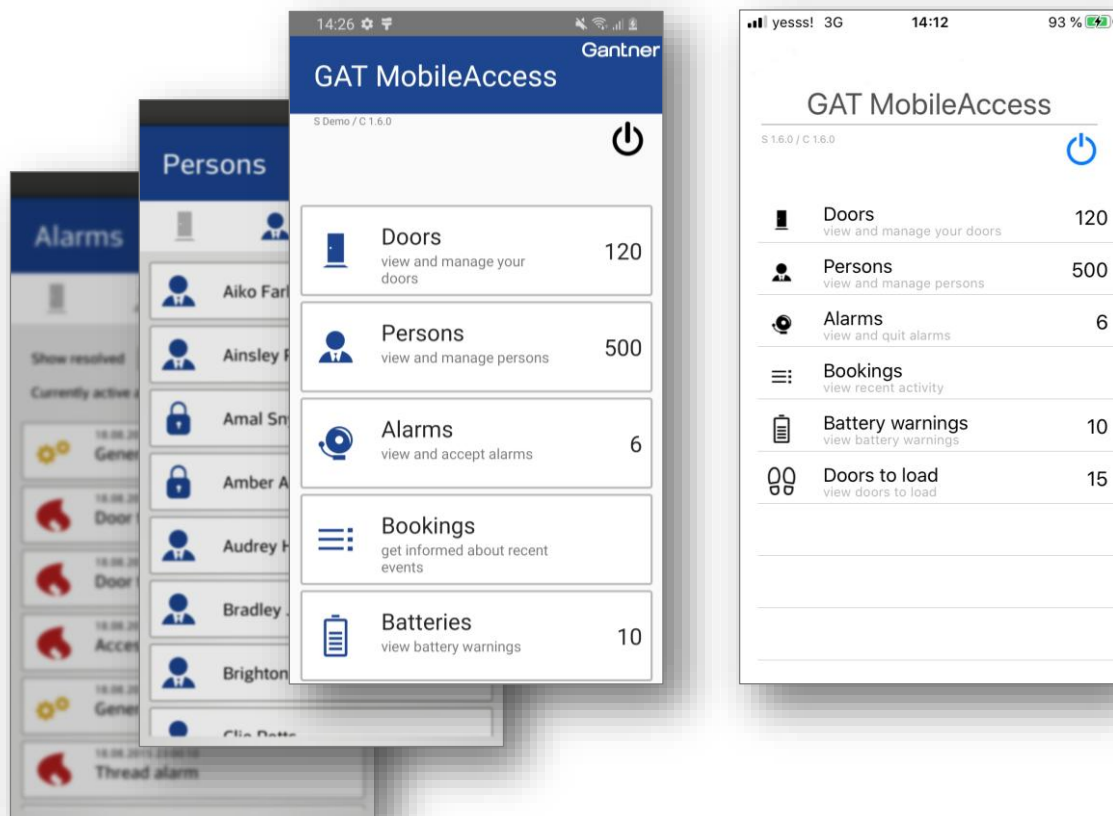


GAT Mobile Access Management

Mobile App for Access Control Systems



© Copyright 2026 GANTNER Electronic GmbH

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

Liability

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

Trademarks

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

Contact

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

Contact address of manufacturer

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



General Warning and Safety Instructions

Dear Customer,

We congratulate you on selecting a product (device 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.

TABLE OF CONTENTS

1	INTRODUCTION	7
1.1	About this Manual	7
1.2	Chapter Overview	7
1.3	Formatting	8
1.4	Contact and Inquiries	8
2	OVERVIEW	9
2.1	Product Description	9
2.2	Terminology	9
3	INSTALLATION	11
3.1	GAT Mobile Access Server	11
3.1.1	Supported Operating Systems	11
3.1.2	Hardware Requirements	11
3.1.3	Microsoft .NET Framework	11
3.1.4	Additional Software and Hardware Requirements	12
3.1.5	Installation of the GAT Mobile Access Server	13
3.2	GAT Mobile Access App	16
3.2.1	Supported Operating Systems	16
3.2.2	Hardware Requirements	16
3.2.3	Installation of the GAT Mobile Access App	16
4	CONFIGURATION	17
4.1	Configuring the GAT Mobile Access Server	17
4.2	Startup Settings of the GAT Mobile Access Server	21
4.3	Setting Up HTTPS for Mobile Access Management	22
4.4	Establishing a TLS Connection to GAT ACE	33
4.4.1	GAT Mobile Access Configuration	33
4.4.2	GAT ACE 3000 and 7000	34
4.5	Configuring the GAT Mobile Access App	35
4.5.1	Language	37
4.6	Registering a Mobile Device in Matrix	38
5	OPERATION	39
5.1	Startup and Login	39
5.1.1	Login with Username and Password	39
5.1.2	Login with Biometric Recognition	40
5.2	Functionality	42
5.2.1	Area "Doors"	43
5.2.2	Area "Persons"	48
5.2.3	Area "Alarms"	52
5.2.4	Area "Bookings"	55
5.2.5	Area "Batteries"	57
5.2.6	Area "Doors to Load"	58

1 INTRODUCTION

1.1 About this Manual

This manual provides comprehensive information on GAT Mobile Access Management, a solution developed to monitor and control your Gantner access control system via a mobile device. Contained herein are detailed instructions regarding how to install and operate the GAT Mobile Access Management solution. The installation instructions are divided into two sections – one set for the server component and one for the mobile application. To begin operating GAT Mobile Access Management, an initial configuration of the server and application (app) is required. Instructions for this configuration process as well as how to use the mobile app are provided in this manual.

In addition to the necessary hardware devices (door controllers, readers, etc.), software packages including GAT ACE 7000 or GAT ACE 3000 and Matrix are also required to operate GAT Mobile Access Management. Separate documentation is available for these additional software components. Where applicable, important information regarding these components in relation to GAT Mobile Access Management is described in this manual.

This manual is intended for the technical personnel who install and configure the GAT Management Mobile Access server as well as for the end users of the mobile app.

1.2 Chapter Overview

In chapter "2 OVERVIEW" you will find information on the components that make up the GAT Mobile Access Management solution and their intended use. The terms that are often used in this manual are also defined in this section.

Chapter "3 INSTALLATION" contains information on the system requirements that must be met for GAT Mobile Access Management to operate. Additionally, available in chapter 3 are the instructions required to correctly install the server and mobile app.

In chapter "4 CONFIGURATION" you will find a detailed description of the configuration settings that affect how the server and the mobile app function and how these configuration settings are tailored to suit individual requirements.

Chapter "5 OPERATION" contains instructions on how to use the server and mobile app and also what should be observed when operating GAT Mobile Access Management.

1.3 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.

1.4 Contact and Inquiries

For questions related to GAT Mobile Access Management, please contact your local representative or one of the Gantner offices directly. The contact details are available via the following link: www.gantner.com/locations.

2 OVERVIEW

2.1 Product Description

GAT Mobile Access Management is a software package consisting of a server component - a Windows service that operates in the background and is configured and controlled via a graphical user interface - and a mobile app designed for mobile devices such as smartphones or tablets.

The GAT Mobile Access server is installed on a central PC/server running a Windows operating system. Following installation, the server operates in the background as a Windows service and serves as a communication interface between the mobile devices and the GAT Mobile Access app. This communication includes the Matrix and GAT ACE 7000 or GAT ACE 3000 software packages from Gantner that support the app. Therefore, an operational version of GAT ACE 7000 or 3000 and Matrix is always required to use GAT Mobile Access Management.

2.2 Terminology

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

GAT Mobile Access Management

The GAT Mobile Access Management name refers to the complete mobile application package, which consists of a server component and the mobile apps developed for different operating systems.

GAT Mobile Access Server or Service

This term refers to the software installed on a PC/server that manages the communication and configuration requirements between GAT ACE 7000 / 3000 or the access terminals and the mobile devices.

GAT Mobile Access / GAT Mobile Access App

GAT Mobile Access is the app that is installed on the mobile device. The app is available for Android and iOS operating systems and offers the same functionality across all operating systems.

Matrix

Matrix is an access control software from GANTNER that is used to assign and manage access authorizations (including schedules, special days, etc.) for users within the access control system. The software was called GAT Matrix before the name change.

GAT ACE 7000 and GAT ACE 3000

This Gantner developed software solution is installed on a central server and provides an interface between Matrix and the door controllers. GAT ACE 7000/3000 receives data and manages the entire access system providing a means for the user to carry out tasks such as configuring the door hardware and monitoring the status of devices and doors.

GAT ACE 3000 supports the previous generation of door controllers (e.g., GAT Terminal 3100) and readers (e.g., GAT SR 3xx). GAT ACE 7000 is required for the current generation of door controllers (e.g., GAT DC 7200) and Series 7000 readers.

User

In this manual, the term "user" describes the person operating GAT Mobile Access Management. Several users can be created, each with their own personal user name and unique password.

Person

In this document, the term "person" refers to a user of the access system. For every person authorized to access a facility, a personal record in the access control software (e.g., Matrix) is created and a data carrier with a unique number assigned. The record contains personal information such as the personnel number, data carrier number (also known as the card number), PIN code, group assignments, and fingerprint data if applicable.

Data carrier / card

A data carrier or card is used to identify people at the door reader and connected controller. Depending on the reading unit in operation, different types of data carriers such as contactless cards (RFID) or magnetic and infrared cards can be used. The contactless data carriers are also available in various forms such as cards, key fobs or wristbands and available for different identification systems (LEGIC, PROXY, MIFARE®, ISO 15693).

Door controller

The door controllers are installed on or near the doors and are responsible for reading the data carriers of people, verifying their validity, and electronically unlocking/locking the doors. Door controllers are available with integrated or remote readers. The door controllers are configured and managed in GAT ACE 3000.

General Open Function

This function can be activated for each time-managed door controller. Independent of identification through a person, it is possible during a time period to unlock a door, to activate a special relay plan or to suppress alarms.

Threat alarm

Depending on the configuration and personal data settings, a PIN code in addition to a valid data carrier can be programmed for identification and access. In this case, it is also possible to define a threat PIN code. The threat PIN code is combined with the respective personal PIN code to trigger a silent alarm in the event of, for example, a coerced door opening or any other threatening situation.

Bookings

Whenever an event (e.g., user identification, alarm activation, etc.) occurs at a door controller, a booking is recorded in an internal booking log. These bookings can be evaluated and saved with GAT ACE 3000 and displayed on your mobile device via the GAT Mobile Access Management app.

Alarm

An access control system with Gantner door controllers supports different types of alarms. If an alarm occurs, this is indicated in the mobile app and it is possible to respond to the alarm. The term alarm refers primarily to the unauthorized access of a monitored door, however, there are also alarms that notify when a door is held open too long or they can signal any other definable, common operational function.

Batteries

Offline doors (locks) with battery supply generate warning messages when the battery charge gets too low. These can be shown in the GAT Mobile Access Management app (see "5.2.5. Area "Batteries").

Doors to load

Offline doors, which must be uploaded, e.g. because configuration or authorization data for these doors have changed in Matrix, can also be shown in the app (see "5.2.6. Area "Doors to Load").

3 INSTALLATION

Depending on the type of PC/server configuration, firstly observe the system requirements needed for installation. Then follow the instructions described in this chapter to complete the installation process.

3.1 GAT Mobile Access Server

3.1.1 Supported Operating Systems

- Microsoft® Windows® 11 (Pro, Enterprise), 64-bit
- Microsoft® Windows Server® 2016 / 2019 / 2022 / 2025 (Essentials, Standard, Datacenter), 64-bit

Please pay attention that the installation options Server Core, RT, Starter, Home, Small Business and Web editions are not supported.

NOTE! Please note that Gantner Support can only assist when the GAT Mobile Access Server is installed on a German or English version of Windows. In addition, support can only be given when the customer provides all access authorizations required by Support, e.g., access to the Windows account or the SQL database, etc.

NOTE! The customer is responsible for providing any additional licenses required, e.g., for the operating system or database.

3.1.2 Hardware Requirements

- 2 GB minimum hard drive space (system and extended logging).
- Static server IP address for access from mobile devices.
- Optional: Internet connection with a static IP address for external access.
- If anti-virus software is used, the program directory of GAT Mobile Access must be excluded from all anti-virus scans to prevent false alarms.

3.1.3 Microsoft .NET Framework

For the operation of GAT Mobile Access Management, the .NET Framework 4.7.2 must be pre-installed.

3.1.4 Additional Software and Hardware Requirements

In addition to the hardware requirements (Gantner access control system with corresponding door controllers and/or offline door locks), GAT Mobile Access Server requires the following additional software:

- GAT ACE 7000 or GAT ACE 3000

Configuration software for door controllers and offline door locking cylinders. GAT ACE 7000 or GAT ACE 3000 configures the devices of the access control system (controller, readers, door cylinders) and also regulates communication between the devices and the software.

- Matrix

Operating software for the access control system. The main activities in Matrix include assigning access authorization for system users, evaluating the system log, monitoring the status of each access point, and setting calendars/time schedules.

The GAT Matrix Synchronizer software must also be installed, configured and running.

The applications listed above do not have to be installed on the same PC as GAT Mobile Access Management, however, they must be accessible via the network.

NOTE! Please note that an unstable or slow network connection may cause problems when using the mobile app.

3.1.5 Installation of the GAT Mobile Access Server

The installation of the GAT Mobile Access server proceeds as follows.

- ▶ Double-click on the "setup.exe" file in the GAT Mobile Access Management installation package.
 - The installation assistant opens.



Figure 3.1 - GAT Mobile Access server installation - Step 1

- ▶ Click on "Next".

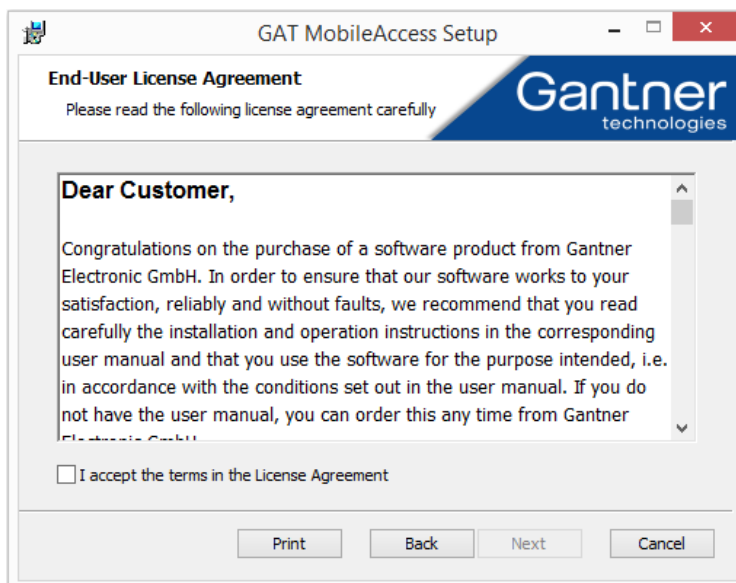


Figure 3.2 - GAT Mobile Access server installation - Step 2

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

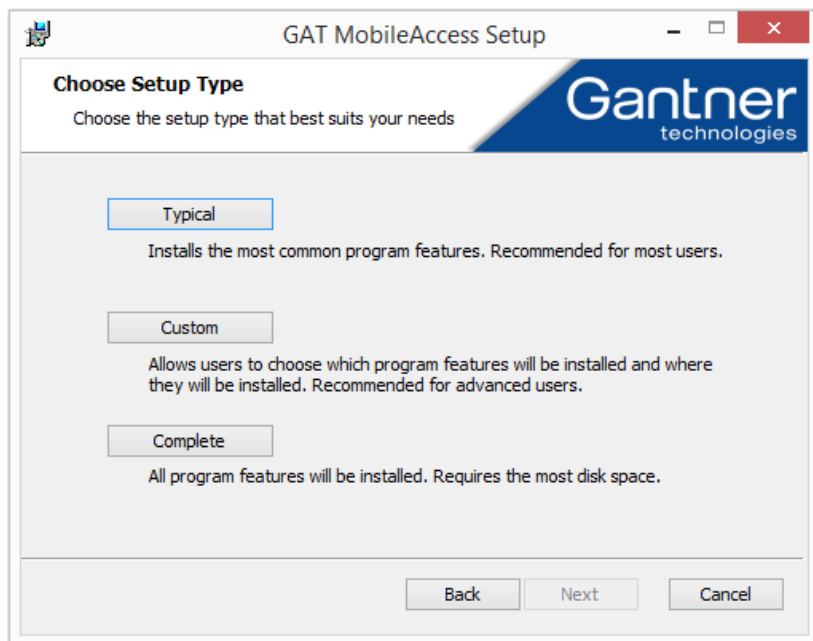
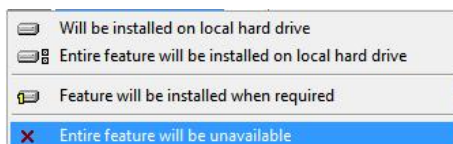


Figure 3.3 - GAT Mobile Access server installation - Step 3

- ▶ Select the type of installation:
 - Typical: Installs GAT Mobile Access Management with the standard configuration. This is the default option for most users.
 - Custom: Allows you to select the installation location and the individual components of GAT Mobile Access Management to be installed.
 - ▶ Select the components you want to install.
 - A white symbol before a component indicates that it is selected for installation.
 - ▶ To change the installation status of a component, click on the icon in front of the component and select the desired action. For example, if the GAT Mobile Access server is already installed on another server/PC and you only want to install the client, select "Entire feature will be unavailable" for the server.



