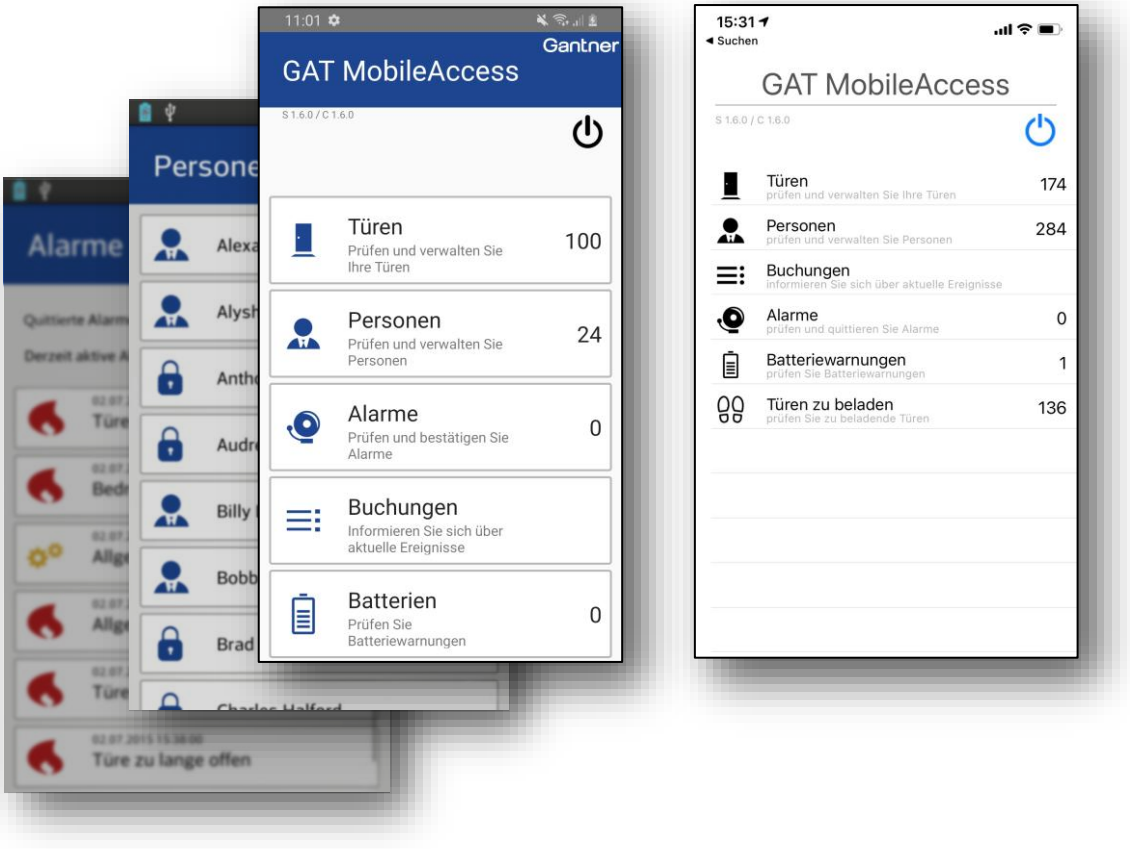
Gantner

GAT Mobile Access Management

Mobiler Zugriff auf Zutrittskontrollanlage



Installation, Konfiguration, Bedienung
Dokumentversion 1.7.1
Softwareversion 1.7.1

© Copyright 2026 GANTNER Electronic GmbH
Alle Rechte vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigung einer Backup-Kopie von Software für den eigenen Gebrauch zu Sicherungszwecken, soweit dies technisch möglich ist und von uns empfohlen wird. Zuwiderhandlungen verpflichten zu Schadensersatz.

Haftung
Ansprüche gegenüber dem Hersteller in Anlehnung an die in diesem Handbuch beschriebenen Hard- und/oder Softwareprodukte richten sich ausschließlich nach den Bestimmungen der Garantie. Weitergehende Ansprüche sind ausgeschlossen, insbesondere übernimmt der Hersteller keine Gewähr über die Vollständigkeit und Richtigkeit des Inhaltes dieses Handbuches. Änderungen bleiben vorbehalten und können jederzeit auch ohne entsprechende Voranmeldung durchgeführt werden.

