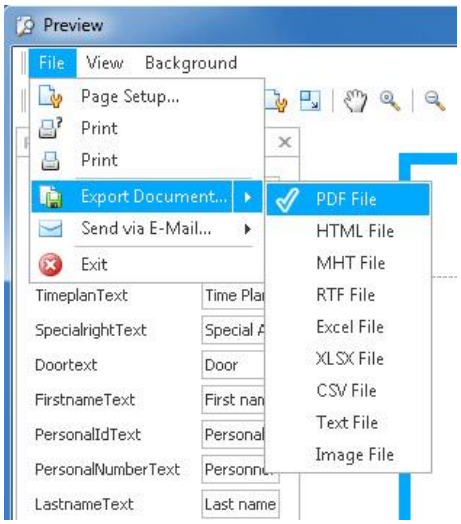


***Figure 5.178** - Export report*

5.21.4 When was a data carrier used for the last time?

With this report it is possible to find out when the data carriers were used the last time. If a group was selected in the authorization matrix all entries (persons and groups) in this group will be shown.

This report does not consider access movements for SALTO doors.

The following window opens after this type of report is selected.

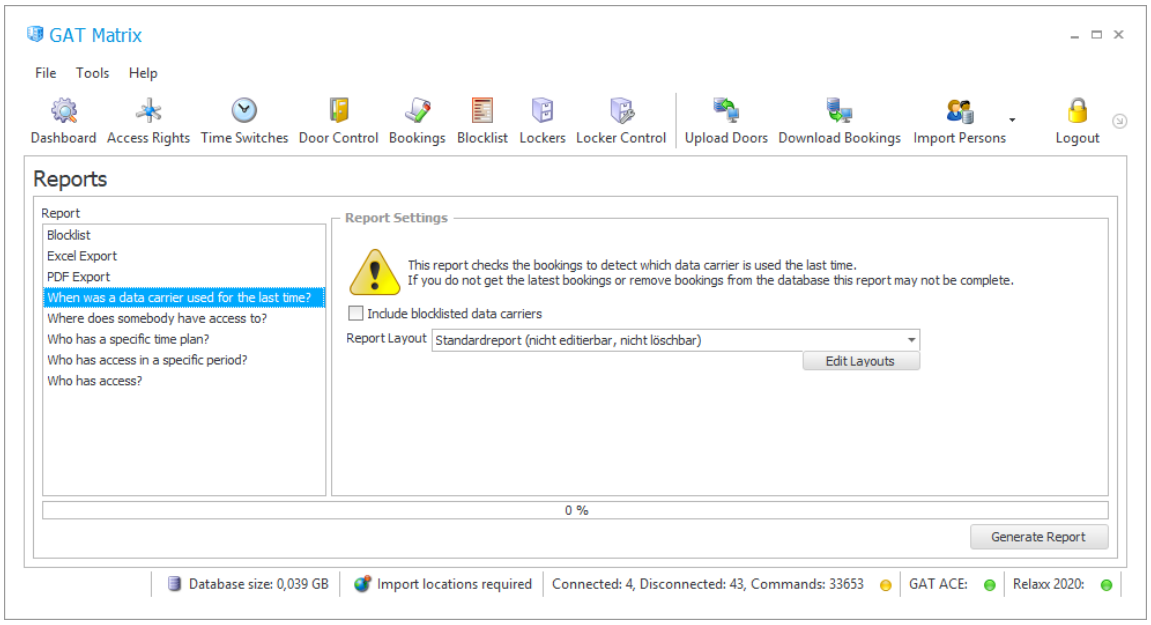


***Figure 5.179** - Generate reports window (When was a data carrier used for the last time?)*

NOTE! Only current bookings are searched for this report. The report may be incomplete if all bookings are not loaded from the controllers.

Here you have the following possibilities:

- Include blocklisted data carriers: If this option is marked, the data carriers that are in the blocklist (see "5.10 Data carrier blocklist") are also displayed. Otherwise, these data carriers will not be listed in the report.
- Report Layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If you have licensed the Report Designer (see "10 LICENSE MANAGEMENT"), you can create a new layout via the “Edit Layouts” button.

► Click on "Generate Report".

- The report opens in a new preview window.

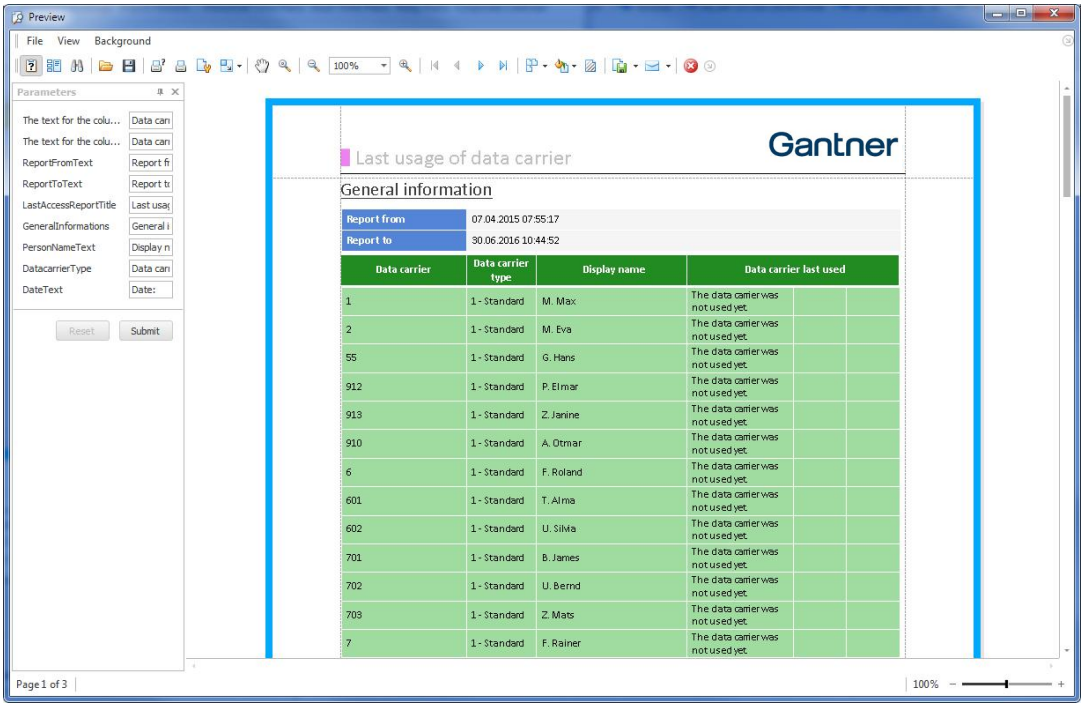


Figure 5.180 *- Preview of report "When was a data carrier used for the last time?"*

All data carriers assigned to the selected persons and the data carrier type are listed here. Displayed in the right column is information on whether the data carrier has been used and, if so, the last time of use.

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

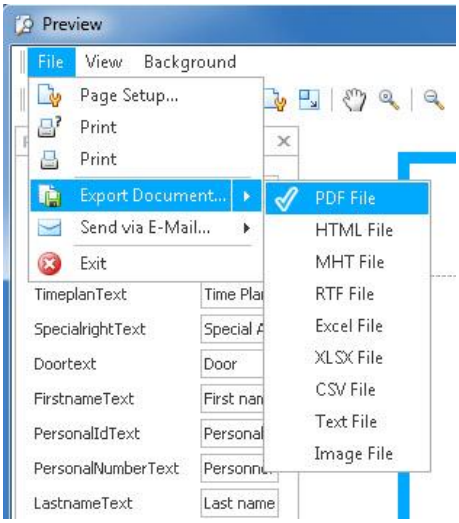


Figure 5.181 *- Export report*

5.21.5 Who has a specific time plan?

This report type allows you to evaluate the time plans assigned to the marked persons a certain time plan is assigned. If a group was selected in the authorization matrix all entries (persons and groups) in this group will be shown.

The following window opens after this type of report is selected.

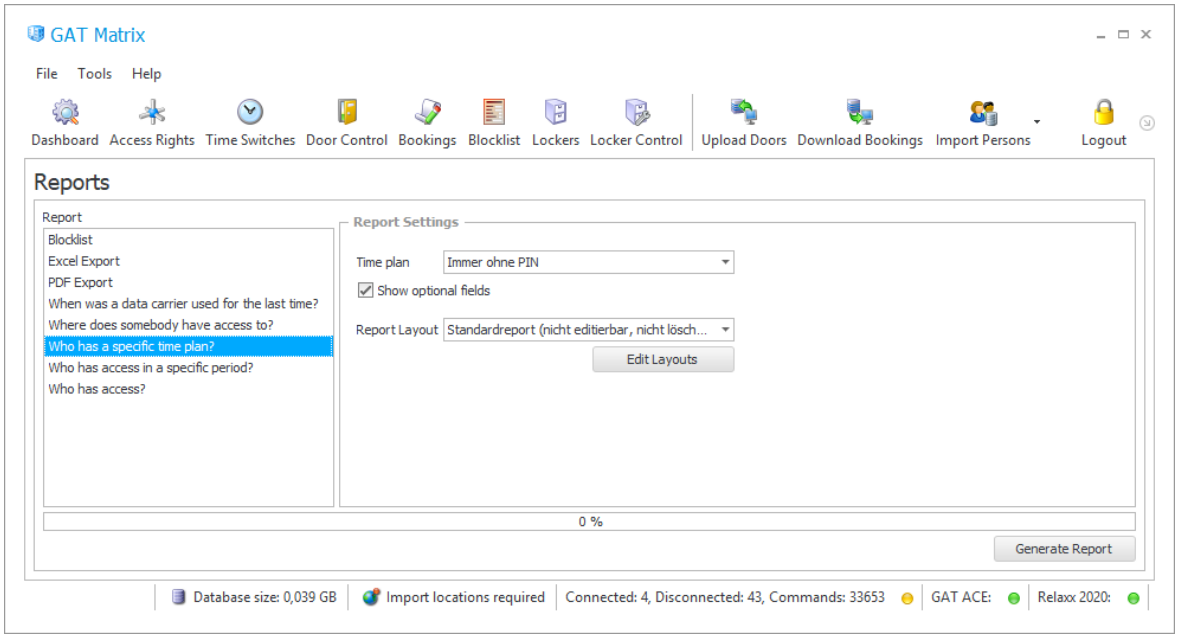


Figure 5.182 *- Generate reports window (Who has a specific time plan?)*

Here the following settings can be made:

- Time plan: Here you can select the time plan you want to search for.
- Show optional fields: If this option is marked the optional fields, which can be defined for persons, will also be exported (see "4.10 Settings for person display").
- Report Layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If you have licensed the Report Designer (see "10 LICENSE MANAGEMENT"), you can create a new layout via the button "Edit Layouts".

► Click on "Generate Report".

  - The report opens in a new preview window.

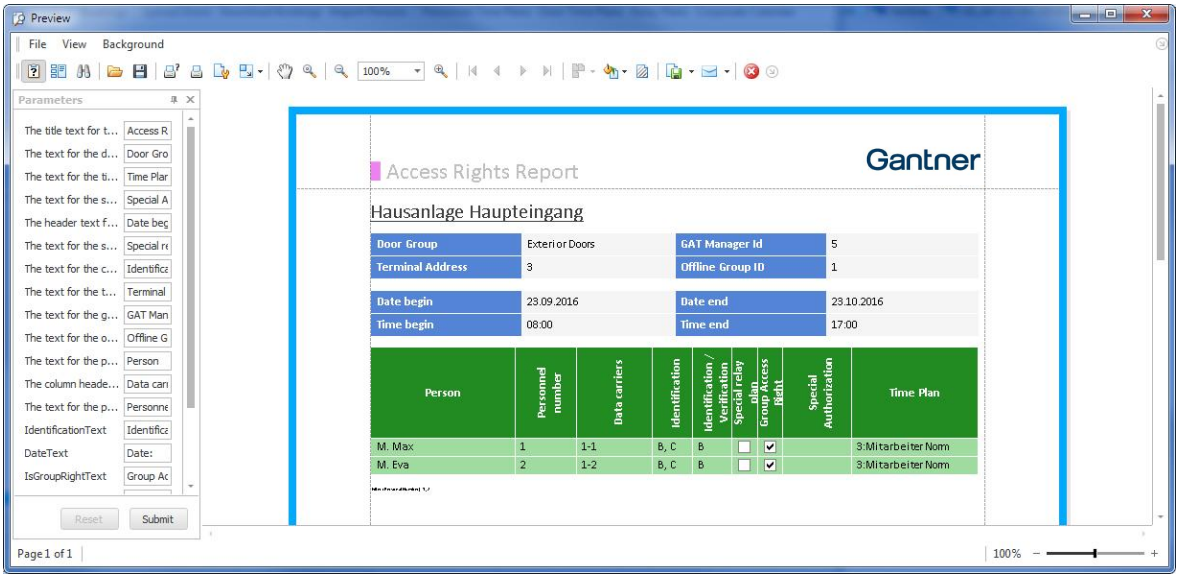


Figure 5.183 *- Preview of report "Who has a specific time plan?"*

Each door is shown in a separate block with general door information displayed first (blue boxes). This includes the door group to which the door belongs, the address of the door's controller, etc. The start and end dates of the entered period are also displayed.

Listed below in green are all persons who had access authorization for the corresponding door during the selected period. For each person, the personnel and data carrier number are shown and additionally, the optional fields if these have been defined (see "4.11 Optional fields for personnel data").

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

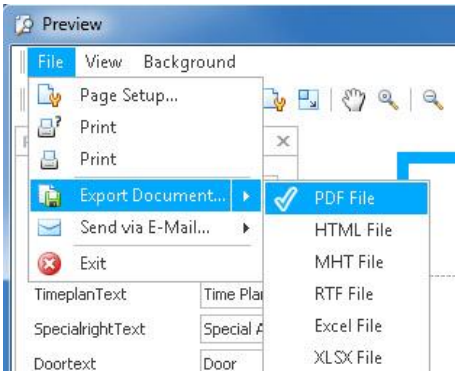


Figure 5.184 *- Export report*

5.21.6 Who has access in a specific period?

This report type allows you to evaluate which persons had access during a specific period (i.e., persons who have a time plan assigned). For each authorized person, the assigned time plan(s) and authorization information are shown. It also applies: if a group was selected in an access matrix, all entries (persons and doors) of this group will be used.

The following window opens after this type of report is selected.

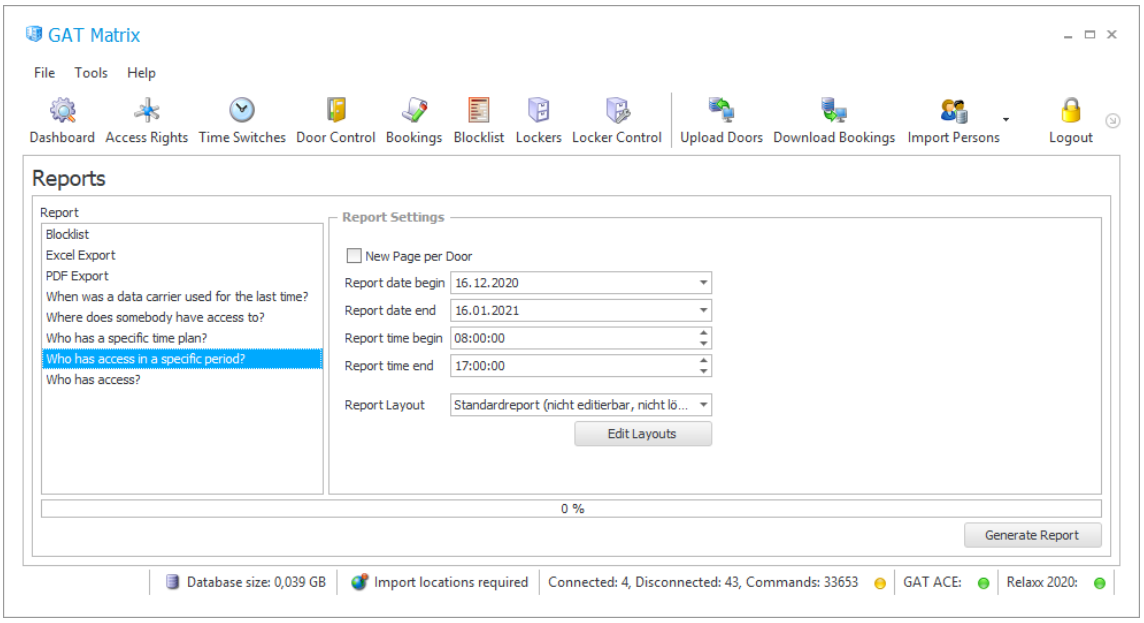


***Figure 5.185** - Generate report window (Who has access in a specific period?)*

The following settings are possible:

- New Page per door: If this option is marked, a new PDF-data file is created for each door.
- Report date/time: Enter the start and end date and time for the time period in which you want to display the access resp. time plans.
- Report Layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If you have licensed the Report Designer (see "10 LICENSE MANAGEMENT"), you can create a new layout via the button "Edit Layouts".

► Now click on "Generate Report".

  - The report opens in a new preview window.

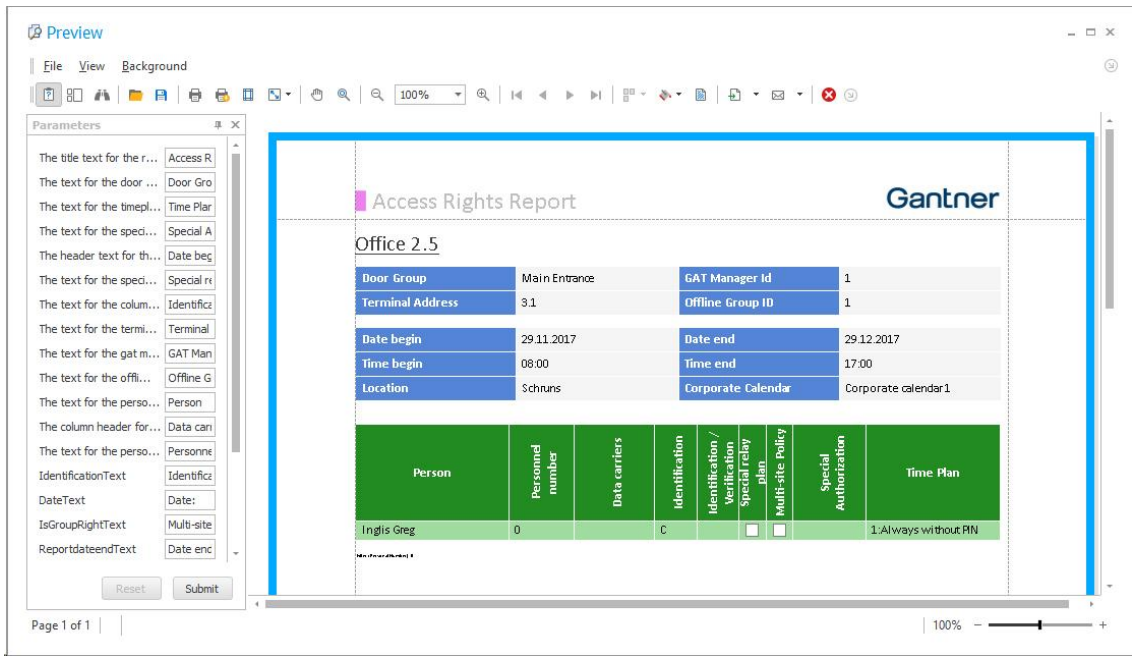


***Figure 5.186** - Preview report – "Who has access in a specific period"*

Each door will be shown in a separate block with certain information. First, general information about the door will be shown (blue fields). This contains the door group, to which the door belongs, the address of the controllers at the door, etc. The start and end times of the set time period are also shown here.

Below, the list of persons follows in green. These persons have access authorization within the selected time period at the door. The access authorization must not be valid during the whole time period, which means that all persons will be shown which have assigned access authorization at least once during the time period. For each person, beside the personal number and data carrier number, detailed information about the access authorization will be shown. The field "Identification "means, that the person must identify yourself with the personal data carrier at the terminal. The field "Identification/Verification" means, that in addition to identification, verification is needed via fingerprint. The type of identification / verification is indicated here by the following abbreviations (B = biometric, C = data carrier, PN = personnel number, P = PIN code). The special authorization (s) is (are) displayed in text form.

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

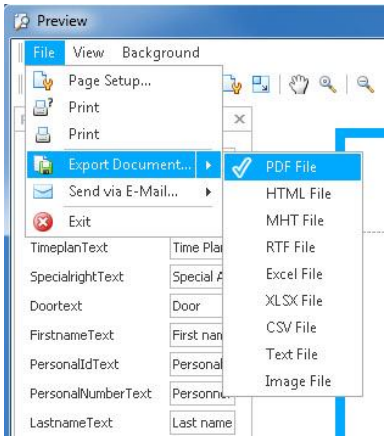


***Figure 5.187** - Report export*

5.21.7 Who has access?

This report type allows you to evaluate which persons had access to selected doors at a specific time. For each authorized person, the assigned time plan(s) and authorization information are shown. It also applies: if a group was selected in an access matrix, all entries (persons and doors) of this group will be used.

The following window opens after this type of report is selected.

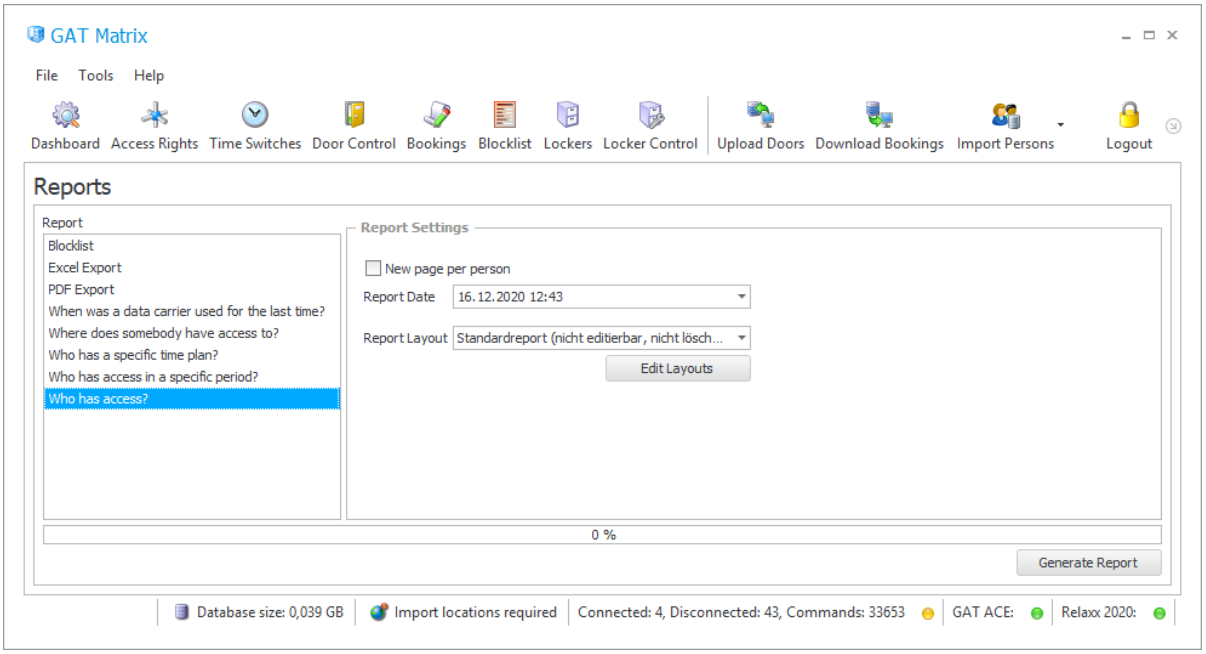


***Figure 5.188** - Generate reports window (Who has access?)*

The following settings are possible:

- New page per person: If this option is marked, for each person a new PDF-data file will begin.
- Report date: Enter the date on which you want to display the access resp. time plans.
- Report layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If you have licensed the Report Designer (see "10. LICENSE MANAGEMENT"), you can create a new layout via the button "Edit Layouts".

► Click on "Generate Report".

  - The report opens in a new preview window.

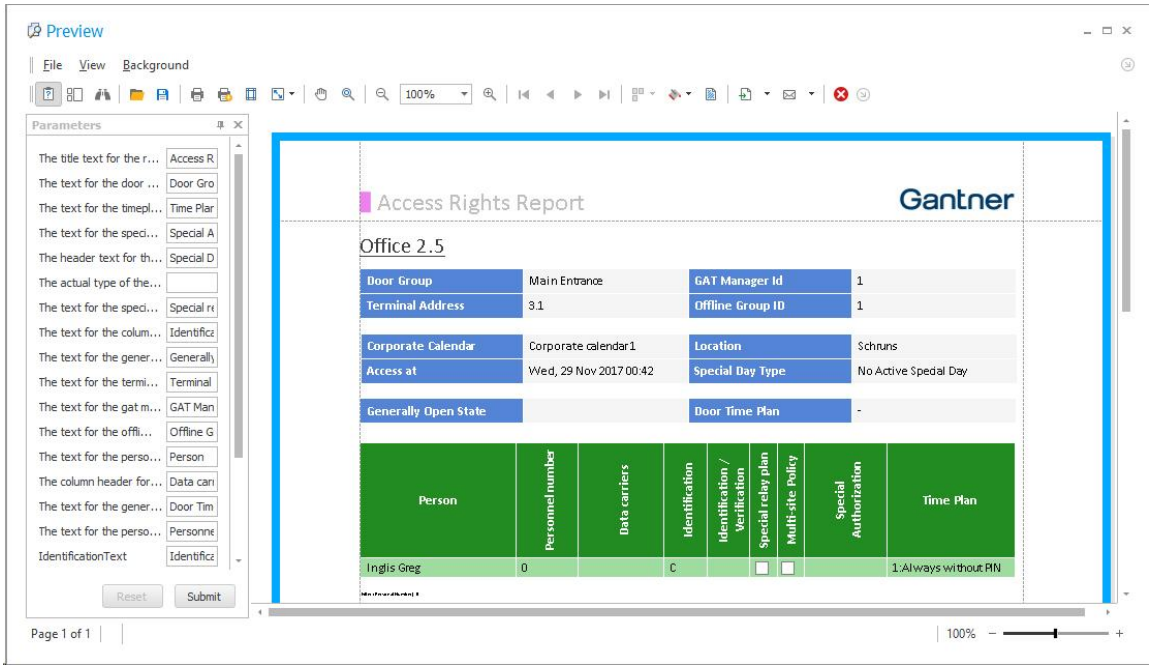


Figure 5.189 *- Preview of report "Who has access?"*

Each door is shown in a separate block with certain information. General information about the person is displayed first (blue fields). This contains the door group, to which the door belongs, the address of terminals at the door, etc. In addition, an assigned door group and the status of the General Open Function will be shown. If the selected time is a special day (see "6 CORPORATE CALENDAR AND LOCATIONS"), then the type of special day is also shown.

Below, the list of persons follows in green. These persons have an access authorization to the selected time at the door. For each person, beside the personal number and card number, detailed information about the access authorization will be shown. The field "Identification "means, that the person must identify yourself with the personal data carrier at the terminal. The field "Identification/Verification" means, that in addition to identification, verification is needed via fingerprint. The type of identification / verification is indicated here by the following abbreviations (B = biometric, C = data carrier, PN = personnel number, P = PIN code). The special authorization (s) is (are) displayed in text form.

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

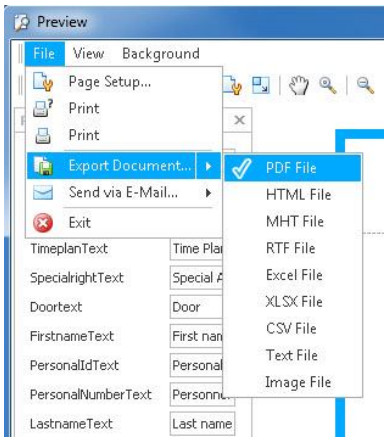


Figure 5.190 *- Report export*

5.21.8 Where does somebody have access to?

The report type allows you to evaluate which door a person had access to at a specific time. It also applies: if one group was selected in an access matrix, all entries of this group (persons or doors) will be used.

The following window opens after this type of report is selected.

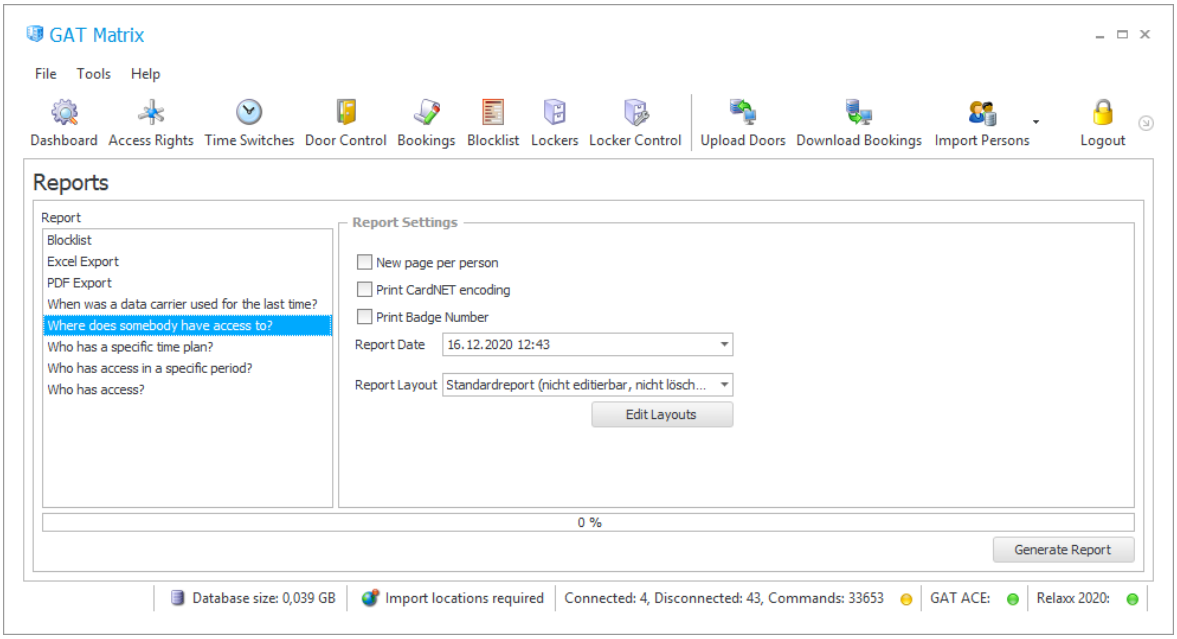


***Figure 5.191** - Generate report window (Where does somebody have access to?)*

The following settings are available:

- New page per person: If this option is marked, a new PDF page is generated for each person.
- Print CardNET encoding: If this option is marked, the CardNET encoding used for the exported data carriers is included in the export.
- Print Badge Number: If this option is marked, the badge numbers of the data carriers is also exported.
- Report Date: Enter the date on which you want to display the access resp. time plans.
- Report Layout: Selection of the layout for the report. Matrix includes a standard layout for this report. If you have licensed the Report Designer (see "10. LICENSE MANAGEMENT"), you can create a new layout via the button "Edit Layouts".

► Click on "Generate Report".

  - The report opens in a new preview window.

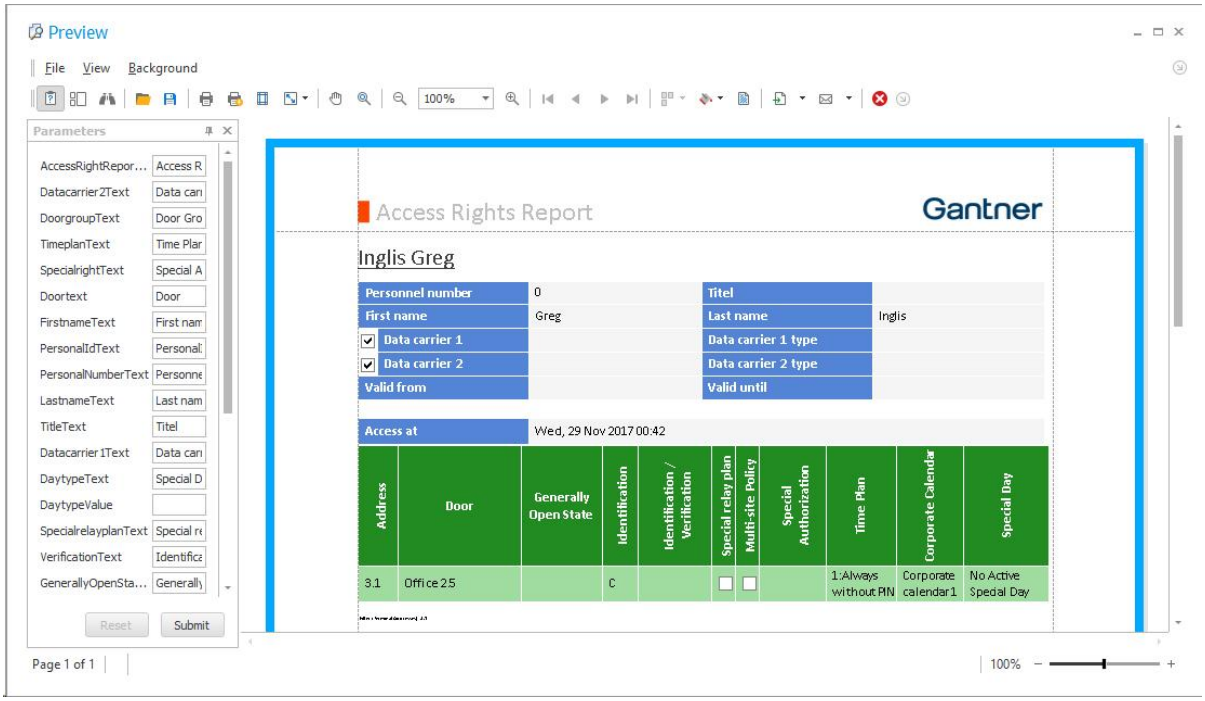


Figure 5.192 *– Preview of report "Where does somebody have access to?"*

Each door is presented in a separate block with specific information. First, general information about the person is displayed (blue boxes). If the selected time for the access information is a special day (see "6. CORPORATE CALENDAR AND LOCATIONS"), the type of special day is also displayed here.