- ▶ Now select the directory where you want to install the GAT Mobile Access server. If you do not want to use the default directory, click on "Browse" to select a different directory.
- ▶ Finally, click on "Next".

- Complete: This type of installation installs all the components of GAT Mobile Access Management and requires the most disk space.
- o After selecting the type of installation, the following window opens in the next step.



Figure 3.4 - GAT Mobile Access server installation - Step 4

- ▶ Click on "Install" and confirm the following authorization request with "OK".
 - o The installation process begins. A green bar indicates the progress of the installation.
- ▶ After installation is complete, click on "Finish" to exit the installation assistant.
 - o The GAT Mobile Access server is now installed and ready for use.

NOTE! Anti-Virus Software:

In regards to anti-virus software, it is vital that the installation directories of the GAT Mobile Access server are excluded from all anti-virus scans. For standard installations this applies to the following directories:

- For 32-bit Windows versions:
"C:\Programme\GAT\GAT MobileAccess"
- For 64-bit Windows versions:
"C:\Programme(x86)\GAT\GAT MobileAccess"

In addition, the GAT Mobile Access service must also be excluded from any anti-virus live scans in order to prevent the triggering of false virus alarms.

Also, read and review Microsoft's information about selecting anti-virus software for computers running SQL Server (see <https://support.microsoft.com/en-us/kb/309422>).

3.2 GAT Mobile Access App

To operate on a mobile device (smartphone or tablet), the appropriate app must be installed on the mobile device. Gantner offers the app for Android and iOS operating systems.

The app for your device can be downloaded from the device's related App Store (Google Play Store, Apple App Store).

NOTE! In addition to the requirements listed below, please take note of the current system requirements described in the documentation of the respective app store.

3.2.1 Supported Operating Systems

- Android (from version 6.0)
- Apple iOS (from version 12.2)

3.2.2 Hardware Requirements

Please note and adhere to the hardware and software requirements for the app as described in the respective app store of your mobile device. Here you will find the applicable requirements in accordance with the app version.

3.2.3 Installation of the GAT Mobile Access App

The simplest way to install the app is to download it from the respective app store to your device.

- ▶ On your mobile device, open the App Store.
- ▶ Enter a search in the app store for "GAT Mobile Access".
 - The GAT Mobile Access app is displayed after a short search.
- ▶ Click on the app then click "Install" in the app window.

Following installation, the following icon is shown on your device.



4 CONFIGURATION

4.1 Configuring the GAT Mobile Access Server

Following installation, the GAT Mobile Access server does not start automatically and must be configured first. To do so, start the "GAT Mobile Access Configuration" application.

- Start the "GAT Mobile Access Configuration" application. Following a standard installation, you will find this application in the path "All Programs" -> "GANTNER Electronic GmbH" -> "GAT MobileAccessService".

NOTE! It is recommended to run this application as an administrator as this allows you to start and stop the GAT Mobile Access server.

Figure 4.1 – "GAT Mobile Access Configuration" user interface

- First, enable all used ports.
By default, the following ports are used:
 - TCP 8234: Access from mobile terminals to the GAT Mobile Access server
 - TCP 8701: Access to GAT ACE 7000
 - TCP 8301: Access to GAT ACE 3000
 - TCP 5228, 5229, 5230: For end user devices via the Firebase Cloud Messaging platform (see note below)

NOTE! If a different port is used for one of the components listed above, the applicable port must be enabled.

NOTE! In order to allow mobile devices to receive messages (push notifications, see "4.5 Configuring the GAT Mobile Access App") via the Firebase Cloud Messaging platform, ports 5228, 5229, and 5230 must be enabled and open. On the server side, only the standard http/https ports are required.

- Connect to the Matrix database. For this step, the following information is required:
 - Database location: This is the SQL database server where the Matrix database is located.
 - Database name: The name of the Matrix database.
 - Use username and password: Select this check box to use a username and password for database access.
 - Database username: If enabled, the username for accessing the database.
 - Database password: If enabled, the password for accessing the database.
- Enter the remaining settings of the GAT Mobile Access server:
 - Service password: This is the password that mobile devices use to connect to the service (default: GAT0815).
 - Session timeout: An inactive mobile device is automatically logged out after a specified period of inactivity (in ms). The device can always log in again subject to the license permits.
 - Demo mode: The GAT Mobile Access server has a demonstration mode. In this mode, the server operates using demo data from the Matrix database. Commands are not sent to GAT ACE 7000/GAT ACE 3000.

NOTE! Never run the demo mode with productive data!
- Now establish a connection to GAT ACE 7000 or GAT ACE 3000.
- Click on the "Interfaces" button.
 - The "Interface definitions" window opens.

The screenshot shows the 'Interface definitions' window with a sidebar on the left containing three items: 'GAT ACE 3000 Matrix Client', 'GAT ACE 7000 Matrix Client' (which is highlighted), and 'GAT Matrix Client'. The main area is divided into two tabs: 'General properties' and 'Available commands'. The 'General properties' tab is active, displaying a form with the following fields and values:

InterfaceName	GatAce7000MatrixClientInterface
DisplayName	GAT ACE 7000 Matrix Client
ParallelProcessGrade	1
AceUsername	
AceUserPassword	
RemoteLocation	V-WEGR-WIN10
PortNumber	8701
ResponseTimeout	20000
MustLogin	☒
Password	*****
PasswordSalt	
Encoding	Unicode (UTF-8)
AccessTokenAudience	
AccessTokenIssuer	
AccessTokenExpiration...	0
RefreshTokenExpiration...	0
Serializer	JSON Serializer
StartOfFrame	02
EndOfFrame	03
EndOfNotificationFrame	04
CommandProtocol	Framing Bytes
IsAuditInterface	☐
IsSslActive	☐
IsAccessTokenValidati...	☒
UseUnicodePassword...	☐
EncryptionPasswordEn...	ASCIIEncoding
RecordId	0
Error	

Figure 4.2 – Setting the interface parameters

- In the left column, click on "GAT Matrix Client".
 - The interface parameters for communicating with Matrix are displayed.

The screenshot shows a window titled 'Interface definitions' with a 'Save all and close' button. On the left, there is a list of interface definitions: 'GAT ACE 3000 Matrix Client', 'GAT ACE 7000 Matrix Client', and 'GAT Matrix Client' (which is selected and highlighted in orange). The main area displays the 'General properties' for the selected 'GAT Matrix Client' interface. The properties are as follows:

InterfaceName	GATMatrixClientInterface
DisplayName	GAT Matrix Client
ParallelProcessGrade	1
RemoteLocation	GEA-VMU-081
PortNumber	8233
ResponseTimeout	20000
MustLogin	☐
Password	*****
PasswordSalt	
Encoding	Unicode (UTF-8)
Serializer	JSON Serializer
StartOfFrame	02
EndOfFrame	03
EndOfNotificationFra...	
CommandProtocol	Framing Bytes
IsAuditInterface	☐
UseUnicodePassword...	☐
EncryptionPasswordE...	ASCIIEncoding
RecordId	0
Error	

- Enter the following data:
 - RemoteLocation: Enter the server name where Matrix is installed. If this is the same location where the GAT Mobile Access Management server is installed, use "localhost".
 - PortNumber: If default port 8233 is not used for Matrix, enter the correct port here.
 - Serializer: What to set here depends on the used Matrix version:
 - for Matrix version 4 and older versions select "Binary Matrix Serializer".
 - for Matrix versions 5 or 6 "Binary Matrix Serializer" or "JSON Serializer" are possible.
 - for Matrix version 7 and higher only "JSON Serializer" is possible.
- All other values can be left as the default setting provided the corresponding values in Matrix were not changed.
- In the left column, click on "GAT ACE 7000 Matrix Client" or "GAT ACE 3000 Matrix Client", depending on which version of GAT ACE you are using.
 - The interface parameters for communicating with GAT ACE 7000 / 3000 are displayed.
- Enter the following data:
 - RemoteLocation: Enter the server name where GAT ACE 7000 / 3000 (the Windows service) is installed. If this is the same location where the GAT Mobile Access server is installed, use "localhost".
 - PortNumber: If default port 8701 is not used for GAT ACE 7000 or default port 8301 not used for GAT ACE 3000, enter the correct port here.
 - Password: If you have assigned another interface password for GAT ACE 7000 / 3000, enter the password here.
 - IsSslActive: If the secure connection via TLS is to be used to connect to GAT ACE 7000 or 3000, select the "IsSslActive" option. The TLS connection must then also be enabled in GAT ACE 7000 or 3000. For further information regarding the TLS connection, see "4.4 Establishing a TLS Connection to GAT ACE").

- IsAccessTokenValidationActive:

This setting is used to enable authentication using JWT tokens, which should always be enabled in combination with TLS (see "4.4 Establishing a TLS Connection to GAT ACE").

- AceUsername, AceUserPassword:

When the validation via access tokens is being used, a valid GAT ACE 7000 user with password must be entered here.

- All other values can be left as the default setting provided the corresponding values in GAT ACE 7000 / 3000 were not changed.
- Click on "Save all and close".

GAT Mobile Access Management operates for 14 days in demo mode and for a further 14 days after entering a license without activation. Therefore, you must purchase a license for Mobile GAT Access Management and enter it as follows.

- In the user interface of the configurator, click on "License".

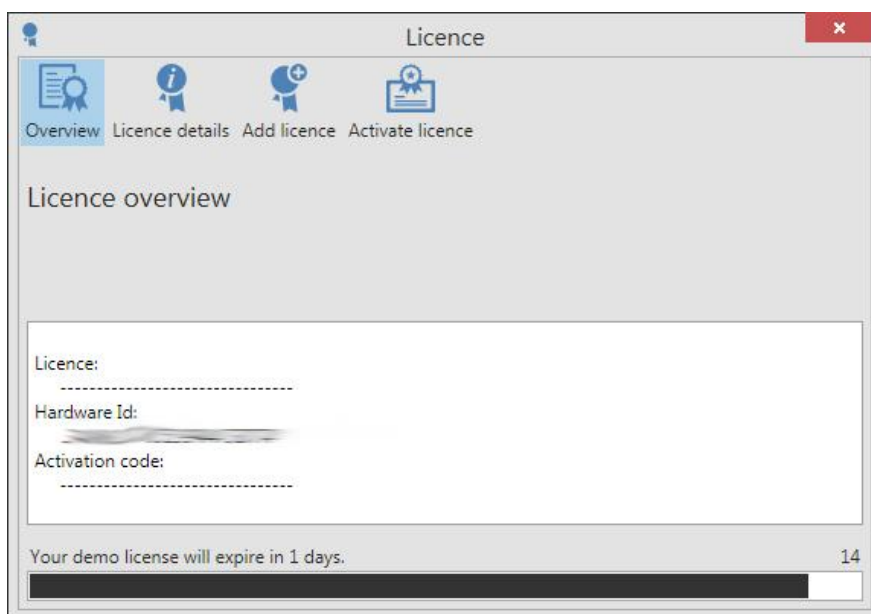


Figure 4.3 – License management

- In the "Overview" tab you will find the license, hardware ID and information about the duration of the license and when you need to enter a license code.
- Click on "Add license" to add a license.

NOTE! You can either type the license code in manually or import it from a file. Please contact your local distributor or the appropriate Gantner subsidiary to obtain a license.

- Click on "Activate license" to activate your license using an activation code.

NOTE! You will receive the activation code from your local distributor or the appropriate Gantner subsidiary. For the activation code you will need your license code and the hardware ID of the PC/server, on which the GAT Mobile Access server is installed.

- In the user interface of the configurator, click on "Save settings" to save all the settings.
- In the user interface of the configurator, click on "Start service" to start the GAT Mobile Access server.

- Wait until a message indicating the successful launch of the server is displayed.
 - Open an internet browser (preferably on another PC) and enter the following URL:
`http://<Server>:8234/MobileAccessService/TestService/wp=<WebServicePassword>`
(replace <Server> and <WebServicePassword> with your configuration details. For <Server> you can use the name or IP address.
Example: `http://mademo.gantner.com/MobileAccessService/TestService/wp=GAT0815`
 - The response is delivered in JSON format and when successful, should look as follows:

```
{"m": "Everything seems to be configured correctly. Please note that the connections to GAT ACE 7000 and 3000 are not checked with this.", "s": true}
```
- NOTE!** For security reasons, delete the browser cache after testing the connection as the web service password is sent along with the test.

4.2 Startup Settings of the GAT Mobile Access Server

When the GAT Mobile Access server and the Matrix database are installed on the same PC, it is possible that the GAT Mobile Access server starts before the SQL database service. In this situation, the connection to the database is not made and the GAT Mobile Access server is not able to provide data.

This issue is easily solved.

- Open the Windows "Run" dialog via the "Windows" + "R" keyboard shortcut.
- Type "services.msc" into the field then click on "OK".
 - The Windows Services window opens.

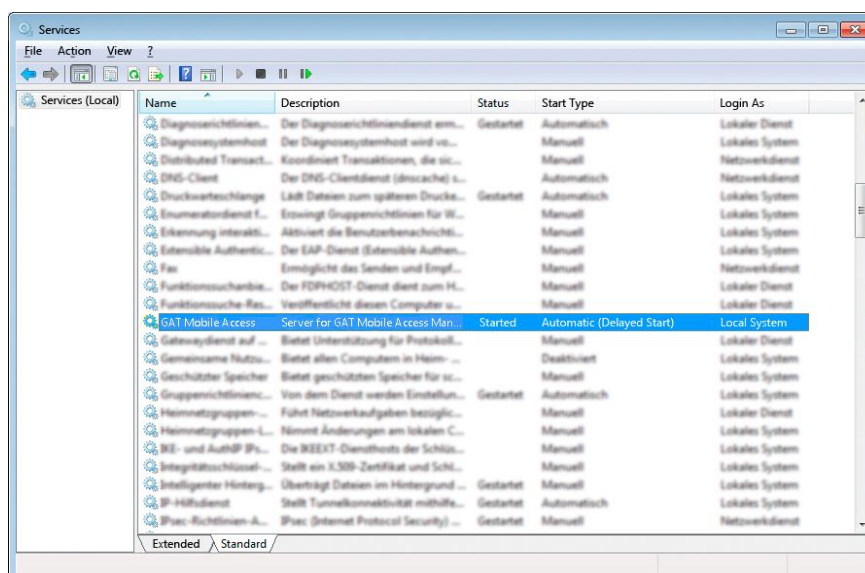


Figure 4.4 - Windows Services

- Here the "GAT Mobile Access" service must be started (see column "State"). You can mark the entry and press "Start" on the left of the list in order to start the service or restart the service with click on "Restart".

4.3 Setting Up HTTPS for Mobile Access Management

This process encrypts the connection between the GAT Mobile Access app on the mobile device and the server of GAT Mobile Access Management. It is recommended to complete this process to ensure security is maintained.