Warenzeichen
An dieser Stelle sei auf die in diesem Handbuch verwendeten Kennzeichnungen und eingetragenen Warenzeichen hingewiesen. Alle Produkt- oder Firmennamen, die in diesem Handbuch erwähnt warden, dienen lediglich Identifizierungs- und Erklärungszwecken und je nach Bezeichnung kann es sich dabei um Warenzeichen oder eingetragene Warenzeichen der entsprechenden Firmen handeln.

Kontakt
Kontaktinformationen für Rückfragen bezüglich GAT Mobile Access Management oder generelle Anfragen finden Sie unten:

Kontaktadressen des Herstellers
GANTNER Electronic GmbH
Bundesstraße 12
6714 Nüziders, Österreich
www.gantner.com/locations

Allgemeine Warn- und Sicherheitshinweise

Verehrte Kundin, verehrter Kunde,

Sie haben sich für ein Produkt (Gerät oder Software) der GANTNER Electronic GmbH entschieden. Wir beglückwünschen Sie zu dieser Wahl. Damit unser Produkt in Ihrer Anlage zu Ihrer Zufriedenheit sicher und ohne Fehler arbeitet, weisen wir Sie auf folgende Grundregeln hin:

1. Installation, Inbetriebnahme, Betrieb und Wartung des erworbenen Produkts haben bestimmungsgemäß, d.h. innerhalb der in der zugehörenden Produktdokumentation aufgeführten technischen Einsatzbedingungen, zu erfolgen.

2. Vor Installation, Inbetriebnahme, Betrieb und Wartung lesen Sie daher unbedingt die entsprechenden Kapitel in diesem Handbuch durch und handeln Sie danach.

3. Falls dennoch einzelne Punkte unklar sein sollten, handeln Sie nicht „auf gut Glück“, sondern fragen Sie bei dem für Sie zuständigen Kundenberater oder bei der Hotline der GANTNER Electronic GmbH nach.

4. Wenn nicht anders festgelegt, trägt der Kunde die Verantwortung für bestimmungsgemäße Installation, Inbetriebnahme, Betrieb und Wartung des Produkts.

5. Kontrollieren Sie direkt nach Erhalt der Ware die Verpackung und das Produkt bzw. den Datenträger optisch auf seine Unversehrtheit. Kontrollieren Sie die Lieferung auch auf ihre Vollständigkeit (-> Zubehörteile, Dokumentation, Hilfsmittel etc.).

6. Wurde die Verpackung durch den Transport beschädigt oder sollten Sie einen Verdacht auf eine Beschädigung oder Fehlfunktion des Produkts haben, darf das Produkt nicht in Betrieb genommen werden. Kontaktieren Sie in diesem Fall Ihren Kundenberater. Er wird bemüht sein, so schnell wie möglich Abhilfe zu schaffen.

7. Die Installation, Inbetriebnahme und Wartung unserer Geräte hat durch entsprechendes Fachpersonal zu erfolgen. Insbesondere elektrische Anschlüsse dürfen nur vom fachkundigen Personal ausgeführt werden. Dabei sind die Installationsvorschriften nach den einschlägigen, nationalen Errichtungsbestimmungen (z.B. ÖVE, VDE, ...) zu beachten.

8. Wenn nicht anders angegeben, hat die Installation und Wartung unserer Geräte ausschließlich im spannungsfreien Zustand zu erfolgen. Dies gilt insbesondere bei Geräten, die an das Niederspannungsnetz angeschlossen sind.

9. Es ist untersagt, Veränderungen am Produkt vorzunehmen sowie Schutz- und Abdeckhauben von Geräten zu entfernen.

10. Versuchen Sie nicht, Produkte nach einem Defekt, einem Fehler oder einer Beschädigung eigenmächtig zu reparieren oder wieder in Betrieb zu nehmen. Kontaktieren Sie in diesem Fall unbedingt Ihren Kundenberater oder die Hotline der GANTNER Electronic GmbH.

11. Die GANTNER Electronic GmbH übernimmt keine Verantwortung für Verletzungen oder Schäden, die Folge eines unsachgemäßen Gebrauches sind.

12. Auch wenn wir uns um Sorgfalt und stetige Verbesserung bemühen, können wir nicht ausschließen, dass sich Fehler in unsere Dokumentationen einschleichen. Wir weisen daher darauf hin, dass die GANTNER Electronic GmbH keine Gewähr für die Vollständigkeit und Richtigkeit des Inhaltes dieses Handbuches übernimmt. Änderungen bleiben vorbehalten und können jederzeit, auch ohne entsprechende Voranmeldung, von uns durchgeführt werden.