Listed underneath in green are the doors to which the person is assigned an access authorization at the selected time. For each door, in addition to Generally Open State, detailed information about the access authorization is displayed. The "Identification" field indicates whether the person must identify themselves at the controller with their personal data carrier in order to gain access. The "Identification / Verification" field indicates whether the person must provide verification via a fingerprint / PIN code in addition to the identification. The type of identification / verification is abbreviated by letters (B = biometrics, C = data carrier, PN = personnel number, P = PIN code). The special authorization(s) are described in text form.

In the "File" menu, you can export the report in several formats (e.g., as a PDF, HTML, or CSV) via the "Export Document" menu item.

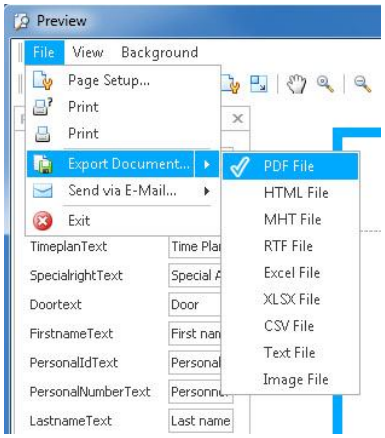


Figure 5.193 *- Report export*

5.22 GAT ACE status

The status bar provides basic information about the communication with GAT ACE and the controllers. The information is constantly updated.



The following icons are used:

... GAT ACE is running, and communication is operating. The number next to “Commands” indicates the number of commands still to be processed by GAT ACE 3000.

… GAT ACE has started and communication between GAT ACE and Matrix is established. However, communication between GAT ACE and one or several controllers is interrupted. The numbers next to "Connected" and "Disconnected" indicated how many controllers are connected and disconnected.

… GAT ACE is not running or communication with GAT ACE has been interrupted. Verify that GAT ACE is running.

… The status of GAT ACE cannot be determined. This status should only appear immediately after startup of the application.



To see a detailed status about GAT ACE, click on the “GAT ACE” text in the status bar. This opens the Dashboard that shows in the top right under “Connections” information regarding all the configured GAT ACE installations.

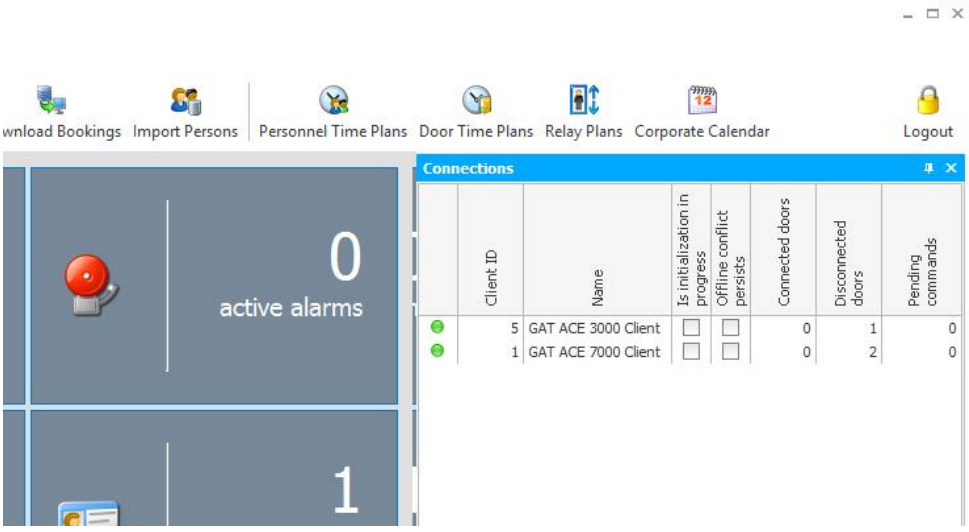


Figure 5.194 *– Detailed status information about the connected GAT ACE installations*

A separate line with different information (e.g., number of doors, unsent commands, etc.) is displayed for each GAT ACE installation.

5.23 Configuring the SALTO JustIN app for access control

The JustIN app can be installed on mobile devices such as smartphones to perform identification at access doors controlled by SALTO locks. The device in this case assumes the role of a data carrier. The authorizations can be set to "live" and also withdrawn again, e.g., if the smartphone is lost. The identification at the door lock is completed via NFC or Bluetooth.

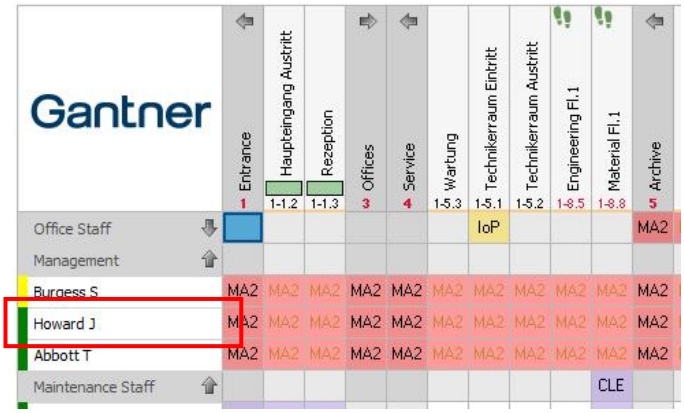
The authorization data is transferred to the JustIN app via the SALTO ProAccess SPACE software. A person who is defined in Matrix can also be linked to the JustIN App and thus access authorizations using plans in Matrix can be defined for the SALTO locks.

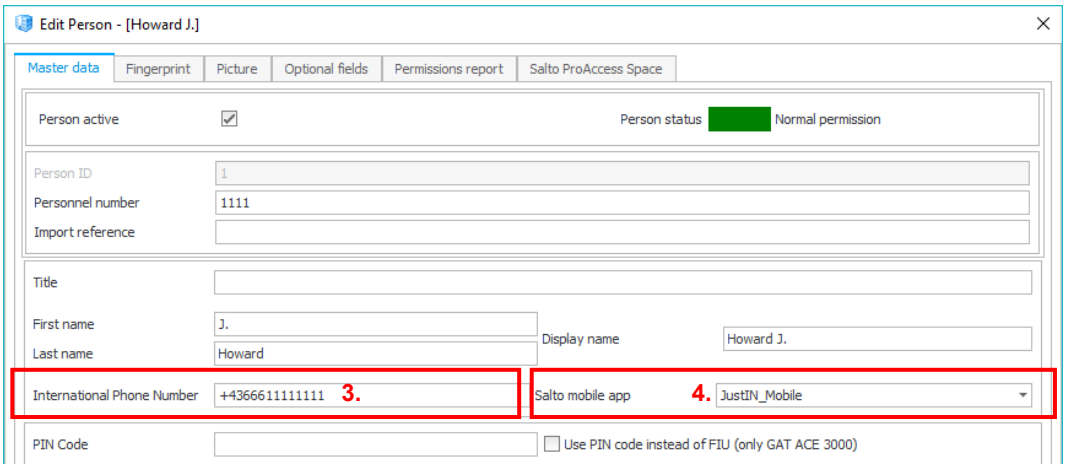
To use the JustIN app with Matrix, complete the following steps:

1. Install the JustIN app onto the smartphone. The app is available for Android and iOS systems.

Android Link to Google Play: **iOS** Link to App Store:

2. Open the personnel window in Matrix by double-clicking on the person in Matrix.

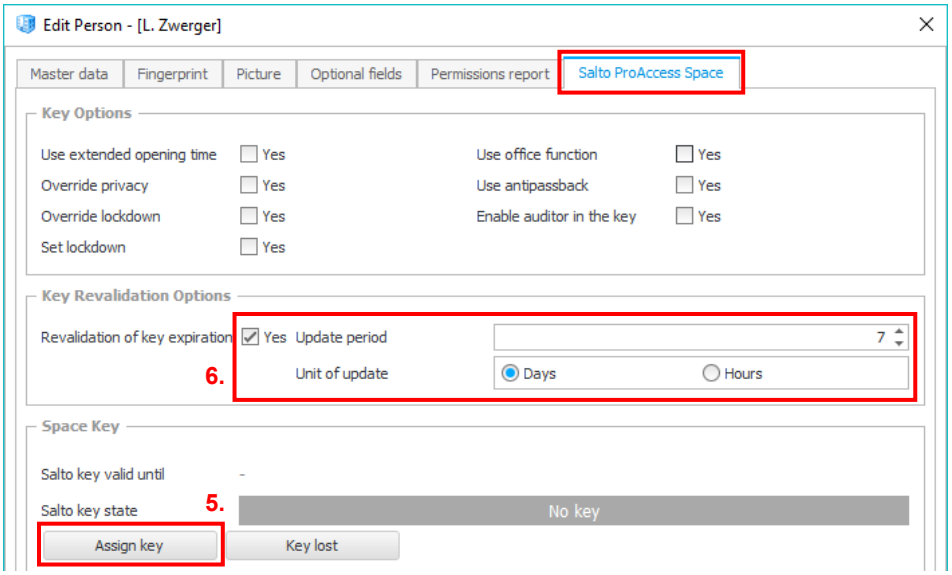




3. Enter the phone number of the smartphone into the "International Phone Number" field.

4. Select the "JustIN_Mobile" option from the "Salto mobile app" menu.

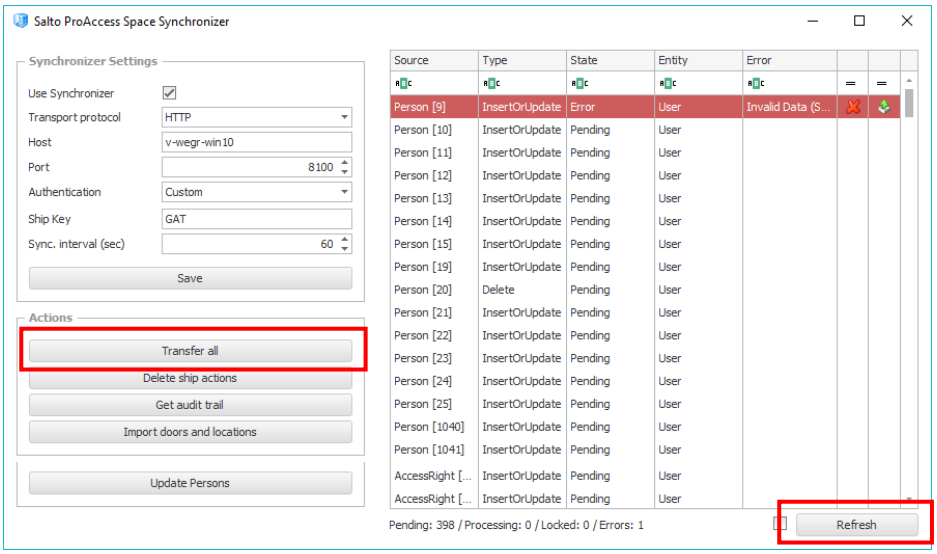
5. Assign the personal data carrier to the person. To do so, place the data carrier onto the Salto reader that is connected to the PC. Now open the "Salto ProAccess Space" tab and click on the "Assign key" button. The state of the key field changes from "No key" to "Assignment pending".
NOTE: This step can also be completed via "ASSIGN KEY" in the Salto ProAccess SPACE software.



6. Also on the "Salto ProAccess Space" tab, select the "Yes" option in the "Key Revalidation" area. In the “Update period” field, enter the value "7" (days).
NOTE: The ProAccess SPACE supports a max. validity of 7 days and therefore no more than 7 days can be selected for the JustIN app. Please note: If a larger value is entered here, it will be automatically changed to 7 days by Matrix.

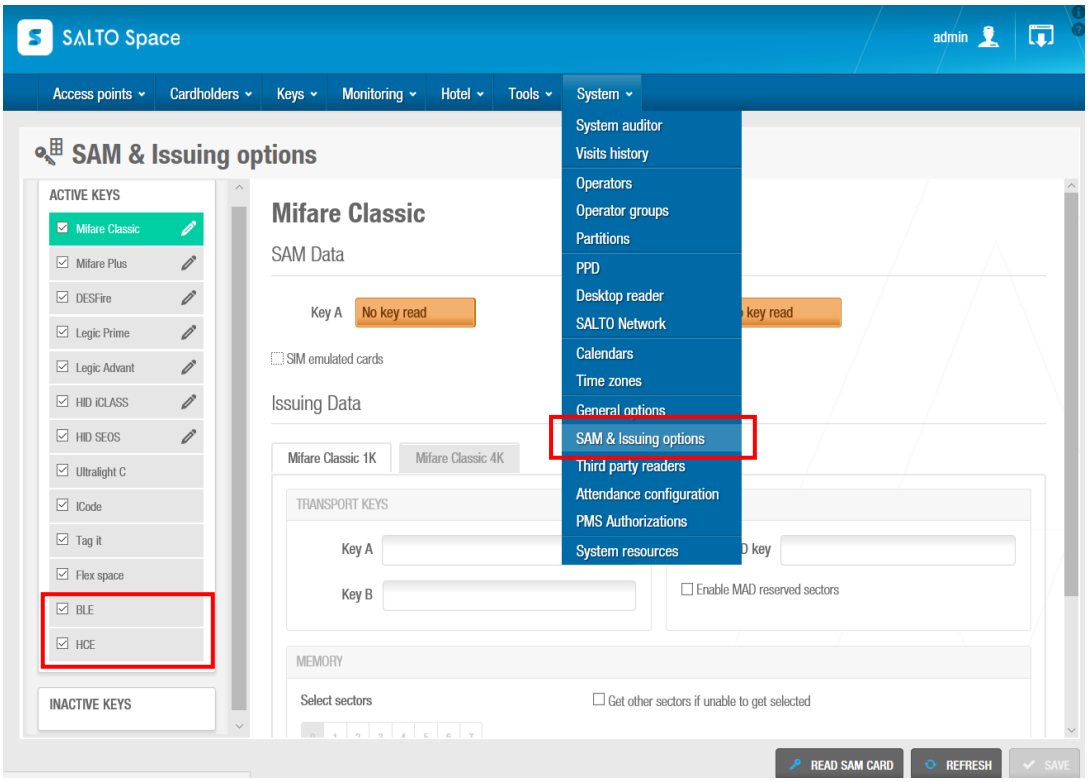
7. Save the personnel data with "OK".

8. Open the window for communication with Salto ProAccess SPACE by selecting the "ProAccess Space Synchronization" option from the "Tools" menu.

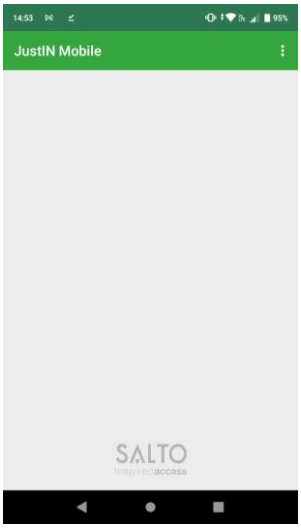


9. The changes to the personnel data are automatically transferred. If this does not work you can upload all data from Matrix into the transfer list by clicking on "Transfer all" and start the transfer by clicking on "Refresh".

10. In the ProAccess SPACE software, the keys "BLE" and "HCE" must be enabled. To do this, click on the "System" menu and select "SAM & Issuing options". Now select the two settings in the left list so that they are displayed in the "ACTIVE KEYS" area instead of the "INACTIVE KEYS" area.

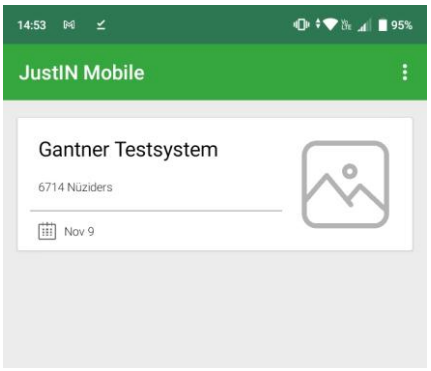


11. After all data is transferred, start the JustIN app on the smartphone.



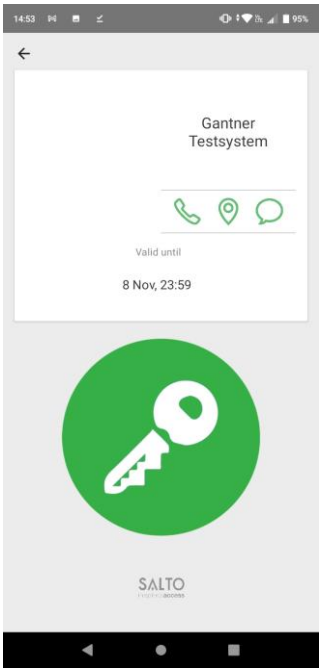
12. For the initial start of JustIN you are asked to enter the PIN code for assignment to the person in Matrix. This code is sent via SMS to the phone number that was entered in the personnel data in Matrix. Enter the 6-digit code in JustIN now.

13. If a data carrier is assigned to the person (see step 5), this data carrier is automatically inserted in JustIN.



The smartphone now acts as the data carrier that was previously assigned to the person in Matrix.

14. To open a door, click on the respective entry in the JustIN app. The screen for door control is shown.



With the symbols  you can display information about the authorization.
Shown at the top below "valid until" is the date until which the authorization is valid.

15. You can unlock the door by pressing the green key symbol . The terminal/lock, which controls the door, must be in range of the smartphone and the data carrier included in the authorization must have permission to unlock the door.

6. CORPORATE CALENDAR AND LOCATIONS

The corporate calendar is used to define the special days, e.g., public holidays or company holidays, of the current year and the years ahead. On these special days, a special day plan for the holiday rather than the default day plan is used to define the applicable authorization for the persons and terminals.

In GAT ACE 7000, GAT ACE 3000, and SALTO ProAccess SPACE, doors can be assigned to locations (see "6.2 Locations") and these locations can be organized hierarchically. In ProAccess SPACE, the locations are referred to as "partitions".
A corporate calendar can be defined for each location. For locations that are subordinate in the hierarchy, the assigned corporate calendar is automatically inherited by the subordinate locations. Inherited calendars can be overridden by directly assigning another calendar.
This function allows you to, for example, manage country-specific holidays or to implement usage-based functions, e.g., for municipal offices and schools.

The corporate calendar and the locations list can be opened via the "Corporate Calendar" toolbar button.

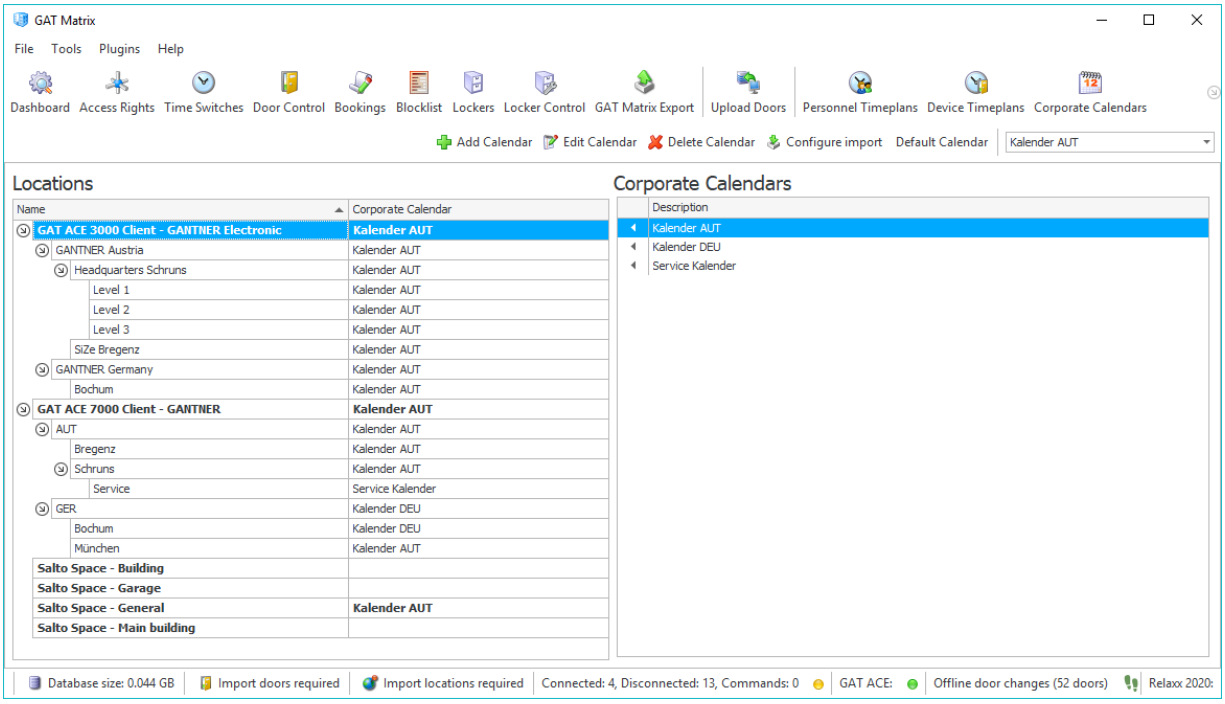


Figure 6.1 *- Corporate calendar list*

All locations (see "6.2 Locations") are displayed on the left and the defined corporate calendars displayed on the right. In the “Default Calendar” field, you can select the calendar that will automatically be used for locations when no calendar is assigned.

► To assign a corporate calendar to a location, select the location and then click on the arrow icon next to the calendar in the corporate calendars list.

NOTE! This function can be activated for each user individually in the user rights configuration. Only users, for whom this function is active, can assign calendars to locations.

6.1 Defining a corporate calendar

► To add a new calendar, click on the "Add Calendar" button.

► To edit an existing calendar, select the calendar and click on the "Edit Calendar" button.

- The “Edit Corporate Calendar” window opens.

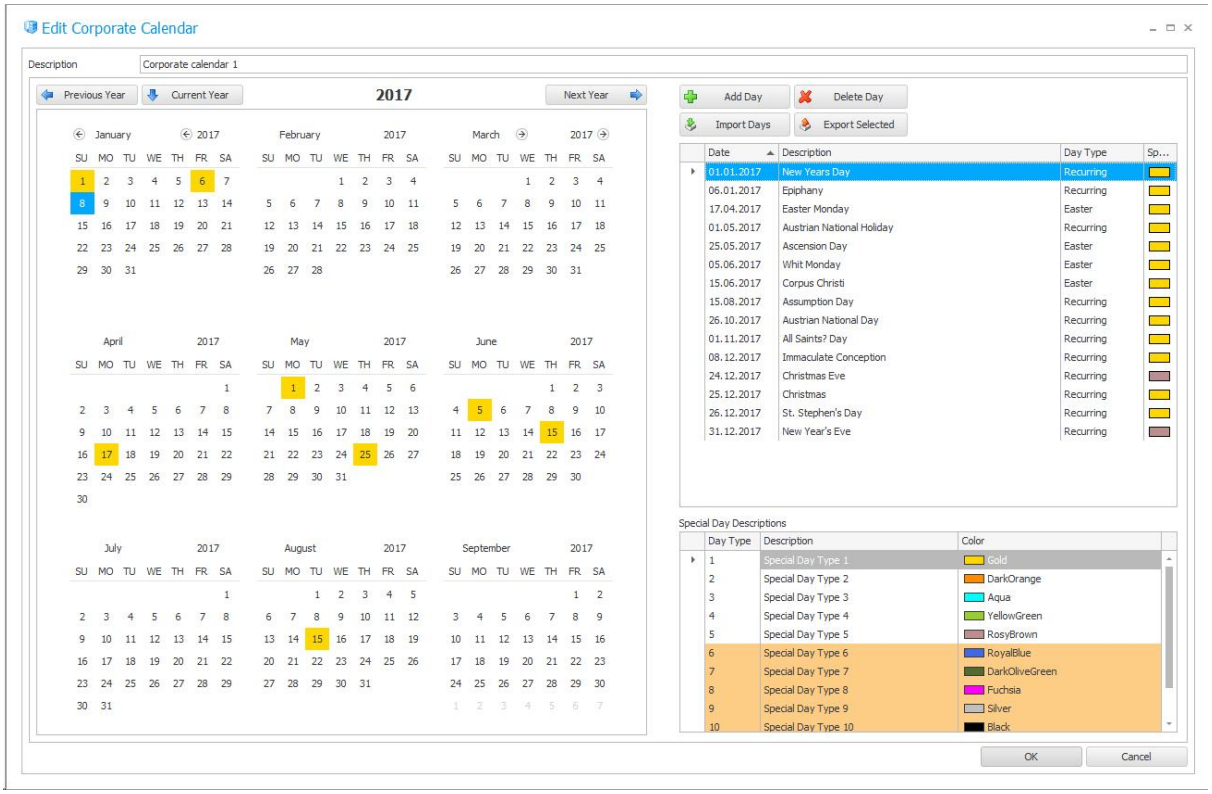


***Figure 6.2** – Defining a corporate calendar*

The name of the selected calendar is shown in the "Description" field at the top. If a new calendar is being created, you must define a name for the calendar here.

On the left side, the days of the current year are shown in calendar format. Use the buttons above to change the displayed year. The current day is marked with a gray rectangle. The colored fields show the special days that are already assigned.

Each special day must be assigned to a type of a special day. The special day types are displayed at the bottom right in the "Special Day Descriptions" field. The special day types marked in white can be used by all software packages (ACE and SPACE). For the special day types marked in orange, the following must be considered:
- GAT ACE 3000: 5 special day types (1 – 5)
- GAT ACE 7000: 10 special day types (1 – 10)
- ProAccess SPACE: 3 special day types (1 – 3)

When only GAT ACE 7000 is being used and not GAT ACE 3000 and/or ProAccess SPACE, these orange markings are not displayed. For each special day type you can change the name and set a color that will be used to display these types of special days in the calendar.

When you click onto a colored field (i.e., special day) in the calendar this day will be marked on the right side of the window in the special day list. In this list it is possible to change the type of special day.

To add a new special day to the special day list, press the “Add Day” button above the list. If you first select the desired day in the calendar view, this day will be used as the date for the new special day. To delete a special day, mark the day and press the “Delete Day” button. Depending on the general deleting confirmation setting (see "4.7. General settings") a window will be opened where the deletion must be confirmed, or the special day will be deleted directly without additional confirmation. Pay attention that special access authorizations defined for that special day are no longer active on that day and the normal access authorizations will be used on that day after updating the changed to the terminals.

To define the settings for a special day, double-click directly onto a day in the calendar view or on the already defined day in the special day list. The following day definition window opens.

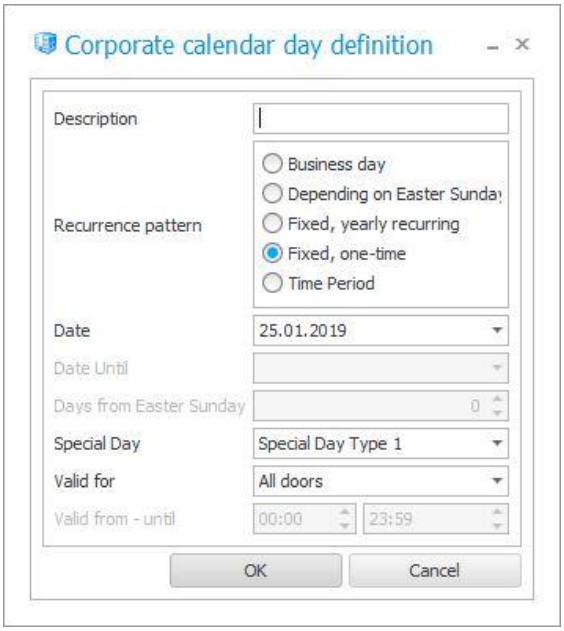


Figure 6.3 *- Day definition for special days*

The following information can be defined for the special day:

- Description: Enter a description for the special day that will be used for display in the special day list.
- Recurrence pattern:

  Select the recurrence of the special day.
  - Business day: Used to overwrite a special day and resets the special day to a business day.
  - Depending on Easter Sunday: Used to define a special day in relation to Easter Sunday. The number of days before or after Easter Sunday that the special day falls on can be entered in the "Days from Easter Sunday" field.
  - Fixed, yearly recurring: Used to define a special day that recurs each year on the same date.
  - Fixed, one-time: Used to define a special day that occurs only in the current year on the defined date.
  - Time Period: A time period with start and end dates is used to define a period of consecutive special days, e.g., company holiday, in one step.

  NOTE! If two or more special days fall on the same day of a year, the special day with the highest day type priority has precedence. The priority of the day types from highest to lowest are: "Business day" -> "Fixed, one-time" -> "Fixed, yearly recurring" -> "Depending on Easter Sunday" Special days defined in “Time Period” have the same priority as “Fixed, one-time” days.

- Date: Enter the date of the special day. The date format depends on which “Recurrence pattern” option is selected.
  - Depending on Easter Sunday: No date can be entered here for this option. See the “Days from Easter Sunday” description.
  - Fixed, yearly recurring: Enter the date in “dd.MM” format.
  - Fixed, one-time: Enter the date in “dd.MM.yyyy” format.
  - Time Period: Enter the start date of the special day period in “dd.MM.yyyy” format. The end date for the period is entered in the “Date Until” field.
- Date Until: Enter the end date of the special day period in “dd.MM.yyyy” format.
- Days from Easter Sunday:
  If the recurrence pattern of the special day is set to "Depending on Easter Sunday", enter the number of days before or after Easter Sunday that the special day falls on.
- Special Day: Select the type of special day here. For GAT ACE 7000, 10 special day types are possible and for GAT ACE 3000, only special day types 1 – 5 are available.
- Valid for: Select either “All doors”, “Online doors”, or “Offline and WiNET doors” to define which doors the special day will affect.
- Valid from - until:
  If required, you can define a specific period for the special day other the default 24-hour period by entering the desired times into the fields.
  NOTE! This setting only applies for online doors that are controlled by a GAT DC 7200. Doors controlled by other GANTNER controllers do not support this function.

The settings of an individual special day or days can be exported, e.g., for backup purposes or to send to another Matrix installation, via the “Export Selected” button, and imported again via the “Import Days” button.

► Select the desired special day(s) from list and click on “Export Selected”.

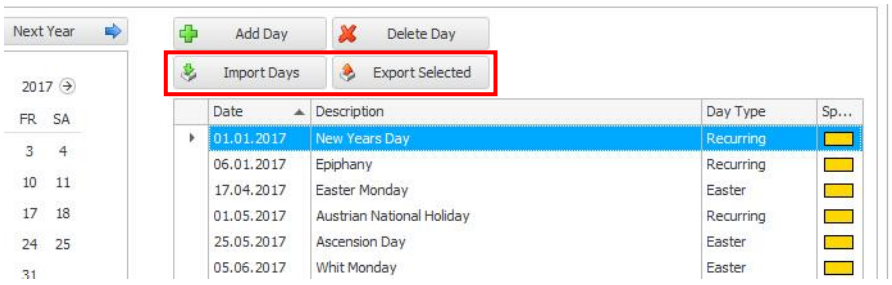


Figure 6.4 *- Export and import special days*

► In the “Save as” window that opens, enter a directory path where the export file will be saved.

► To manually import a special day file into Matrix, click on “Import Days” and enter the directory path where the file is saved.

► To setup the automatic importation of a special day file, click on the “Configure Import” button on the main page.

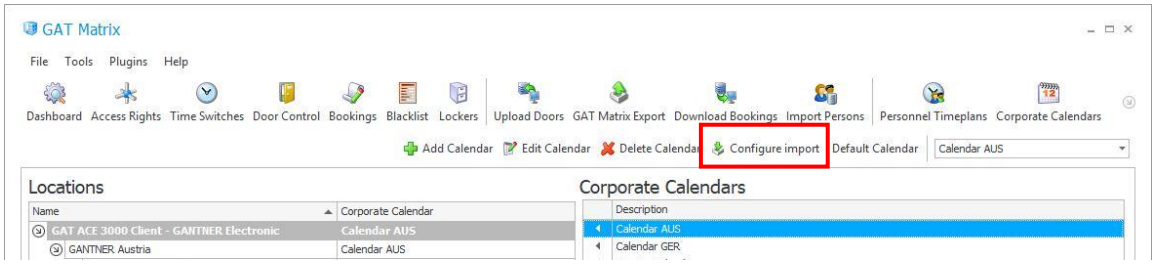


Figure 6.5 *- “Configure import” button*

- The “Special day import” window opens.

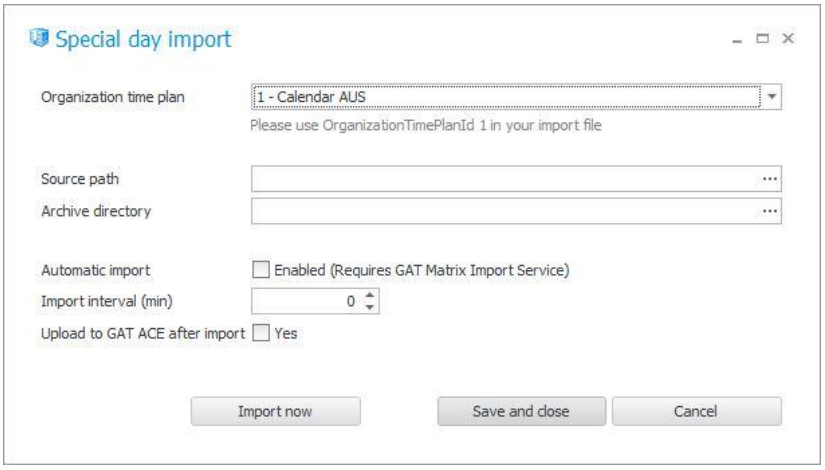


Figure 6.6 *- Configuration of the special day import*

The following information can be defined for the special day import:

- Organization time plan: Select an organization time plan where the special day file will be imported to.
- Source path: Enter the directory path where the special day file is saved.
- Archive directory: Define an archive directory for the special day file. Following importation, the special day file (under “Source path”) is moved to the archive directory and renamed “`gatmatrix_otpimport.archive.<<OrganisationCalenderId>>.<<DateAndTime>>`” (Example: `gatmatrix_otpimport.archive.1.20190710151800`)
- Automatic import: Select this option if you want to enable the file to be imported automatically.
- Import interval (min): When the previous “Automatic import” setting has been selected, define here the intervals (in minutes) between each importation. Note that the interval begins to countdown after the import is completed.
- Upload to GAT ACE after import: When this option is selected, the data is automatically loaded to GAT ACE after importation.

See “Appendix D Formats and File Specifications” for information on the required formatting of the special day file.