The following prerequisites must be met before setting up HTTPS for Mobile Access Management:

- Mobile Access Management installed (see chapter “3 INSTALLATION”).
- HTTPS certificate available.
- DNS and port forwarding completed.

Installing the IIS (Internet Information Service) Web Server

- Open “Server Manager”.
- Click on “Add Roles and Features”.
- In the “Roles” list, add the “Web Server (IIS)” role and click on “Install”.

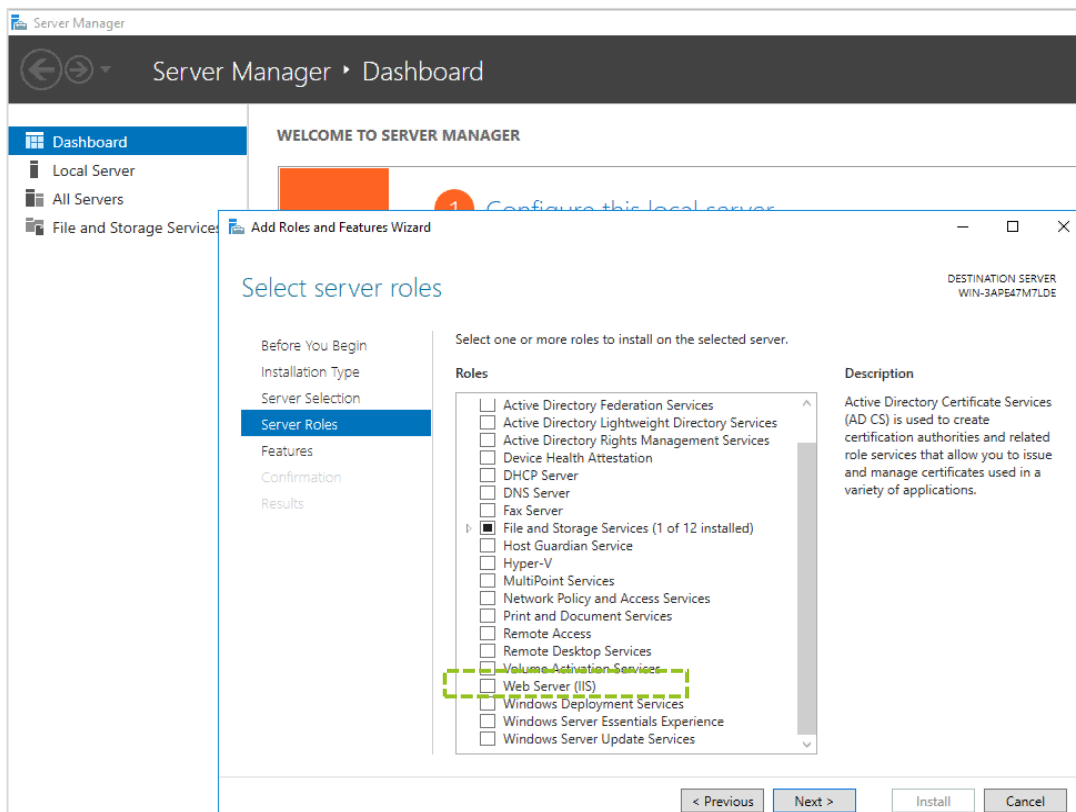


Figure 4.5 – Server Manager – Add “Web Server (IIS)” role

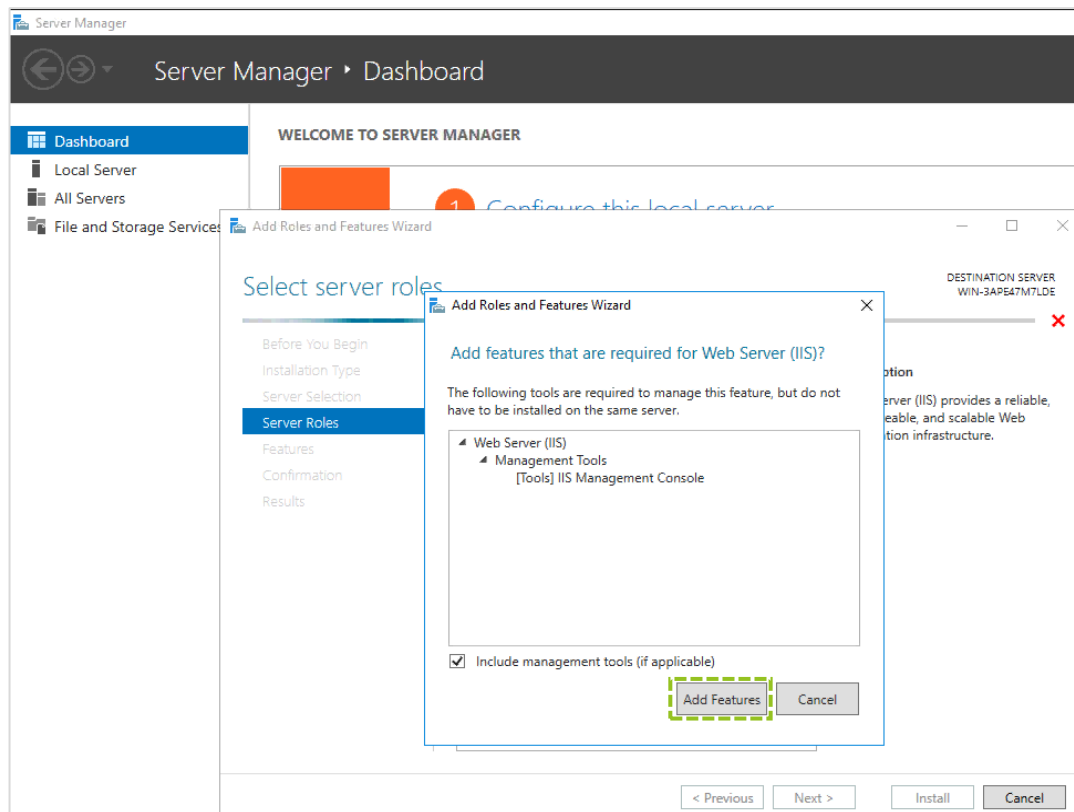


Figure 4.6 – Server Manager – Add “Web Server (IIS)” role

- The “Add Roles and Features Wizard” opens.
- ▶ Leave these settings as default and click on “Add Features”.
 - The installation wizard installs the IIS Web Server, which may take a few minutes to complete.

Installing ARR (Application Request Routing)

- ▶ To install “Application Request Routing”, go to <https://www.microsoft.com/web/downloads/platform.aspx>.
- ▶ Click on “Install this extension”, and then “Save file” in the installation window.
 - The download for “Microsoft Web Platform Installer 5.0” starts.
- ▶ Install the extension after it has downloaded.
- ▶ Following installation, click on “Application Request Routing” in the top-right side of the window.
 - The following window is displayed.

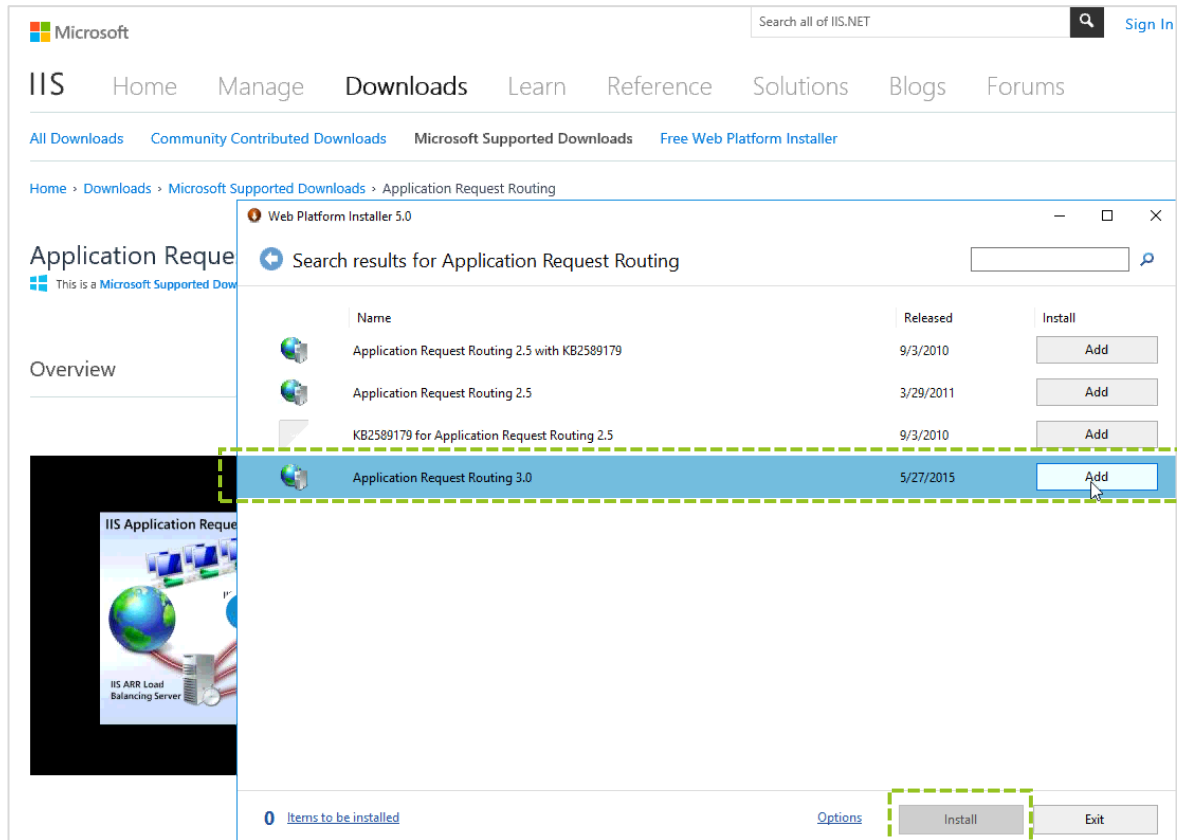


Figure 4.7 – Microsoft Web Platform 5.0 – Application Request Routing

- Click on “Add” for “Application Request Routing 3.0” and then click on “Install” at the bottom of the window.

Configuring the IIS Web Server

- Open “Internet Information Service (IIS) Manager” from the Windows Start menu (under “Windows Administrative Tools”).
- To enable application request routing, open the IIS server home page and click on “Application Request Routing”.

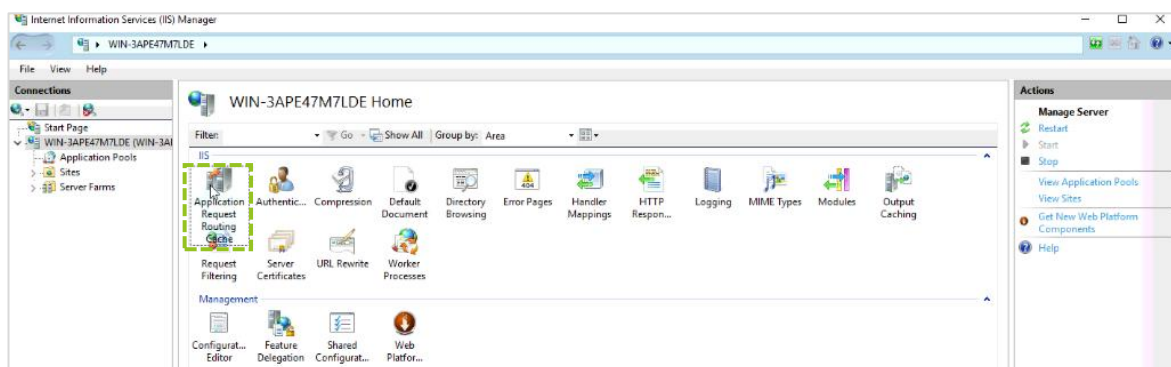


Figure 4.8 – IIS Manager – Application Request Routing

- In the “Actions” column to the right, click on “Server Proxy Settings...”.

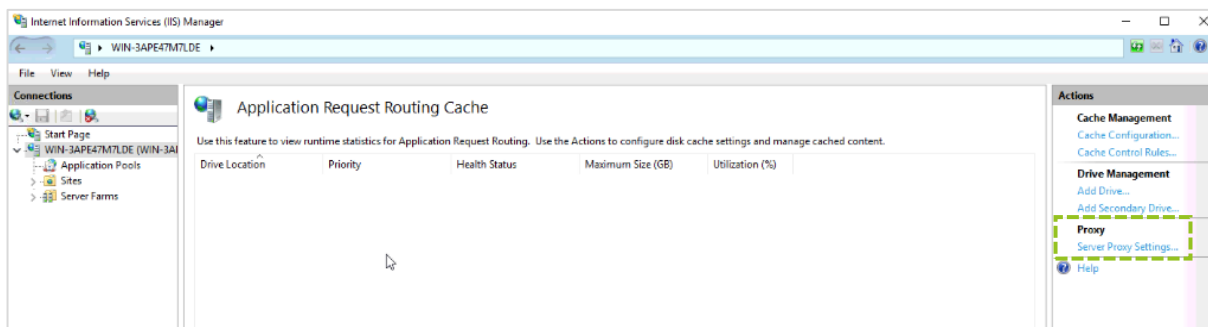


Figure 4.9 – IIS Manager – Server Proxy Settings

- Select the “Enable proxy” option (leave the other settings unchanged), and then click on “Apply” in the “Actions” column to the right.

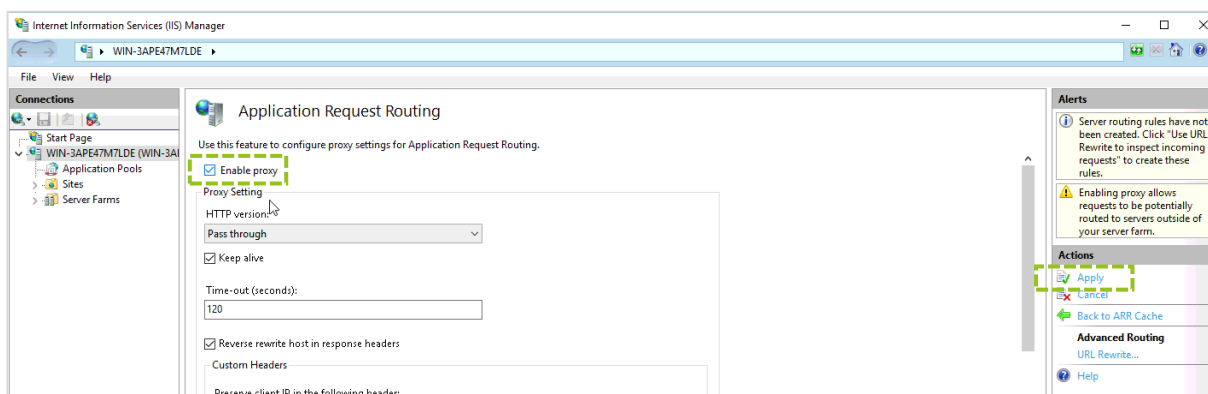


Figure 4.10 – IIS Manager – Enable proxy option

- Return to the IIS server home page and click on “Server Certificates” to import the certificate for HTTPS.

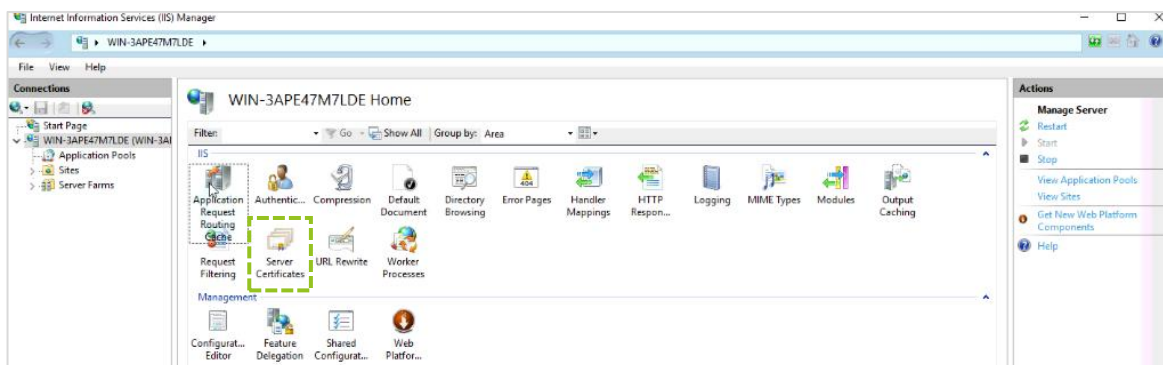


Figure 4.11 – IIS Manager – Server Certificates

- In the “Actions” column to the right, click on “Import...”.
- In the “Import Certificate” window, enter the file location and password of the certificate, and then click on “OK”.