13. Wenn Sie auf Fehler am Produkt oder in der produktbegleitenden Dokumentation stoßen oder wenn Sie Verbesserungsvorschläge haben, wenden Sie sich bitte vertrauensvoll an Ihren Kundenberater oder direkt an die GANTNER Electronic GmbH.

14. Aber auch wenn Sie uns nur mitteilen wollen, dass alles reibungslos funktioniert hat, sind wir über Ihre Nachricht erfreut.

Wir wünschen einen erfolgreichen Einsatz unserer Geräte. Wir würden uns freuen, Sie alsbald wieder als Kunden begrüßen zu dürfen.

INHALTSVERZEICHNIS

1 EINLEITUNG 7
1.1 Zu diesem Handbuch 7
1.2 Kapitelübersicht 7
1.3 Formatierung 8
1.4 Ansprechpartner bei Rückfragen 8

2 ÜBERSICHT 9
2.1 Produktbeschreibung 9
2.2 Begriffsdefinitionen 9

3 INSTALLATION 11
3.1 GAT Mobile Access Server 11
3.1.1 Unterstützte Betriebssysteme 11
3.1.2 Hardwareanforderungen 11
3.1.3 Microsoft .NET Framework 11
3.1.4 Weitere notwendige Software und Hardware 12
3.1.5 Installation des GAT Mobile Access Server 13
3.2 GAT Mobile Access App 16
3.2.1 Unterstützte Betriebssysteme 16
3.2.2 Hardwareanforderungen und Berechtigungen 16
3.2.3 Installation der GAT Mobile Access App 16

4 KONFIGURATION 17
4.1 Konfiguration des GAT Mobile Access Servers 17
4.2 Starteinstellungen des GAT Mobile Access Dienstes 21
4.3 Einrichten von HTTPS für Mobile Access Management 22
4.4 Einrichtung einer TLS Verbindung zu GAT ACE 33
4.4.1 GAT Mobile Access Configuration 33
4.4.2 GAT ACE 3000 und 7000 34
4.5 Konfiguration der GAT Mobile Access App 35
4.5.1 Sprache 37
4.6 Registrieren eines mobilen Geräts in Matrix 38

5 BEDIENUNG 39
5.1 Erster Start und Login 39
5.1.1 Login mittels Benutzername und Passwort 39
5.1.2 Login mittels Biometrie-Erkennung 40
5.2 Funktionen 42
5.2.1 Bereich "Türen" 43
5.2.2 Bereich "Personen" 48
5.2.3 Bereich "Alarme" 52
5.2.4 Bereich "Buchungen" 55
5.2.5 Bereich "Batterien" 57
5.2.6 Bereich "Türen zu beladen" 58

1 EINLEITUNG

1.1 Zu diesem Handbuch

Dieses Handbuch enthält die Beschreibung der GAT Mobile Access Management Lösung für die Überwachung und Kontroller Ihrer Zutrittskontrollanlage von Gantner. Sie finden in diesem Handbuch alle Informationen zur Installation und den Betrieb der GAT Mobile Access Management Lösung. Die Beschreibung der Installation ist dazu in zwei Teile (für die Serverkomponente und die mobilen Apps) aufgeteilt. Für den Betrieb dieser Lösung ist eine einmalige Konfiguration des Servers und der Apps notwendig. Die Beschreibung der Konfiguration ebenso wie die Bedienung der mobilen Apps finden Sie ebenfalls in diesem Handbuch.

Für die Verwendung von GAT Mobile Access Management ist neben der Hardware (Türcontrollern, Leser etc.) auch immer eine Installation der Softwarepakete GAT ACE 7000 oder GAT ACE 3000 und Matrix notwendig. Für diese Komponenten sind eigene Beschreibungen verfügbar. Wichtige Informationen für diese Komponenten in Bezug auf GAT Mobile Access Management werden in diesem Handbuch beschrieben.

Zielgruppe dieses Handbuchs sind der Techniker, der den GAT Mobile Access Management Server installiert und konfiguriert, sowie die Endanwender der moblien App.

1.2 Kapitelübersicht

In Kapitel "2 ÜBERSICHT" finden Sie einen Überblick über die Bestandteile von GAT Mobile Access Management und deren vorgesehene Anwendung. Hier werden außerdem die Begriffe definiert, die in diesem Handbuch verwendet werden.