NOTE! Please note that after making changes to the organization time plan, all terminals (offline terminals as well) must be uploaded again in order to implement the changes.

If a special day is active on the current date, the special day is displayed in the status bar of Matrix.



6.2 Locations

Locations are defined in GAT ACE 7000 or GAT ACE 3000 to organize larger access systems into smaller units, e.g., branch offices or different departments. The controllers and doors are then assigned to these locations. In Matrix, you can use these locations and assign a separate corporate calendar to each location in the calendar view. Locations can also be defined in the ProAccess SPACE software. There these are called "partitions". The functionality however is analogous to the GAT ACE locations.

NOTE! In order to view the locations, you must first import them. From GAT ACE 7000 and/or GAT ACE, the import is started via the "Import doors and locations" menu item (see "5.4 Importing doors and locations from GAT ACE") and from ProAccess SPACE via the "ProAccess Space synchronization" menu item (see "5.5 Importing doors and locations from SALTO ProAccess SPACE").

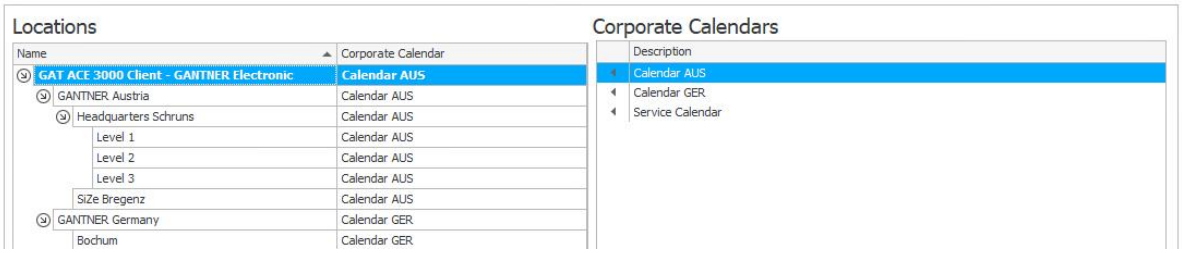


Figure 6.7 - *Assigning corporate calendars to the locations*

Displayed on the left in a hierarchical arrangement are the locations and their respective assigned corporate calendars (“Corporate Calendars” column). The field to the right lists all the corporate calendars that have been created in Matrix and visible to the current user. The locations are divided here into the groups for GAT ACE 7000 / 3000 and ProAccess SPACE.

► Select a location.

► Click on the arrow symbol next to the corporate calendar.

- The corporate calendar is assigned to the selected location.

Note that a corporate calendar cannot be assigned to multiple ProAccess SPACE sites (partitions) simultaneously. You must define a separate corporate calendar for each site. This does not apply to the GAT ACE sites, i.e., a calendar can be assigned to several sites from GAT ACE at the same time.

In the access rights view, you can see which corporate calendar is assigned to a terminal by clicking on a field in the terminal column that has a time plan assigned (personnel time plan or terminal time plan).

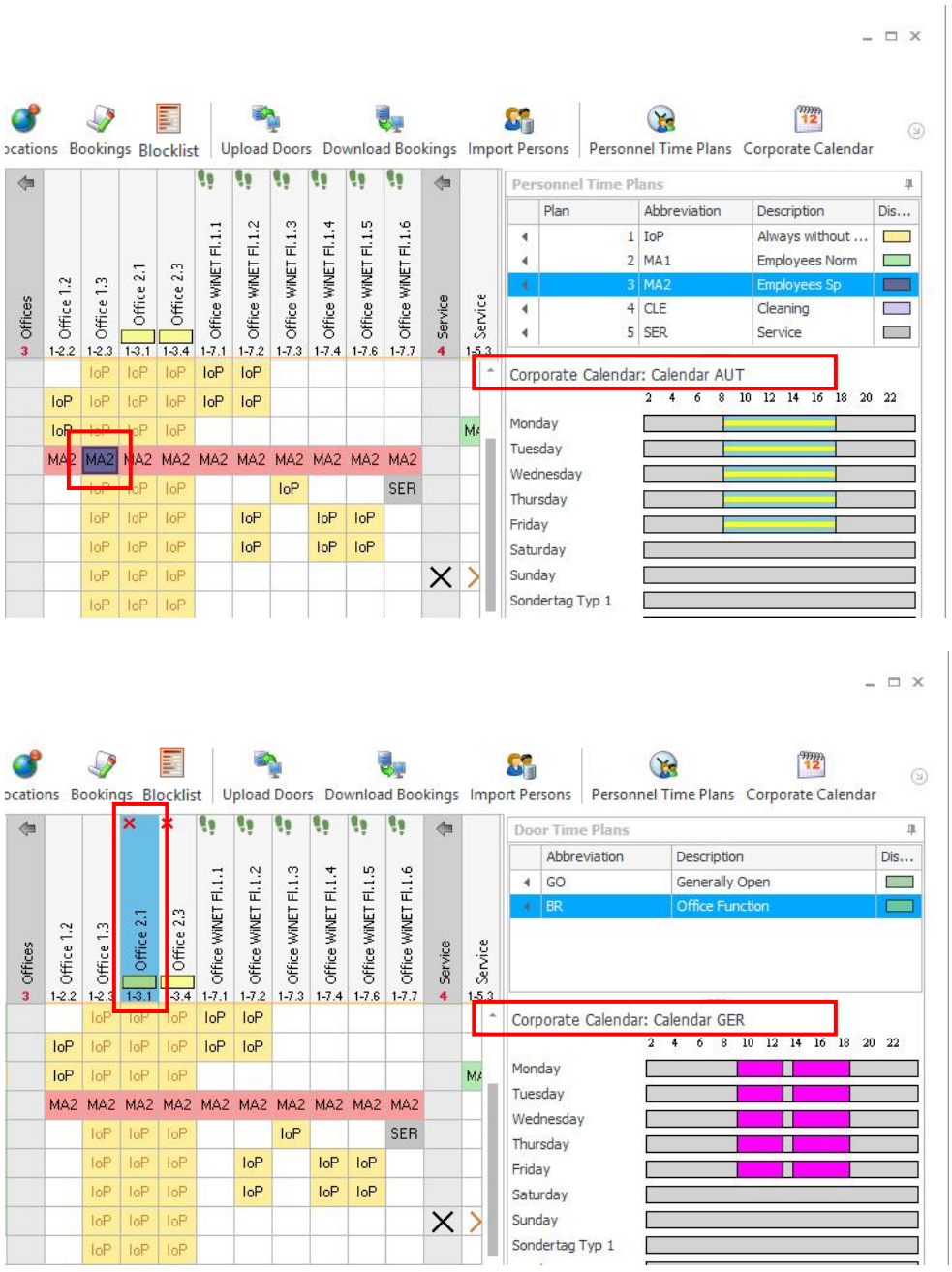


***Figure 6.8** - Display of the corporate calendar assignment in Matrix*

7. BOOKINGS

Every controller and offline lock log all events that occurred at the terminal, e.g., valid identification, access attempt without identification, alarm, etc., in the internal memory. For each event, a booking is generated with time and date of the event, data carrier number that caused the event, access code, direction information, etc.

The bookings of the controllers and offline locks can be read and viewed in Matrix. Click on the "Bookings" toolbar button to display the bookings list.

The bookings page displays both the bookings from the GAT ACE installations and the bookings from a ProAccess SPACE installation (if used).

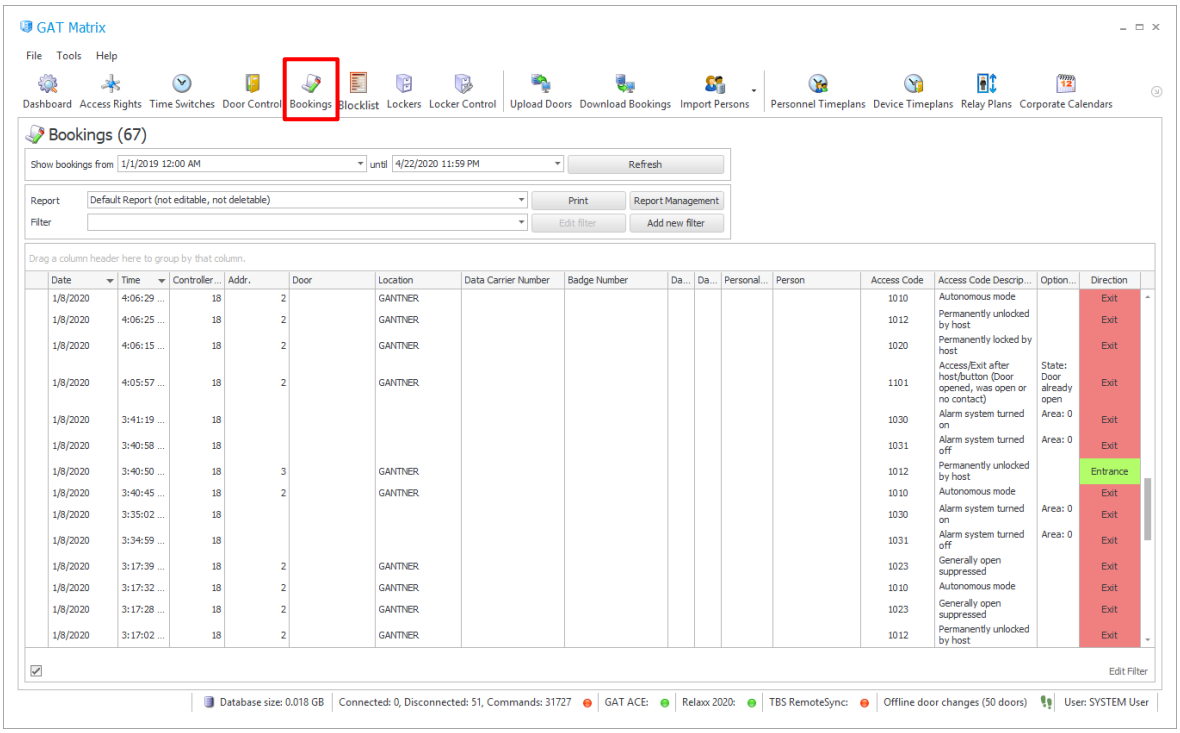


Figure 7.1 *- Bookings list of Matrix*

► To import the bookings, click on the "Download Bookings" icon in the toolbar.

- Matrix loads all the bookings from the GAT ACE and ProAccess SPACE installations. These are loaded in packages, which is why it may take some time until all bookings are loaded.

NOTE! Please note that in GAT ACE you can activate the bookings cleaning function. This function is deactivated by default. But when it is activated, the bookings are deleted by GAT ACE after one 1 year, no matter if they have been sent to Matrix or not. Therefore, the bookings should be imported on a regular basis.

► To update the bookings list, enter the desired date and time period (fields "from" and "until") and click the "Refresh" button.

The following information is shown in the bookings list:
- At the top behind "Bookings" the number of bookings in the list is shown in parenthesis.
- The columns "Date" and "Time" shows when the booking was made.
- The column "Controller number" indicates the number of the controller where the booking was made.
- The column "Address" indicates the network address of the controller where the booking was made.
- The column "Door" indicates the door or controller where the booking was created.
- The column "Data Carrier Number" shows the number of the data carrier that created the booking.
- The columns "Data Carrier Type" and “Data Carrier Type Name” shows the number and name of the data carrier type used to create the booking (see "5.6.4 Defining data carrier types").
- The column "Person" shows the name of the person who caused the booking. The person is determined from the data carrier which was used for the booking.
- The column "Personal number" shows the personnel number defined for the person.
- The column "Badge number" shows the ID number for the data carrier defined in the personnel data.
- The column "Access Code" indicates the type of booking.
- The column "Access Code Description" describes the access code. This is either a default text for the booking code or it can also be changed individually for each terminal (see "7.3 Access code descriptions“).
- The column "Optional Data" contains miscellaneous information, e.g., wrong pin code, status information, etc. depending on the booking code.
- The column "Direction" shows in which direction the booking was made. It is possible to have at a door, for example, one controller with two readers -- one on the outside and one on the inside. The controller controls entry access via one reader on the outer side of the door and controls exit access via the second reader on the inner side of the door. The color indicates the type of booking. Green = Entry, Red = Exit, Yellow = Status Booking.

Certain filter criteria can be defined in order to filter the bookings list so that only certain bookings are displayed (see "7.1.3 Filter bookings").
Furthermore, reports for printing and exporting the booking list can be defined. For each report, comprehensive settings can be defined for formatting the print/export accordingly (see "7.2 Export and print bookings with booking reports").

7.1 Sorting, grouping, & filtering bookings

You can adjust how the bookings list is displayed as desired. The columns can be moved and arranged, and you can group the bookings list according to certain characteristics. In addition, complex filters can be created that group various search criteria with logical links.
The display of the bookings list (column arrangement, etc.) and the filter settings are saved individually for each Matrix user and reloaded after logging into Matrix.

7.1.1 Sort bookings

In order to sort the bookings, click on a header of a column in the booking list. The booking list will be sorted alphabetically using that column. By clicking repeatedly on the column header, the sorting can be changed between ascending and descending sorting.

The columns can be rearranged by dragging them with the left mouse button to another position.

7.1.2 Group bookings

To group the bookings first make sure that the grouping is enabled. Therefore, right-click onto a column header of the booking list and select the "Show Group By Box" option from the menu.

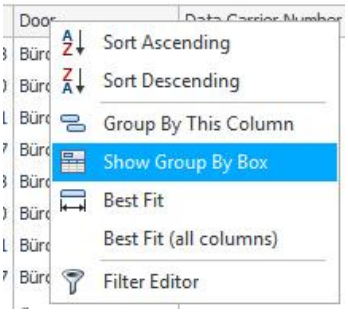


Figure 7.2 *- Activate grouping of bookings*

At the top of the booking list a bar is shown with the text "Drag a column header here to group by that column". Drag the header of a column onto the bar to group the bookings under that column. By dragging several columns onto this area, the bookings are grouped according to the order the headers were dragged.

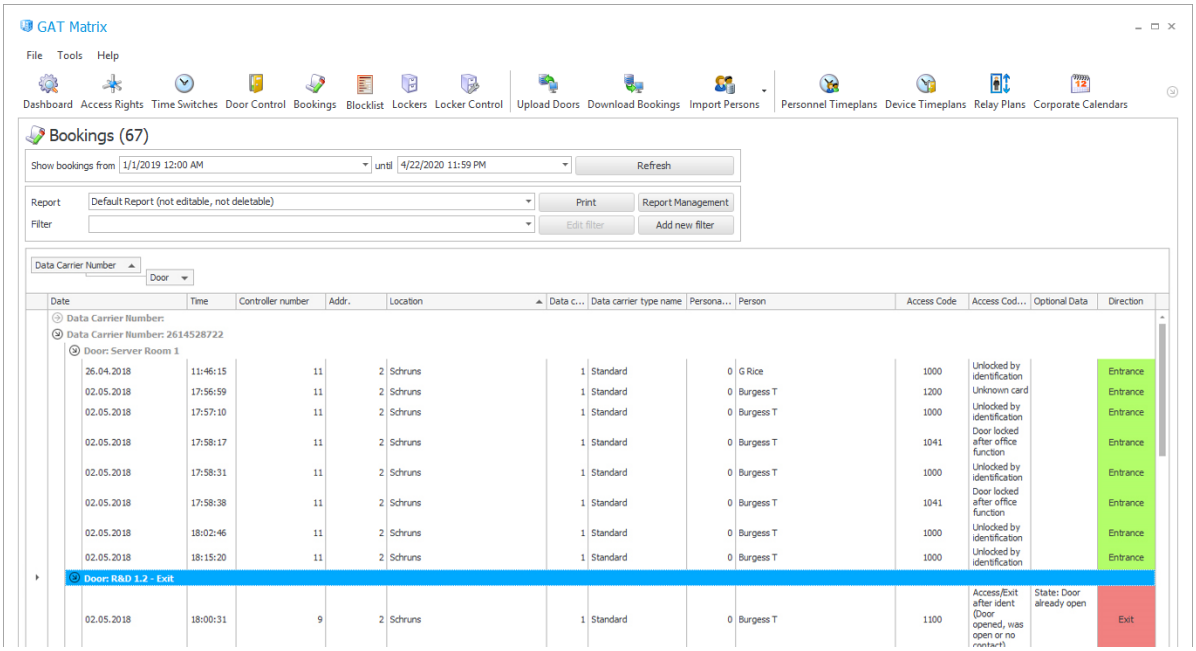


Figure 7.3 *- Grouping bookings*

In this example, the bookings are first grouped by "Data Carrier Number". The bookings with data carrier number 2614528722 are displayed expanded, so that the next level of grouping (Door) is visible. The bookings in this group are displayed.

In order to remove the grouping of a column, drag the group from the bar down to the column headers of the booking list.

ATTENTION! As some data (e.g., card number, card type, etc.) is not stored in SALTO bookings, evaluations according to these criteria in combined GANTNER/SALTO systems can lead to results that are only partially correct.

NOTE! If the group is dragged too far down directly into the booking list, the mouse cursor will show a black "X". If the mouse button is released in this state, the group (resp. column) will be deleted. If you restart Matrix, the column will be visible again.

7.1.3 Filter bookings

Time filter

Bookings can be filtered by time so that only bookings within a certain period are shown.

► Enter the desired period in the upper date and time fields.

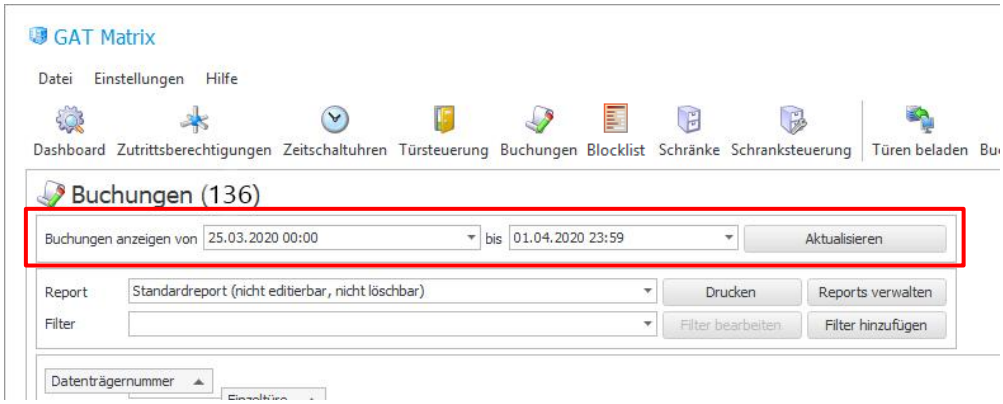


Figure 7.4 *- Filtering bookings by a time period*

► Click on "Refresh".

- Only those bookings logged in the selected period are displayed.

Filter editor

A filter editor is also available in which complex filters can be defined to filter the bookings according to certain criteria. To open the filter editor:

► Right-click on the header of the booking list. In the menu, select the "Filter Editor" option.

or

► Right-click below the bookings list onto the "Filter Editor" option.

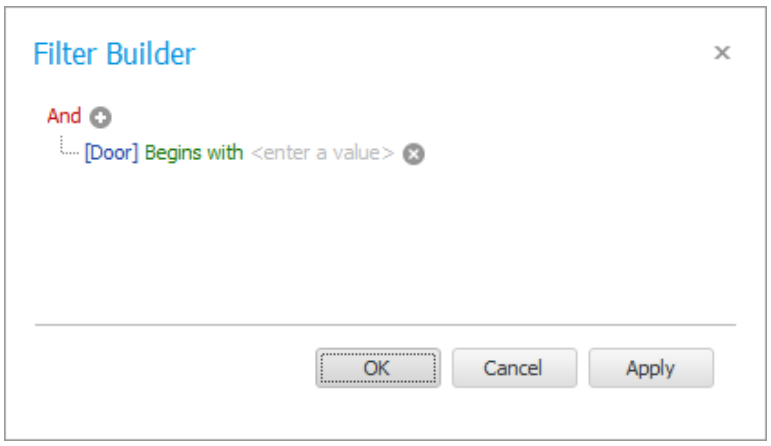


Figure 7.5 *- Filter editor for filtering bookings*

Here several filter criteria can be defined as text lines. A filter criterion is defined in three steps:
- Click on the blue text (in Figure 7.5 "[Door]") and select the information that shall be filtered.
- Click on the green text (in Figure 7.5 "Begins with") and select the type of filter checking.
- Click on the gray text (in Figure 7.5 "<enter a value>") and enter the value (number or text) that will be used for filtering.

By clicking on the plus sign on the right of the red "And" text more filter criteria can be added and defined by repeating the previous three steps. By clicking on the red “And” you can define how multiple filter criteria should be combined.

After all filter criteria are defined, press "Apply" to apply the filter to the booking list. The filter editor will remain open and the filter can be adjusted. If the filter confirms your expectations, confirm with "OK".

On the bottom of the bookings list the active filter will be shown. You can easily enable / disable the current filter by checking / unchecking the checkbox on the left or select another filter, in case you have defined several filters, by clicking on the little arrow symbol to the right of the filter.

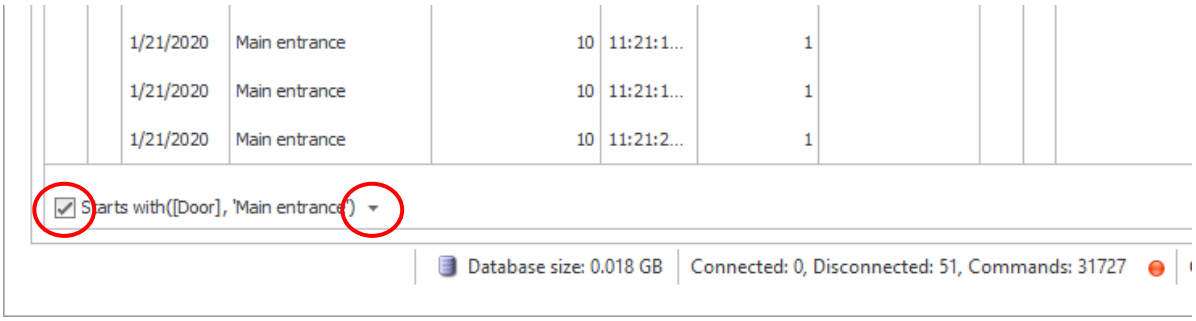


Figure 7.6 *– Active filter criteria*

To display all bookings in the booking list again, deactivate the filter. To do this, right-click on the header of the booking list and select "Clear filter for this column" from the menu. Alternatively, you can click the “X” on the left side next to the filter.

Save and load filter settings

The combination of time filter, filter editor settings, and bookings list layout can be saved and reloaded. This allows the bookings list to be quickly adapted to several individual requirements without having to re-enter the settings each time. Saving and loading of the filter settings is possible in the "Filter" field above the bookings list as shown below.

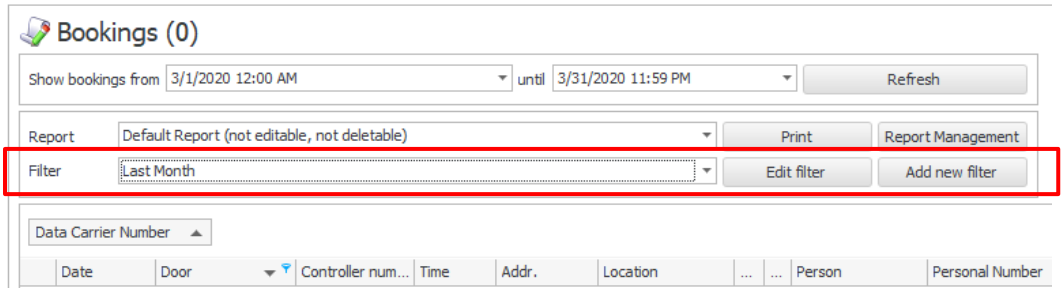


Figure 7.7 *– Saving and loading filter settings*

► If filter settings have been saved already, select a setting from the menu next to the "Filters" field.
  ○ The periods and display settings defined in the filter are loaded and the bookings list is displayed according to these settings.
► To edit the selected filter settings, click on "Edit filter" after selecting the filter.
  ○ The "Booking filter" window opens (see next step).
► To define new filter settings, click on "Add filter".
  ○ The "Booking filter" window opens.

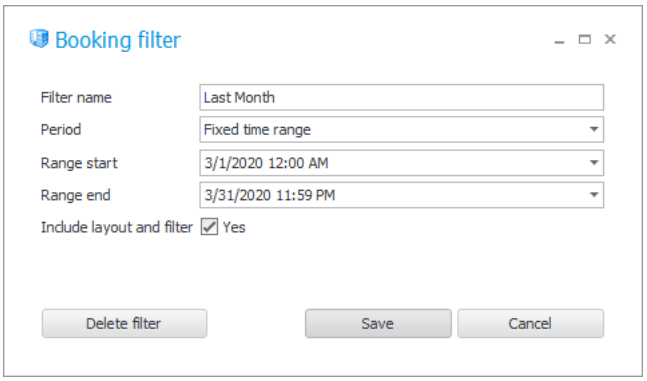


***Figure 7.8** – Editing filter settings*

► Enter the following data here:

- Filter name: Name for the filter settings.
- Period: Select here how the period should be defined.
  Fixed time range: Define the start and end time for the desired period in the "Range start" and "Range end" fields.
  Month, week, day: Here, you can choose between the current or previous month, week, or day. Matrix will then continuously update this booking display based on the current date.
- Include layout and filter: When this option is selected, the currently set filter and the layout of the bookings list are saved and can be loaded later together with the time settings by selecting the filter settings.

► With the "Delete filter" option, the currently displayed filter settings can be deleted.

7.1.4 Show and hide columns in the bookings list

► Right-click on a header in the bookings list and select "Column Chooser".

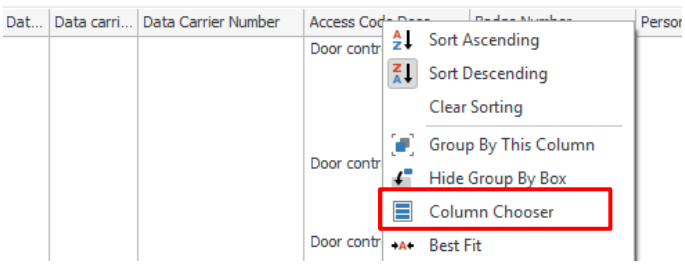


***Figure 7.9 -** Select columns in the booking list*

- The "Customization" window opens.

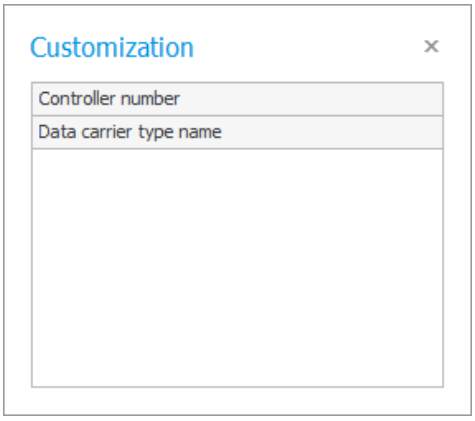


***Figure 7.10** - Hidden columns*

- All columns that should not be shown in the bookings list are displayed here (in the example, the "Controller number" and "Data carrier type name" columns).

► To hide another column, drag the column header from the bookings list into this window.

- The column is displayed in the Customization window.

► If you want to show a column again, drag it from the "Customization" window to the desired position in the bookings list.

7.1.5 Filter authorization matrix

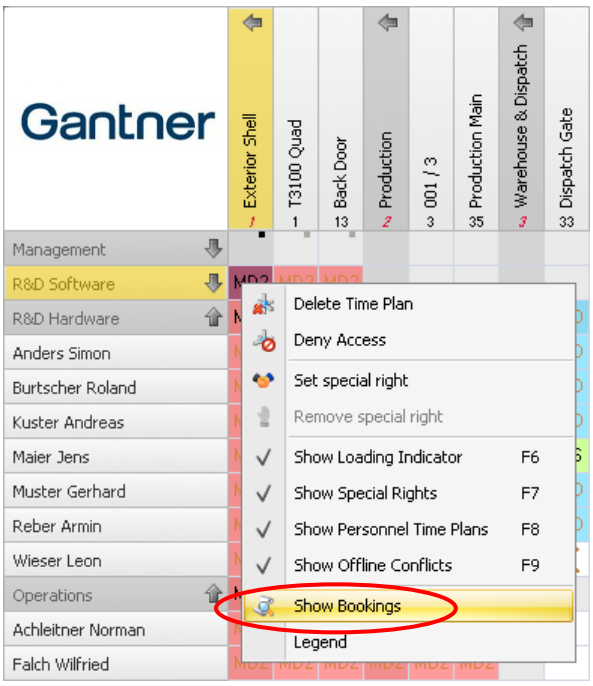


***Figure 7.11** – Show bookings from Matrix*

In the authorization matrix you can use the “Show Bookings” entry from the context menu to show the bookings of a certain person at a certain door. This function will be enabled if a single cell is selected. After selecting the entry from the context menu, the bookings window will be opened with the appropriate filter set.

If the selected cell is a person group / door group, the bookings of all persons / doors in the group will be shown. In the example in Figure 7.11, showing the bookings of “Management” / “Exterior Shell” would show the bookings of all persons inside “Management” for all doors inside the group “Exterior Shell”.

This function is also available when clicking on a person group, person, door group or door on the left / top. For persons, the bookings of this person at all doors will be shown. For a person group, the bookings of all persons inside the group at all doors will be shown. For doors and door groups, this function works the same way whereas the bookings of all persons at the specific door(s) will be shown.

7.2 Export and print bookings with booking reports

Bookings in Matrix can be printed or exported into another data format. In order to print or export bookings so called booking reports must be used. They can be designed directly in Matrix and they define the layout of the print and export.
In order to print or export bookings proceed with the following steps:

1. Sort and filter the bookings list so that the printed/exported bookings are displayed.
2. Select a booking from the bookings list to print out.
3. Above the bookings list, select the required report in the "Report" field.

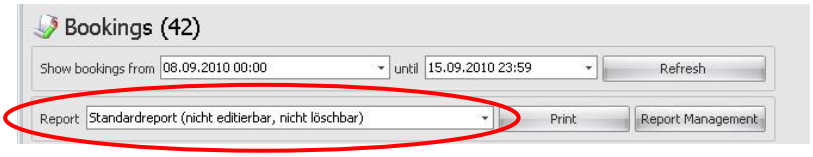


***Figure 7.12** – Booking reports*

4. Press the "Print" button. A preview of the report is displayed. In the menu of this preview you can select the desired export format under the "File" → "Export Document".

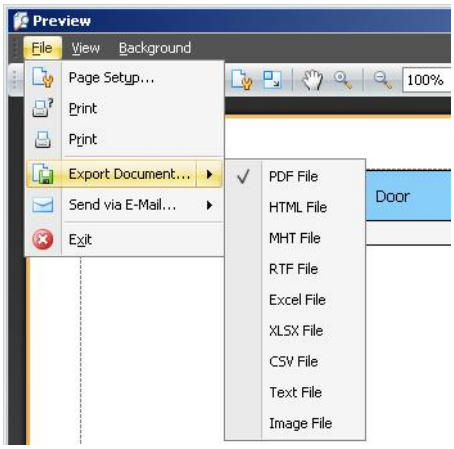


***Figure 7.13** – Selecting an export format*

5. After selection of an export format, a new window will be opened, in which the export settings must be defined. The window depends on the selected format.

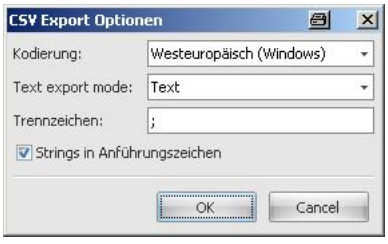


***Figure 7.14** – Define the settings for the selected export format (example for CSV file export)*

If you select an export format, the format is marked so that the next time you want to export a report only "Export Document…" must be selected.

6. In order to print the bookings as shown in the preview window, select one of the "Print" menu items in the "File" menu. The "Print" menu item with the question mark will first open the printer dialog where you can select the desired printer and define its settings. The menu item without question mark will directly print the report with the previously selected printer.

7.2.1 Configuration of booking reports

The configuration of booking reports is done with the integrated Report Designer. In order to make changes to a defined report or to generate a new report click the button "Report Management" in the report field above the booking list.

NOTE! In order to use the Report Designer, you need the appropriate license (see "10 LICENSE MANAGEMENT").

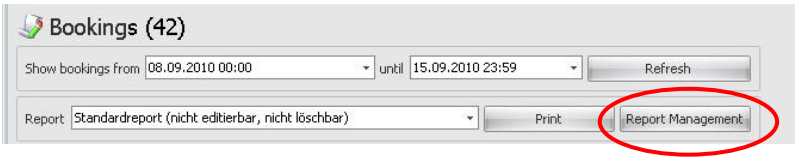


Figure 7.15 *– Manage booking reports*

The window "Booking Report Overview" will be opened.

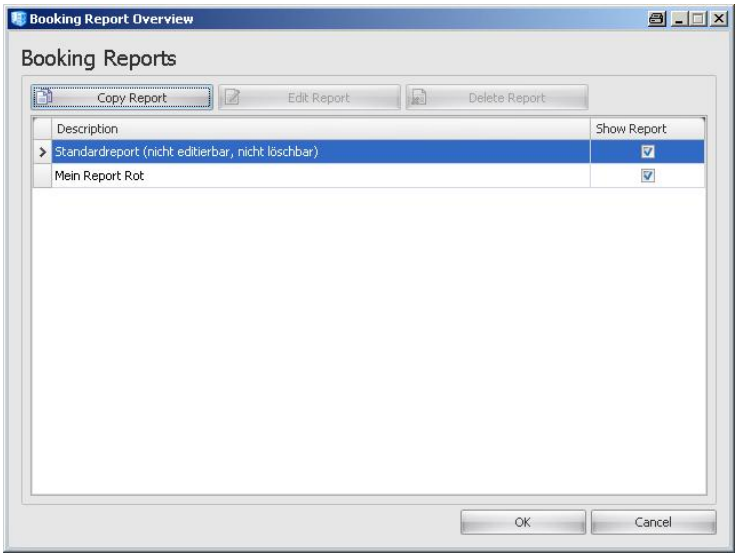


Figure 7.16 *– Booking Report Overview*

Here all available reports will be listed. The reports where the option field in the column "Show Report" is selected will be available for selection in the booking list. The other reports will not be available.