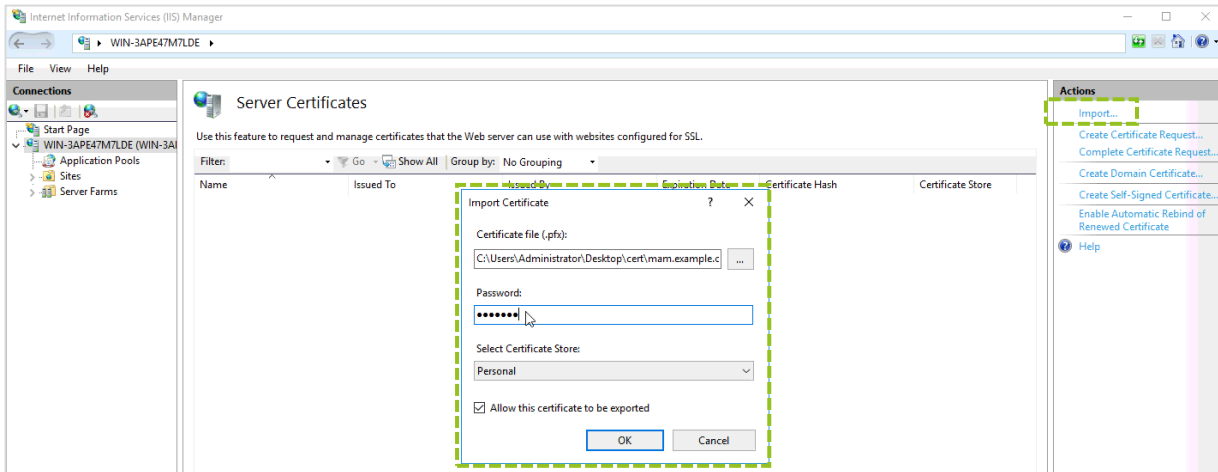


Figure 4.12 – IIS Manager – Import Certificate

- In the “Connections” column to the left, open the “Sites” folder, right click on the “Default Website”, and then select “Remove” from the menu.

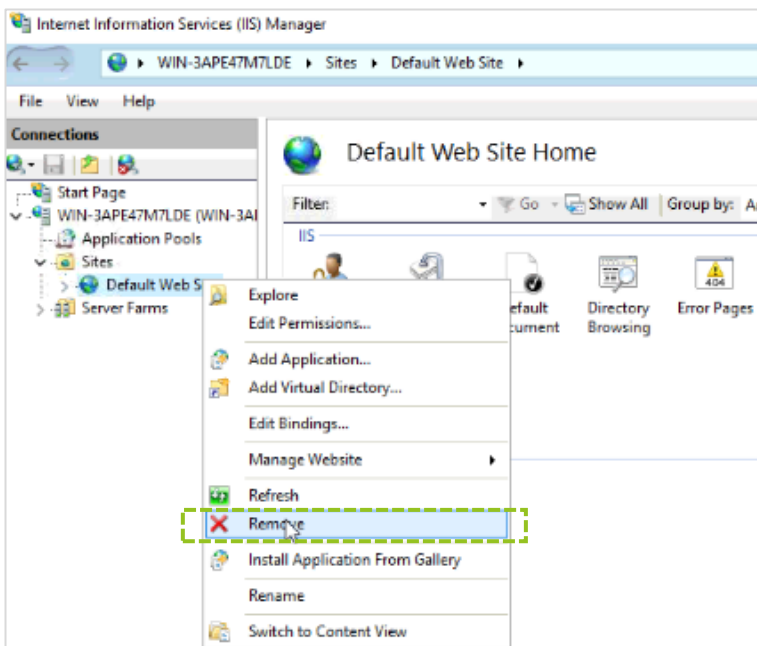


Figure 4.13 – IIS Manager – Remove default website

- In the “Connections” column to the left, right click on the “Sites” folder, and then select “Add Website” from the menu.

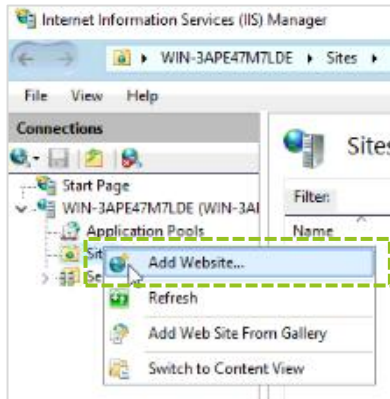


Figure 4.14 – IIS Manager – Add new website

- The “Add Website” window opens.

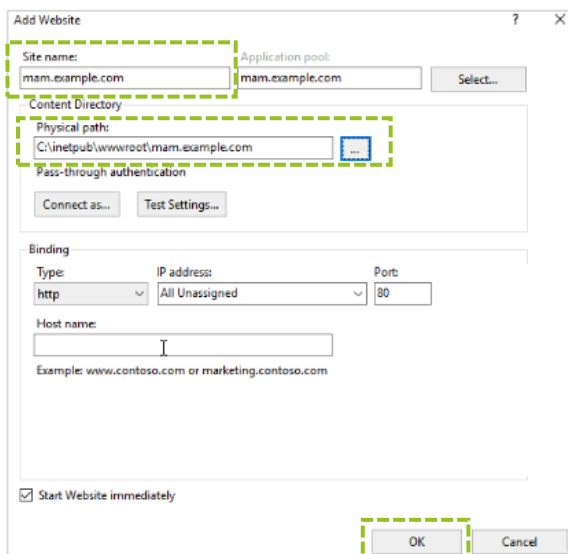


Figure 4.15 – IIS Manager – Add Website

- Enter the following information:
 - Site name: Enter the domain name that will be used for Mobile Access Management, e.g., `mam.example.com`
 - Physical path: Enter the path of the website, e.g., `C:\inetpub\wwwroot\mam.example.com`.
- Click on “OK” to save the settings.

- Open the created website and click on “Bindings...” in the “Actions” column to the right.
- Click on “Add” to add another binding for this site, and then configure the following settings in the “Add Site Binding” window:
 - Type: Select “https” from the menu.
 - Host name: Enter the DNS name of the website, e.g., mam.example.com
 - SSL certificate: Select the imported certificate (as imported via “Server Certificates” on the IIS home page).

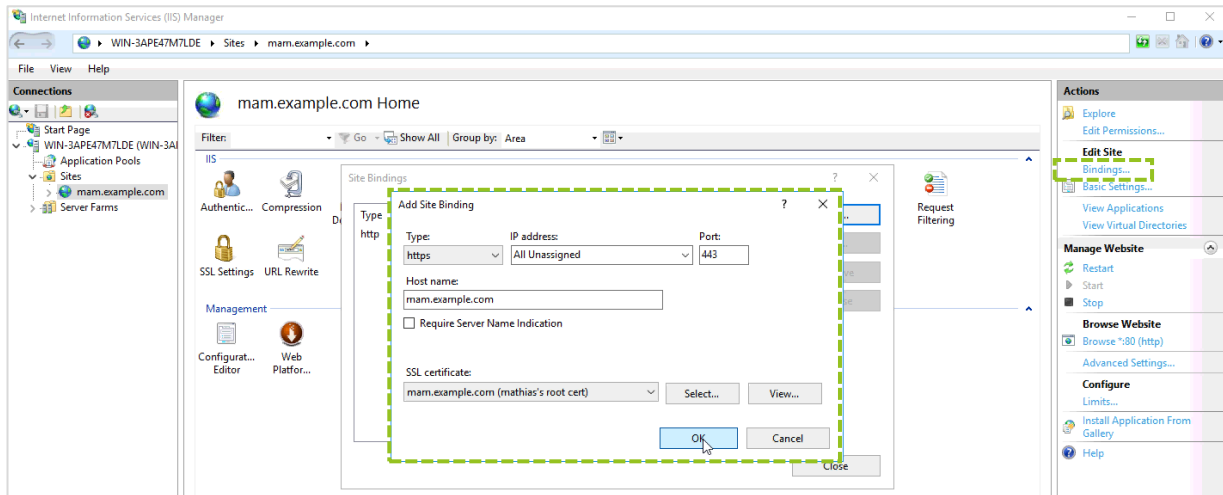


Figure 4.16 – IIS Manager – Add Site Binding

- Click on “OK” to save the settings, and then click on “Close” in the “Site Bindings” window.
- On the home page of the current site, click on “URL Rewrite”.

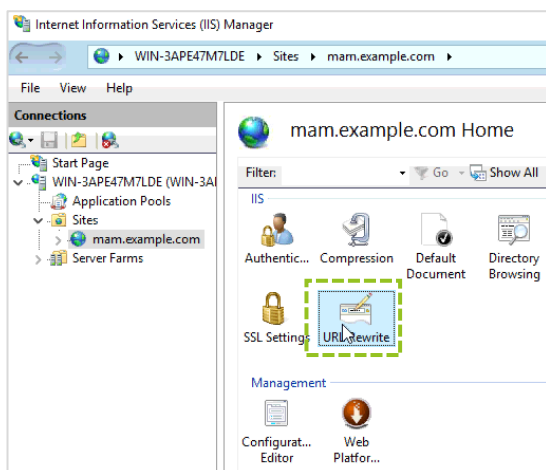


Figure 4.17 – IIS Manager – URL Rewrite

- In the “Actions” column to the right, click on “Add Rule(s)...”.

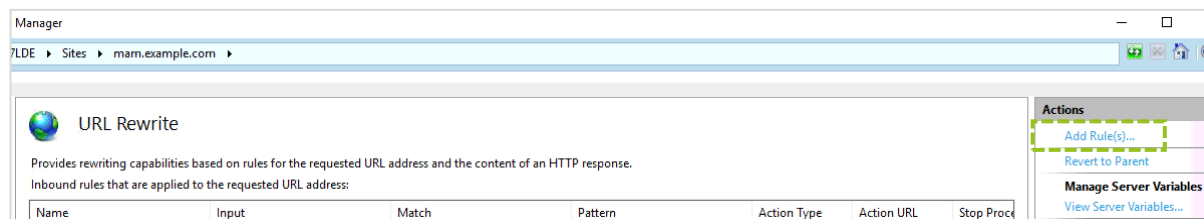


Figure 4.18 – IIS Manager – Add Rule(s)

- In the “Add Rule(s)” window, select “Blank rule”, and then click “OK”.

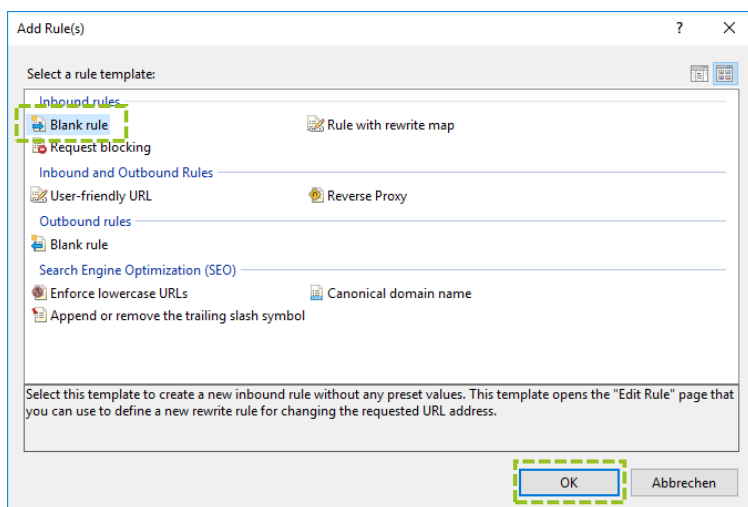


Figure 4.19 – IIS Manager – Blank rule

- In the “Edit Inbound Rule” window, configure the following settings:
 - Name: Enter “HTTP to HTTPS” into the field.
 - Pattern: Enter “(.*)” into the field.

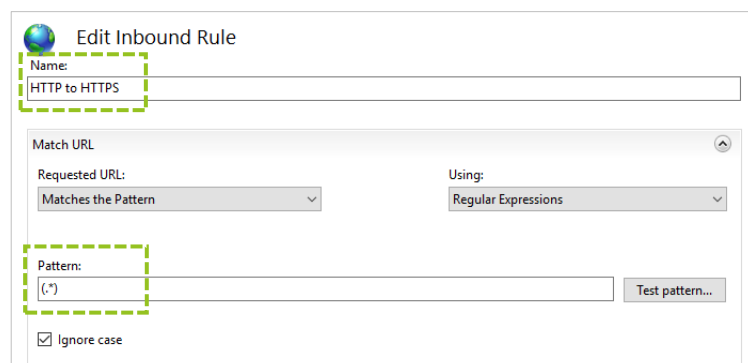


Figure 4.20 – IIS Manager – Edit Inbound Rule

- Open the “Conditions” menu, and then click on “Add...”

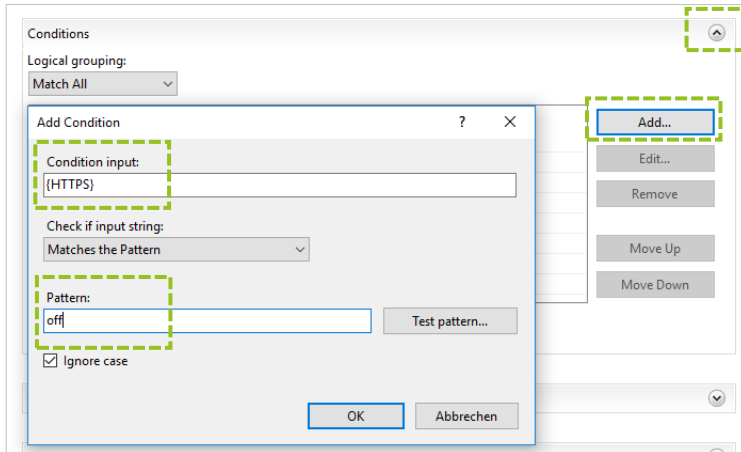


Figure 4.21 – IIS Manager – Add Condition

- In the “Add Condition” window, configure the following settings, and then click “OK”:
 - Condition input: Enter “{HTTPS}” into the field.
 - Pattern: Enter “off” into the field.
- Open the “Action” menu, and configure the following settings:
 - Action type: Select “Redirect” from the menu.
 - Redirect URL: Enter “https://<domain name>/{R:1}” e.g., “https://mam.example.com/{R:1}”.
 - Redirect type: Select “Permanent (301)” from the menu.