In Kapitel "3 INSTALLATION" finden Sie die Systemanforderungen, die für GAT Mobile Access Management notwendig sind, sowie alle Informationen für die korrekte Installation des Servers und der mobilen Apps.

In Kapitel "4 KONFIGURATION" finden Sie die Beschreibung aller Konfigurationseinstellungen für den Server und die mobilen Apps und wie die Konfiguration durchgeführt werden kann.

In Kapitel "5 BEDIENUNG" finden Sie die genaue Anleitung, wie der Server und die mobilen Apps verwendet werden und was bei der Bedienung zu beachten ist.

1.3 Formatierung

Zur Anzeige von wichtigen, sicherheitskritischen Informationen wird in diesem Handbuch folgende Formatierung verwendet (mit Beispieltext):

HINWEIS! Nach diesem Signalwort folgt in diesem Handbuch ein Hinweistext den Sie unbedingt lesen und befolgen müssen. Der Hinweistext enthält wichtige Informationen.

Diese Hinweise sind unbedingt zu lesen und zu befolgen.

Zur Anzeige von wichtigen, aber nicht sicherheitskritischen Informationen wird in diesem Handbuch folgende Formatierung verwendet (mit Beispieltext):

Der Text neben diesem Symbol enthält interessante Informationen über den aktuellen Abschnitt. Sie müssen diesen Text nicht unbedingt lesen, die Informationen helfen Ihnen aber, die Beschreibung in diesem Abschnitt besser zu verstehen oder geben interessante Tipps für die Bedienung der Software.

Aktionsschritte, die der Benutzer ausführen muss, und die Resultate dieser Aktionen werden wie folgt formatiert.

- ► Nach diesem Symbol steht eine Handlungsaufforderung, die Sie ausführen sollen.
  - ○ Dieses Symbol kennzeichnet das Resultat nach Ausführung des vorigen Handlungsschrittes.

1.4 Ansprechpartner bei Rückfragen

Bei Fragen in Zusammenhang mit GAT Mobile Access Management wenden Sie sich bitte an die für Sie zuständige Vertretung oder direkt an eine der Gantner Niederlassungen. Die Kontaktdaten sind über den folgenden Link zu finden: www.gantner.com/locations

2 ÜBERSICHT

2.1 Produktbeschreibung

GAT Mobile Access Management ist ein Softwarepaket bestehend aus der Serverkomponenten - ein Windows-Dienst, der im Hintergrund läuft und mit einer grafischen Benutzeroberfläche konfiguriert und gesteuert werden kann - und der mobilen App für mobile Endgeräte wie Smartphones oder Tablets.

Der GAT Mobile Access Server wird auf einem zentralen PC/Server mit Windows Betriebssystem installiert und läuft dann als Windows Dienst im Hintergrund. Dieser Dienst dient als Kommunikationsschnittstelle zwischen den mobilen Endgeräten mit der installierten GAT Mobile Access App und den Softwarepaketen Matrix und GAT ACE 7000 und GAT ACE 3000 von Gantner. Für die Verwendung von GAT Mobile Access Management ist deshalb auch immer eine GAT ACE 7000 bzw. 3000 und Matrix Installation notwendig.

2.2 Begriffsdefinitionen

Einige Begriffe werden in diesem Handbuch immer wieder verwendet. Lesen Sie bitte die Definition dieser Begriffe, und merken Sie sich deren Bedeutung.

GAT Mobile Access Management
Bezeichnet das Kompletpaket, bestehend aus der Serverkomponenten und den mobilen Apps für die verschiedenen Betriebssysteme.

GAT Mobile Access Server bzw. GAT Mobile Access Dienst
Die Software, die auf einem PC oder Server installiert wird und die Kommunikation und Konfiguration zwischen GAT ACE 7000 / 3000 bzw. den Zutrittsgeräten und den mobilen Endgeräten regelt. Der Begriff Dienst und Server wird in diesem Handbuch synonym verwendet.

GAT Mobile Access bzw. GAT Mobile Access App
Die Software, die auf dem mobilen Endgerät installiert wird. Diese App ist für die Betriebssysteme Android und für iOS verfügbar und bietet für alle Betriebssysteme den gleichen Funktionsumfang.