After installation of Matrix, a standard report is already available. This booking report cannot be altered. In order to make a new report mark the standard report and click on the button "Copy Report". A copy of the standard report will be generated. The name of this new report can be changed by clicking once on the name of the report in the list (here "Mein Report Rot").

In order to configure the new report, mark it in the list and then select the button "Edit Report". The Report Designer will be opened. It can take some time so please be patient while the designer is opened.

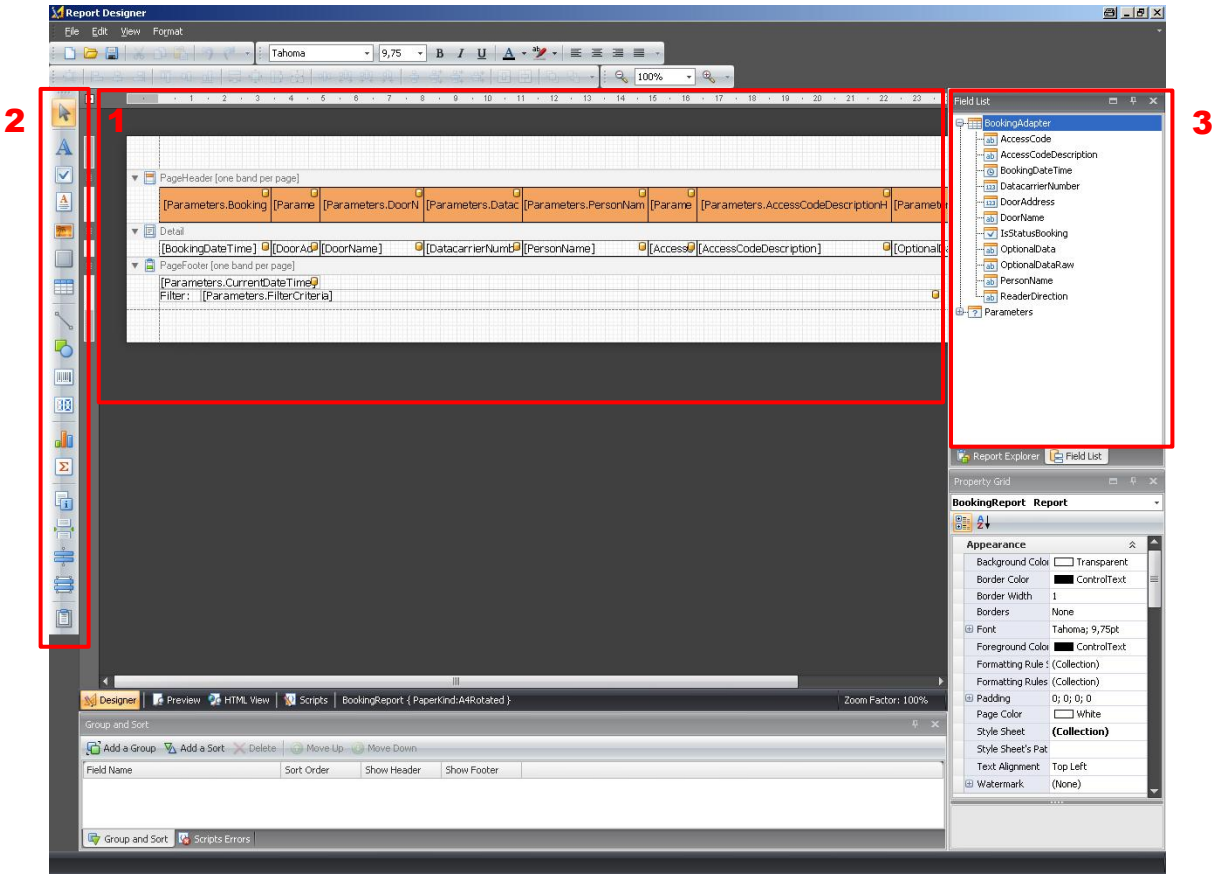


Figure 7.17 *– Report Designer*

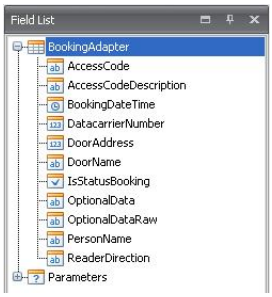
The report designer is only available in English language. Its design is similar to the layout of Microsoft's Visual Studio. The most important areas are marked with a red rectangle in the figure above.

1 - Design area: In the middle of the window, you see the design area where you can define the layout of the report.

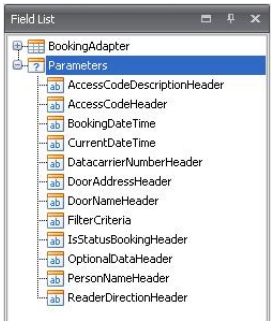
2 - Tool bar: Here you find the tools for defining the design, i.e., for inserting control elements like text, circles, rectangles, tables, lines, etc.

3 - Field list: In the area "Field List" you find the booking and information fields supplied by Matrix, which can be placed on the report. If the area "Field List" is not shown, select the menu item "Windows" → "Field List" in the "View" menu in order to mark this menu item and show the field list.

The field list is divided into two groups:



Below the group "BookingAdapter" all fields, which can be part of a booking (e.g. door, person, data carrier number, access code, etc.) will be shown. These fields are used as list fields for the booking reports. When the booking report is exported or printed each booking will be shown in a new line and in the "BookingAdapter" fields the corresponding values of each booking will be shown.



The fields below the group "Parameters" are independent of the bookings and will be shown exactly like they are placed on the report layout. These fields can be used for example to insert the headlines of the inserted booking table or to insert the current date/time or the set filter criteria.

After the layout of the booking report is defined, the Report Designer can be closed with the menu item "Exit" in the "File" menu. The design will be saved automatically and inserted in the list in the bookings overview window. The option field in the last column must be marked if the report shall be selectable in the booking list.

7.3 Access code descriptions

Each booking in a controller and lock is stored with an access code which defines the type of booking. Matrix allows you to specify special descriptions for each access code in English and German languages. For each door, a code can be independently defined (if desired). The access code descriptions are used to display the bookings in the booking list.

► To set or edit the access code descriptions, select the menu item "Access Code Description" in the menu "Tools". The window "Access Code Descriptions" will be opened where you see a table to define custom access code descriptions.

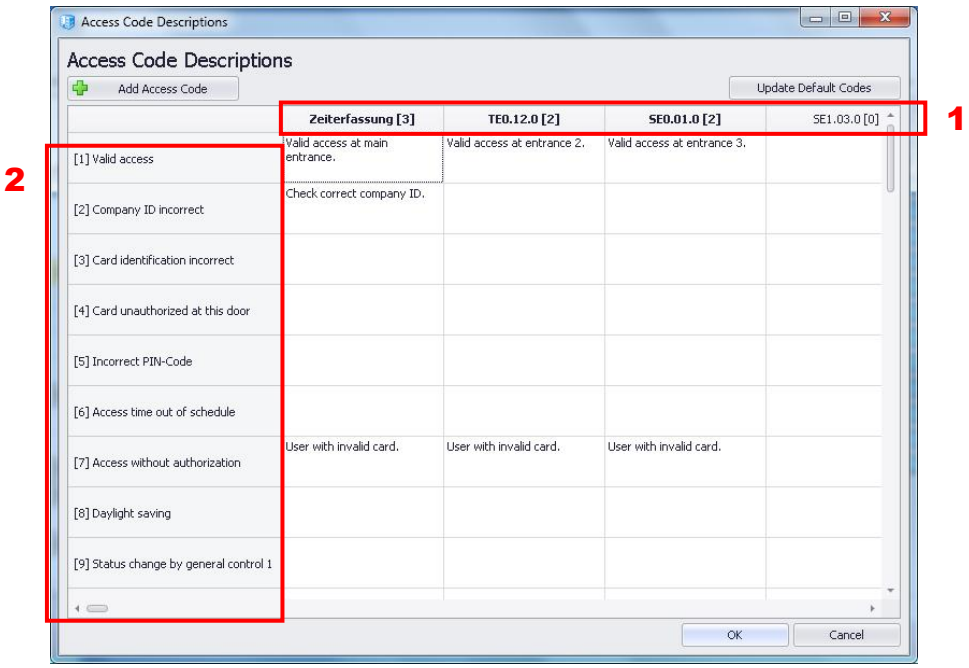


Figure 7.18 *- Access code description table*

The defined doors are listed in the headline of the table (1). The access codes with their standard descriptions, which will be used as default for all doors, are listed in the left column of the table (2). English and German texts are displayed separately with each language indicated by [DE] and [EN]. To overwrite an access code description for a certain door, complete the following steps.

- Search for the door in the headline (1).
- Search the booking code, which description shall be overwritten, in the left row (2).
- Enter another description for the access code directly into the field of the table (3) where the column of the door and the row of the booking code intersect.

The total number of user-defined access code descriptions for a door is shown in square brackets next to the door name, e.g., [3] for “Zeiterfassung” in the example above.

7.3.1 Reload default values of the access codes

With the button "Update Default Codes" you can reload the default texts of access codes in the currently selected language in Matrix. They will then be shown in the left column in the window.

7.3.2 Add access code

To add a new access code to the list (2) click on "Add Access Code". The following window will be opened.

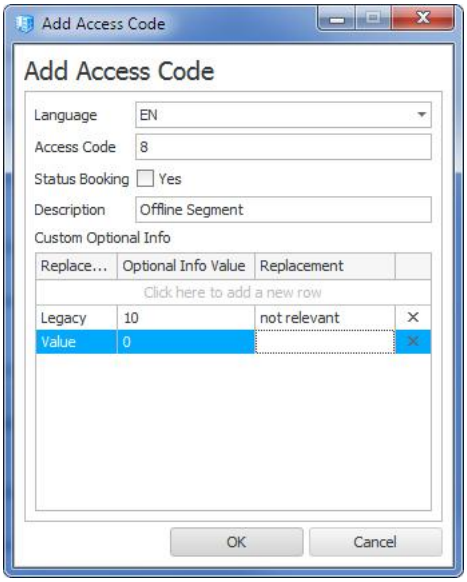


Figure 7.19 *- Add a custom access code*

In the first field, select the language of the bookings text.

In the second box, enter a unique access code number and a standard description in the “Description” field then press "OK" to confirm. The access code can only consist of a character or a max. 4-digit number and can only be used once for German and once for English in the access code list (2).

To define the code as a status booking select "Yes" for the "Status Booking" option.

In the list "Custom Optional Info" values and replacement texts for each of these values can be entered. A booking where the "optional info" data corresponds to one of the values in this list the replacement text will be shown instead of the regular booking text that will otherwise be used for the booking. For example, at a door a status input can be defined as "General Monitoring Input" and be used for monitoring the emergency power supply. When the value "A" and the replacement text "Emergency Power Active" is entered it is possible to directly show this text in the bookings list for a booking that was made when the emergency power was activated.

8. ACTIVITY JOURNAL

The activity journal holds all events and activities that were performed by the users of the Matrix. It is possible to sort the activities with different filters and to generate reports of activities.

► To open the activity journal, select the menu item "Activity Journal" in the menu "Tools".

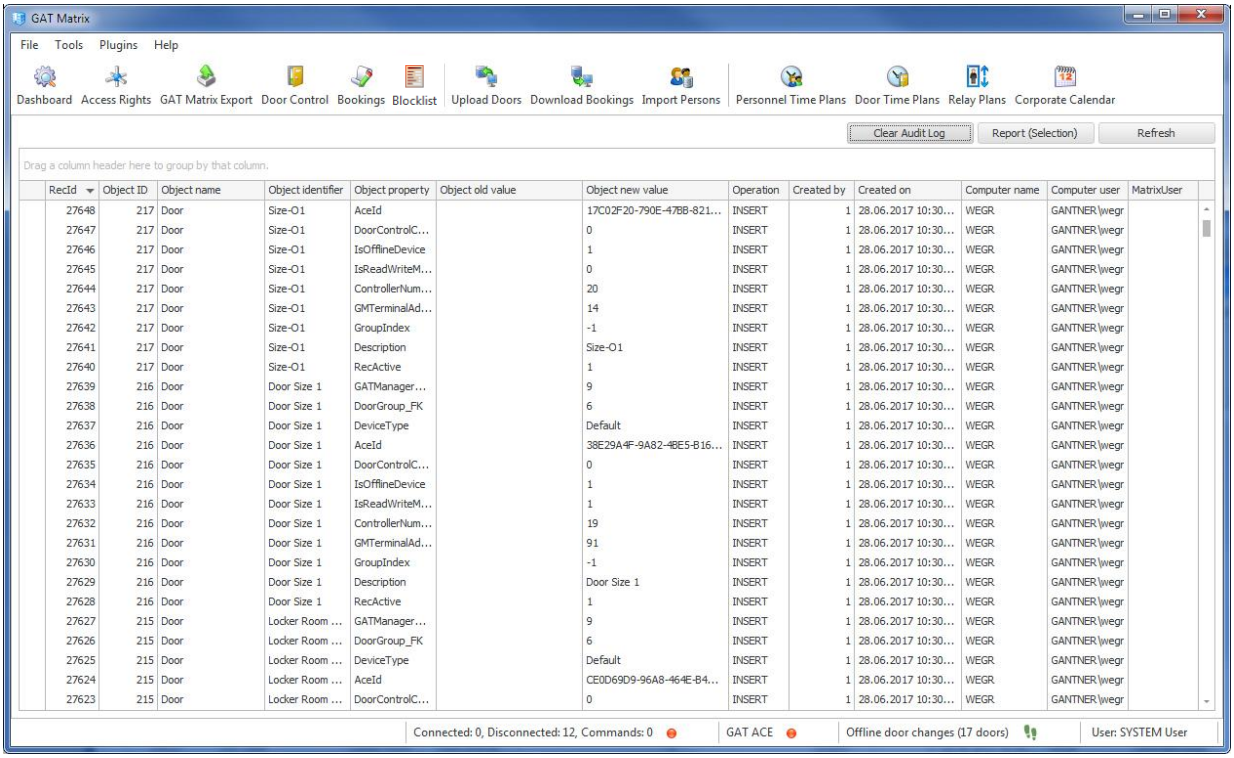


Figure 8.1 *- Activity Journal*

In order to refresh the activity journal, press the button "Refresh" at the top of the list.

The table shows each recorded activity in a new line. For each activity, the following information will be shown.

- RecId: Continuing number of each activity
- Object ID: Identification number of the object, which refers to the activity
- Object name: Name of the appropriate object. An object can be e.g., a "Software-Object" (used for error correction or the like) or also a door, person etc.
- Object identifier: For an object, a more detailed description, if available, will be shown. For example, for an activity, which concerns a door, is here the door description.
- Object property: Describes which property of the object has changed. In Figure 8.1, the description of the door will be changed at the marked action.
- Object old value: If a property of an object was changed, the changed (old) value of the property is here.
- Object new value: If a property of an object was changed, the new value of the property is here.

- Operation: Describes, which action of the activity on the object was carried out (e.g., "UPDATE" for changing a property or "INSERT" for adding an object).
- Created by: Creator of the activity.
- Created on: Time of the activity
- Computer name: Name of the computer, on which the activity was created
- Computer user: Username for the database in which the activity will be stored.
- Matrix user: Username of the user currently logged in to Matrix.

8.1 Refresh, sort, group, and delete the activity list

For sorting and grouping in the Activity Journal, the following actions can be carried out:

Display refresh
In order to actualize the Activity Journal, click on the button "Refresh", right above the table.

Sorting
To sort the list by a certain column, click on the title of that column. The width of a column can be adjusted with the mouse by dragging the column separator in the title of the list.

Group the list
You can also group the list by dragging the list heads onto the dark-grey field above the list and you can apply filters to display only certain activities in the list. This is done the same way as for the booking list. See chapter "7. BOOKINGS" for more information.

Delete activity journal
Depending on the usage frequency of the Matrix, the activity journal increases at different rates and thus occupies more space on the database server. With the button "Audit cleanup", you can delete the entries in the activity journal up to a selectable time. After selection of this button, the following window opens:

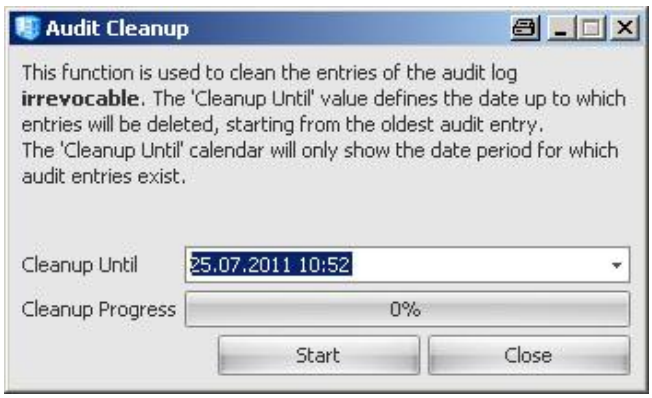


Figure 8.2 *- Delete Activity Journal*

Select in the field "Cleanup Until" the day and time, up to on which the activity should be deleted, and confirm with the button "Start". All activities, which are older than the selected time, will be deleted.

Depending on the computing power of the database server as well as the size of the Activity Journal, the delete process can take several minutes or up to one hour.

After the deletion, the activities of the database (and thus the table display) are deleted but the database still occupies the same space on the hard disk of the database server. Therefore, following the deletion, a notification is shown in which you can select whether the database should be compressed in order to release the hard disk space.



Figure 8.3 *- Should the database be compressed message*

With the button "No", you return to the activity journal without compressing the database. With the button "Yes", the following database window opens in which you can compress the database with the button "Shrink Database". The compression process usually takes less than 1 minute.

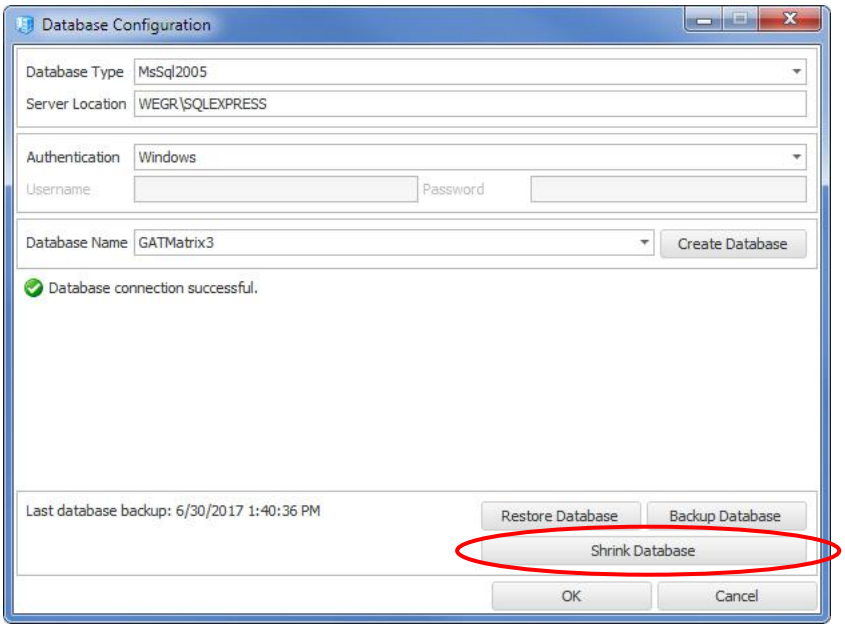


Figure 8.4 *- Database information*

When you shrink the database, the transaction log is truncated, and the applicable hard disc space is released. The data from Matrix is retained by this operation.

You can also open the database window later anytime (select "Options" from the “Tools” menu) and shrink the database.

8.2 Generate reports

In order to generate a report of certain activities sort the list accordingly and mark the desired entries in the list. You can mark several entries by clicking on the while holding the SHIFT or STRG key of the keyboard. To select all displayed activities, press STRG+"A" on the keyboard. Next press the button "Report Selected" at the top of the list to generate a report of the selected activities. In the report window you can choose to print the report, to export the report to a file, to generate a PDF file from the report, or to send the report via email.

9. AUTHORIZATION MANAGEMENT

Matrix offers the possibility to define different users having different levels of access in the application. This is done by a simplified role base access control system. Every user can be assigned to exactly one role whereas the user's permissions are being inherited from the role. A role represents a collection of permissions for certain function blocks in the application. Furthermore, the system allows overriding the permissions on user-level.

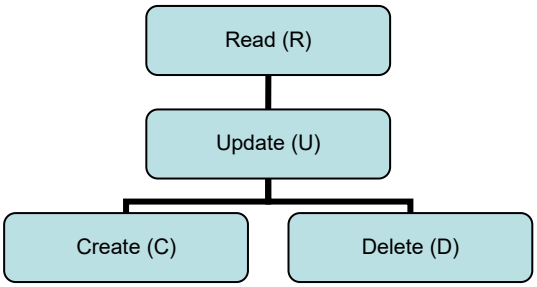
9.1 Function blocks

A function block is a group of simple actions (e.g., add a new time plan, assign personnel time plan at a certain door etc.) in the application for which permissions can be granted at once. Depending on the function block, you can assign Create, Read, Update and Delete (CRUD) or Execute (E) permissions.

Execution permissions can be assigned if the user should or should not be allowed to execute an action. An example for this is the "Door Upload" function block. It does not make sense to define CRUD permissions for this function block since nothing can be created or deleted.

On the other side, you can give CRUD permissions for the "Personnel Time Plan Management" function block. It is possible to define that some users may only view the personnel time plans and others are also allowed to modify or delete them.

The CRUD permissions are organized in a hierarchical way. This means that it is not possible to give Update permission without having Read permission. The diagram on the right shows the organization of the access levels.

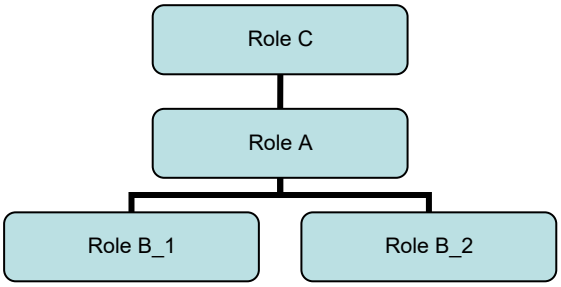


Matrix defines the following function blocks:

- Personnel Time Plan Management (CRUD)
- Door Time Plan Management (CRUD)
- Organization Time Plan Management (CRUD)
- Bookings View (E)
- Door Upload (E)
- Door Import (E)
- Access Right Management (CRUD)
- Access Code Management (CRUD)
- Person Management (CRUD)
- Complete Door Initialization (E)
- Person Import Definition (E)
- Person Import Execution (E)
- Audit Log (E)
- Database Settings (CRUD)
- Special Rights Management (CRUD)
- User Management (CRUD)
- Role Management (CRUD)

In addition to the CRUD and Execution permissions, you can give the Grant (G) permission for every function block. The grant permission gives a user the possibility to pass the own permissions of a certain function block to another user. Therefore, the user must have the grant permission for this function block and the role/user to which the permission is assigned is a child of the logged-in user.

For the figure on the right side this would mean that a user with role A and Grant permission for a certain function block would also be allowed to pass its own permissions to the roles B_1 and B_2. But the user cannot pass more permissions than his own permissions. (A user cannot give CRUD permissions if he only has RU permissions).



9.2 Role management

A role represents a collection of permissions for the function blocks defined in the software. Roles are organized in a hierarchical way. 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 (as far as the user has the “User Management” permission and the “Role Management” permission given).

Matrix comes with one superior role, the SYSTEM role. The SYSTEM role contains exactly one user, the SYSTEM user who is allowed to do anything in the application. Every role is therefore a descendant of the SYSTEM role.

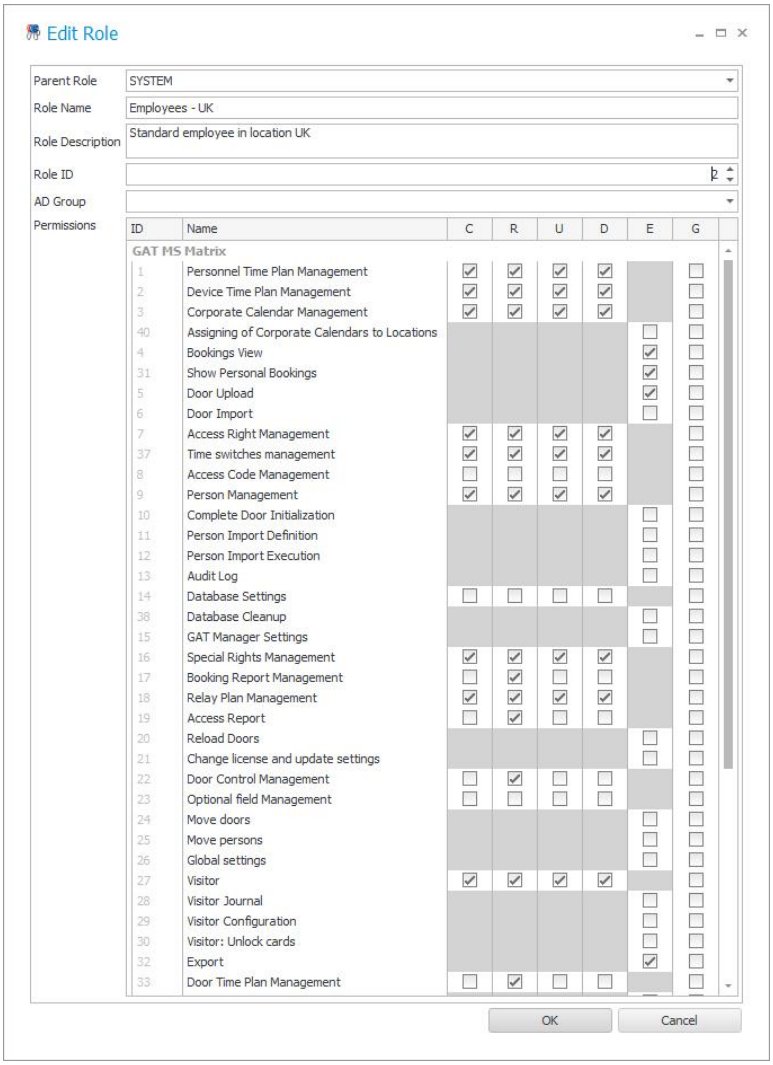
The maximum rights a role can have are the rights of its parent role. Removing a right from a parent role will also delete the right from any descendant.

To define a new role, open the role overview by selecting the “Role Management” item from the menu. Clicking “Add role” will open a window, where the settings for the role can be defined. Every role must have a unique name and a description. The role ID will automatically be calculated and is only relevant when external applications are involved. Furthermore, you have to select a parent role from which the new role inherits.

Depending on the parent role selected, you will or will not be able to set certain permissions for certain function blocks. If you have completed your settings, proceed by pressing OK.

In the following figure it was possible to set permissions for every function block defined in Matrix. This is because the logged-in user is the SYSTEM user, who has Grant permissions for every function block. With the option fields behind the functions, it is possible do define which permissions shall be valid for which functions. The abbreviations mean.

- C: Creating data sets for the function
- R: Reading data sets of the function
- U: Updating/editing data sets of the function
- D: Deleting data sets of the function
- E: Executing actions in connection with this function
- G: Granting permissions for this functions to other users



NOTE! The "AD Group" field allows you to select a group from the Active Directory to assign via the role to the users in this group. You do not have to create your own user in Matrix for these users. For more information see “9.4 Active Directory".

NOTE! For the last two fields in the "General" section you can specify whether users assigned to the role being edited have the ability to create or edit existing roles and other users.

Figure 9.1 *– Role settings under the SYSTEM user*

In the following figure, the logged-in user only has Grant permission for four function blocks. Therefore, the user can only grant permissions for these function blocks.

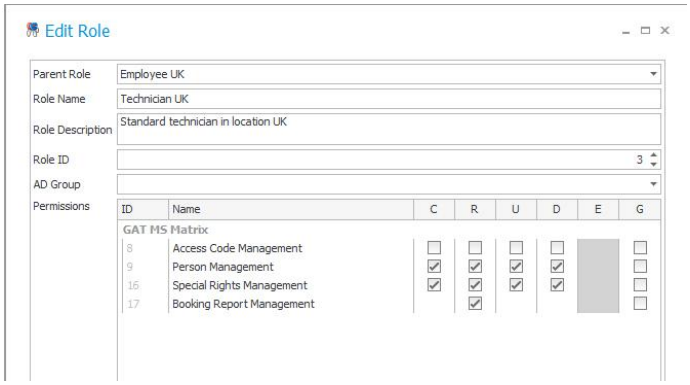


Figure 9.2 *- Role settings for a user with fewer grant permissions*

9.3 User management

A user is identified by a unique username and a password, which is used to prevent other people from login under this user account. Every user in Matrix must be assigned to exactly one role. It is impossible to have users that are not assigned to a role. The user will inherit the permissions from the role.

In addition, there is the possibility to override the permissions inherited from the role by explicitly setting permissions for a certain function block for the user. These user permissions will also exist, if the permissions for the function block are changed on role level.

When defining a user, you have to specify a unique username and also a display name for the user. The display name will be displayed in the log files. Enter the password and also repeat the password once to be sure not to have mistyped the password. If "User Auto Logout" is enabled, the user is automatically logged out of Matrix after a period of inactivity. If this field is not checked, this function has no effect.

The user ID is automatically calculated and only relevant if external applications are involved. Lastly, assign a role to the user. The permissions for the function blocks are set depending on the role to which the user is assigned.

Now, you can override the role permissions by explicitly setting user permissions in the table. Permissions that are set explicitly on user level will be marked with ochre background. To clear an explicitly set permission, right click on the given cell with the right mouse button.

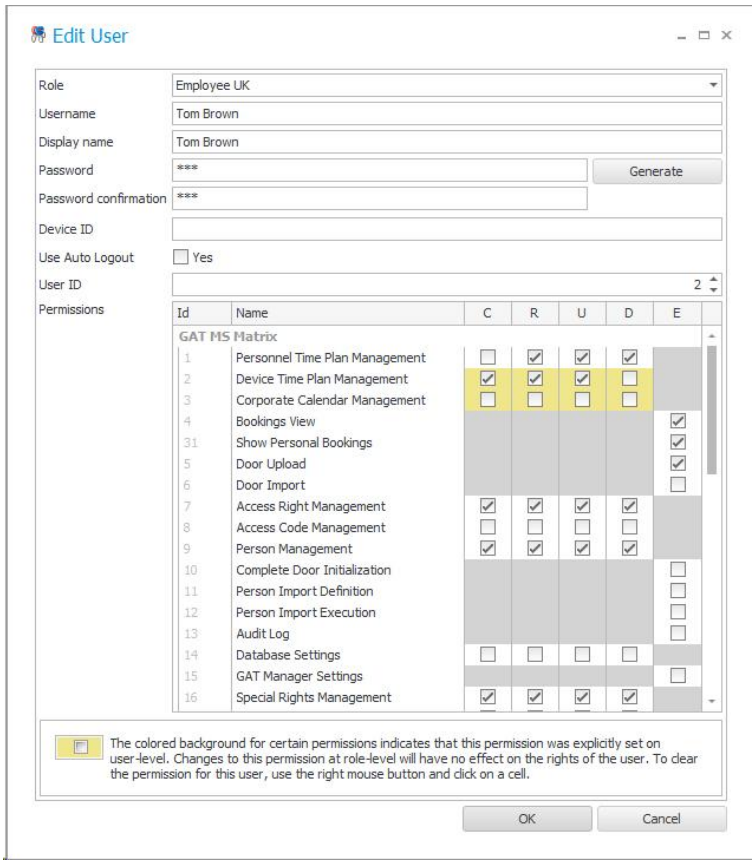


Figure 9.3 *- User settings*

NOTE! The "Device ID" field is important when using GAT Mobile Access Management. This ID assigns the user to their mobile device (smartphone, tablet). For more information, see the GAT Mobile Access Management manual.

9.4 Active Directory

With the Active Directory function, the users of Matrix can be authorized using their Active Directory details as defined in their network. The advantage of this is that you do not need to create each user individually in Matrix. To use the function, you must first activate it in Matrix and assign a role to the Active Directory group that the desired users belong to.

NOTE! A corresponding license is required for this function.

9.4.1 Configuring the Active Directory function

► Select "Active Directory" from the "File" menu.

- The “Active Directory Configuration” window opens.

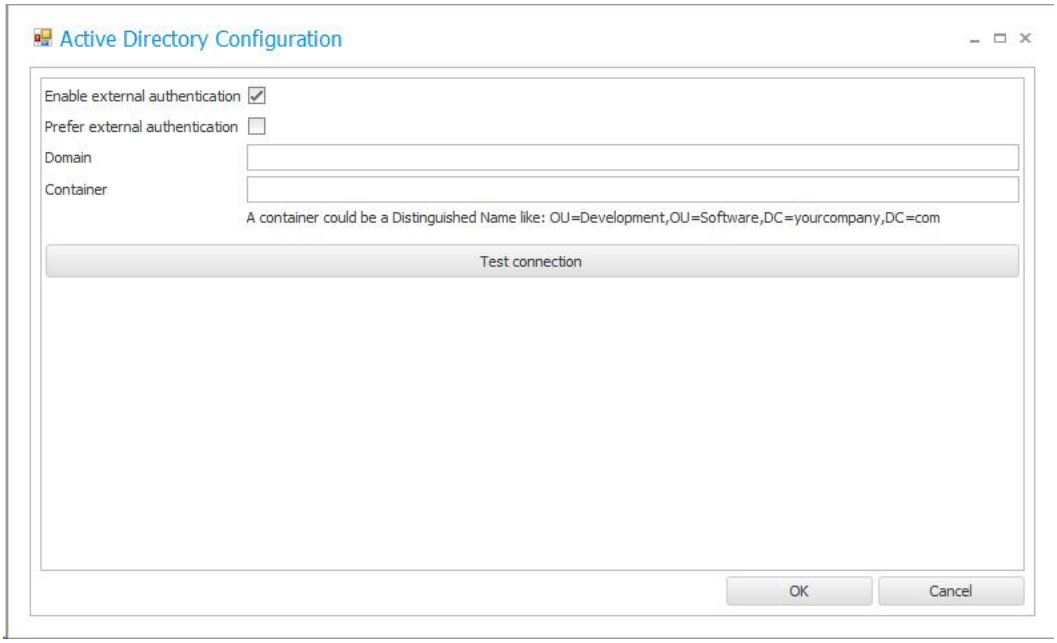


***Figure 9.4** – “Active Directory Configuration” window*

► To use Active Directory, select the "Enable external authentication" option.