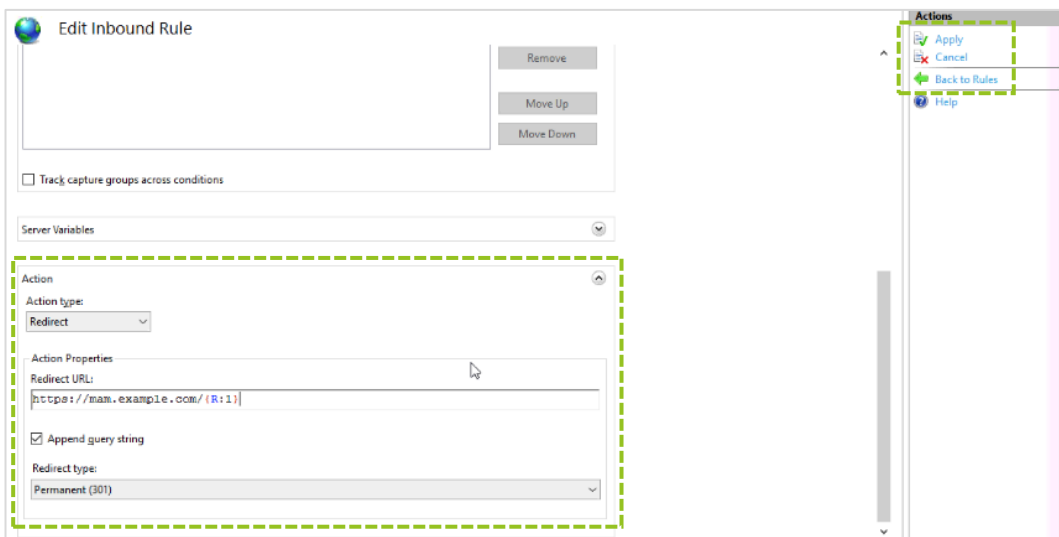
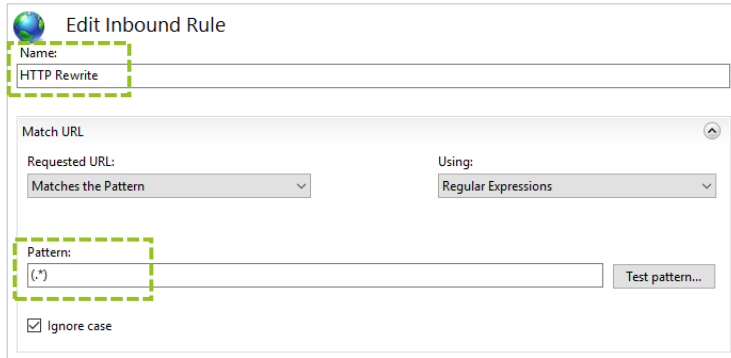


Figure 4.22 – IIS Manager – Action

- In the “Actions” column to the right, click “Apply”, and then click “Back to Rules”.

- Add another rule by clicking on “Add Rule(s)...” and “Blank rule”. Configure the following settings:
 - Name: Enter “HTTP Rewrite” into the field.
 - Pattern: Enter “(.*)” into the field.



Edit Inbound Rule

Name: HTTP Rewrite

Match URL

Requested URL: Matches the Pattern Using: Regular Expressions

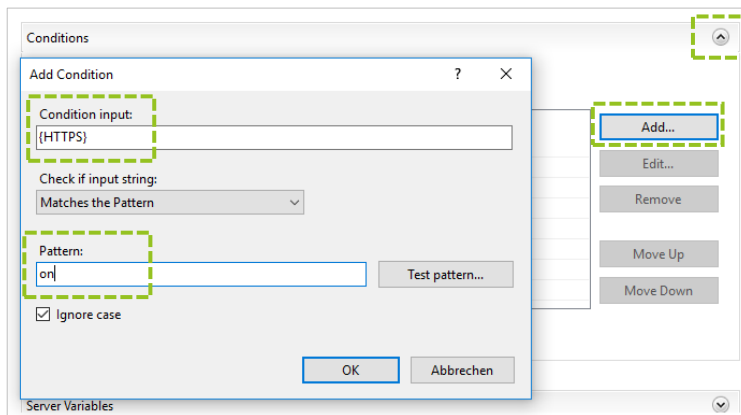
Pattern: (.*)

☒ Ignore case

Test pattern...

Figure 4.23 – IIS Manager – Edit Inbound Rule

- Open the “Conditions” menu, and then click on “Add...”



Add Condition

Condition input: {HTTPS}

Check if input string: Matches the Pattern

Pattern: on

☒ Ignore case

OK Abbrechen

Test pattern...

Conditions

Add... Edit... Remove Move Up Move Down

Server Variables

Figure 4.24 – IIS Manager – “Add Condition” window

- In the “Add Condition” window, configure the following settings, and then click “OK”:
 - Condition input: Enter “{HTTPS}” into the field.
 - Pattern: Enter “on” into the field.

- Open the “Action” menu, and configure the following settings:
 - Action type: Select “Rewrite” from the menu.
 - Rewrite URL: Enter “http://<internal path to Mobile Access Management service>:8234/{R:1}”, e.g., http://localhost:8234/{R:1}
 - Mark the “Stop processing of subsequent rules” option.



Figure 4.25 – IIS Manager – “Action”

- In the “Actions” column to the right, click “Apply”.
 - The setup for HTTPS is now complete.
- To check that it is functioning, open a web browser and enter the following URL:

http://<your domain name>/MobileAccessService
(e.g., http://mam.example.com/MobileAccessService)

 - A page such as the following should be shown. Confirm that the URL has changed from “http://...” to “https://...”.

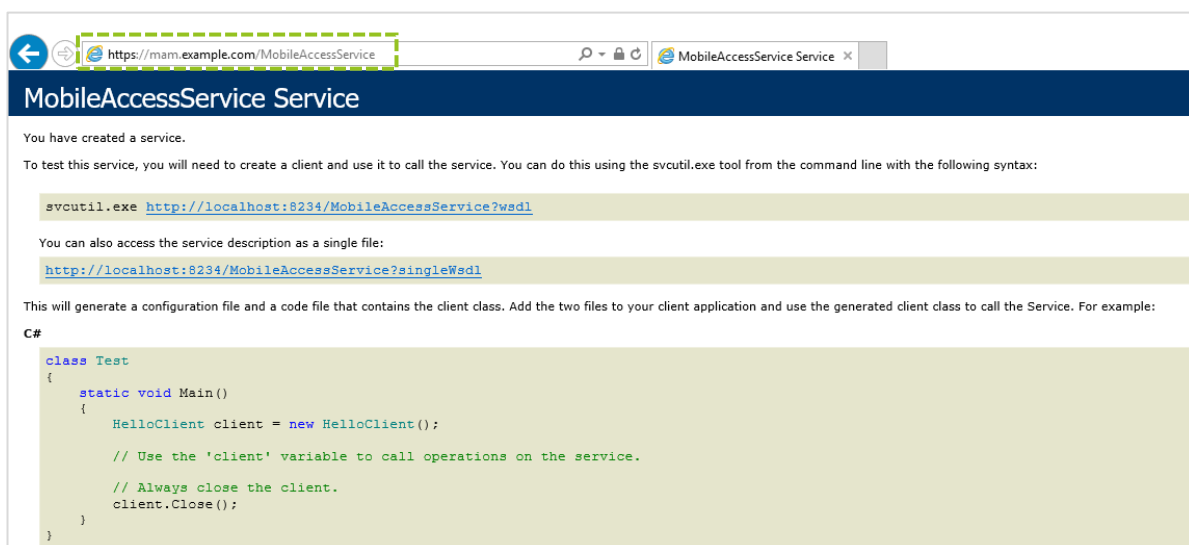


Figure 4.26 – Testing the HTTPS connection

4.4 Establishing a TLS Connection to GAT ACE

The communication between the GAT Mobile Access Server and GAT ACE 3000 or 7000 can be optionally encrypted using the TLS protocol (previously called SSL). A certificate provided by the customer can be used for this, or a self-signed certificate can be generated.

TLS must be activated for the GAT Mobile Access Server as well as in the configuration file of GAT ACE 3000 or 7000.



Please also read the detailed information regarding the TLS connection in the GAT ACE manual.

4.4.1 GAT Mobile Access Configuration

To enable TLS encryption for GAT ACE, proceed as follows.

- In the GAT Mobile Access Configuration, click on "Interfaces".
 - The following window opens.

The screenshot shows the 'Interface definitions' window with the following configuration for 'GAT ACE 7000 Matrix Client':

Parameter	Value
InterfaceName	GatAce7000MatrixClientInterface
DisplayName	GAT ACE 7000 Matrix Client
ParallelProcessGrade	1
AceUsername	
AceUserPassword	
RemoteLocation	V-WEGR-WIN10
PortNumber	8701
ResponseTimeout	20000
MustLogin	☒
Password	*****
PasswordSalt	
Encoding	Unicode (UTF-8)
AccessTokenAudience	
AccessTokenIssuer	
AccessTokenExpiration...	0
RefreshTokenExpiration...	0
Serializer	JSON Serializer
StartOfFrame	02
EndOfFrame	03
EndOfNotificationFra...	04
CommandProtocol	Framing Bytes
IsAuditInterface	☐
IsSslActive	☒
IsAccessTokenValidati...	☒
UseUnicodePassword...	☐
EncryptionPasswordE...	ASCIIEncoding
RecordId	0
Error	

Figure 4.27 - Configuring the interface parameters

- On the left, select the GAT ACE client that you want to configure (GAT ACE 7000 for example).
- Enable the "IsSslActive" parameter.

- If desired, also enable "IsAccessTokenValidationActive". This parameter specifies whether authentication using JWT tokens is enabled, which should always be active in connection with TLS. After enabling the parameter, enter the following information:
- AceUsername: Username for logging in to GAT ACE.
- AceUserPassword: Password for logging in to GAT ACE.
- Confirm by clicking on "Save".

4.4.2 GAT ACE 3000 and 7000

In GAT ACE 3000 or 7000, TLS must be enabled in the configuration file, which is a text file that you can open in a text editor. An entry must be made in this file and to do this for GAT ACE 7000, complete the following steps:

- Open the "GATAce7000.cfg" file in the default path of the GAT ACE 7000 software.



```

22 <password TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">z86d3tImkM8z1sUbh7ho0NwtwOcEx26PS8NM04sDHY=</pa
23 <portnumber TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">8700</portnumber>
24 <refreshtokenexpirationinseconds TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">604800</refreshtokenexpir
25 <remotelocation TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">V-WEGR-WIN10</remotelocation>
26 <responsetimeout TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">2000</responsetimeout>
27 <serializer TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">JSON Serializer</serializer>
28 <sslcertificatethumbprint TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">85E711B85CFE1417D5EDE15229CF3AC
29 <startofframe TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">02</startofframe>
30 <storelocation TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">CurrentUser</storelocation>
31 <useunicodepasswordencoding TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">False</useunicodepasswordencod
32 </Ace7Interface>
33 <MatrixInterface TYPE="GROUP" ID="0" TEXT="MatrixInterface" DESCRIPTION="MatrixInterface">
34 <accesstokenexpirationinseconds TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">3600</accesstokenexpiratio
35 <commandprotocol TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">FramingBytes</commandprotocol>
36 <displayname TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">
37 </displayname>
38 <encoding TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">utf-8</encoding>
39 <endofframe TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">03</endofframe>
40 <endnotificationframe TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">04</endnotificationframe>
41 <isaccesstokenvalidationactive TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">False</isaccesstokenvalidat
42 <isauditinterface TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">False</isauditinterface>
43 <issslactive TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">True</issslactive>
44 <mustlogin TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">True</mustlogin>
45 <password TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">EK7WhmpODxRE+HZchNc5XtVIsH1d73aiJShc50RozCM=</pa
46 <portnumber TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">8701</portnumber>
47 <refreshtokenexpirationinseconds TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">604800</refreshtokenexpir
48 <remotelocation TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">V-WEGR-WIN10</remotelocation>
49 <responsetimeout TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">2000</responsetimeout>
50 <serializer TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">JSON Serializer</serializer>
51 <sslcertificatethumbprint TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">830114C1E61E541F68298EB4CA4143FF
52 <startofframe TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">02</startofframe>
53 <storelocation TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">CurrentUser</storelocation>
54 <useunicodepasswordencoding TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">False</useunicodepasswordencod
55 </MatrixInterface>
56 <BuildingMgmtInterface TYPE="GROUP" ID="0" TEXT="BuildingMgmtInterface" DESCRIPTION="BuildingMgmtInterf
57 <accesstokenexpirationinseconds TYPE="FIELD" ID="0" TEXT="" DESCRIPTION="">3600</accesstokenexpiratio

```

Figure 4.28 – Configuration data for GAT ACE 7000

- In the "MatrixInterface" section, set the value of "issslactive" to "True".
- For authentication using JWT tokens, also set the "isaccesstokenvalidationactive" option to "True".
- Restart the GAT ACE 7000 service.

The same setting is necessary for GAT ACE 3000. The name of the configuration file is "GATAce3000.cfg", and the setting can be found there in the "issslactive" line within the "GatAceMatrixServerInterface" section.

i In the GAT ACE 7000 and 3000 manuals, additional information is available on activating TLS encryption and installing the necessary certificate.

4.5 Configuring the GAT Mobile Access App

After installing the app, you can adjust the configuration settings that affect the entire app. Several configurations can be saved, each with different login data. GAT Mobile Access remembers the selected configuration so that it is used for each subsequent login unless another configuration is selected manually.

NOTE! The following description shows the settings in the Android app. The settings are the same for the iPhone app.

- ▶ Start the app.
- ▶ On the login screen, press the "Settings" icon. Depending on the operating system, this is displayed as follows.

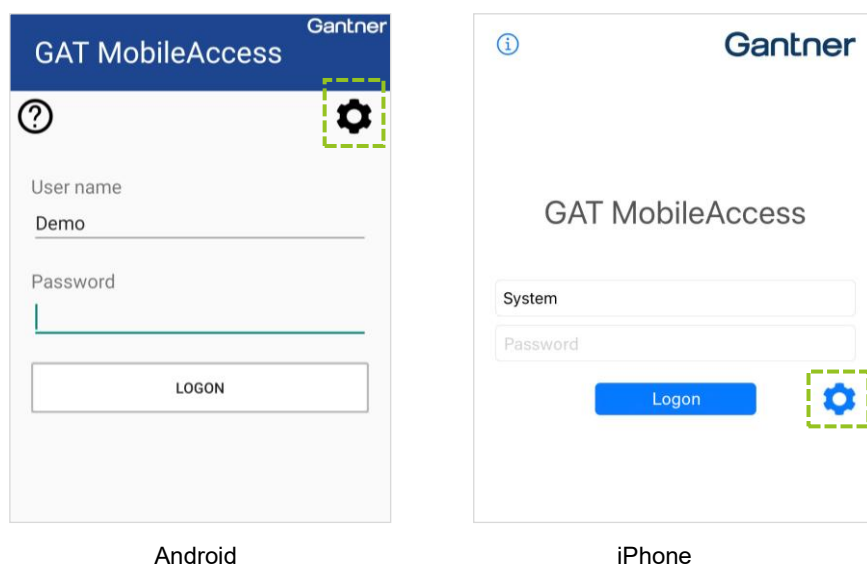


Figure 4.29 – Configuration settings page

- The list of defined configurations opens. The currently active configuration is marked with a tick (here "GAT Mobile Access Demo Server"). The configuration will be used to log in to the app.

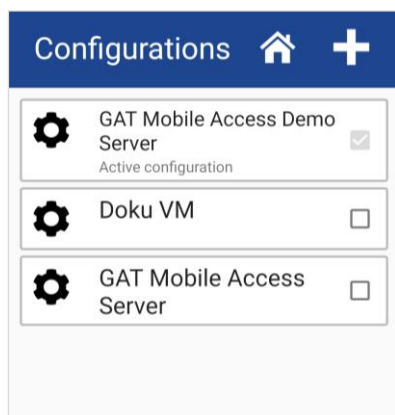


Figure 4.30 – App settings for Android

- ▶ To activate another configuration, press the box to the right of the desired configuration or press an inactive configuration for a few seconds and then select "Set as active configuration" from the menu that appears.
 - The configuration is marked with a tick and displayed in the top position.
- ▶ The "🏠" icon returns you to the login screen.
- ▶ You can create a new configuration via the "+" icon.
- ▶ You can change the configuration settings by pressing a configuration.
 - In both cases, the settings page of the configuration opens.
 - The configuration is divided into two tabs: "Server" and "Content" (shown beside each other on Android and beneath each other on iPhone).