► Both external authentication via Active Directory and internal user identification can be used. If you prefer to use the Active Directory for authentication, select the "Prefer external authentication" option.

► In the "Domain" field, enter the name of the network domain.

► Click on "Test connection".

- All Active Directory groups are displayed in their domain.

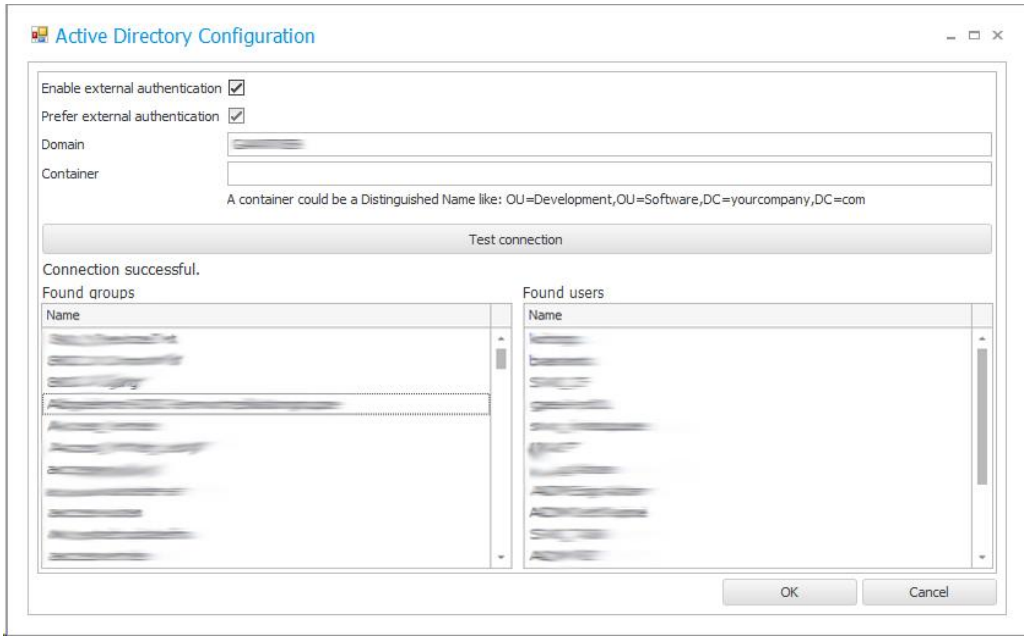


***Figure 9.5** – Active Directory groups and users*

- ► When you select a group, the users in this group are displayed on the right.
- ► Right-click on a group name that contains the users who can log into Matrix.
    - o A pop-up menu with "Use this Distinguished Name" is displayed.
- ► Select this menu item.
    - o The group is entered as a Distinguished Name in the "Container" field. As a result, only this group name is displayed during role definition. Otherwise, all groups are shown in the Active Directory.
- ► Confirm with "OK".
- ► You now have to create a role. To do this, select "Role management" from the "File" menu.
- ► Create a new role via the "Add role" button or edit an existing role via the "Edit role" button.

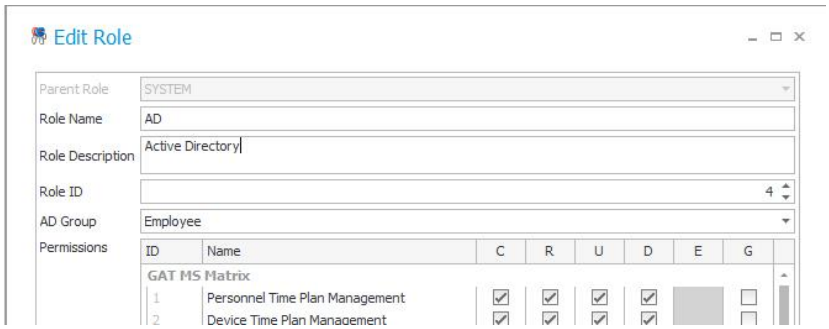


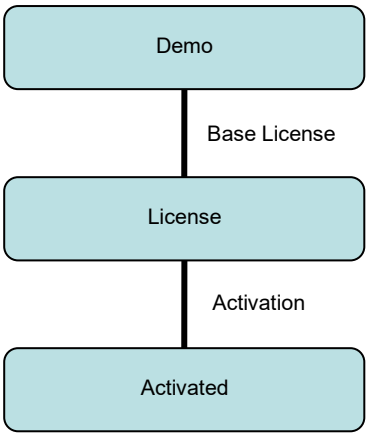
***Figure 9.6** - Assigning a group from Active Directory to a role*

- ► In the "AD Group" field, select the desired group from the Active Directory.
- ► Define the rights for the users.
    - o The users in the selected group now have the rights defined in the role and can log in to Matrix using their usernames and passwords.

10. LICENSE MANAGEMENT

The functions that can be used in Matrix are managed through licenses. A license contains information about, e.g., whether a function can be used in the software or how many terminals you are allowed to manage. If no valid license is provided for a certain function, the settings in the authorization system will have no effect, since the function cannot be used because of the missing license. For the acquisition of a license, please contact your reseller.

To begin, Matrix is set to run in demo mode. In this mode, only certain functions can be used. The default values of the functions that can be licensed will apply, as stated in the following paragraphs. The software has to be licensed within14 days of installation at the latest. Otherwise, the software will refuse to run.



Licensing the software is achieved by a base license that can be purchased from your reseller. The base license includes the number of online / offline doors and additional functions that can be managed. After the license key extension of the software, you can use the software for another 14 days before you need to activate the software. An activation code is required for activation. The activation code is bound to your computer using a hardware ID, whereas the hardware ID allows a unique identification of your computer. Activation can be completed automatically online (see "10.4 Product activation").

NOTE! The hardware ID does not contain any data about the configuration of your computer.

Besides the base license, you can acquire extension licenses that allow the usage of further functions of the software (e.g., report generator). Extension licenses do not require activation.

10.1 License overview

The following functions in Matrix can be licensed:

Base license
- Number of online and offline doors (default: 1 online door)

Expansion licenses

- RW and Additional Functions:	Additional functions including the CardNET function, additional number of controllable doors, and the report designer.
- Door Management:	For door control.
- Export Plugin:	See "12 MATRIX EXPORT".
- Multi-Site Capability:	See "5.9 Multi-site policy".
- SAP Interface:	A license for importing in the SAP CC1 format and a license for the SAP HRPDC format are available (see "5.7.2 Importing via SAP).
- LDAP Integration:	Active Directory interface (see "9.4 Active Directory").
- TBS Integration:	Interface for integrating the TBS biometric reader and software (see "5.6.8 TBS system (biometrics)").
- License Plate Recognition:	Vehicle license plate as data carrier (see "5.6.10 Settings for license plate recognition").

To show the license overview window, choose “Help" → "License Information”. The window as shown in Figure 10.**1** will appear. The window shows the base license, the hardware ID of your computer as well as the activation code. In addition, you see the time remaining until licensing / activation of your software is required.

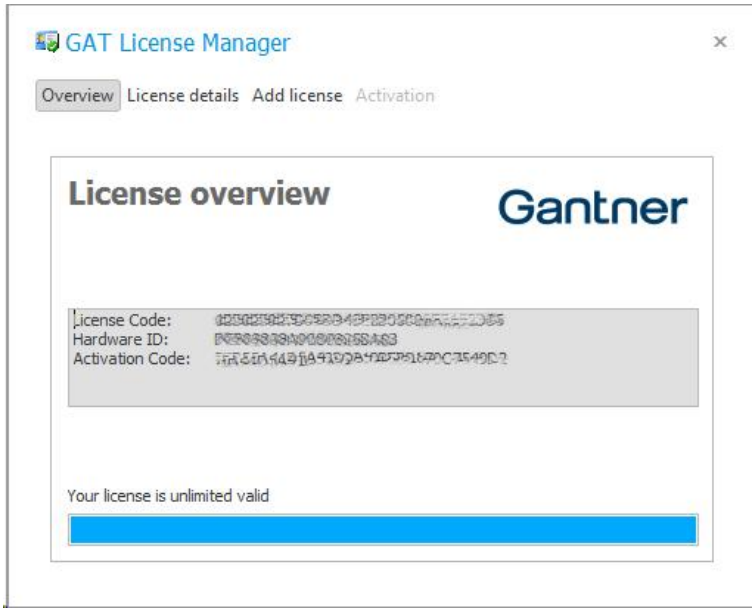


Figure 10.1 *- License overview*

10.2 License details

Choosing “License details” from the toolbar will show the following window where all the licenses acquired will be shown.

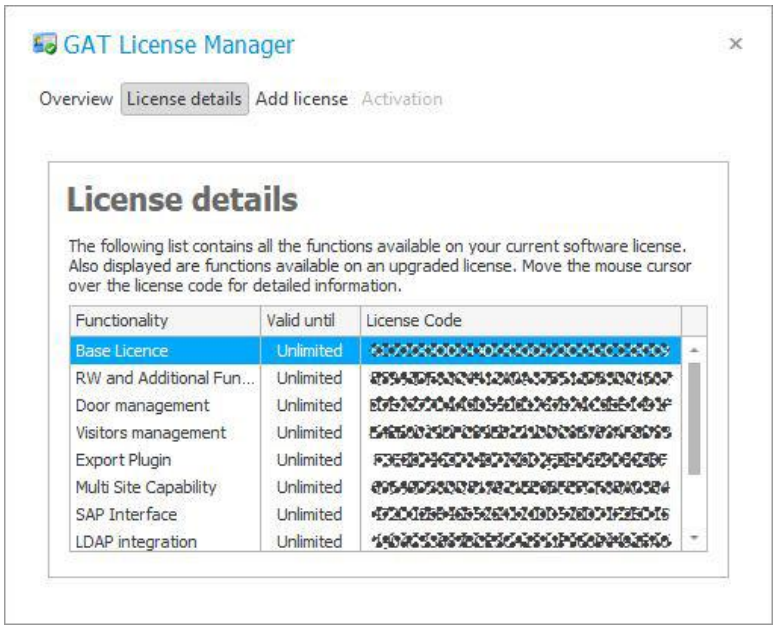


Figure 10.2 *- License details*

For each function that can be licensed, the corresponding license code will be shown. “Functionality” in this context stands for a collection of simple functions that can be licensed by a single license code.

Moving the mouse over the license code will show these simple functions (e.g., Online Door Limit, Report Generator, etc.) and their state (e.g., enabled disabled, etc.).

10.3 Adding licenses

The button “Add license” is used to add new license codes to the software.

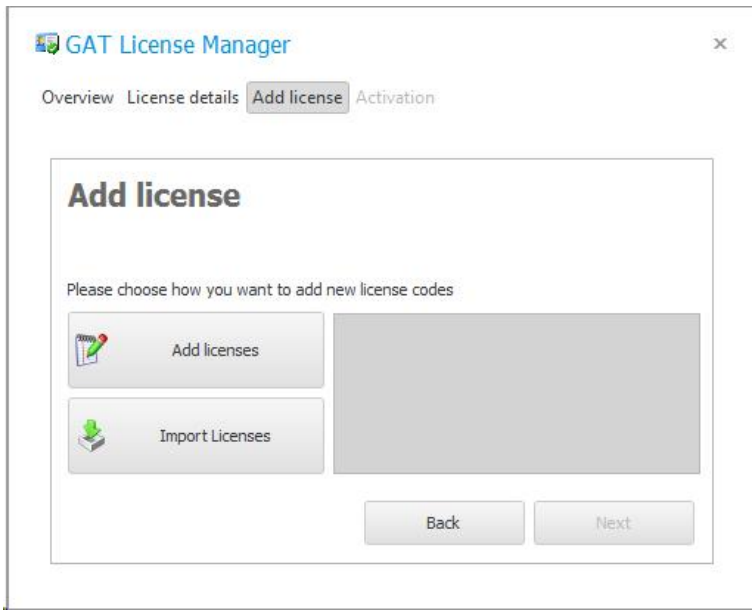


Figure 10.3 *- Adding licenses*

You can either choose “Add Licenses” and afterwards enter all the license codes in the textbox, or otherwise choose “Import Licenses” and select the license file received from your reseller.

With additional licenses, e.g., for door control, it is possible that the license is only valid for a certain period, e.g., until the end of 2020. This is shown in the license details window (see Figure 10.2).

10.4 Product activation

The button “Activation” is used to activate Matrix.

NOTE! It is not possible to work with Matrix if the software is not activated within the 14-day period.

Activation is possible online or by phone (see the following steps for both options).

► For **online activation**, select "I would like to activate my product over the internet" and click "Next".

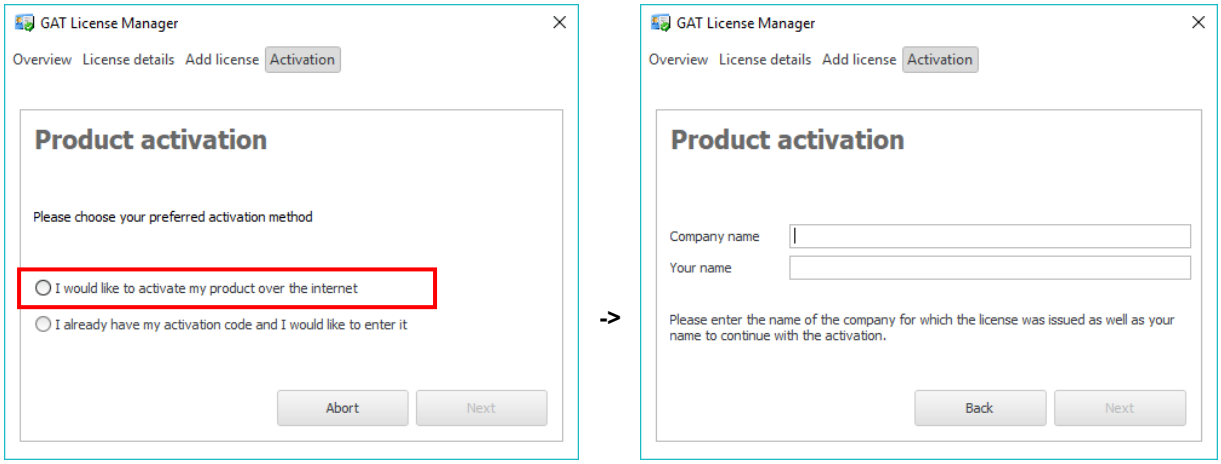


Figure 10.4 *- Product activation online – Steps 1, 2*

► Enter the name of your company and the responsible person and select "Next".

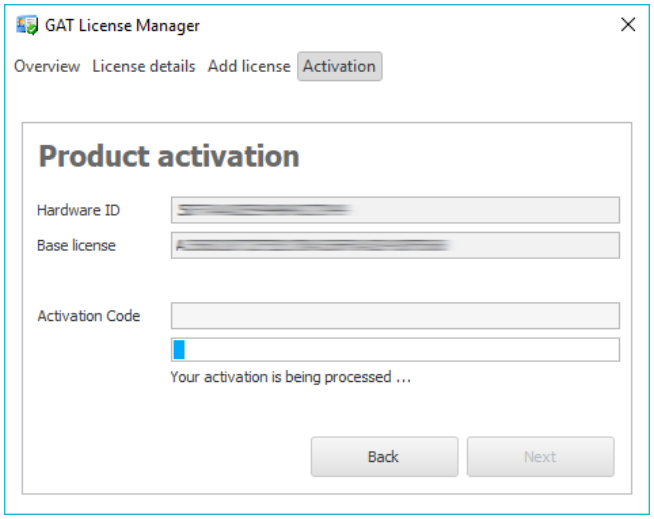


Figure 10.5 – *Product activation online – Step 3*

- Here you will see the hardware ID number of your installation and the base license code. The activation code is automatically requested from the GANTNER license server.

► If the query does not work (e.g., if the license server cannot be reached), the following window is displayed.

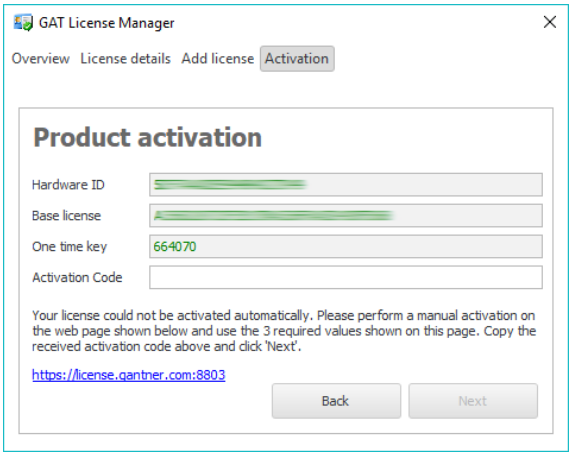


Figure 10.6 – *Product activation online – Step 4*

- A code is displayed in the "One time key" field that is only valid for a short time. You can use this code to complete the activation manually.

► Open the website of the GANTNER license server by clicking on the displayed link or enter the address "https://license.gantner.com:8803" manually in a browser.

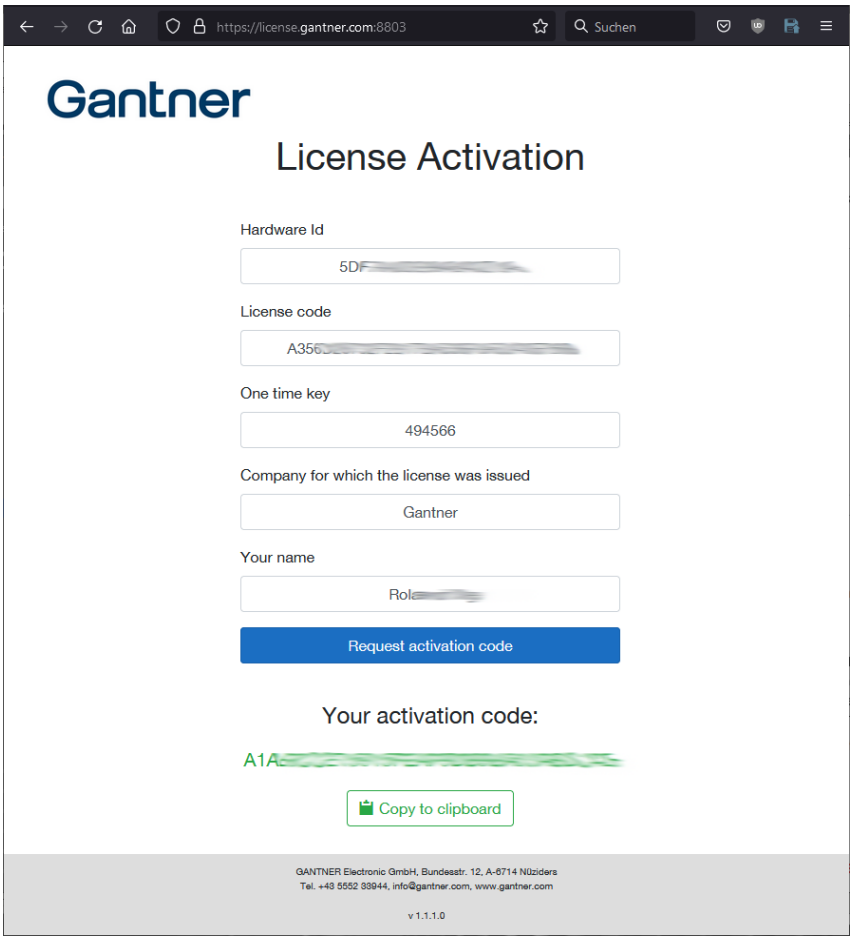


Figure 10.7 – *Product activation online – Step 5*

► Enter the information here as displayed or entered in Matrix and select "Request activation code".
  ○ The activation code is generated and displayed.
► Copy this code into the activation window in Matrix (see step 4) and confirm with "Next".
  ○ If entered correctly, Matrix is now activated, and a corresponding notification is displayed.

► For **telephone activation**, select "I already have my activation code and I would like to enter it" and click "Next".

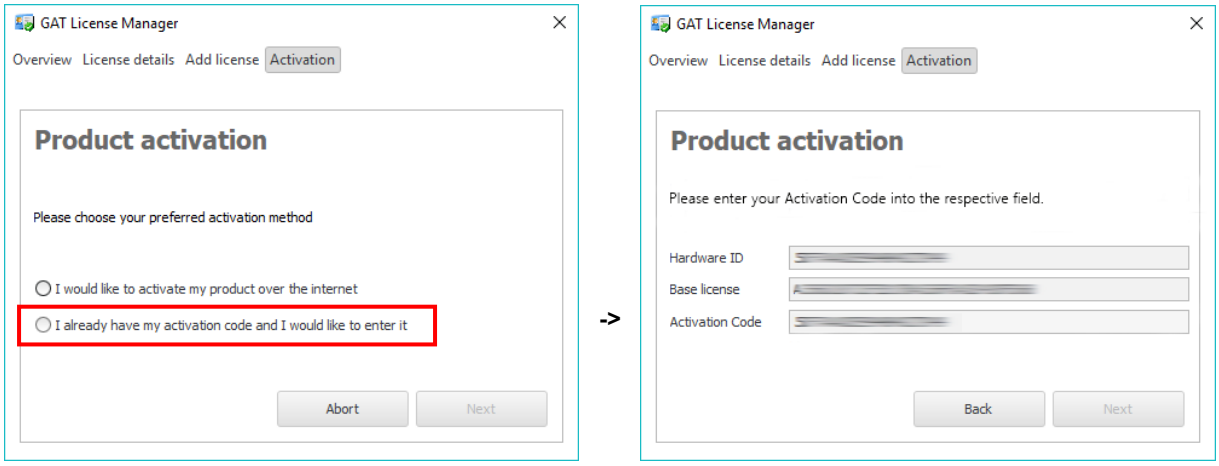


Figure 10.8 – *Product activation via telephone activation code*

► You will receive the activation code after sending your base license and hardware ID (first two fields in the window) to your sales partner.
  ○ After receiving the activation code, enter it into the "Activation Code" field then press "Next". If the code was entered correctly, Matrix is activated.

10.5 Licensing for SALTO doors

When using SALTO doors, they do not have to be included in the Matrix license.

However, a corresponding license for the ProAccess SPACE software is required for the SALTO doors. This license must consist of a general license such as "SPAONLINE", which includes at least option 0008 "Automatic Key Assignment" and option 0018 "SHIP Interface". Depending on the customer's needs, additional options can/must be added (e.g., 0033 "BlueNET").

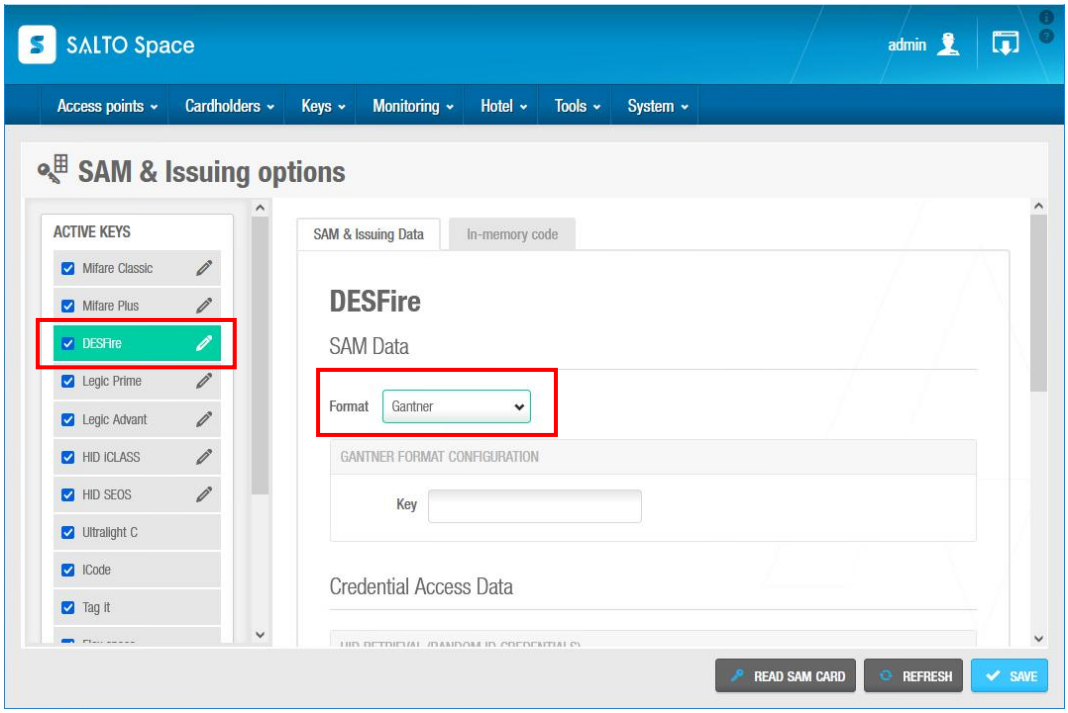
The following figure shows an overview of the licenses available for ProAccess SPACE. For the most up-to-date information on ProAccess SPACE licensing, please refer to the ProAccess SPACE documentation.

		SPABASIC	SPAONLINE	SPAIDSYS	SPAPART	SPADEMO	SPATRIAL
	Users	4 000 000	4 000 000	4 000 000	4 000 000	20	4 000 000
	Doors	65 000	65 000	65 000	65 000	20	65 000
	Expiration period	No expiry	No expiry	No expiry	No expiry	No expiry	90 days
Functions							
	OPT-Nr						
Lockers	0001	Included	Included	Included	Included	Included	Included
Online Monitoring	0004	Included	Included	Included	Included	Included	Included
Lockdown	0005	Not included	Included	Included	Included	Included	Included
Antipassback	0006	Not included	Included	Included	Included	Included	Included
Event Stream	0007	Not included	Included	Included	Included	Included	Included
Automatic Key Assignment	0008	Not included	Included	Included	Included	Included	Included
Roll Call	0009	Not included	Included	Included	Included	Included	Included
Limited Occupancy	0010	Not included	Included	Included	Included	Included	Included
Card printing module	0012	Not included	Not included	Included	Included	Included	Included
Visitors management	0013	Possible add-on	Possible add-on	Included	Included	Included	Included
Department Operator	0011	Not included	Not included	Not included	Included	Included	Included
Locations & Function	0015	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Mobile users module	0016	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Database Synchronization	0017	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
SHIP Integration	0018	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Graphical Mapping compatibility	0019	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
SAM Custom Keys	0020	Included	Included	Included	Included	Included	Included
SAM Custom Keys defined by user	0029	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Not included	Not included
RFnet wireless	0021	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Alarms & Communication	0032	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
SALTO BLUEnet wireless	0033	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Elevator integration feature	0035	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
SALTO BLUEnet wireless Lockers	0036	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Attendance Reporting	0037	Not included	Included	Included	Included	Included	Included
Hotel module	0022	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
BAS Integration	0023	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included
Mobile Guest Keys	0028	Possible add-on	Possible add-on	Possible add-on	Possible add-on	Included	Included

Table 10.1 *- Licenses for ProAccess SPACE*

If SALTO doors are also to be displayed and controlled in Matrix Door Management ("Door Control"), the number of SALTO doors must be considered in the Door Management license.

NOTE: If SVN data carriers are used and the correct type is selected ("SVN GANTNER") in ProAccess SPACE, the options 0020 and 0029 are no longer required.



11. PERSONS IMPORT SERVICE

The person import service is used to execute an automatic import of persons to Matrix. The import will also be executed if Matrix is not running since the application is running as a windows server. Further, the service can immediately load the imported persons to GAT ACE and, if used, ProAccess SPACE. The persons can immediately access the doors since their access rights are inherited from the person group that they were imported to.

For the installation of the person import service you have to execute the "`SetupPersonImportService.exe`" file and follow the instructions of the setup wizard. The installation of the import service must not be on the same computer as the one where Matrix is installed. It is only important that the computer, on which the service is installed, has access to the file containing the persons that should be imported and also to the synchronization directory with GAT ACE / ProAccess SPACE.

The setup will then install a service called "Matrix - Person Import Service" on your system. In the service control center, you can modify the settings (user account the service is running) according to your needs.



Figure 11.1 *- Details of the windows service control center with the Matrix - Person Import Service*

In the next step you have to configure the database settings of the service. Therefore, start with configuring the database settings for Matrix. Afterwards, you copy the file "hibernate.cfg.xml" from the user's application data directory:

From Windows 8: `C:\Users\%%username%%\AppData\Roaming\GAT\Matrix`
From Windows Server 2008: `C:\Users\%%username%%\AppData\Roaming\GAT\Matrix`

To the installation directory of the import service:

For 32-bit Windows: `C:\Program Files\GAT\Matrix - Person Import Service`
For 64-bit Windows: `C:\Program Files (x86)\GAT\Matrix - Person Import Service`

The configuration of the service is now complete.

For further configuration of the import service, you can use Matrix as explained in chapter "5.7 Import persons". The service will automatically apply the settings once you change them in Matrix.

NOTE! For the Matrix Import Service (for personnel and booking import) the settings of Matrix are used for the connection to the database server and for the database authentication mode. For this reason, it is recommended to use the "Mixed Mode (SQL Server Authentication and Windows Authentication)" for the registration at the SQL server. If this is not possible and the Windows details for user login are used (e.g., with Active Directory), then the Matrix Person Import Service must run under the same Windows user and not with the default "System" user. For more information see chapter "3 INSTALLATION" and Appendix A.

12. MATRIX EXPORT

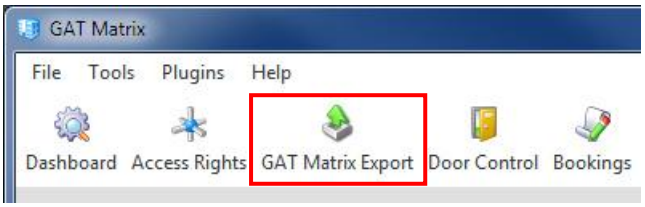
The Matrix Export plugin allows you to export usage reports for services used in the access system, e.g., for parking or food expenses. This is done by calculating the number of entries into the parking garage or the food expenditures using a terminal or reader.
An additional function of the export plugin is the ability to export the Matrix personnel data to a file.

► To install the Export plugin, run the "`setup.exe`" file in the "`GAT-Matrix-Export_Vxxxxxx`" directory found on the installation data carrier.
  ○ The installation wizard starts, which guides you through the installation.



***Figure 12.1** - Installation of the Matrix Export plugin*

► Click on "Next" and follow the instructions. You can click on the "Next" button to install the plugin with the default settings. The export plugin is installed in the Matrix directory (default: `C:\Program Files (x86)\GAT\Matrix\Plugins`).
► If Matrix is already running, exit Matrix.
► Start Matrix and log in.
  ○ The “Matrix Export” icon is displayed in the toolbar.



► Click on the “Matrix Export” icon.
  ○ The Matrix Export plugin starts.

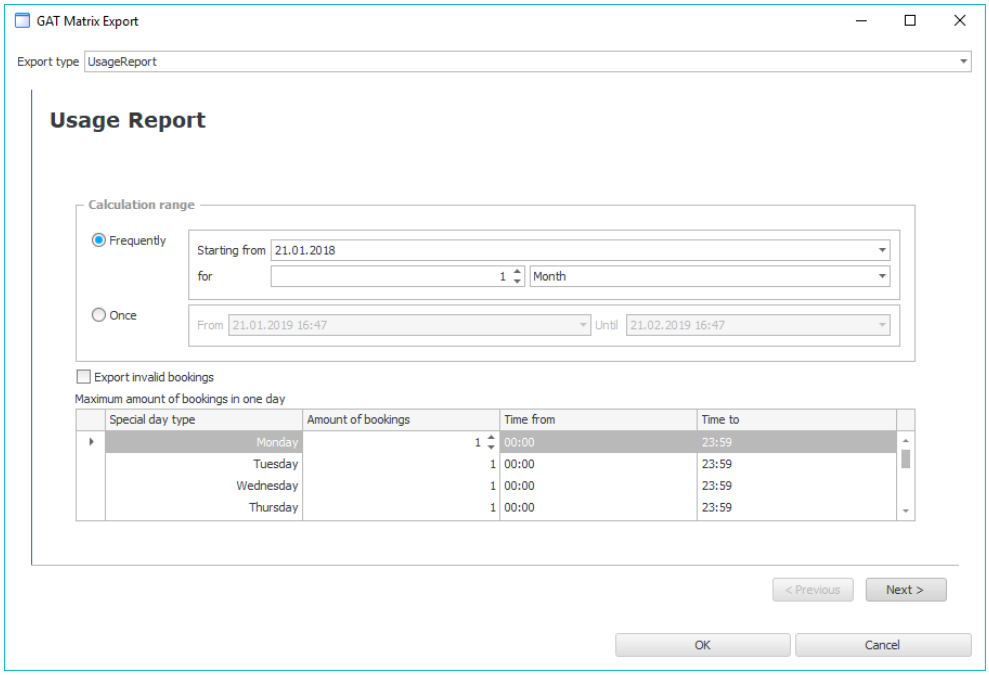


***Figure 12.2** - Matrix Export – Main window*

There are three export types available:

- "Usage Report" = Export of the usage report
- "Person Export" = Export of the personnel data
- "EcoLockManagerExport" = Export of personnel data in a .csv file for use with GAT ECO.Lock Manager software.

For all export types, different settings, such as the type of exported data, the selection of the export file, and the export time, etc., are available. These settings are defined on different windows, which are explained in the following pages. The settings are saved so that they do not have to be re-entered when the export plugin is used again.

12.1 Usage report

This type of export contains the bookings made by persons at selectable devices during a selectable period, thereby allowing you to calculate, e.g., parking usage or food expenses.

► Select "UsageReport" in the "Export type" field.

► In the "Calculation range" field, select the period during which the usage number is counted and totaled.

- Frequently: Counting is from the date entered for the period entered in the field below (in picture = 1 month).
- Once: Here you can define a calculation period with a specific start and end date.