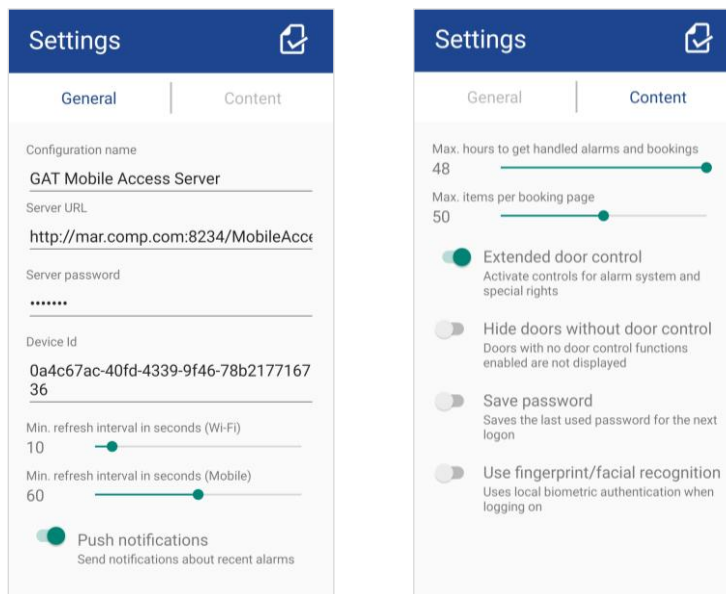


Figure 4.31 – App settings for Android

- ▶ On the "Server" page, define the following settings.
 - Configuration name: Enter a name for the configuration here.
 - Server URL: This is the URL where the GAT Mobile Access Management server is contacted. Enter the URL in the following format:
`http://<Server>:8234/MobileAccessService`
 The <Server> field must be replaced with the correct server IP address or name entered between the brackets, e.g., the demo server has the name `mademo.gantner.com`). The port 8234 and MobileAccessService are the default values and applicable for a standard installation without any modifications.
 - Server password: The password of the GAT Management Mobile Access server, as defined during installation (default = GAT0815).
 - Device ID: Here the ID of your mobile device is displayed. You must enter this device ID in Matrix to register your mobile device (see below).
 - Min. refresh interval in seconds (Wi-Fi):
 When the mobile device is connected via a LAN connection, the app content is automatically updated at the defined interval shown here (in seconds). Note that different areas of the app can deviate from this setting.

- Min. refresh interval in seconds (Mobile):

When the mobile device is connected via a GSM connection, the app content is automatically updated at the defined interval shown here (in seconds). Note that different areas of the app can deviate from this setting.
- Push notifications: Specify here whether you want to receive push notifications from the server. Please note that both the mobile device and the GAT Mobile Access Management server must be configured to receive push notification services (Firebase Cloud Messaging). Not all mobile devices support push notifications. Changes to this setting are activated following a successful login.

NOTE! Also take note of the information regarding the availability and performance of the respective push notification service.
- On the "Content" page, define the following settings.
 - Max. hours to get handled alarms and bookings:

Bookings and processed alarms are only displayed for a definable number of hours. Bookings and processed alarms that occurred before this time are not displayed.
 - Max. items per booking page:

Number of bookings that are displayed per page. If there are significant delays in the presentation of the bookings data, please reduce this value.
 - Extended door control: On the "door control" page, this option enables the additional controls for monitoring and special rights.
 - Hide doors without door control:

When this setting is enabled, only those doors for which the door control function is enabled in Matrix are displayed.
 - Save password: Save the password last used to login so it is automatically available for the next login.

ATTENTION! Note that by activating this setting there is an increased security risk for the system should your mobile device become lost or stolen.
 - Use fingerprint/facial recognition:

When this setting is enabled, the biometric recognition of the mobile device (fingerprint or face recognition) can be used to log in to the app instead of a password (see "5.1 Startup and Login").
- To save the changes to the configuration, press the "" icon.
- If you want to delete a configuration, press a configuration (only inactive configurations) for a few seconds and select "Delete configuration" from the menu displayed.

4.5.1 Language

The GAT Mobile Access Management app supports English and German. When the app is installed on a mobile device set to operate in German, German is automatically used for the app, otherwise English is used.

4.6 Registering a Mobile Device in Matrix

To use a mobile device with GAT Mobile Access Management, the mobile device must be first registered and assigned to a user in Matrix. Complete this procedure as follows:

- ▶ Open Matrix and go to the "File" menu -> "User Management" menu item).
- ▶ Select the desired user profile from the list then click on the "Edit User" symbol.
 - The following window opens.

Id	Name	C	R	U	D	E
34	Multi-site management					☐
35	Active directory settings					☐
36	Blacklist	☐	☒	☐	☐	
GAT Mobile Access Management						
100	Doors Management	☒	☒	☒	☒	
101	Persons Management	☒	☒	☒	☒	
102	Alarms Management	☒	☒	☒	☒	
103	Bookings Management	☒	☒	☒	☒	
104	Battery Warnings Manage...	☒	☒	☒	☒	
105	Doors to Load Management	☒	☒	☒	☒	
General						
1	Role Management	☐	☐	☐	☐	
2	User Management	☐	☐	☐	☐	

Figure 4.32 – Editing user details in Matrix

- ▶ In the "Device ID" field, enter the device ID of each mobile device separated by a semicolon ";". The device ID is found in the settings under "Device ID" (see previous section).

NOTE! Ensure to enter the device ID in case-sensitive format.

- ▶ Set the desired permissions in the section "GAT Mobile Access Management".

NOTE! The ID of a mobile device remains active as long as the app is installed and updated. However, the device ID may need to be updated if the requirements of individual platforms are changed.

i If the mobile app is registered in an access system and you want to use the app in another system, you must first uninstall the app and reinstall it afterwards. This is necessary so that the push notifications in the new system work correctly. This procedure generates a new device ID, which must then be entered into the new system (Matrix) as described above.

5 OPERATION

In this chapter you will find an overview of the functionality of the GAT Mobile Access app. The operation described in this section is based on the Android operating system; however, the app is designed to operate in a similar manner across all platforms. Any platform-specific exceptions are specially noted.

5.1 Startup and Login

When the GAT Mobile Access server and the GAT Mobile Access app are both configured as required, you can use the app for the first time. To do this, you must log in with your user account.

To log in, the combination of username or the biometric recognition via fingerprint or facial recognition supported by the mobile device can be used. To use biometric recognition, it must be enabled in the configuration ("Use fingerprint/facial recognition" setting -> see "4.5 Configuring the GAT Mobile Access App").

ATTENTION! When you have finished using the app, always log out via the  icon to maintain system security. The login screen is displayed after you have logged out.

5.1.1 Login with Username and Password



This login option can always be used, even if biometric recognition is enabled.

- Start the app.
 - If biometric recognition is disabled, the input fields for username and password are displayed.

Android

iPhone

Figure 5.1 – Login screen for username and password on the various operating systems

- If biometric recognition is enabled, only the username is displayed initially. By pressing "LOGON", the option for biometric recognition (see next page) is displayed. Press "CANCEL" here. The biometric recognition is canceled, and Figure 5.1 is displayed.

- ▶ Enter your username and password.
 - NOTE!** As your mobile device was assigned to your user profile in Matrix (see "4.6 Registering a Mobile Device in Matrix"), you use the same username and password to log in to the app as you do for logging in to Matrix.
- ▶ Now press "LOGON".
 - The start screen of GAT Mobile Access is displayed.

NOTE! If GAT Mobile Access is operating in demo mode, enter "demo" for both the username and password.

5.1.2 Login with Biometric Recognition

Biometric recognition can be enabled via the option "Use fingerprint/facial recognition" in the settings. The biometric function of the mobile device is used. For fingerprint identification, the mobile device must therefore have a fingerprint reader and you must have already scanned a fingerprint. The same applies for face recognition using an integrated camera and a face previously scanned on the mobile device.

- ▶ Start the app.
 - If biometric recognition is enabled, only the username field is displayed when GAT Mobile Access is started.

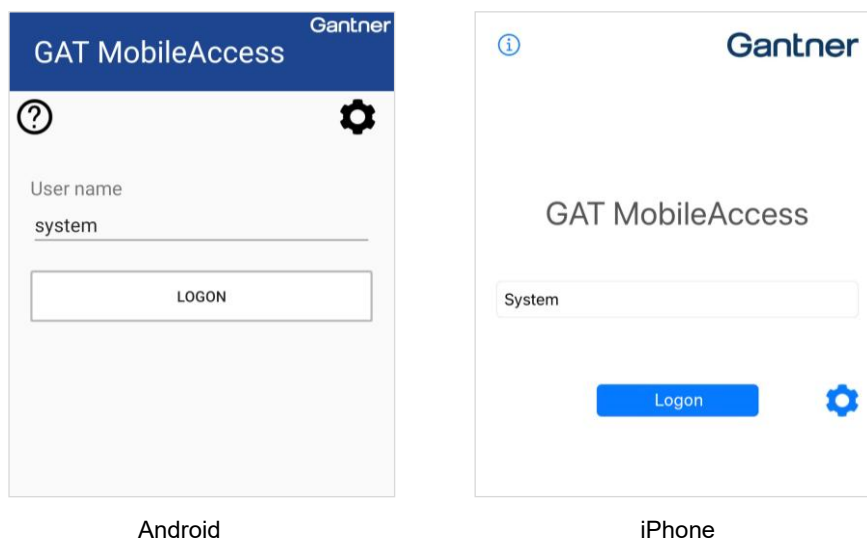


Figure 5.2 - Login screen for biometrics on the various operating systems

- ▶ Press "LOGON".
 - The following options for biometric recognition are displayed.

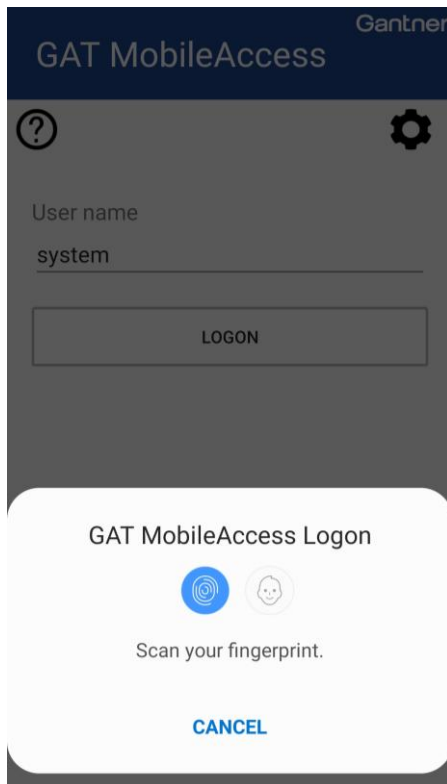


Figure 5.3 - Biometric recognition selection

- ▶ Select the type of biometric recognition (left symbol = fingerprint or right symbol = face recognition).
- ▶ Depending on your selection, identify yourself with your fingerprint or your face on the mobile device.

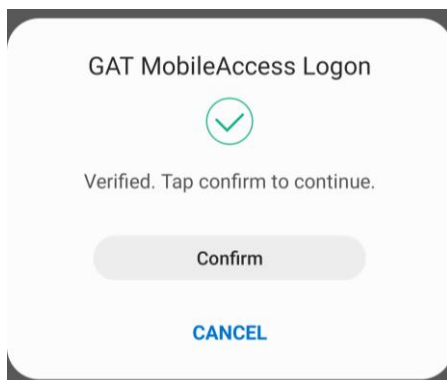


Figure 5.4 - Biometric recognition successful

- ▶ Click on "Confirm".
- ▶ Via "CANCEL" you can also cancel the biometric recognition and log in with your username and password.
 - When using biometric recognition for the first time, the password must be entered again.
 - For each subsequent login, you are logged into GAT Mobile Access immediately after recognizing your fingerprint or face, without having to enter a password.

5.2 Functionality

After logging in the start screen of GAT Mobile Access is displayed.

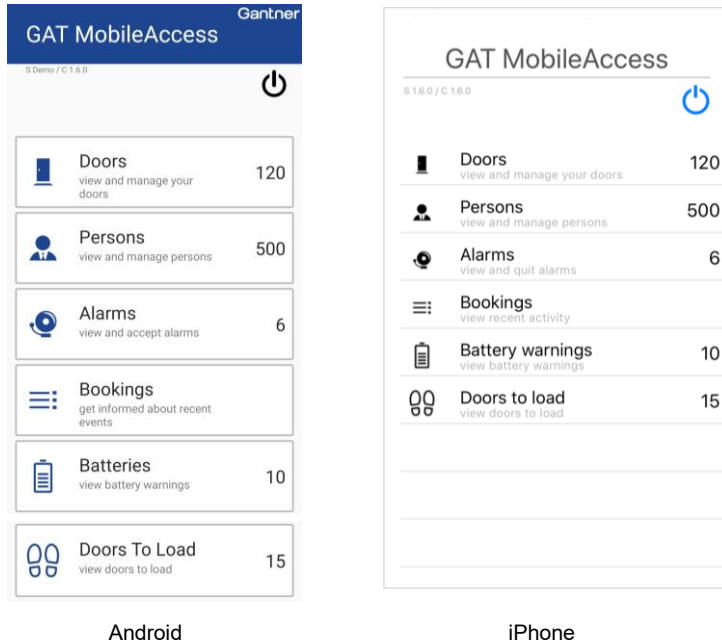
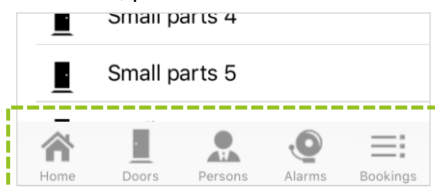


Figure 5.5 – Start screen of GAT Mobile Access on the various operating systems

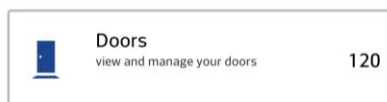
For the operation of GAT Mobile Access, the start screen is divided into several areas:

- Doors: Here you can view the status of each door and also directly control the door (lock, open, general lock or general open).
- Persons: This area organizes the users of the access system. You can see the data carrier assigned to each person, block/unblock a person, and view the bookings and alarms for each person.
- Alarms: In this area you can view, process, and delete any alarm that occurs in the access system.
- Bookings: Here all the bookings, i.e., user activity such as entries, exits and time bookings as registered by the door controllers, which occur in the access system are available. For each booking the person who created the event is identifiable.
- Batteries: Here you can see the battery warnings for offline doors that show when the battery charge level has fallen below a certain value or when the batteries are completely empty.
- Doors to load: This area shows which offline doors need to be loaded.

- To open an area, press the applicable icon on the start screen.
- If the doors, persons, alarms, or bookings areas is open, you can switch directly to another area on an iPhone. To do this, press the icon of the desired area at the bottom of the GAT Mobile Access screen.



5.2.1 Area "Doors"



This area shows all the currently defined and visible door groups, as configured in Matrix.

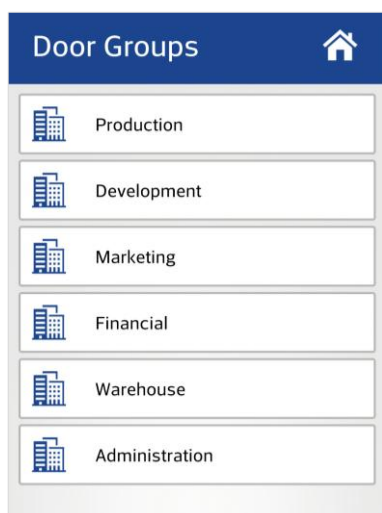


Figure 5.6 – Door groups

- Select a door group.
 - All doors assigned to the door group are displayed.

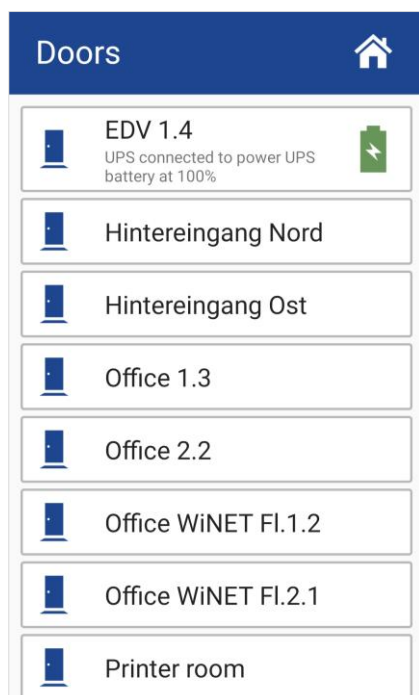


Figure 5.7 – Doors assigned to a door group

- The status of each door is available based on the following icons.

 = Door is open/unlocked.

 = Door is closed/locked.

 = Door is generally open.