- ► The "Export invalid bookings" option allows you to also export invalid bookings, e.g., if the personnel number is missing or not valid. When this option is not selected, these invalid bookings are not exported.
- ► In the "Maximum amount of bookings in one day" field, you can specify the maximum number of bookings per calendar day (weekdays and special days). In addition, a period can also be defined per day that calculates only the bookings in this period.
  Parking Use Example: When a value of 1 is set for each weekday (Monday to Friday) and 0 set for Saturdays, Sundays, and special days, this means that one parking garage entry is counted per day, even if the person enters and exits the garage several times. No parking garage entry is counted on weekends and special days. The total is then calculated from the number of entrances entered (max. 1 per weekday) for the defined period.
- ► Click on "Next".
  - ○ The following window is displayed.

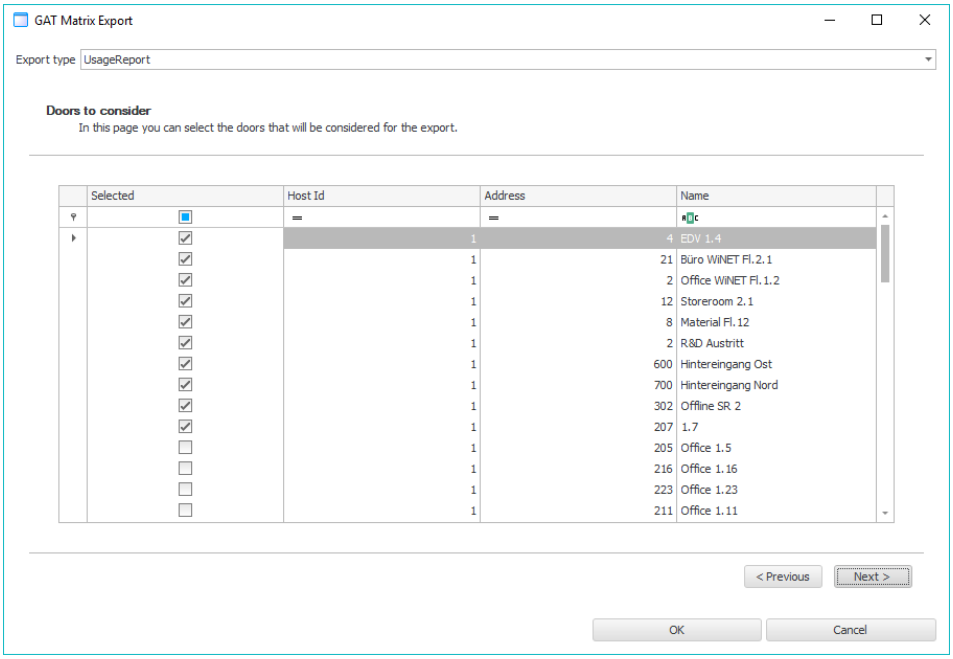


***Figure 12.3** - Matrix Export – Usage Report, settings page 2*

- ► Select the devices where use of the personal data carriers is to be counted, e.g., for parking garage entry, select the garage entrance terminal, or for food calculation, select the terminal/reader controlling the food service.
- ► Click on "Next".
  - ○ The following window is displayed.

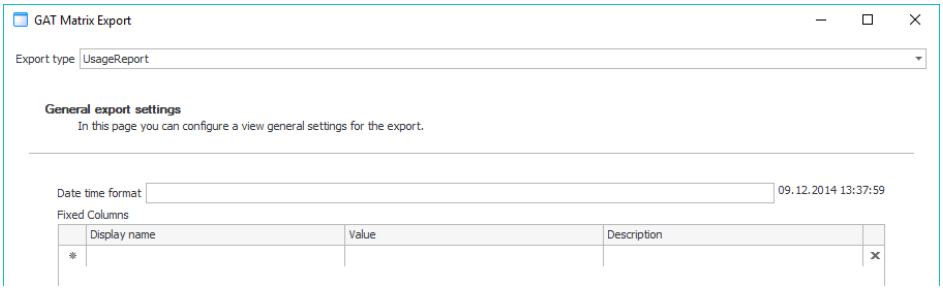


***Figure 12.4** - Matrix Export – Usage Report, settings page 3*

- In the "Date time format" field, define the formatting for the display of the date and time during export. The default formatting is used without input here. An example of the current date and time formatting is shown to the right of the input field. The formatting is entered analogously to the definition in Office programs.
  Examples: "dd.MM.yyyy hh:mm:ss" = "09.07.2017 16:40:20" or
  "ddd, d. MMMM yyyy, hh:mm" = "Tue, 9. July 2017, 16:40"
- In the "Fixed Columns" field, you can define the columns for export, which should always have a constant value. For example, in the first column, always enter "P1" for parking space 1, enter "Name1" (displayed in Matrix) and "P1" in "Display name". The column must be set as column 1 (see below).
- Click on "Next".
  - The following window is displayed.

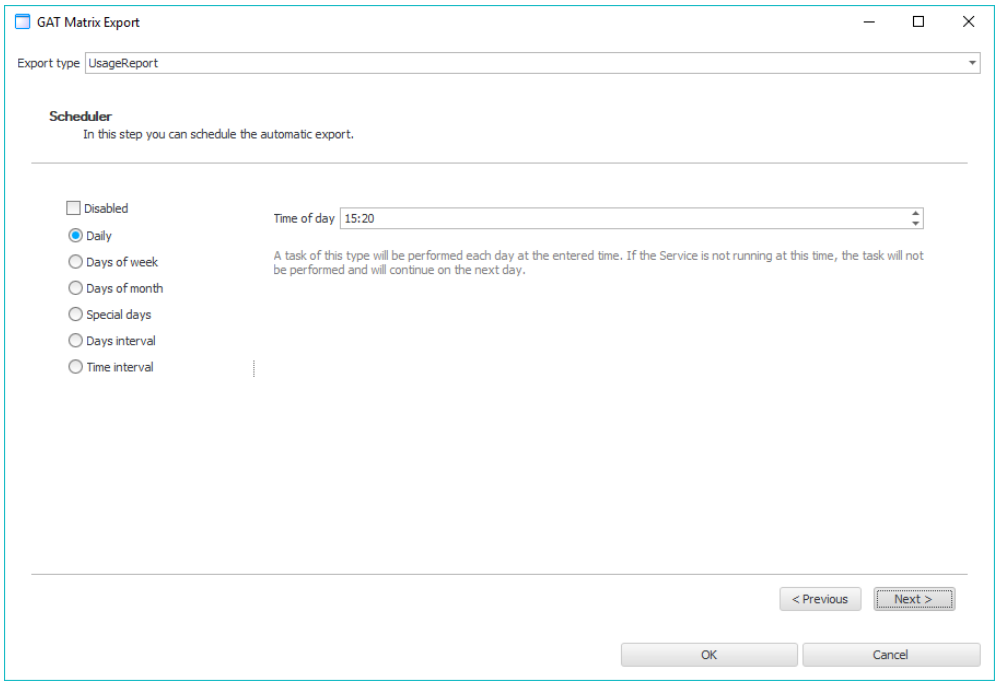


***Figure 12.5** - Matrix Export – Usage Report, settings page 4*

- Here you can set a specific time for Matrix to perform the export automatically. Select the type of period on the left and enter the desired time on the right.
- If you want to perform the export manually rather than automatically, select "Disabled".
- Click on "Next".
  - The following window is displayed.

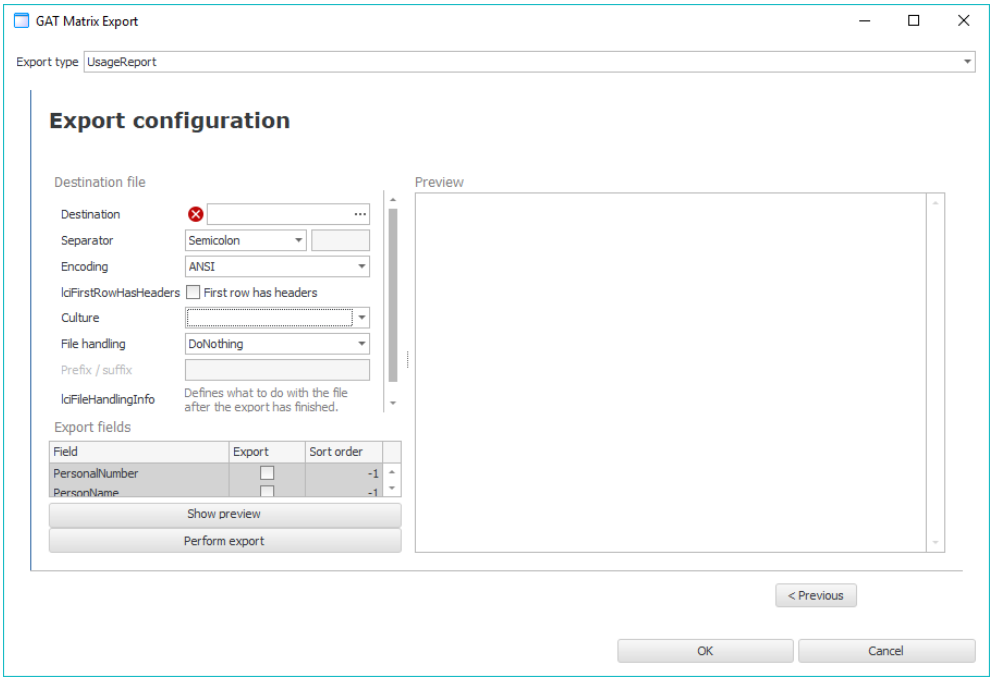


***Figure 12.6** - Matrix Export – Usage Report, settings page 5*

► Define the type of export file in the fields under "Destination file".

- Destination: Click on the "..." symbol. A window opens where you must enter a folder and file name for the export file. Matrix must have write permission for the folder.
- Separator: Select the character for separating the individual columns in the export file. By selecting "[Other]", you can enter a specific separator in the field to the right.
- Encoding: Select the type of character encoding for the export file (ANSI, Unicode, or ASCII).
- lcFirstRowHasHeaders: When selected, this option enters the column headings in the first line of the export file.
- Culture: Here you can change the language of the export file (e.g., en-US for America or de-DE for Germany).
- File handling: The "DoNothing" option saves the export file as specified in the "Destination" field.
  The "Append Date and Time" option adds the date and time to the file name.
  The "Prefix / suffix" field allows you to enter characters that will be added to the beginning or end of the file name.

► Under “Export fields”, select the fields to be exported in the "Export" column. The "BookingsCount" field contains the number of bookings for each data carrier and period.

- ► You can specify the order of the fields in the export file from left to right in the "Sort order" column. The columns are ordered from left to right starting with the lowest number. The sort order is assigned automatically when the fields are selected, or you can adjust the order manually by changing the numbers.
- ► Click on "Show preview" to preview the export file in the right field.
    - ○ The individual persons or data carriers with the selected fields are displayed.

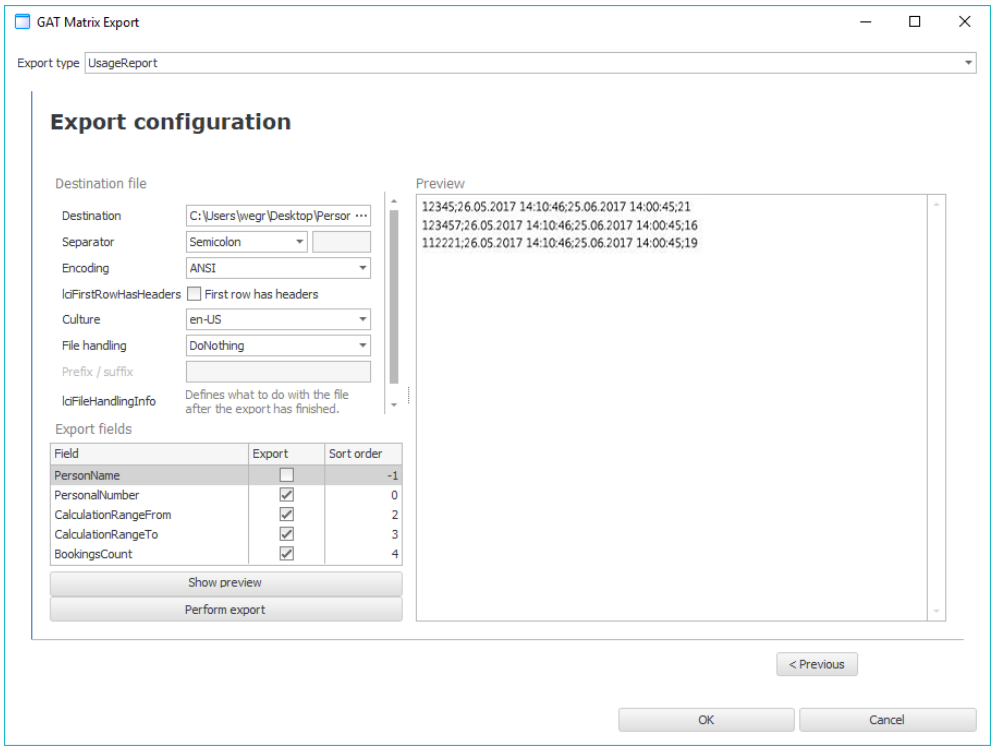


***Figure 12.7** - Matrix Export plugin – Usage Report export preview*

- ► If you want to export now, click on "Perform export".
- ► Alternatively, click on "<Previous" to scroll through the settings pages to change settings, e.g., when the preview does not look as desired.
- ► Press "OK" to confirm the settings. The Matrix service will perform the export according to the settings at the specified times.

In order for the automatic export of the Usage Report to function, the Matrix service must be running and the defined directory accessible and writable.

12.2 Person export

This type of export contains all the personnel information in Matrix, which can be individually configured and exported for each person.

► Select "PersonExport" in the "Export type" field.

○ The following window is displayed.

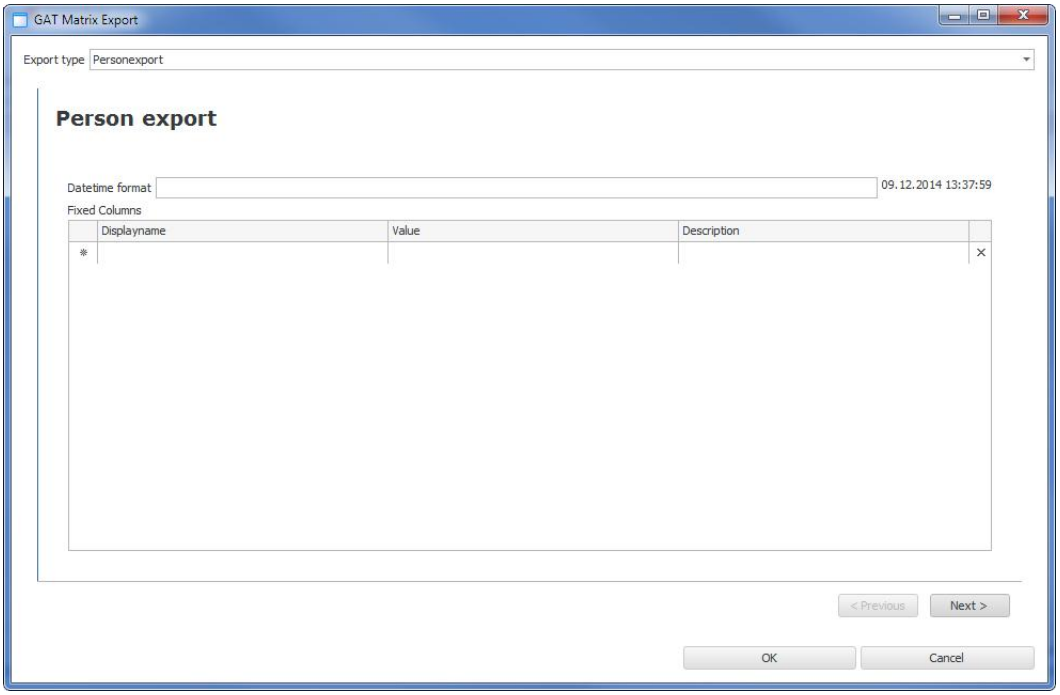


***Figure 12.8** - Matrix Export plugin – Person export, settings page 1*

► In the "Date time format" field, define the formatting for the display of the date and time during export. The default formatting is used without input here. An example of the current date and time formatting is shown to the right of the input field. The formatting is entered analogously to the definition in Office programs.
Examples: "dd.MM.yyyy hh:mm:ss" = "09.07.2017 16:40:20" or
"ddd, d. MMMM yyyy, hh:mm" = "Tue, 9. July 2017, 16:40"

► In the "Fixed Columns" field, you can define the columns for export, which should always have a constant value. For example, in the first column, always enter "P1" for parking space 1, enter "Name1" (displayed in Matrix) and "P1" in "Display name". The column must be set as column 1 (see below).

► Click on "Next".

○ The following window is displayed.

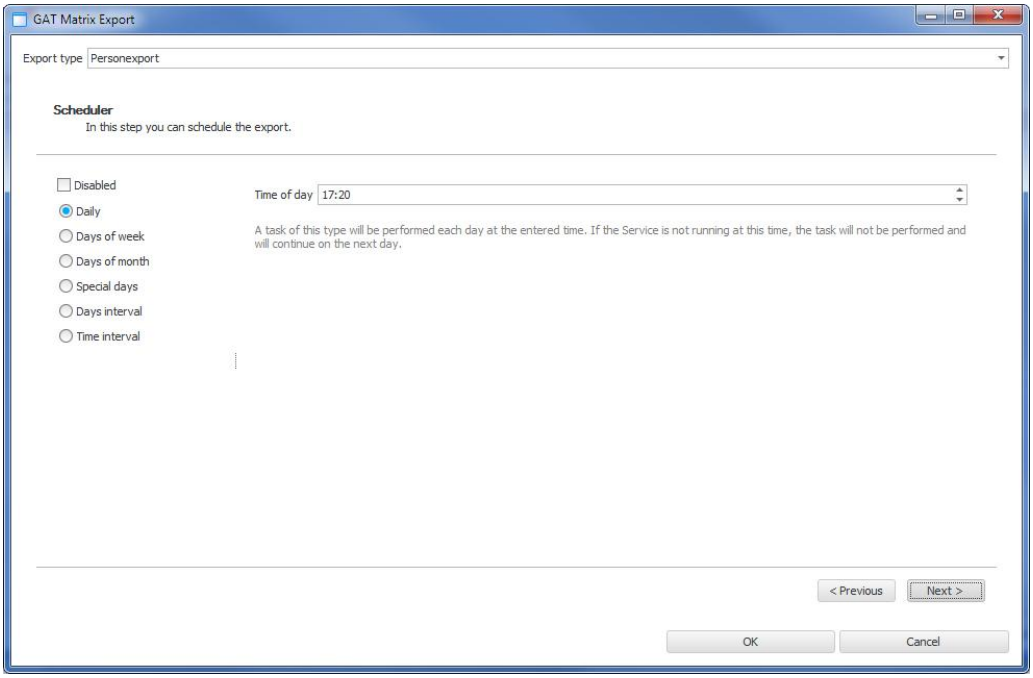


***Figure 12.9** - Matrix Export plugin – Person export, settings page 2*

- ► Here you can set a specific time for Matrix to perform the export automatically. Select the type of period on the left and enter the desired time on the right.
- ► If you want to perform the export manually rather than automatically, select "Disabled".
- ► Click on "Next".
  - ○ The following window is displayed.

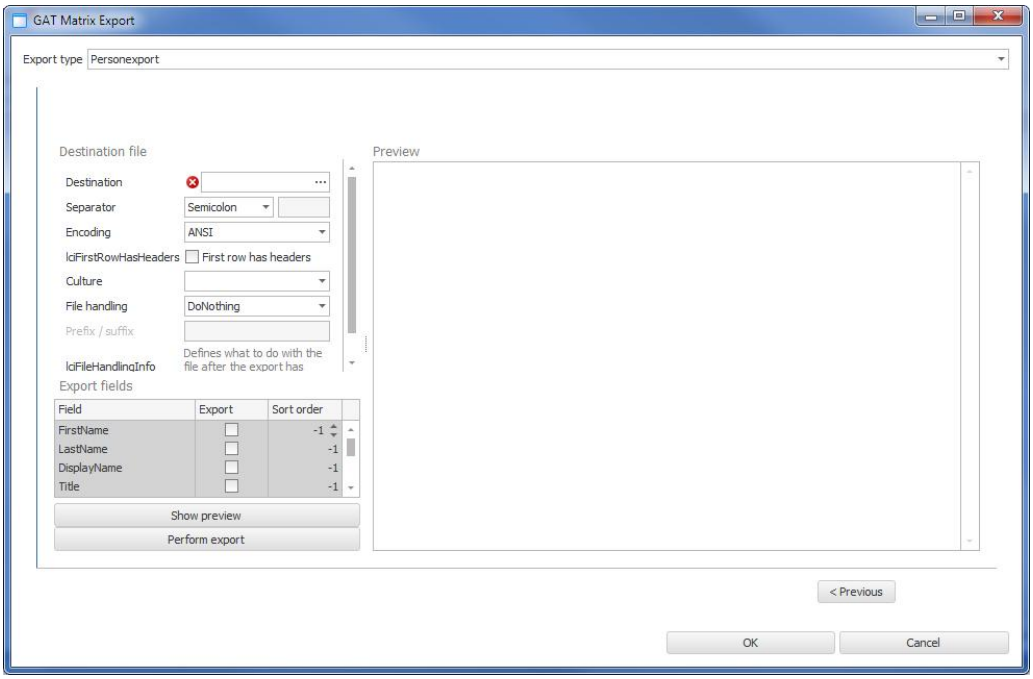


***Figure 12.10** - Matrix Export plugin – Person export, settings page 3*

► Define the type of export file in the fields under "Destination file".

- Destination: Click on the "..." symbol. A window opens where you must enter a folder and file name for the export file. Matrix must have write permission for the folder.
- Separator: Select the character for separating the individual columns in the export file. By selecting "[Other]", you can enter a specific separator in the field to the right.
- Encoding: Select the type of character encoding for the export file (ANSI, Unicode, or ASCII).
- IcFirstRowHasHeaders: When selected, this option enters the column headings in the first line of the export file.
- Culture: Select here the language of the export file (e.g., en-US for America or de-DE for Germany). If the date format was entered manually in the previous window (Figure 12.8), it has a higher priority and the Culture setting selected here will be ignored for the date.
- File handling: The "DoNothing" option saves the export file as specified in the "Destination" field.
  The "Append Date and Time" option adds the date and time to the file name.
  The "Prefix / suffix" field allows you to enter characters that will be added to the beginning or end of the file name.

► Under “Export fields”, select the fields to be exported in the "Export" column.

► You can specify the order of the fields in the export file from left to right in the "Sort order" column. The columns are ordered from left to right starting with the lowest number. The sort order is assigned automatically when the fields are selected, or you can adjust the order manually by changing the numbers.

► Click on "Show preview" to preview the export file in the right field.

○ The individual persons or data carriers with the selected fields are displayed.

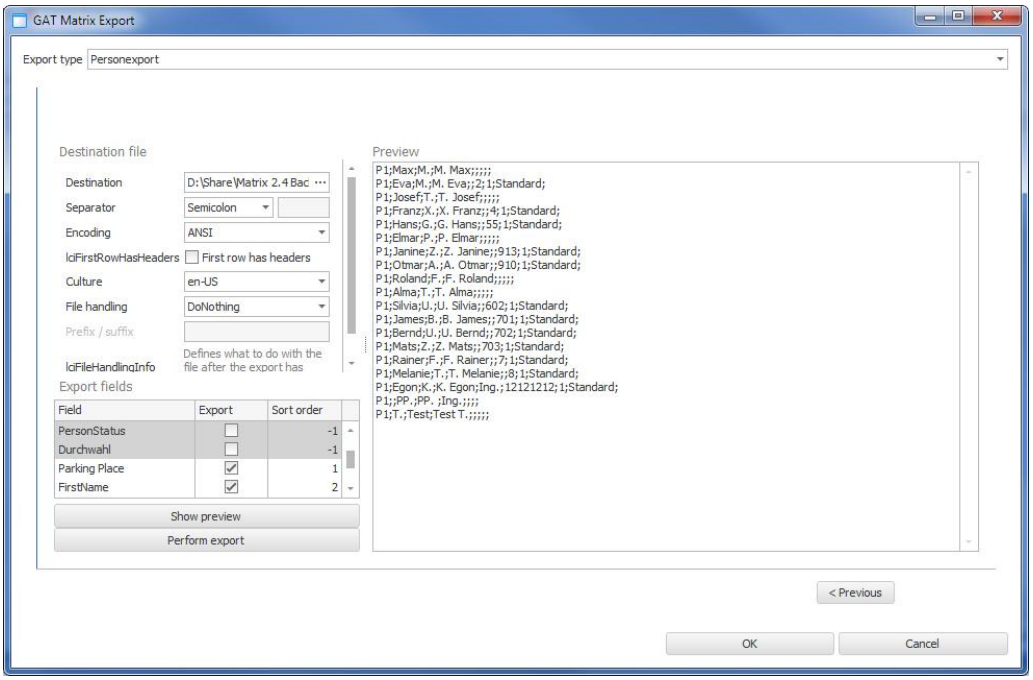


***Figure 12.11** - Matrix Export plugin – Person Export preview*

- ► If you want to export now, click on "Perform export".
- ► Alternatively, click on "<Previous" to scroll through the settings pages to change settings, e.g., when the preview does not look as desired.
- ► Press "OK" to confirm the settings. The Matrix service will perform the export according to the settings at the specified times.

In order for the automatic export of the Usage Report to function, the Matrix service must be running and the defined directory accessible and writable.

12.3 Exporting the personnel data for GAT ECO.Lock Manager

This type of export contains all the personnel information in Matrix. This data is saved in a .csv file that is formatted to be used with the GAT ECO.Lock Manager software.

- ► Select "EcoLockManagerExport" in the "Export type" field.
  - ○ The following window is displayed.

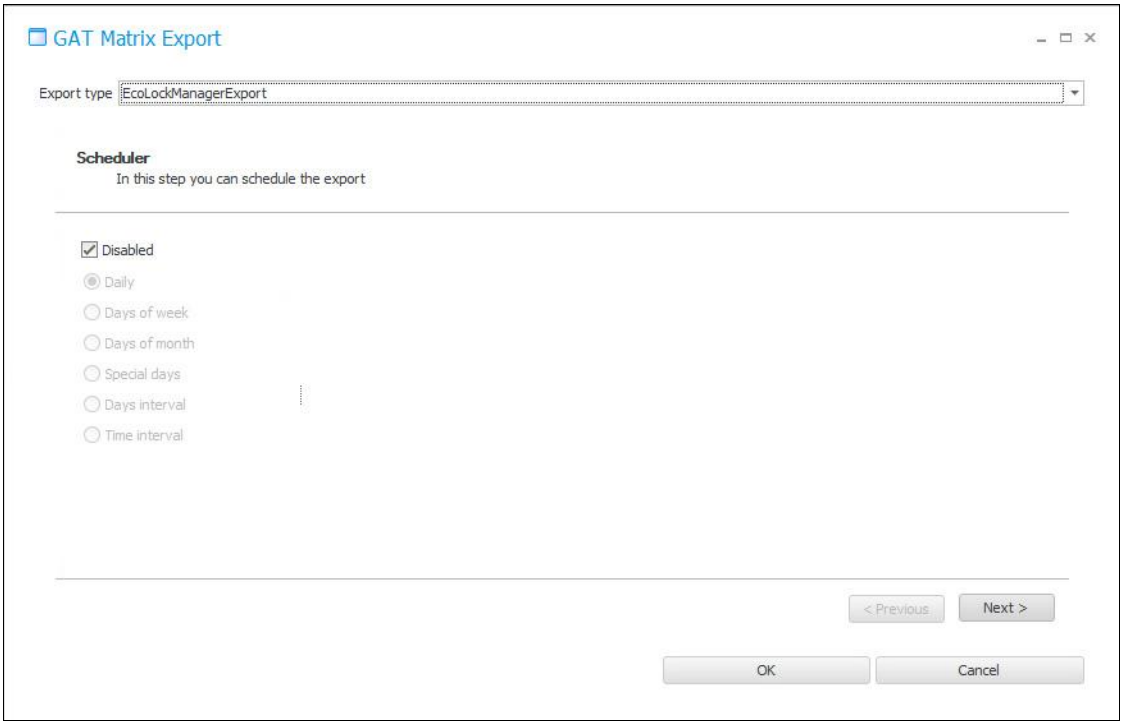


***Figure 12.12** - Matrix Export plugin – GAT ECO.Lock Manager Export, settings page 1*

- ► Here you can set a specific time for Matrix to perform the export automatically. Select the desired time interval on the left and enter the time on the right.
- ► If you want to perform the export manually rather than automatically, select "Disabled".
- ► Click on "Next".
    - ○ The following window is displayed.

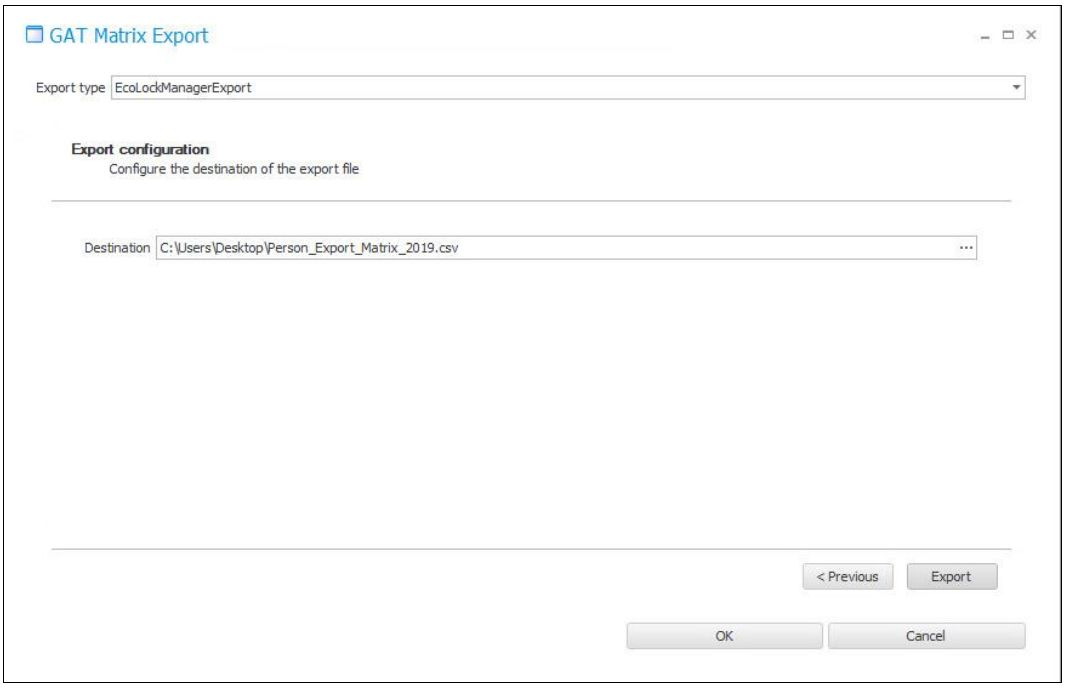


Figure 12.13 *- Matrix Export plugin – GAT ECO.Lock Manager Export, settings page 2*

- ► Define the path and file name for the export file in the "Destination" field. You can enter this information manually or click on the "..." symbol, which opens a window where you can enter a folder and file name for the export file. Matrix must have write permission for the folder.
- ► If you want to export now, click on "Export".
- ► Alternatively, click on "<Previous" to scroll through the settings to change settings.
- ► Press "OK" to confirm the settings. The Matrix service will perform the export according to the settings at the specified times.

In order for the automatic export of the Usage Report to function, the Matrix service must be running and the defined directory accessible and writable.

13. DATA PROTECTION

13.1 General Data Protection Regulation (GDPR)

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

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

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

Definitions of Personal Data and Data Processing

Personal data includes all data that directly or indirectly allows you to draw conclusions about a specific person, e.g., email, name, photo, etc. Sensitive personal data is personal data that is particularly worthy of protection, e.g., biometric 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 access control. The following sections outline what has to be done with regard to access control and what options Matrix offers. The instructions are summarized in the following sections.

13.1.1 Perform an inventory analysis

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

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

13.1.2 Create a processing directory

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

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

In access control, GANTNER has paid attention to the **Principle of Data Minimization** and the **Principle of Purpose Limitation**. Only data that is necessary for the operation of the systems is stored. Essentially, an ID number, which is used as an identification feature, and the name of the person are stored. Other data, e.g., a PIN code or personnel number, is optional and serves to increase security or 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 time recording data is passed on to the time recording software for processing after being acquired.

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 via the user management system in Matrix by allowing only authorized persons to access the software and by limiting the software users to access only the data needed to perform their tasks.

13.1.3 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.

13.1.4 Comply with information requirements and declarations of consent

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

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

The data storage period depends on the requirements for access traceability as well as the present/absent bookings that you need in your company. By deleting data, the **Principle of Storage Limitation** can be met.

Available from version 4.1 of Matrix onwards are three important options that meet the requirements of the GDPR:

- From version 4.1, it is possible to automatically delete the access bookings after a configurable time period. For the deletion, it can be defined whether personal bookings or system-related bookings are deleted. Different time periods can be set for both types of bookings.
- The log recordings for user activities can also be deleted after a configurable time period.
- The right to be forgotten was also considered. For example, personal data is completely deleted from the database when it is deleted. Previously, the persons were set to inactive so that the correct names for the display of bookings were still available. In version 4.1, it is possible that a name is not displayed if the booking creation and the deletion of the person overlap in time.

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

In summary, we would like to point out that with Matrix version 4.1 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.

APPENDIX A: INSTALLATION OF SQL SERVER

This section outlines the most important points for the installation of Microsoft® SQL Server® 2019 Express. To configure them, you can use MS SQL Server Management Studio Express, which can be downloaded from the Microsoft homepage. Database servers allow many more configuration options. Contact your database administrator for advanced configuration settings.

Matrix requires a database server with database for storing personnel data, etc. You can use a free Express version of Microsoft SQL Server. The Microsoft® SQL Server® 2019 Express version is included with the Matrix installation package. It is also possible to use an existing database server for Matrix.

NOTE! It is recommended to install Microsoft SQL Server Management Studio to create an ideal environment for Matrix support and maintenance tasks.

The installation of the Microsoft SQL Server can be completed during the installation of Matrix or by clicking on a separately downloaded setup file. The installation assistant will guide you through the installation of Microsoft SQL Server.

After confirming the license conditions, the "Setup Support Files" are installed, and the installation wizard opens. The individual installation steps are displayed to the left and the editable settings for the current installation step are displayed in the middle of the window. First, you are asked whether you want to use Microsoft Update to check for updates. It is recommended to select this option. Then click "Next".

► The following window opens with a selection of components to install ("Feature Selection").

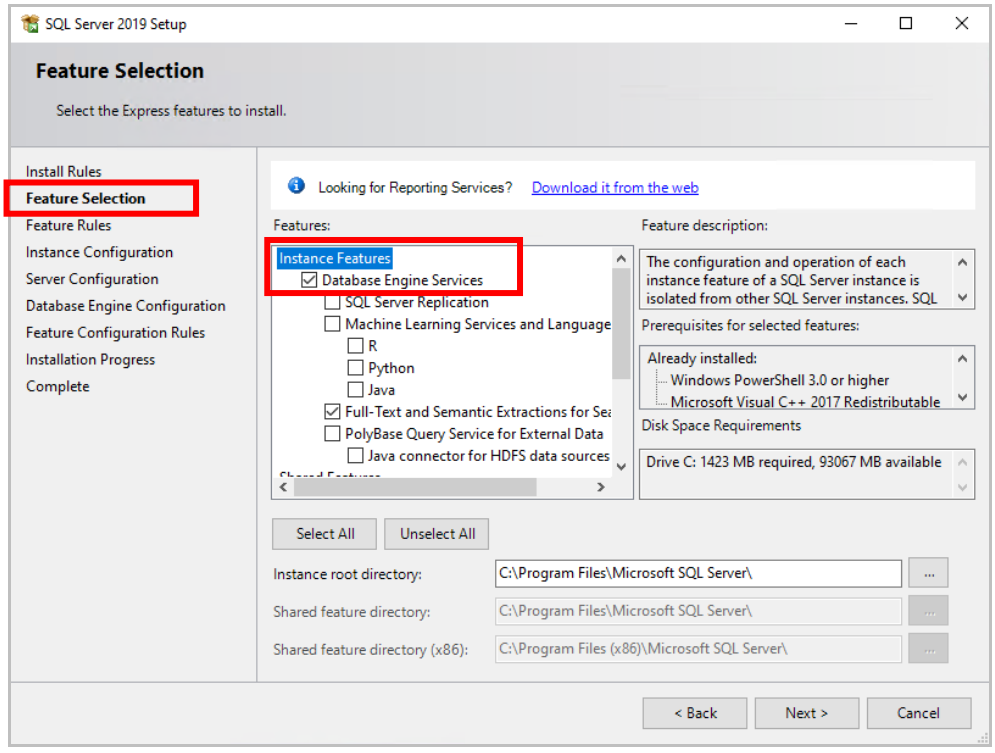


***Figure A.1.** – Microsoft SQL Server 2019 Express – Installation options*

► Here it is important to enable the option "Database Engine Services". This will install the SQL Server as a Windows service.

► Click on "Next >" until the following window is displayed ("Instance Configuration").

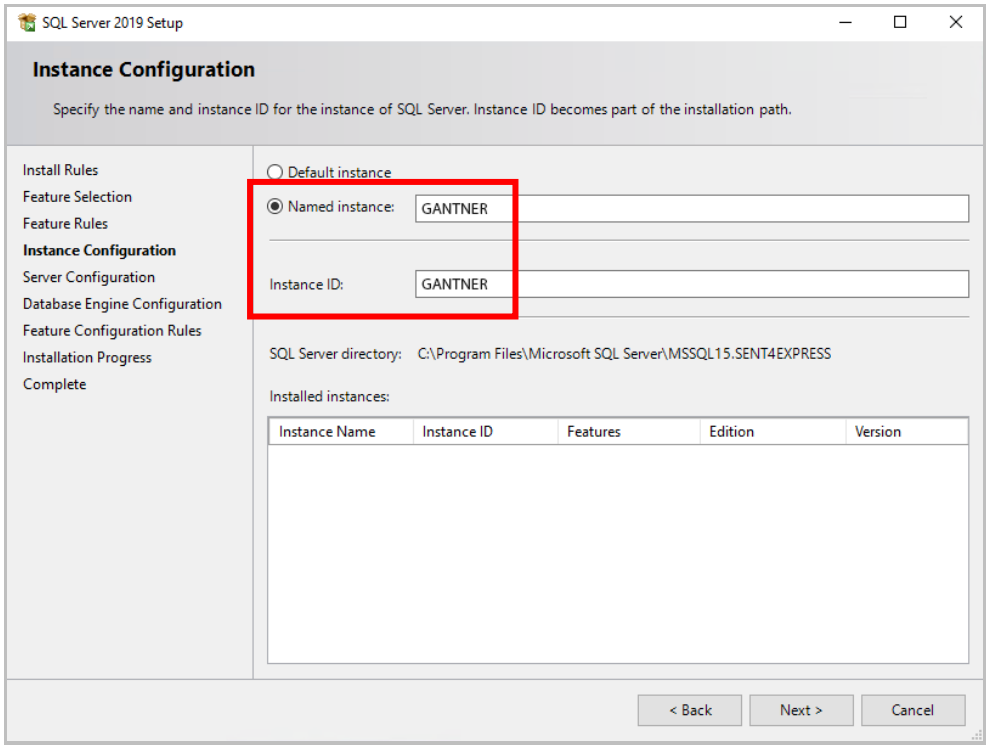


Figure A.2 *– Microsoft SQL Server 2019 Express – Instance configuration*

► GANTNER recommends that Matrix, and all GANTNER software products, has its own instance of SQL Server. To do this, enter a name for the instance in the fields "Named instance" and "Instance ID" (e.g., "GANTNER").

► Click on "Next >" until the following window ("Database Engine Configuration") is displayed.

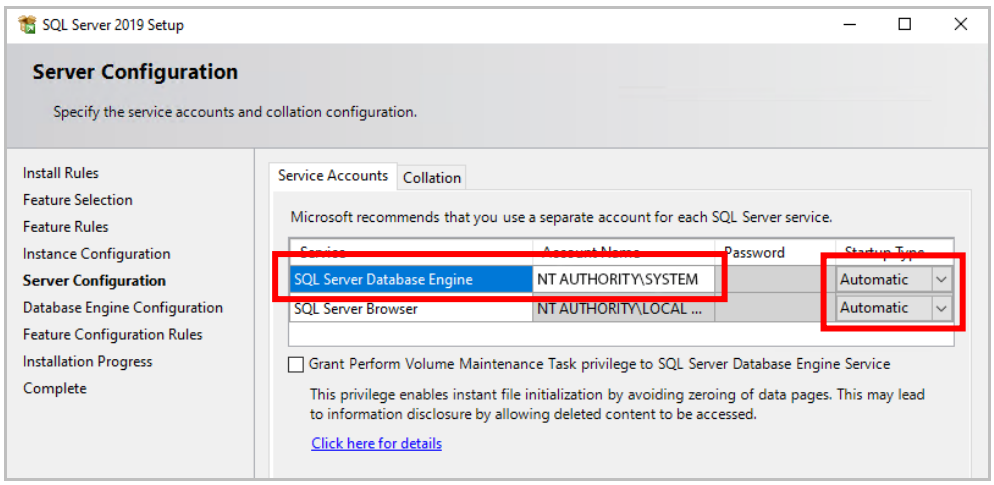


Figure A.3 *– Microsoft SQL Server 2019 Express – Server configuration*

Here, the user account, which is to run under the SQL Server, must be specified. If you have created a dedicated user account, which is to run under the SQL Server, this can be specified here. Otherwise, the account 'NT AUTHORITY \ SYSTEM" should be used. The “Startup Type” option must be set to "Automatic" to ensure that the Windows services start automatically.

Click on "Next>" to go to the next "Database Engine Configuration" window.

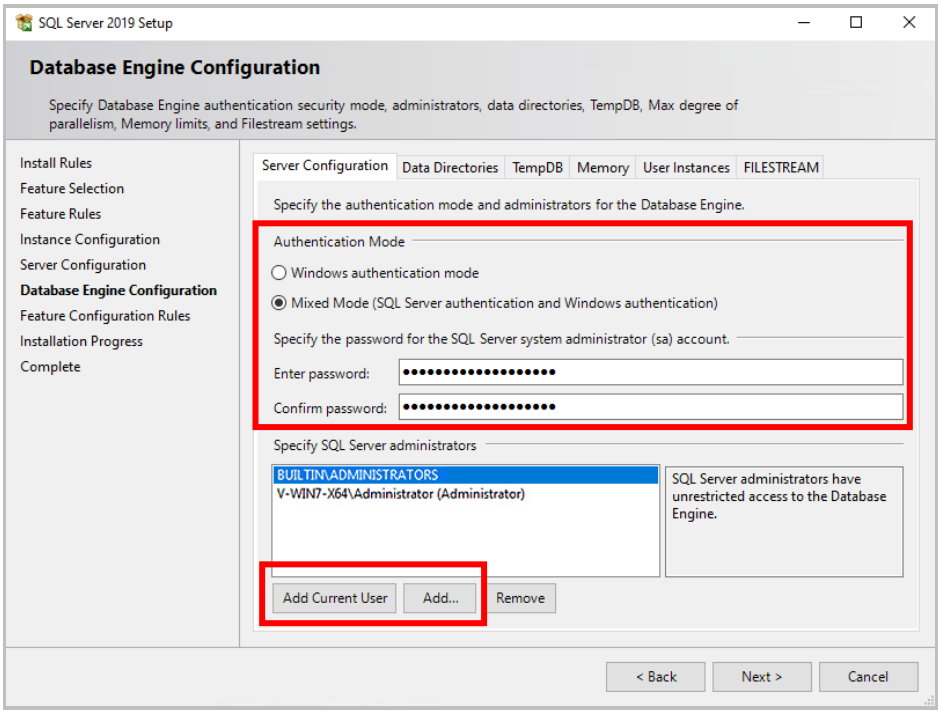


***Figure A.4** - Microsoft SQL Server 2019 Express – Database connection*

- The identification method and the administrators of the SQL Servers must be defined here. Select "Mixed Mode" and enter a password, which must then be used in Matrix for the user "sa". A strong password should be used, i.e., at least 10 characters, capital letters, lowercase letters and numbers. Please refer to your IT guidelines.
- Furthermore, Windows user accounts can be entered, which then have administrator rights on the server. This can be done via the "Add Current User" and "Add" buttons.
- Finally, click onto "Next >" several times until the installation is complete.

APPENDIX B: INSTALLATION OF MATRIX

When Matrix is being installed for the first time and there was no previous access software from GANTNER Electronic GmbH installed in the system, perform the following steps for installation.

1. **Installation of GAT ACE**
   For new installations, it is recommended to use GAT ACE 3000 or GAT ACE 7000 (for the new Generation 7 door controllers). The installation of GAT ACE 3000 and GAT ACE 7000 is described in the corresponding user manual.

2. **Starting the installation of Matrix**
   Start the setup program "`Setup.exe`". The installation wizard checks the installed components. The following components are required for Matrix:
   - . NET 8.0 Windows Desktop Runtime
   - Database (e.g., Microsoft SQL Server 2019 Express)
   If these components are not installed yet, the following window opens where a corresponding message is shown. The .NET 8.0 Windows Desktop Runtime is included in the Matrix installation package.
   Click on the "Continue" button in the window that shows the necessary components, and the installation wizard will guide you through the installation.

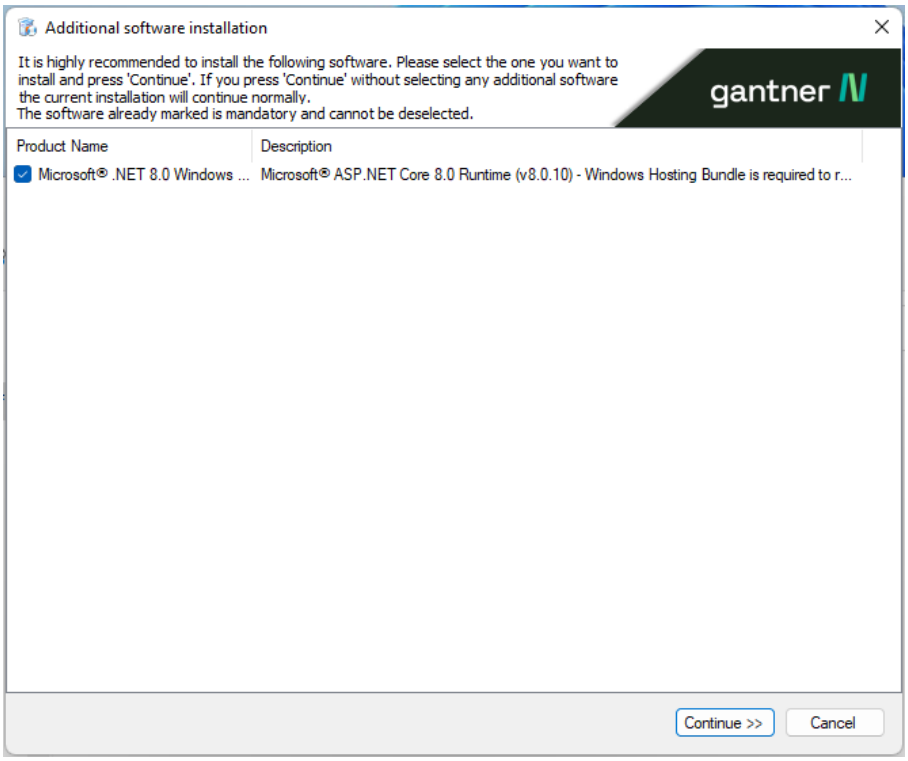


Figure B.1. *– Installation wizard*

In addition, the required versions of other GANTNER software products are also displayed. Update to the required versions if you have installed this software.



3. **Installation of Matrix**
   After all components necessary for Matrix are installed, the following window is shown informing that Matrix can be installed.

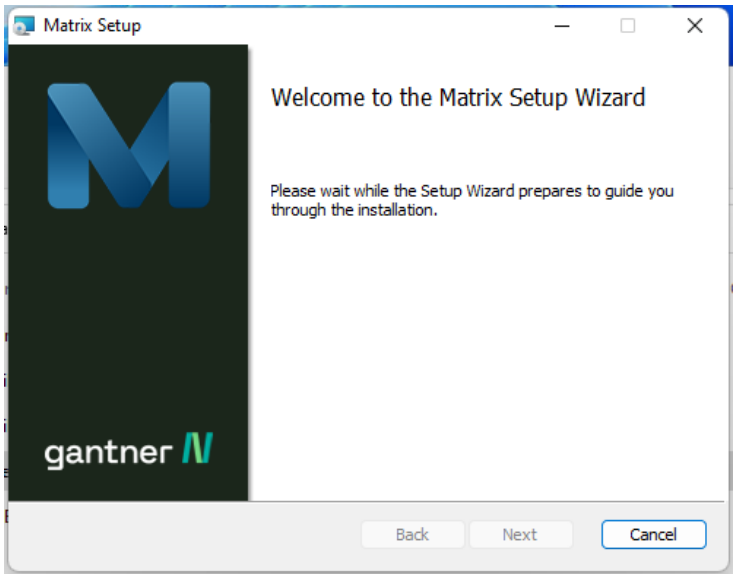


Figure B.2 *– Matrix Installation Assistant – Step 1*

Click on "Next". An information window is shown, which explains the collection of usage statistics. This data is anonymized, which means no user data is stored. The data helps us to improve Matrix. If you do not wish to record this data, you can deselect this option in the general settings (see “4.7. General settings”). Mark the field “I have read and understood the terms of use” and click on "Next".



Figure B.3 *– Matrix Installation Assistant – Usage statistic and privacy policy*

The license information is displayed. Please read this information and mark the field "I accept the terms in the License Agreement" if you want to proceed with the installation. Click on "Next". Now you can select the type of installation.

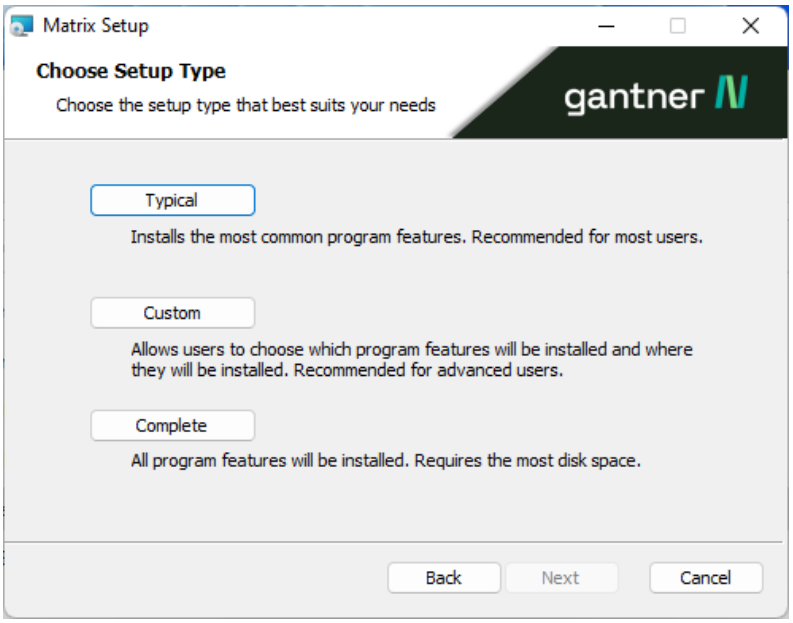


Figure B.4 *– Matrix Installation Assistant – choose setup type*

With "Typical", only Matrix will be installed. With "Complete", Matrix and the person import module will be installed. With "Custom", an additional window is displayed where you can select the options to be installed, i.e., if a module shall be installed with Matrix, or only installed later when required, or not installed at all.

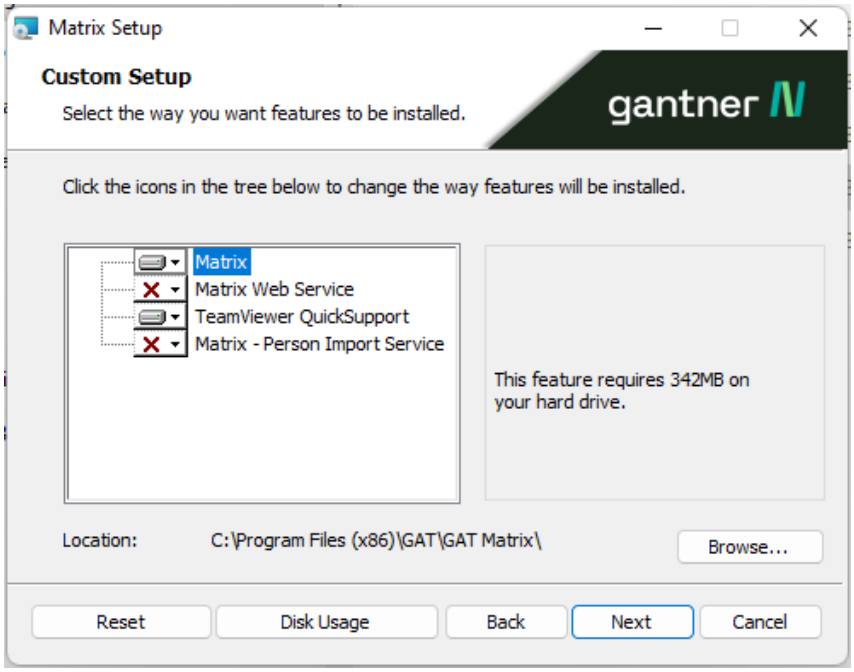


Figure B.5 *– Matrix Installation Assistant – select components to be installed*

In the example shown above, the components “Matrix - Person Import Service" and "Matrix Web Service" will not be installed, and the other components will be installed.

Install "Matrix Web Service" only on the server or the single computer where the central Matrix installation is located!
No installation is required on the other workstations where Matrix Web will be used. The centrally installed Matrix Web Service can be accessed via a web browser.

NOTES:

- The TeamViewer Software allows you to grant the GANTNER Support Team or your sales partner remote access to your PC. This enables fast and easy support in case of technical problems. The access can be controlled and denied any time. If you do not need this software, or if the software is not allowed to be installed on the PC, you can select to not install TeamViewer.
- The "Matrix - Person Import Service" can be used to import persons and bookings from external sources (e.g., personnel database and booking log files) into Matrix at regular intervals, e.g., to automatically transfer new employees to the Matrix authorization management and update the bookings list.
- The "Matrix Synchronizer" must be installed and used if you run two or more Matrix workstations in parallel. This is used to control and check the operation between these workstations.
- The "ProAccess Space Synchronizer" is only needed if the SALTO ProAccess SPACE software is used and the authorizations for the SALTO door locks are edited within Matrix.

Click on "Next" and then on "Install" in the displayed "Ready to install Matrix" window. This will start the installation of Matrix.

4. **Shortcut of Matrix**
   After installation, a shortcut to Matrix is shown on the Windows® desktop. You can start Matrix via this shortcut.

5. **Antivirus software and firewall settings**
   When antivirus software is installed, or will be installed in the future, on a computer where Matrix and GAT ACE are operating, the GAT installation directory (e.g., "C:\Program Files (x86)\GAT") must be excluded from all scans.

   Depending on the type of antivirus software, the programs "GAT.GATMS.MatrixModule.exe", "GAT.ACE.exe", "GAT ACE 3000 Service.exe", and "GAT ACE 7000 Service.exe" must also be excluded from live antivirus scans.

   Also note the necessary antivirus settings required for the SQL Server (see the Microsoft specifications at https://technet.microsoft.com/en-en/library/ms144228.aspx). Antivirus software must not be permitted to scan the folder that contains the database, and there must be no backups of this folder made.

   Furthermore, it should be noted that when installed on multiple PCs/servers the applicable ports used for communication between Matrix and GAT ACE must not be blocked by a firewall (see “4.4 Settings of the network services (clients)”). In addition, the database port must be enabled. By default, this is SQL port 1433, however, a different SQL database port may be configured for individual customers - please contact the respective IT department.

6. **First start of Matrix**
   When starting Matrix for the first time, further settings for the database connection, GAT Manager Client, and Matrix Client, as well as for the license server (Matrix Web Service) must be defined. These settings are described in the chapter "4 FIRST STARTUP OF MATRIX". The information is described briefly in the following steps.

7. **Database**
   Select "SQL Server" for the Authentication Method. IN the field "Server Location" enter the location where the database server is located followed by the instance name of the database (in case of the local PC this is for example "127.0.0.1\ GANTNER"). After that click onto "Create Database" and enter a designation for the database (“GATMATRIX” in the following example). When creating the database information please note:
   - Name of database
   - User of database
   - Password of database

   If an additional workplace is being installed (Matrix Client), this data will be required and not the user "sa"!

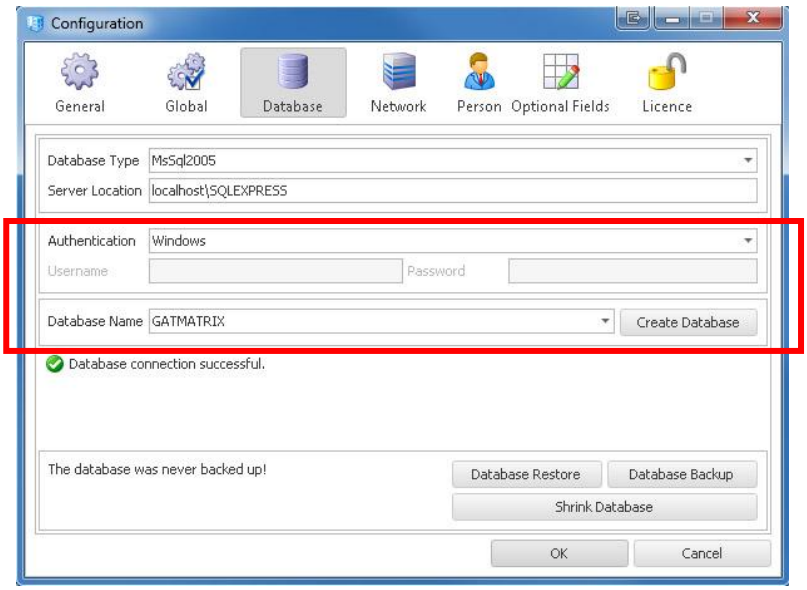


Figure B.6 *– Database settings for Matrix*

8. **Base license**
   You must enter the base license for your Matrix installation within 14 days after installation, or else Matrix cannot be used anymore. The license is entered as described in chapter "10 LICENSE MANAGEMENT". After input of the license Matrix and the clients must be restarted.
   Change the setting to "Store license on the license server". This guarantees that all Matrix clients will always have the same license data and must only be registered once.

9. **Activation**
   Matrix must be activated within 14 days after input of the base license. For this please send the following data via email to our GANTNER Sales department:
   - Base license
   - Hardware-ID
   - Customer data

   You will receive the activation code, which allows to activate Matrix.

10. **Additional users**
    If another user is working on the server with Matrix, this user must have read and write permissions for the user directory. Furthermore, on Windows 8 or higher the user must also have read and write permissions for the "ProgramData" folder. For the new user, the noted SQL settings must also be entered again.

11. **Matrix clients**
    The Matrix Clients must have read and write permission for the folder "C:\ProgramData\GAT\".

12. **Persons and door groups**
    Please make door groups in Matrix and import the doors from GAT ACE. Then also make the groups for the persons and insert the persons.

13. **Uploading doors**
    After all data and persons are uploaded to Matrix, the doors can now be uploaded in GAT ACE.

    NOTE! The device memories must be initialized completely when uploading!

APPENDIX C: SALTO PROACCESS SPACE INTEGRATION

Matrix can be used together with the SALTO ProAccess SPACE software solution. The SALTO access locks, doors, and data carriers of the SALTO system are configured in ProAccess SPACE. The SALTO components can be imported into Matrix to manage GANTNER and SALTO door authorizations in a common interface.
Follow these instructions to configure the collaboration between Matrix and ProAccess SPACE.

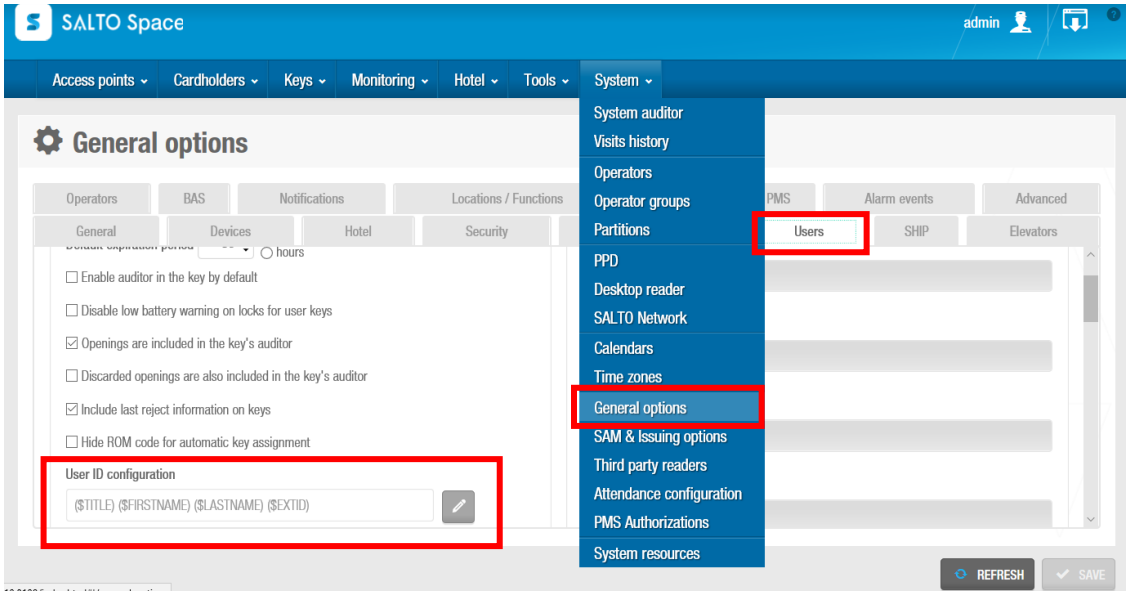
Some instructions are optional and only required if the functions are to be used. All instructions for a standard installation are described here.

1. **Installation and configuration of SALTO ProAccess SPACE**
   Follow the SALTO ProAccess SPACE software instructions to configure your system. ProAccess SPACE can be downloaded from the following link: https://softwarearea.saltosystems.com.

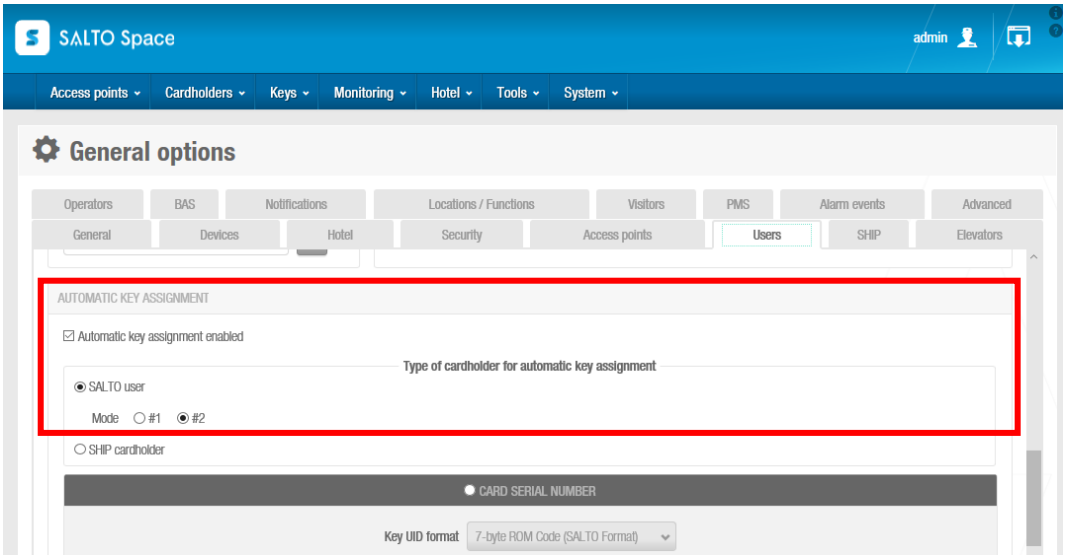
2. **Install local IO bridge**
   Also install the local IO bridge to be able to use the SALTO NCoder with Matrix.

3. **Settings in ProAccess SPACE**
   In ProAccess SPACE, the following settings have to be considered:

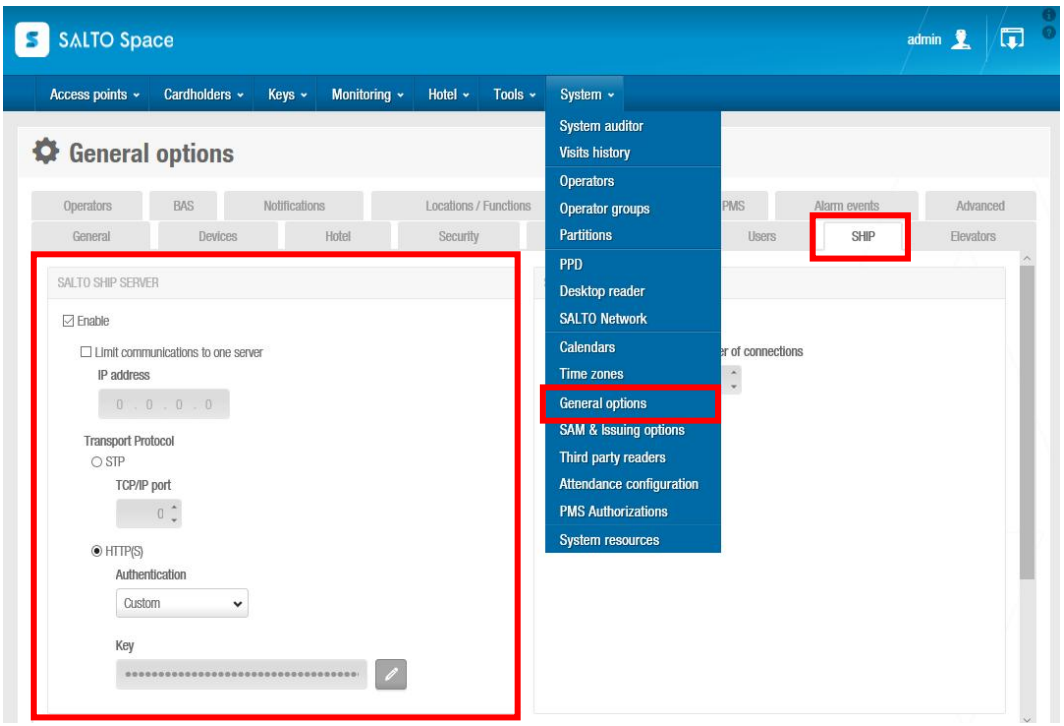
   ► Under menu "System" > "General options" > tab "Users", define the display of person names and also configure this display to the same format in Matrix (see "4.10 Settings for person display"). It is important that the "Ext ID" number of the persons is included here (see "5.6.2. Settings for persons in ProAccess SPACE").



   ► Under menu "System" > "General options" > tab "Users" in the "Automatic Key Assignment" section, specify which data carrier number is to be used for automatic data carrier assignment (see "5.6.3 Authorizing and configuring data carriers for persons").



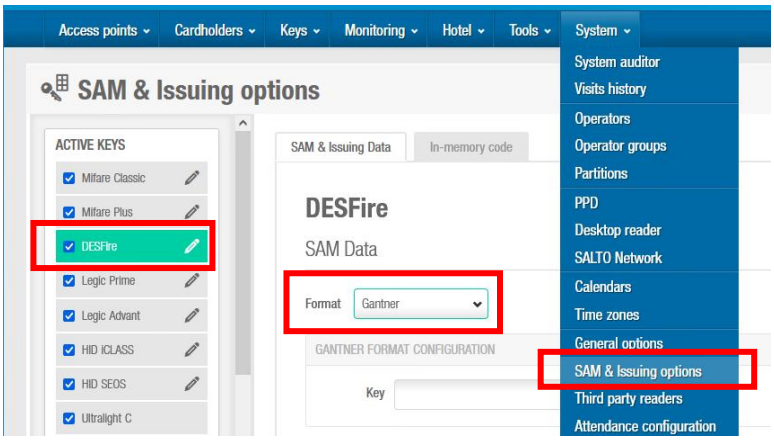
► Under menu "System" > "General Options" > tab "SHIP", enable the SHIP server and define the port and the communication settings. For the IP address, enter the server on which GAT ACE 7000 is running or leave the address as 0.0.0.0.