 = Door is generally locked.

 = An alarm has been triggered at the door (see "5.2.3. Area "Alarms").

 = A UPS is used to supply the door controller. This symbol with the text "UPS connected to power" indicates that the main power supply is OK and that the UPS and the door controller are being supplied via mains power. The charge in the UPS battery is also displayed.

 = A UPS is used to supply the door controller. The main power supply to the UPS has failed and the door controller is currently being supplied by the UPS. The charge of the UPS battery is indicated by a numerical value and symbol:

 ... Battery charge above 50%

 ... Battery charge between 20% to 50%

 ... Battery charge below 20%

► Select a door.

- Information about the door is displayed. The door information is divided into three sub-areas: "Control", "Alarms", and "Bookings".

NOTE! In order for the door status to be displayed, it must be activated in the "Door Control" area of Matrix (double-click on the door and select the "Show door state" setting in the "Data points" tab).

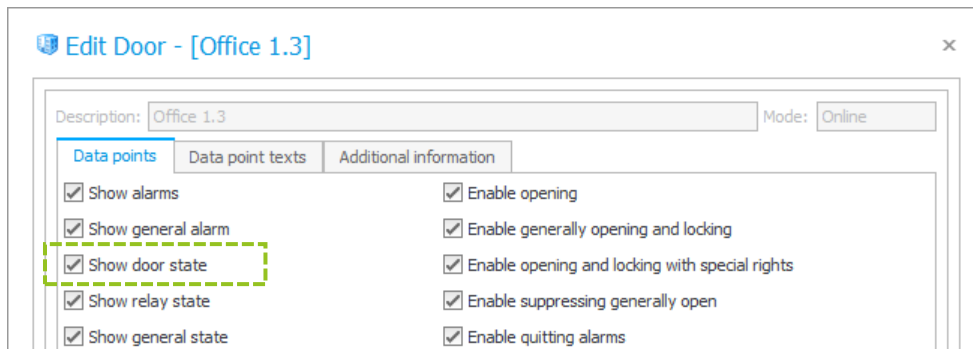


Figure 5.8 - Activate door status in Matrix

Sub-area "Control"



In this sub-area, the current status of the selected door is available and various commands to control the door can be sent.

NOTE! Depending on the data points enabled for the door in Matrix, various options are displayed here. The data points are listed to the right in the “Edit Door” window. To open the window, double-click on the door in Matrix and open the “Data points” tab.

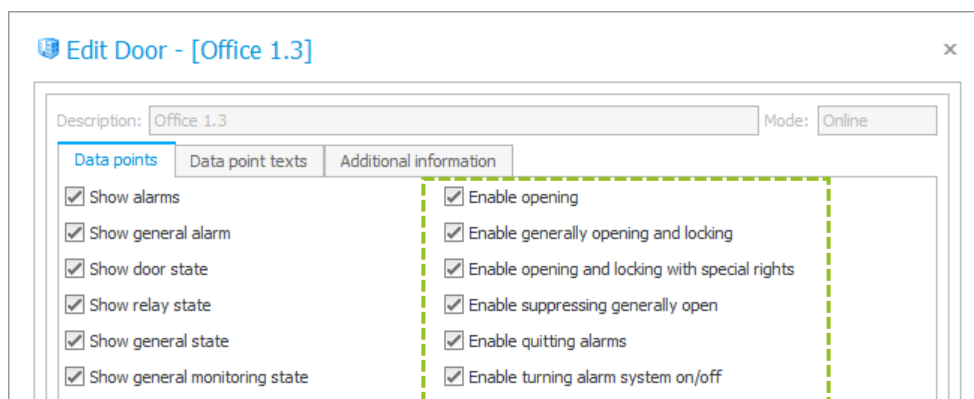


Figure 5.9 - Enable data points for door control in Matrix

The following picture shows the data points required to allow all possible control options.

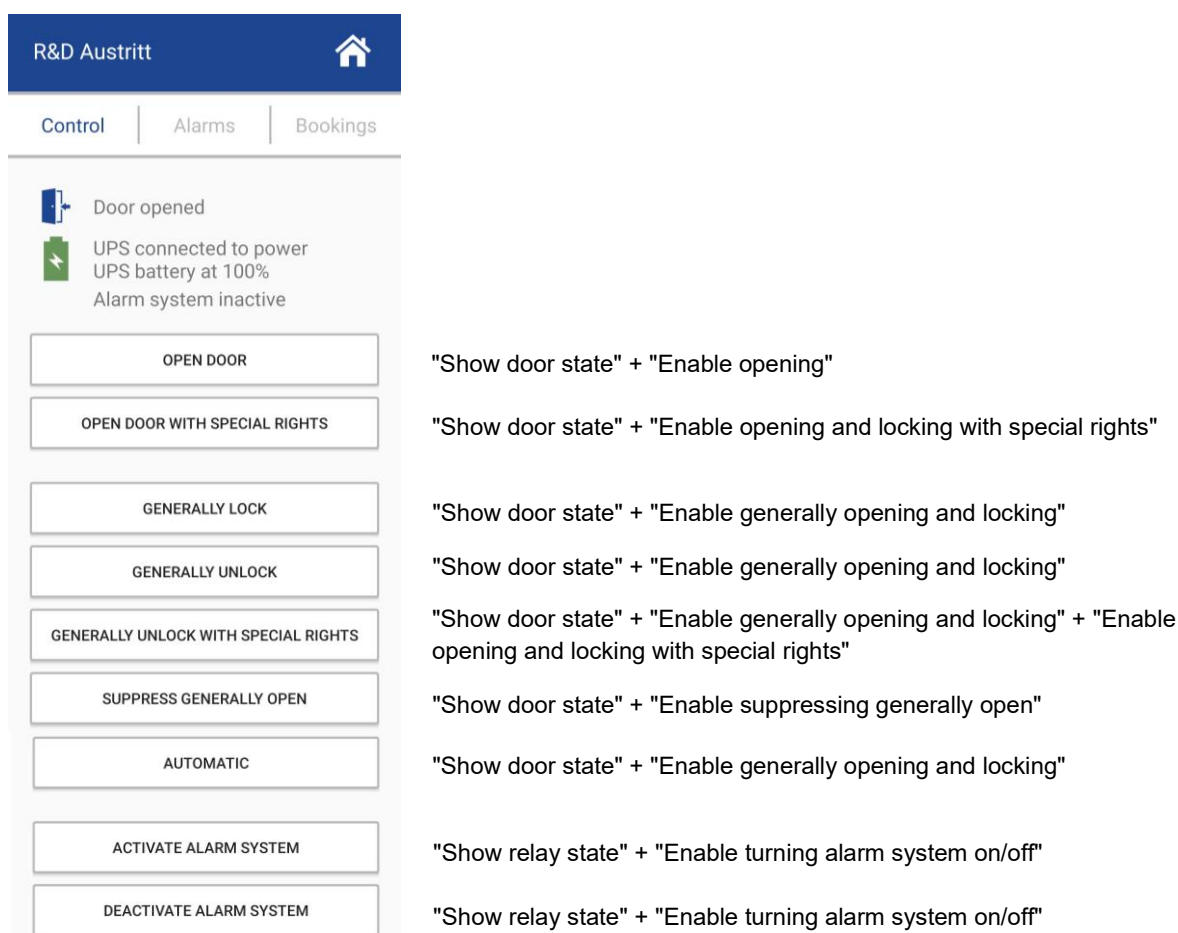


Figure 5.10 - Area "Doors" – Sub-area "Control"

The door status is displayed in the upper area with text and a corresponding symbol. Here, you can also see whether an EMA (monitoring by alarm system) is enabled or disabled.

The status of an emergency power supply (UPS) is also displayed here (if being used). The symbol shows information about the charge status of the UPS and whether the main power supply is operating or not.

 = This symbol with the text "UPS connected to power" indicates that the main power supply is operating, and the UPS and door controller are being supplied via mains power. The charge in the UPS battery is also displayed.

 = The main power supply to the UPS has failed and the door controller is currently being supplied by the UPS. The charge of the UPS battery is indicated by a numerical value and symbol:

 ... Battery charge above 50%

 ... Battery charge between 50% to 20%

 ... Battery charge below 20%

You can control the door by pressing the applicable button. The following actions are possible:

- OPEN DOOR: The door is unlocked for the configured time. When the time frame expires, the door is reset to its previous state (e.g., generally lock/unlock).
- OPEN DOOR WITH SPECIAL RIGHTS: The door is unlocked for the configured time and, if defined, any door controller relay set to "special rights" (relay configuration via GAT ACE) is activated. This allows, for example, a gate normally set to open for pedestrians to open for a car instead.
- GENERALLY LOCK: The door is locked and cannot be opened with a valid data carrier.
- GENERALLY UNLOCK: The door is unlocked and can be opened without a data carrier (e.g., for a frequently used door).
- GENERALLY UNLOCK WITH SPECIAL RIGHTS: The door is generally unlocked and the relay with the "special relay" function is also activated.
- SUPPRESS GENERALLY OPEN: This function suppresses the general open and general locking function as well as the general open schedule on the door. Only the personnel schedules apply and the door can be unlocked and locked according to the stored authorization plans.
- AUTOMATIC: The door is reset from generally lock or generally unlock mode to the "normal" mode of operation, in which user access is determined by the defined schedules and personnel data.
- ACTIVATE/ DEACTIVATE ALARM SYSTEM: These functions allow you to enable/disable the alarm system for the door.

NOTE! Some functions are only available if the "Extended door control" option in the settings is enabled (see "4.5 Configuring the GAT Mobile Access App").

Sub-area "Alarms"

In the "Alarms" sub-area, all current door alarms are displayed.

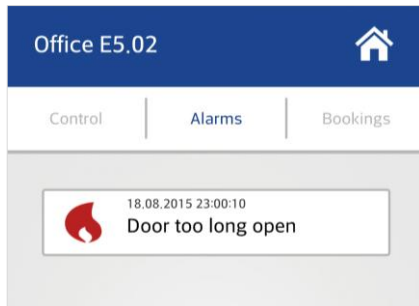


Figure 5.11 - Area "Doors" – Sub-area "Alarms"

- ▶ Press an alarm message to view the alarm details.
 - Details of the alarm are displayed. For more information, see "5.2.3. Area "Alarms".

Sub-area "Bookings"

In the "Bookings" sub-area, the last five bookings for the door recorded during the configured period are displayed.

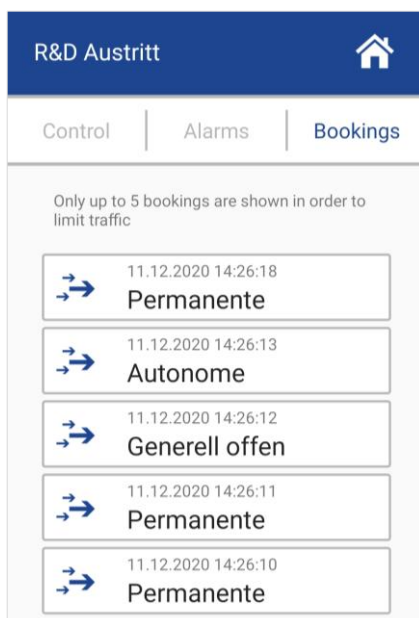


Figure 5.12 - Area "Doors" – Sub-area "Bookings"

- ▶ Press on a booking to view the booking details.
 - Details of the booking are displayed. For more information, see section "5.2.4 Area "Bookings".

5.2.2 Area "Persons"



Persons

view and manage persons

500

This area shows all the currently defined and visible groups of people, as configured in Matrix.

Person Groups



Marketing

R&D Software

R&D Hardware

Product management

Sales

Support

Production

Figure 5.13 – Person groups

- ▶ Select a group of people.
 - The people assigned to the group are displayed.

Persons



Aiko Farley

Ainsley Porter

Amal Snyder

Amber Allison

Audrey Hart

Bradley James

Brighton Sharbino

Figure 5.14 – Persons in a person group

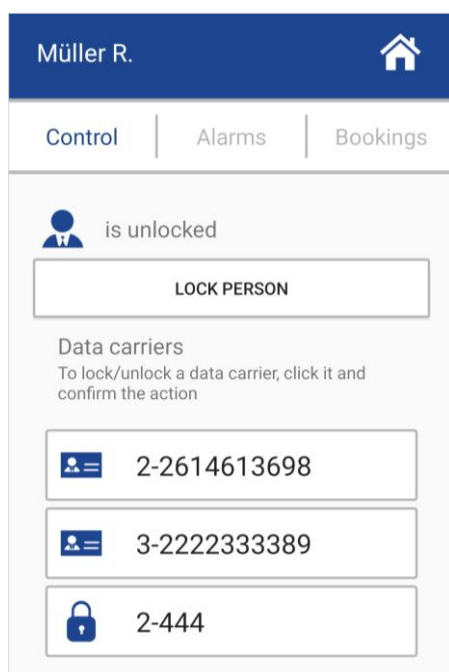
- The current status of each person can be viewed based on the following icons.
 -  Person is unlocked and has access authorization depending on their authorization settings.
 -  Person is locked and has no access authorization.

► Select a person.

- The details of the person are displayed. The user information is divided into 3 sub-areas - "Control", "Alarms", and "Bookings".

Sub-area "Control"

In the "Control" sub-area, the current status of each person within the group is displayed. The person and their assigned data carrier can be locked or unlocked here.



The status of a person indicates whether the person is locked or unlocked. Unlocked means that the person is authorised to access doors within the facility, according to the settings defined for the person in the authorisation data, door configurations, and schedules. Locked means that the person is not authorized to access any door within the facility. The person's status is displayed with text and a corresponding icon at the top of the page.

Figure 5.15 – Area "Persons" – Sub-area "Control"

- If you want to lock an unlocked person, press the "LOCK PERSON" button.
 - The icon and text for the person changes to  is locked
- If you want to unlock a locked person, press the "UNLOCK PERSON" button.
 - The icon and text for the person changes to  is unlocked

After selecting one of the two functions, a delete command is sent to the GAT ACE software, which updates the corresponding data in all door controllers. Please note that this may take some time and, for offline doors, may require on-site loading of the door.

NOTE! From Matrix version 7.1.2 and GAT ACE 7 onwards, the door controllers are updated automatically in the background. Older Matrix versions require manual updating of the controllers.

NOTE! When importing persons data into Matrix, the door controllers are also reloaded. Therefore, the manual reloading process may be omitted if you have set the automatic importation of persons data to occur at regular intervals.

- ▶ With the latest app and Matrix versions, changes to persons are displayed live. With older versions prior to app version 1.7.1 and Matrix version 7.1.2, manual updates were often necessary by pressing F5 in Matrix in order to see the changes on screen.
- ▶ To block or unblock a data carrier assigned to the person, press the desired data carrier. The icons indicate which data carriers are blocked or unblocked. A blocked data carrier no longer has access authorization.



Sub-area "Alarms"

All the current alarms activated by the selected person are displayed here. An example of a typical alarm scenario occurs when the person holds the door open for longer than the defined maximum period after they have unlocked the door using their data carrier.

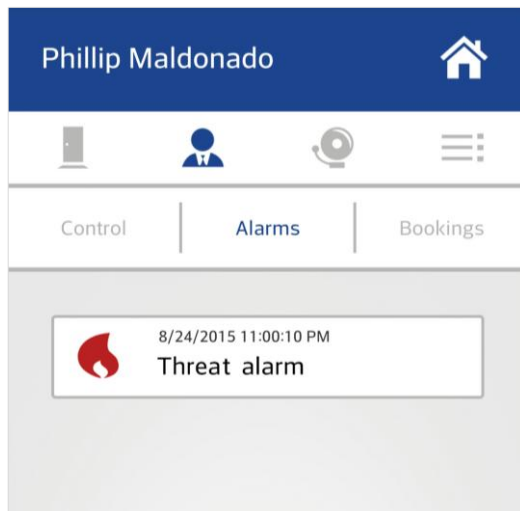


Figure 5.16 - Area "Persons" – Sub-area "Alarms"

- ▶ Press on an alarm to view the alarm details.
 - You are directed to the alarm notification. For more information, see "5.2.3. Area "Alarms".

Sub-area "Bookings"

Here the last five bookings for the current person recorded during the configured period are displayed.

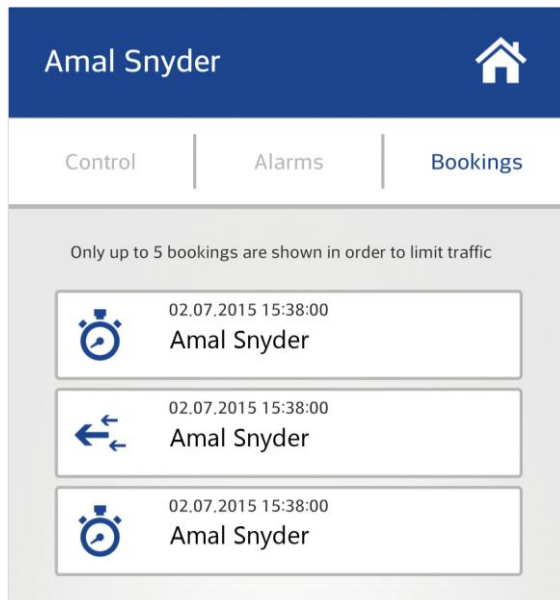


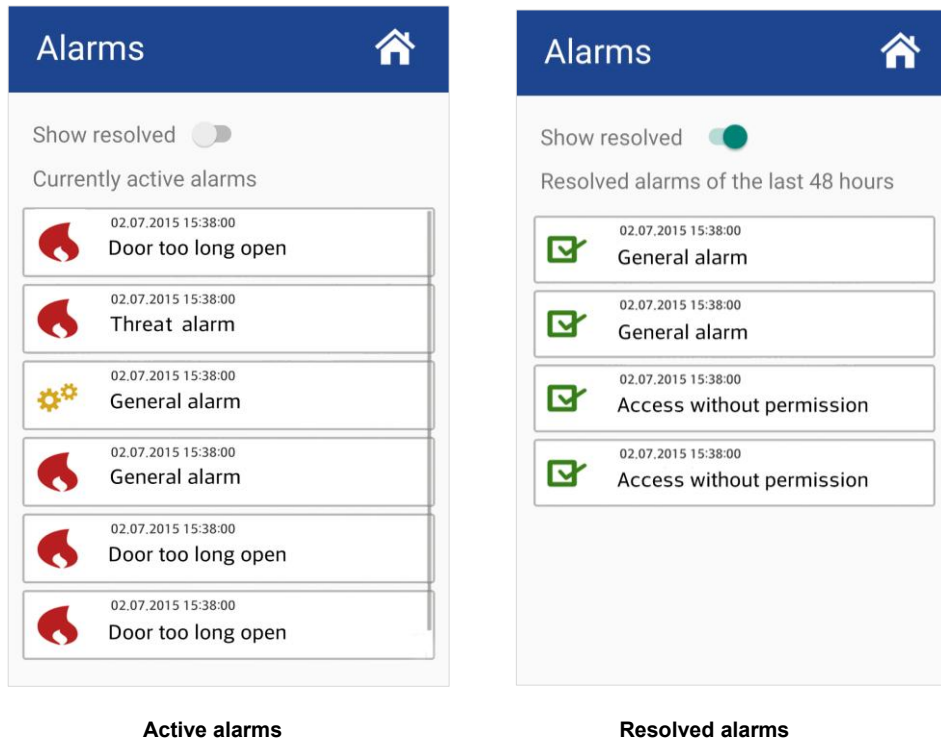
Figure 5.17 - Area "Persons" – Sub-area "Bookings"

- ▶ Press on an booking to view the details.
 - You are directed to the booking details. For more information, see section "5.2.4 Area "Bookings".

5.2.3 Area "Alarms"



The alarms area displays all the alarms that occur in the access control system. You can switch between viewing all active alarms and all previously acknowledged alarms.



Active alarms

Resolved alarms

Figure 5.18 - Display of the triggered alarms in the access control system

- Change between each display by sliding the "Show resolved" switch across.
 - The display changes each time you move the switch between "On" and "Off".
 - If the switch is set to "Off", only the active alarms are shown. Alarms that are still active but currently being resolved or monitored are represented by the symbol.
 - If the switch is set to "On", only resolved alarms from the defined time frame are displayed (see "4.5 Configuring the GAT Mobile Access App").
- Select an alarm.
 - A detailed view of the alarm is displayed.

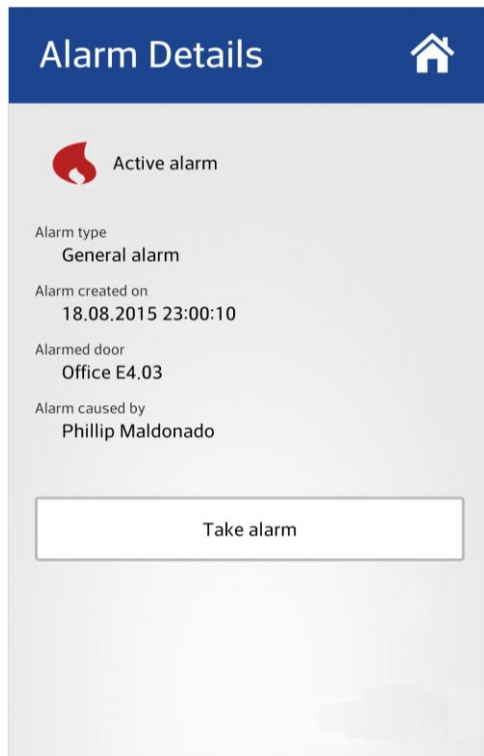


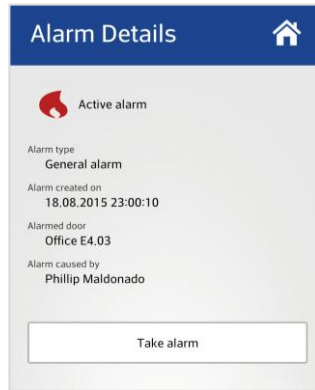
Figure 5.19 – Alarm details of an active alarm

- In this view, the following alarm details are available:
 - Alarm status: "Active alarm", "In process", "Resolved"
 - Alarm type: The type of alarm is displayed. The following types are possible:
 - Door too open long: This alarm is triggered when the door remains open longer than the defined maximum period after valid unlocking.
 - Duress: Triggered by entering a duress PIN code.
 - General alarm: This alarm is activated when a relay with the input setting "General Alarm" is triggered.
 - Access without permission: The door was opened without valid permission. This can be caused by, for example, a break-in.
 - Alarm created on: The date and time when the alarm was triggered.
 - Alarmed door: Name of the door at which the alarm was triggered.
 - Alarm caused by: Name of the person who triggered the alarm.

Alarm Resolution

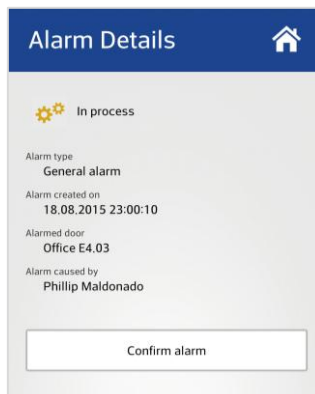
An alarm is resolved by completing the following three steps. Alarm status information for each respective step is displayed.

1.  Active alarm:



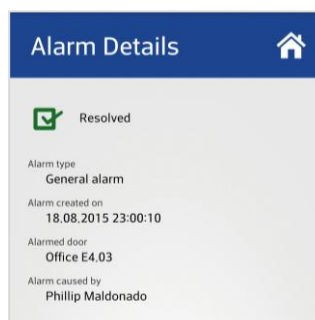
A new alarm is registered in the system and must be acknowledged. A qualified system user must first confirm they are aware of the alarm. For this purpose, the user must press the "Take alarm" button on the alarm details page. Following this, the alarm status changes to "In process".

2.  In process:



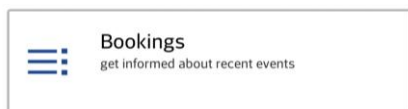
The alarm has been acknowledged by an authorized user and is currently being processed. The user must now determine the cause of the alarm and if necessary, implement additional measures to ensure the alarm does not reoccur. Once this is done, the user must press the "Confirm alarm" button.

3.  Resolved:



The alarm has been processed and the cause of the alarm determined and rectified. Resolved alarms are displayed in a separate view on the alarm display page and are further available for evaluation in the settings for the defined time frame (see "4.5 Configuring the GAT Mobile Access App").

5.2.4 Area "Bookings"



This area displays all the bookings that were created during the time frame configured in the app settings. The display is divided into several pages and the number of bookings, which are displayed per page, can also be defined in the app settings (see "4.5 Configuring the GAT Mobile Access App").

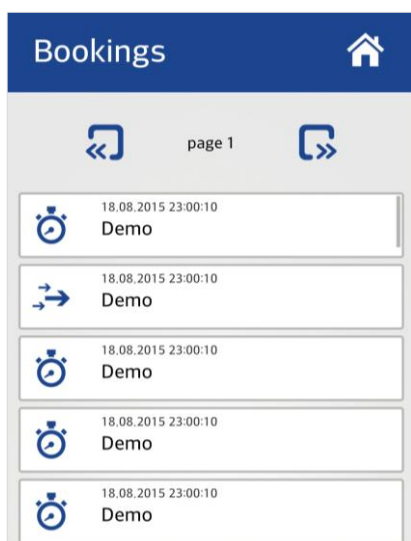


Figure 5.20 – Bookings area

- ▶ Use the  and  symbols to scroll through each page of booking notifications.
- ▶ Press on a booking to view the booking details.
 - The booking details are displayed.

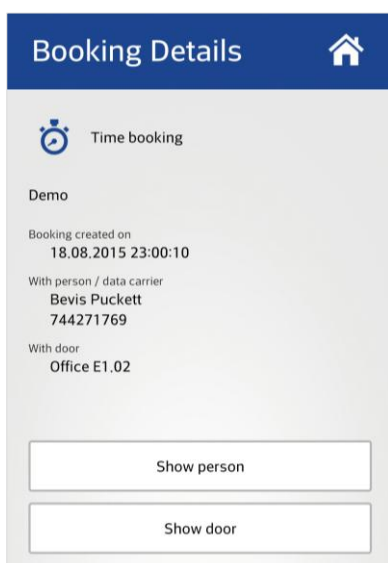


Figure 5.21 – Booking details

- On this page, the following details for the booking are available:
 - Booking type: The type of booking as indicated by the icon and text is shown on the first line.
 -  Entry: This booking shows when a person has entered a door as registered by the controller.
 -  Exit: This booking shows when a person has exited a door as registered by the controller.
 -  Time booking: This booking shows an executed time booking as registered by a time recording terminal.
 - Booking created at: Date and time when the booking was created in the door controller.
 - With person / data carrier: Name of the person who has created the reservation. In addition, the number of the disk is displayed, with which the book was created.
 - With door: Name of the door where the booking was created.
- ▶ Press "Show person" to see the person who created the booking.
 - The display changes and the details of the person are displayed.
- ▶ Press "Show door" to see the door where the booking was created.
 - The display changes and the details of the door are displayed.

5.2.5 Area "Batteries"



This area displays all the battery alarms generated by offline doors (locks). The number of current battery warnings is displayed in the "Batteries" field.

i The battery warnings are transmitted via a data carrier, a transport device, or via a wireless interface. Therefore, they do not always show the current status but the state at the last readout. It is important to change the batteries early enough so that the relevant locks can still be operated.

- Select "Battery Warnings" in the start screen.
 - The currently active battery warnings are displayed with the name of the lock and a symbol.

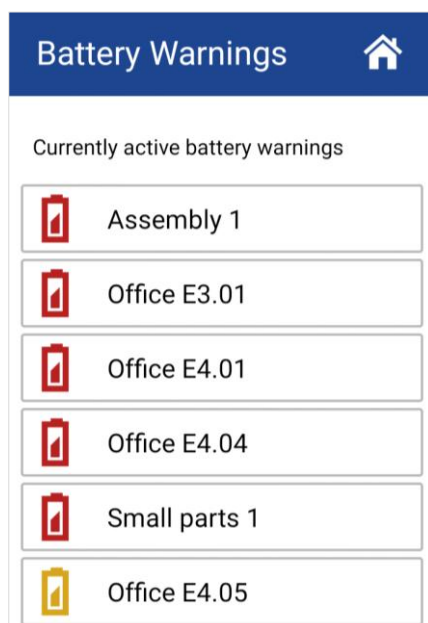


Figure 5.22 – Battery warnings

- Two different symbols are used for the battery warnings:
 -  Battery charge low: The offline lock is still able to be used but the battery is almost empty and must be replaced.
 -  Battery is empty: The battery is empty and must be replaced. The offline lock is no longer able to be used.
- To view the details of a battery warning, press on the warning.
 - A window with details of the battery warning is displayed.

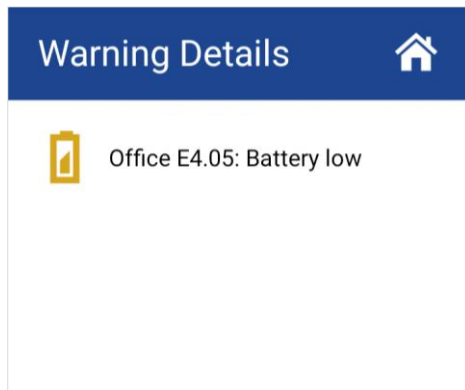
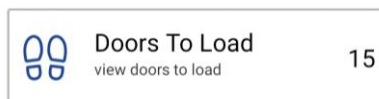


Figure 5.23 – Details of a battery warning

- ▶ Replace the battery(s) according to the description of the offline locks used with the offline doors. This process usually comprises the following steps:
 1. Replace the old battery with a new, fully charged battery.
 2. Reset the offline lock with the associated battery data carrier (= reset battery warning).
 3. Reload offline lock.
 4. Synchronize the offline configuration transport device with the PC or with GAT Mobile Access Management.The battery warnings are not shown in the app only after all the steps are completed.

5.2.6 Area "Doors to Load"



This area displays all the offline doors that still need to be updated with settings, e.g., configuration or permission settings, which have been changed to Matrix. The number of offline doors that require updating is displayed in the "Doors to load" field.

i Be aware that the configuration settings in the doors/locks are only up-to-date after the offline doors are uploaded using a programming device or wirelessly, and the desired function is active.

- ▶ Select the "Doors to load" area in the start screen.
 - All doors that currently require updating are displayed.

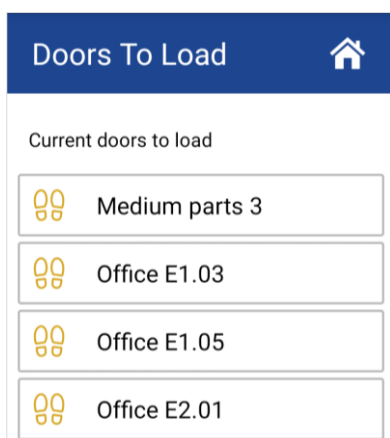


Figure 5.24 – Offline doors that still need to be updated

- ▶ Select an offline door to view the details.
 - The loading details, e.g., the address of the offline door, are displayed.

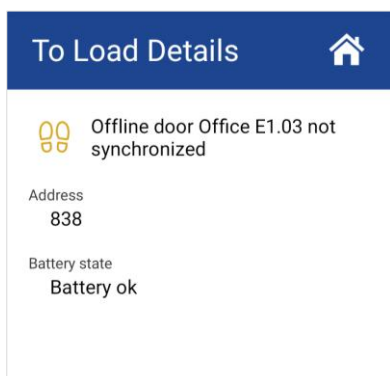


Figure 5.25 – Details of an offline door requiring updating

- ▶ Depending on the lock type, update the displayed offline doors using a programming device or wirelessly.
- ▶ After updating using a programming device, you can synchronize it again with the PC or GAT Mobile Access Management. The loading indications are not shown in the app only after this step has been completed.

Note:

This manual is valid as of 17th March 2026. It is subject to change.

Amendments may occur at any time without notice!

The information in this manual is valid for GAT Mobile Access Management version 1.7.1 or later.



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