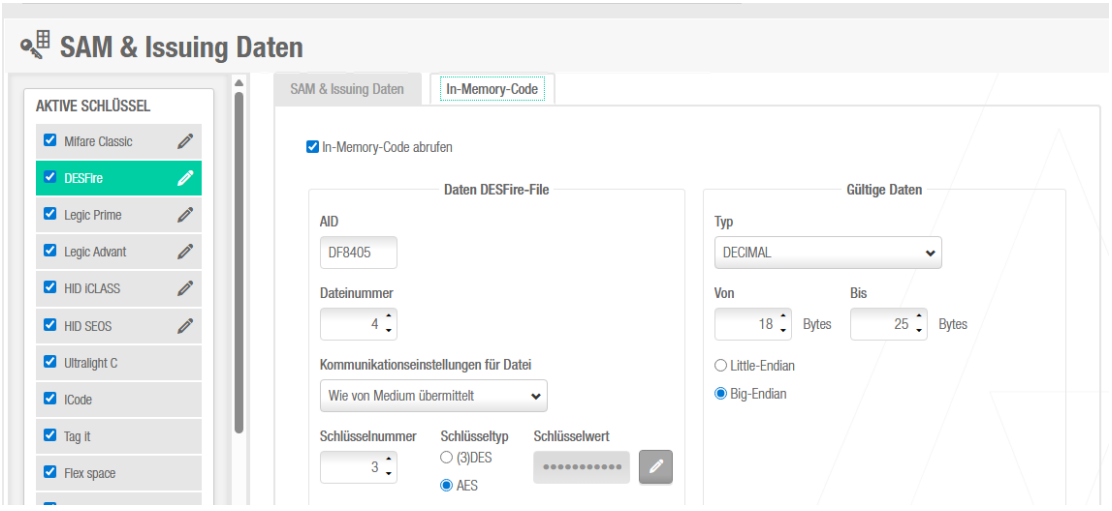
► In ProAccess SPACE, create the doors and other hardware components, e.g., the NCoder.

► Additional settings and requirements are necessary for the SVN function. SVN (Salto Virtual Network) is comparable to the CardNET function from GANTNER, which is used for offline doors/locks and in which the authorization data for the doors/locks is stored on the user data carriers. With the GANTNER SVN implementation, the SVN data can also be edited and written at GANTNER readers. To use this function, the following additional settings must be made:

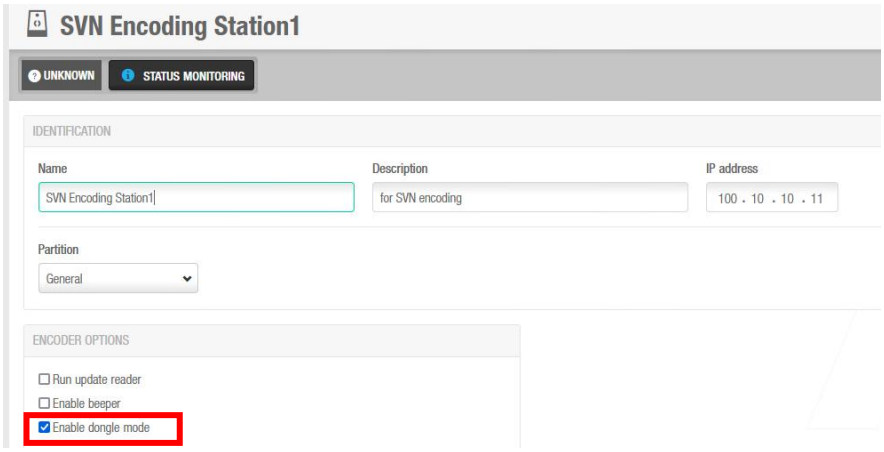
- For GANTNER SVN it is necessary to use MIFARE DESFire data carriers, which are coded with the GANTNER SVN segment.
- The data carriers (coding with GANTNER SVN segment) can be prepared using the G7 Coding App (see documentation of this app).
- In ProAccess SPACE, the format "Gantner" has to be selected via the setting "System" -> "SAM and Issuing Data" -> "DESFire". The options 020 and 029 are then no longer necessary (see "10.5. Licensing for SALTO doors").



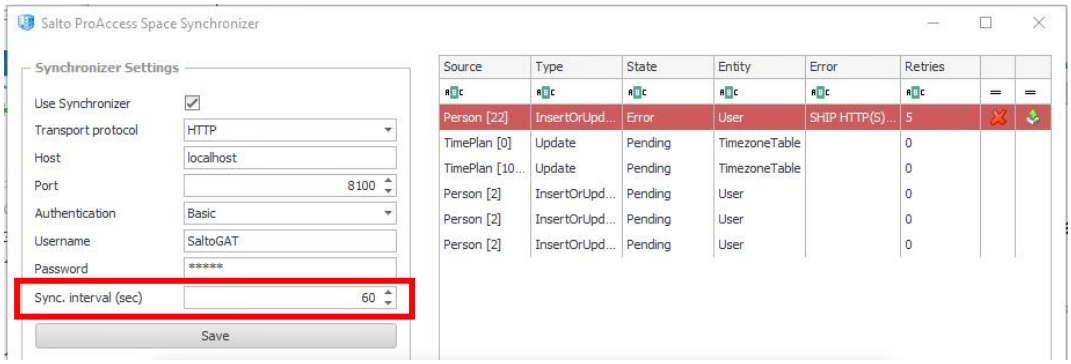
- On this settings page when selecting GANTNER format then also the key (field "Key") must be entered. This key is the "FID Read Key", which is provided by GANTNER for the system.
- In the same menu on the sub-page "In-memory code" the following settings must be made:



- The values for AID (DF8405) and file number (4) must be entered like shown in the picture.
- In the area "Valid data" you must enter the values like shown here:
  - "Type" = DECIMAL
  - "From" … "To" = 18 bytes … 25 bytes
  - Select "Big-Endian"
- SVN data are always coded for each site separately. For this, a dongle encoder is required. Which encoder shall perform the coding can be set by activating the setting "Enable dongle mode" for the corresponding encoder (in ProAccess SPACE -> "System" -> "SALTO Network" -> "ENCODER"). If many SVN data updates are completed at the same time, several dongle encoders can be used in parallel to improve the system performance.



- In the GAT DC 7200 controller settings, the SVN function must also be activated (similar to GAT ACE 7000), in order to enable the connected readers to read and write the SVN data. Refer to the GAT DC 7200 manual for information.
- The performance when updating the GANTNER SVN data at a reader can be improved if the SALTO ProAccess Space Synchronizer is operating with a higher sync interval (e.g. 60 seconds).



4. Installation of SALTO ProAccess SPACE Synchronizer

This Windows service runs in the background and provides communication between Matrix and the ProAccess SPACE software. You can select to install the service in the installation wizard during the installation of Matrix or also afterwards with the "Change" function in the installation wizard.

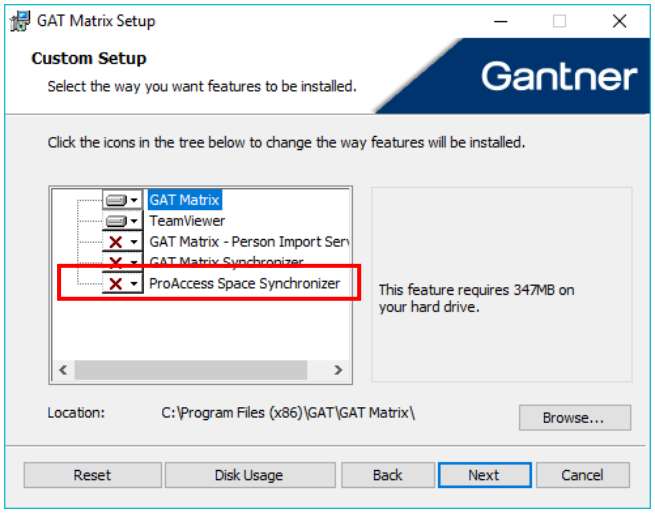
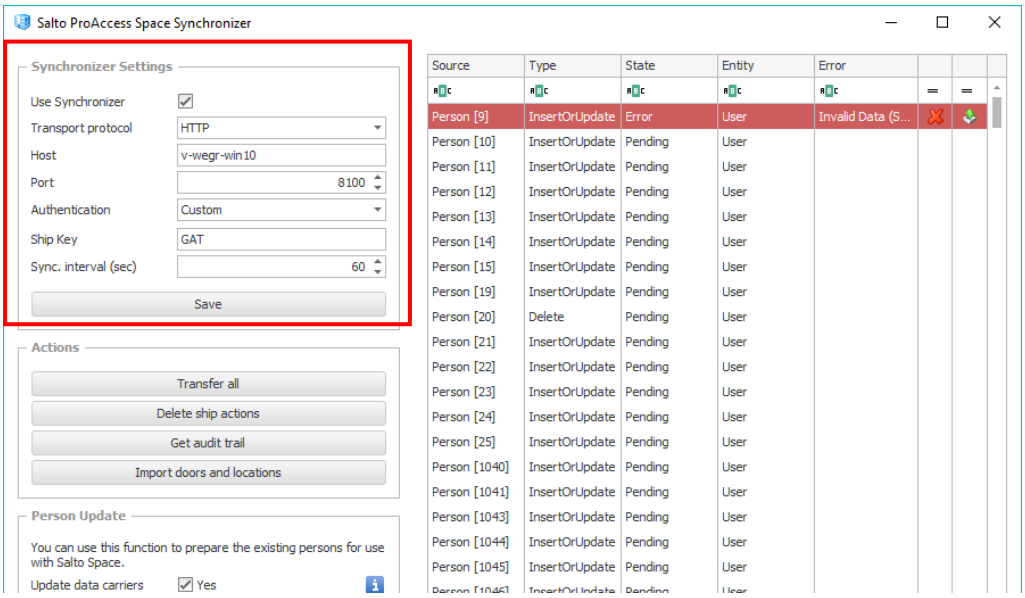


***Figure** - Matrix Installation Wizard - ProAccess SPACE Synchronizer*

5. Activate SALTO ProAccess SPACE Synchronizer

The use of SALTO ProAccess SPACE must be activated. Only then are all functions available for SALTO ProAccess SPACE.

► To do this, open the "ProAccess Space Synchronization" menu item in the "Settings" menu. The following window is displayed.



► Enable the "Use Synchronizer" option and configure the connection settings that you also used in SALTO ProAccess SPACE.

- Transport protocol: Select the transmission protocol here (default = http).
- Host: Enter here the computer name or IP address of the computer on which the SALTO ProAccess SPACE software is installed.
- Port: Port number for communication with the Synchronizer. Default = 8100.
- Authentication: Here you can select the type of login to SALTO ProAccess SPACE. Default is "Custom". Depending on the selected authentication, enter the ship key or the username and password.
- Sync. Interval (sec): Here you can define the time interval for the periodical update of the Ship commands.
  Note: An average value is 5 seconds. If the SVN function is used, the value should be set higher (approx. 30 to 60 seconds) in order not to restrict ProAccess SPACE and to speed up SVN coding.

► Click on "Save".

6. Settings in Matrix for persons and data carriers for ProAccess SPACE

- Set the default values for the data carriers and persons of SALTO persons (see "4.10 Settings for person display").
- Define the data carrier types for SALTO (see "5.6.4 Defining data carrier types").

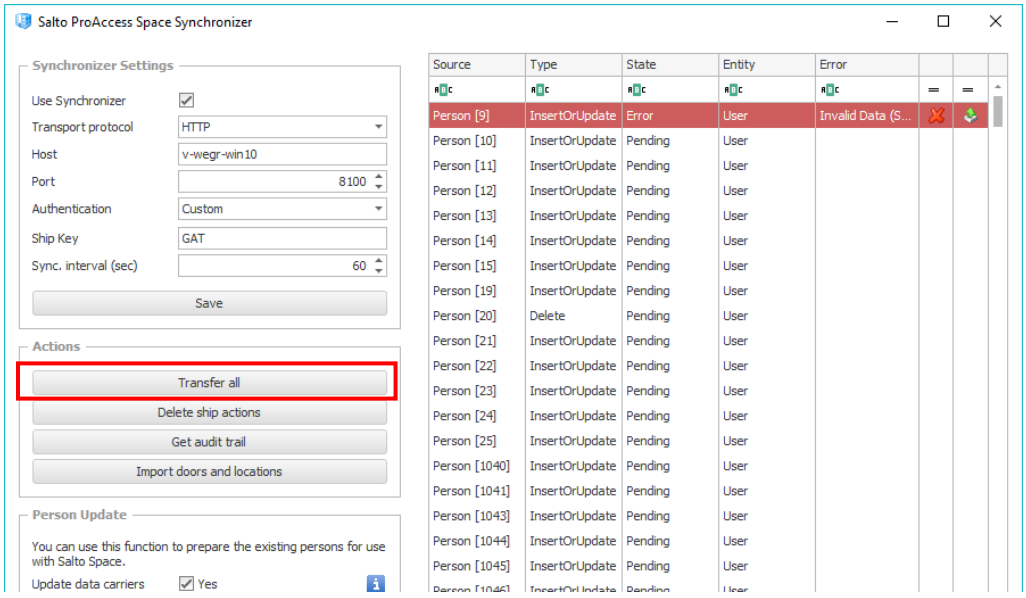
- Update the existing persons in Matrix so that they can be used for SALTO ProAccess Space (see "5.6.6. Automatically preparing existing persons for SALTO ProAccess SPACE" or "5.6.1 Defining personnel master data").

7. **Import doors and locations from ProAccess SPACE**
   Import the doors and locations (called "partitions" in ProAccess SPACE) into Matrix. See the instructions in "5.5 Importing doors and locations from SALTO ProAccess SPACE".

8. **Update time plans for ProAccess SPACE**
   Convert the GANTNER plans (device and employee plans) for use with SALTO ProAccess Space (see "5.11 Defining personnel time plans" and "5.12 Defining door time plans").

9. **Assign calendars to ProAccess SPACE**
   Assign the operating calendars to the locations ("partitions") that were imported from ProAccess SPACE (see "6 CORPORATE CALENDAR AND LOCATIONS").

10. **Test communication with GAT ProAccess SPACE Synchronizer**
    Load all data to ProAccess SPACE once to test the correct communication. To do this, select the "Transfer all" function in the "ProAccess SPACE Synchronizer" window.



If the option at the bottom right near "Refresh" is activated, it is possible to observe how the individual commands in the list are processed. The list must become empty after a few seconds, depending on the size of the system. This ensures that the data transfer between Matrix and ProAccess SPACE is configured correctly and that the changes in Matrix have an effect on the SALTO doors.

APPENDIX D: FORMATS AND FILE SPECIFICATIONS

Person import – CSV import file format

There is the possibility to import personnel data from a text file into Matrix (see “11. PERSONS IMPORT SERVICE”). This is a useful function, for example, to easily import personnel data from another application.

The following format settings are required for the import file:
- File format: .csv
- The import file must be saved with UTF-8 format so that special characters are correctly displayed.
- Columns must be separated by delimiter symbols. For these symbols different characters like semicolons, commas or tabulators can be used. It is further possible to use a user specified character as delimiter. In this case this sign must be input in the person import of Matrix.
- Each line must be closed with a CR/LF (0x0D/0x0A) sign (i.e., single data sets).

Import file structure

Field	Places	Characters	Mandatory field
Data carrier 1	11/X(5)	0-9	Yes/No(1)
Data carrier 2	11/X(5)	0-9	No
First name	100	Text	No
GATAccessDate	X	Date in German format (DD.MM.YYYY)	No(2)
GATAccessTime	X	Time in German format (HH.MM)	No(2)
GATAccessTimeFlag	1	0-2 0 … GATAccessTime is not used 1 … GATAccessTime used for the "Valid from" time 2 … GATAccessTime used for the "Valid to" time	No
ImportReference	255	Text	Yes/ No(1)
Last name	100	Text	Yes
Person ID	8	0-9	Yes/ No(1)
Person group	X	0-2,1 Billion	Yes
PIN Code	8	0-9	No
Title	255	Text	No
Valid from	X	Date and time for start of validity period for a person. Format depends on the configured format (see "5.7 Import persons"). Example: Format "en-US" -> "20/12/2015 8:10 PM"	No
Valid until	X	Date and time for end of validity period for a person. Format depends on the configured format (see "5.7 Import persons"). Example: Format "en-US" -> "20/12/2015 8:10 PM"	No
Data carrier type 1	X(6)	0-255	Yes/No(3)
Data carrier type 2	X(6)	0-255	Yes/No(3)
E-Mail	255	The person’s email address. The string must be a valid email address.	No
Phone number	255	The person’s phone number. The phone number begins with "+" and must be a valid number, e.g. "+43555233944".	No
Gender	1	Information about the person’s gender. The following four values are possible: 0: no information given 1: male	No

		2: female 3: diverse If the field is empty, or another value is given, "0" (no information given) will be used automatically.	
Optional field(4)	X(4)	X(4)	No
Optional field(4)	X(4)	X(4)	No
:	:	:	:

(1) Depending on the criteria that is used for import.
(2) Mandatory field if GATAccessTimeFlag is set to 1 or 2.
(3) Only if data carrier is specified and the default type is not used.
(4) Different data and data types are possible, depending on the defined optional fields in the personnel data (see "4.11. Optional fields for personnel data")
(5) If the data carrier type is used as default type for GAT ACE 3000, only 11 digits are possible for the data carrier number. But when used for GAT ACE 7000 the data carrier number can be longer.
(6) Import ID of the desired data carrier types (see "5.6.4. Defining data carrier types").

Table Appendix D.1 - *Structure of the CSV person import file*

NOTE! For GAT ACE 3000 systems, the personnel number must be unique when performing anti-pass-back checks or when using fingerprints for identification verification.

NOTE! For GAT ACE 3000 systems, a person may only use one data carrier when an anti-pass-back check is to be made.

Person import – SAP CC1 import file format

It is also possible to import persons into Matrix directly from a file in SAP CC1 format (see “5.7.2 Importing via SAP”).

The following formatting is required for the import file:
- File format: SAP CC1 format with fixed field lengths and without separators, as specified in the following table.
- Characters in UTF-8 format.
- The lines must be terminated with CR/LF.

Import file structure

Field Name	Type	Length	Text
ZAUSW*	NUMC	8	Time identification number
BEGDA*	DATS	8	Start of validity period of the mini master record
ENDDA*	DATS	8	End of validity period of the mini master record
ZAUVE*	CHAR	1	Identification version
PERNR	NUMC	8	Personnel number
ENAME	CHAR	40	Employee’s name (edited)
SNAME	CHAR	40	Employee’s name (can be sorted)
INFO1	CHAR	8	Variable information field
INFO2	CHAR	8	Variable information field
INFO3	CHAR	8	Variable information field
INFO4	CHAR	8	Variable information field
INFO5	CHAR	8	Variable information field
INFO6	CHAR	8	Variable information field

INFO7	CHAR	8	Variable information field
INFO8	CHAR	8	Variable information field
INFO9	CHAR	8	Variable information field
INFOA	CHAR	8	Variable information field
IMAIL	CHAR	1	Mail indicator of the time evaluation error
MOABW	NUMC	2	Absence/attendance group
MOLGA	NUMC	2	Country group
BDEGR	CHAR	3	Subsystem link group
ZEITY	CHAR	1	Work schedule group
ZDGBE	CHAR	1	Authorization for business trips
ZANBE	CHAR	2	Entry check group
ZPINC	CHAR	4	Personal code
ZMAIL	CHAR	1	Mail characteristic from time record. info type

* Key field of the table

***Table Appendix D.2** - Structure of the SAP person import file (SAP CC1 file)*

Calendar import – special day import file format

There is the possibility to import the special day definitions from a text file into the “Calendar” of Matrix (see “6 CORPORATE CALENDAR AND LOCATIONS”).

The following formatting is required for the import file:

Separator

- Fields: comma or semicolon
- Data sets: CR/LF

Encoding

- ANSI / Windows Default

File name

- Freely definable but unique for each operating calendar
- Data sets of other operating calendars can also be in one file, but only those that match the current operating calendar are used for the import. Thus, a customer can, for example, export all days into a single file and then only have to copy this for each operating calendar

Header

- Fixed names (at least the first three characters must match exactly)
- Free sequence
- Mandatory in line 1

Records

- All fields mandatory

Import file structure

Field	Description
OrganizationTimePlanId	The ID of the operating calendar to which the day should be imported (will be displayed in the import configuration dialog)
Date	The date of the special day in the format dd.MM.yyyy. Days in the past are ignored.
From	The time from which the special day should apply in the format HH:mm Only relevant for OperationMode Online (1) - otherwise Default 00:00
Until	The time up to which the special day should apply in the format HH:mm Only relevant for OperationMode Online (1) - otherwise Default 23:59
Description	The name of the special day. Max. length = 255 characters

SpecialDay	The index or the internal name of the special day: - 0 or SpecialDay1 = special day 1 - 1 or SpecialDay2 = special day 2, etc.
OperationMode	The index or internal name of the door operation mode to which the special day is to apply: - 0 or All = all doors - 1 or Online = online doors - 2 or OfflineWinet = offline or WiNET doors

Table Appendix D.3 - *Structure of the special day import file*

Example:
OrganizationTimePlanId;Date;From;Until;Description;SpecialDay;OperationMode
1;07.11.2019;00:00;23:59;Event morning;0;0
1;07.11.2019;13:00;16:50;Event afternoon;0;1
1;07.11.2019;00:00;23:59;Event offline doors;1;2

APPENDIX E: DATABASE BACKUP

The Matrix database can be backed up by the user in the database configuration (see "4.1. Database settings"). It is also possible to save the backup on a network drive. Certain settings, which are described on the following pages, must be made to achieve this.

NOTE! The "Restore Model" of the Matrix database is set to "Simple" by default when the database is created by Matrix. To select the optimum restore model, you should consider the restoration goals and requirements for the database as well as if you want to use log backups.

NOTE! The following instructions only apply when the SQL server is started as network service in the Windows services and not when the SQL service is started as user or system.

1. Create a new directory, for example with the name "SQLBackup".
2. Open the settings window of the folder by pressing onto the directory with the right mouse button and selecting "Properties" from the pop-up menu.
3. In the opened window, go to the second "Sharing" tab and click on the "Advanced Sharing…" button.
4. Select the "Share this folder" option.

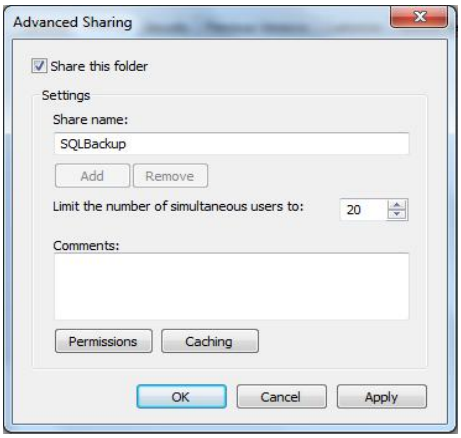


Figure E.1 *- Sellback Properties - Advanced Sharing*

5. Click the button "Permissions". The window "Permissions for SQLBackup" is opened.

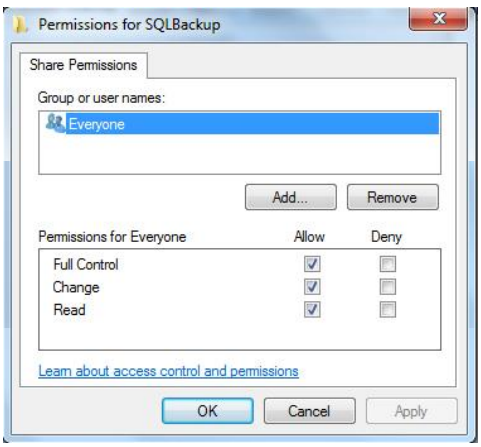


Figure E.2 *- SQLBackup Permissions*

6. Here the entry "Everyone" must selected in the top field "Groups or usernames" and in the bottom field "Permissions for Everyone" the option "Allow" must be marked for each entry.

7. Next click onto "Add…" and the window "Select User or Groups" is opened.

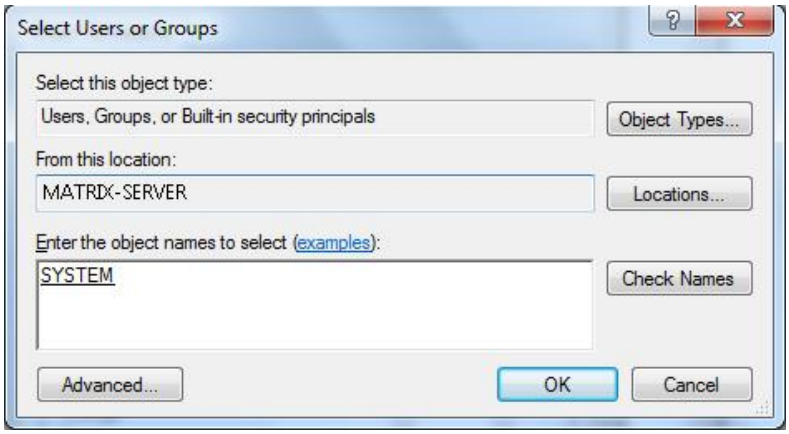


***Figure E.3** - SQLBackup Permissions - User Groups*

8. In the bottom input field enter "SYSTEM" (depending on the system also "network" or "net" may be possible, but "NETWORK SERVICE" should not be used) and then click on "Check Names". Another window is opened where the matching names are displayed. Select "SYSTEM" and confirm twice.

9. Now on the register card "Share rights" another entry "SYSTEM" is shown. This entry also requires all rights to be set to "Allow" in the lower field.

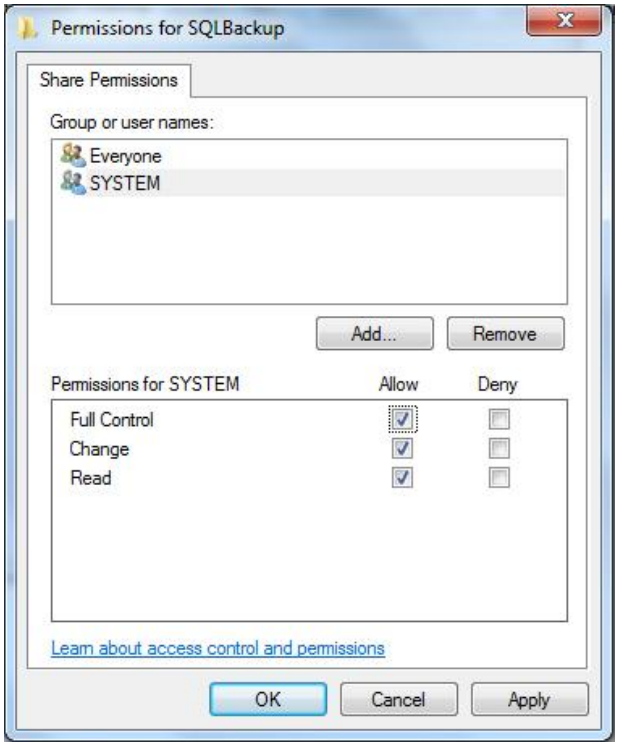


***Figure E.4** - SQLBackup Permissions*

10. Press "Apply" and then "OK", in order to save the settings. The window "Properties of SQLBackup" is shown again.

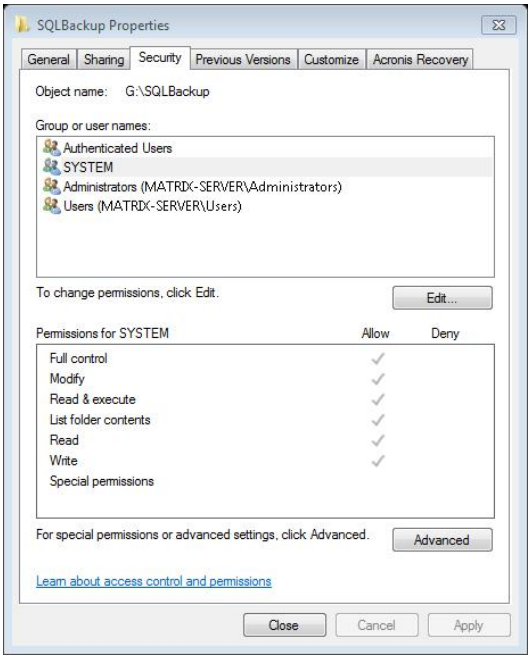


Figure E.5 *- SQLBackup Permissions - Security Settings*

11. On the "Security" tab, click on the "Edit…" button below the "Group and usernames:" field. The "Security" window opens.

12. With the button "Add…" in this window please add the users "Everyone" and "SYSTEM" in the same way as described in step 7.

13. Next, all rights must be set to "Allow" for all users as described in step 9.

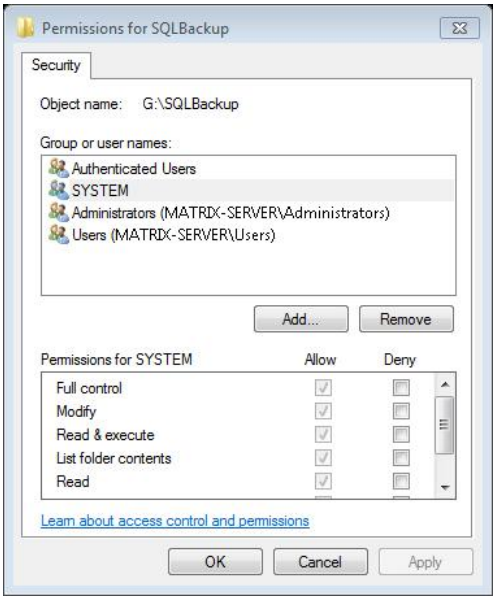


Figure E.6 *- SQLBackup Permissions - Security Settings*

14. After confirmation with "OK" and closing the properties window the shared directory "SQLBackup" can be accessed and data be written to the directory by the SQL Server Express, if it is started as network service.

15. In Matrix it is now possible to edit the path of the shared directory when selecting "Database Backup" (see "4.1. Database settings"). The path must be entered with a "\" sign at the end.
Example: \\PC-name\SQLBackup\
PC-name is the network name of the PC where the shared directory is located.

16. For a final check open the service window of Windows ("Windows" key + "R" button -> enter "Services" and press "OK").

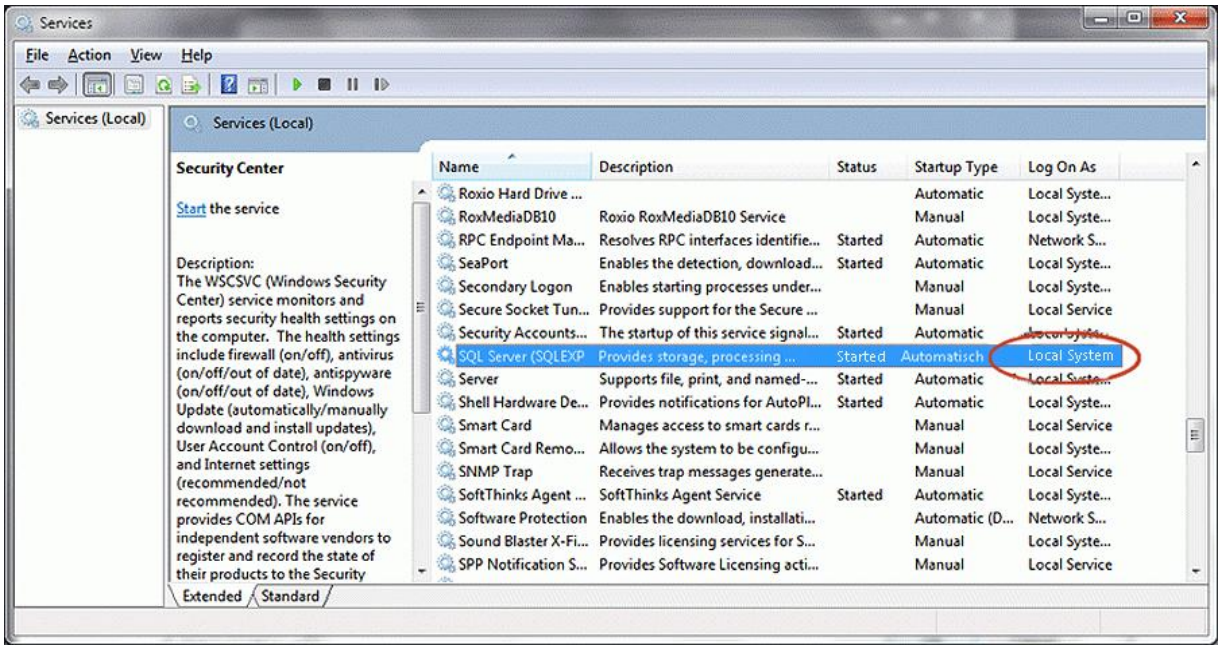


Figure E.7 *- Windows Services - Settings*

17. In the "Log On As" column for "SQL Server (SQLEXPRESS)", the user who is running SQL Server Express is shown. If another user is entered here instead of network service, you also need to assign the corresponding rights for the shared directory for this user as described in step 7 (e.g., for "Local System" this would be the user "SYSTEM"). Please note that to run SQL Server Express with the user "Network Service" is not recommended.

APPENDIX F: PORT LIST

The following ports are required for communication between Matrix and the applications listed below.

NOTE! These ports must not be blocked by a firewall or similar application.

Application	Standard Port	Description
SQL Server	1433 (for standard SQL installations)	To store Matrix data
SALTO ProAccess SPACE	8100	For communication with the SALTO ProAccess SPACE software (if used).
GAT License Server	8232	To store licenses in a central place
Matrix Synchronizer	8233	To distribute notifications between multiple Matrix clients
GAT Mobile Access	8234	Handles communication with mobile devices (Android/iPhone)
Relaxx	8237	Communication with Relaxx software from GANTNER for the control of a locker locking system
GAT ACE 3000	8301	To upload authorizations and download bookings and states to/from controllers
GAT ACE 7000	8701	To upload authorizations and download bookings and states to/from controllers

Note:
This manual is valid as of November 24th, 2025. It is subject to change.
Amendments and changes can be made without prior notice at any time.
This manual is valid for version 7.1.0 of Matrix.



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

Part No.: 859590

www.gantner.com