Matrix
Die Zutrittskontrollsoftware von Gantner, mit der die Vergabe und Verwaltung der Personenberechtigungen (inklusive Zeitpläne, Sonderberechtigungen, etc) für die Zutrittsanlage durchgeführt wird. Frühere Bezeichnung ist GAT Matrix.

GAT ACE 7000 und GAT ACE 3000
Diese Software von Gantner ist auf einem zentralen Server installiert und bildet die Schnittstelle zwischen den Türcontrollern und der Matrix Software. GAT ACE 7000/3000 übernimmt und überwacht die gesamte Konfiguration mit den Geräten und dient auch zur Konfiguration und Überwachung der Gerätezustände.
GAT ACE 3000 unterstützt die ältere Türcontroller (z. B. GAT Terminal 3100) und Lesergeneration (z. B. GAT SR 3xx). Für die aktuellen Türcontroller (z.B. GAT DC 7200) und Leser der Serie 7000 wird GAT ACE 7000 benötigt.

Benutzer
Der Begriff "Benutzer" bezeichnet in diesem Handbuch die Person, die GAT Mobile Access Management bedient. Es können mehrere Benutzer mit jeweils eigenem Benutzernamen und Passwort angelegt werden.

Person
In dieser Beschreibung bezeichnet "Person" die Anwender der Zutrittsanlage. Jede Person besitzt einen Datenträger mit einer eindeutigen Nummer. Für jede Person (jeden Datenträger), der in der Anlage zutrittsberechtigt sein soll, muss ein Personalsatz in der Zutrittskontrollanlage (z. B. Matrix) angelegt werden. Dieser Personalsatz enthält Daten wie die Personalnummer, Datenträgernummer (auch als Kartennummer bezeichnet), PIN-Code, Gruppenzuweisungen oder Fingerabdruckdaten.

Datenträger / Ausweis
Datenträger oder auch Ausweise genannt, werden benutzt, um sich an Lesern, die an einem Controllern angeschlossen sind, zu identifizieren. Abhängig von der verwendeten Leseeinheit sind unterschiedliche Arten von Datenträger einsetzbar, wie z. B. kontaktlose Ausweise (RFID) oder auch Magnet- und Infrarotkarten. Die kontaktlosen Datenträger sind in verschiedenen Formen, wie Karten, Schlüsselanhänger oder Armbänder und für unterschiedliche Identifikationssysteme verfügbar (LEGIC, PROXY, MIFARE®, ISO 15693).

Türcontroller
Bezeichnet in dieser Anleitung die an den Türen installierte Geräte, welche die Datenträger von Personen lesen und die Berechtigung überprüfen und entsprechend die Türen elektronisch ent- und verriegeln. Es sind Türcontroller mit integrierten oder abgesetzten Lesern verfügbar. Türcontroller werden in GAT ACE konfiguriert und verwaltet.

Generell-Offen Funktion
Diese Funktion kann für jeden Türcontroller zeitgesteuert aktiviert werden. Mit einer Funktion ist es möglich, während einer Zeitspanne unabhängig von einer Identifikation durch eine Person eine Tür generell zu entriegeln, einen Sonderrelaisplan zu aktivieren oder Alarme zu unterdrücken.

Bedrohungsalarm
Für einen Zutritt kann je nach Konfiguration und Personaldaten neben einer gültigen Identifikation mittels Datenträger auch noch eine PIN-Code Eingabe erforderlich sein. Es ist in dem Fall zusätzlich möglich, auch noch einen sogenannten Bedrohungs-PIN-Code zu definieren. Dieser kann mit dem jeweiligen persönlichen PIN-Code kombiniert werden, um im Fall einer erzwungenen Türöffnung einen stillen Bedrohungsalarm auszulösen.

Buchungen
Bei jedem Ereignis (z.B. Identifikation einer Person, Alarmmeldungen, etc.), das an einem Türcontroller auftritt, generiert der Controller eine Buchung im internen Buchungsspeicher. Diese Buchungen können mit GAT ACE ausgelesen, gespeichert und ausgewertet werden und lassen sich mittels GAT Mobile Access Management auf der mobilen App anzeigen.

Alarm
Eine Zutrittsanlage mit Gantner Türcontrollern unterstützt verschiedene Alarmtypen. Tritt ein Alarm auf, wird dies in der mobilen App angezeigt und es kann auf den Alarm reagiert werden. Unter Alarm versteht man nicht nur einen unerlaubten Aufbruch einer überwachten Tür. Es gibt auch Alarmtypen die ein zu langes öffnen einer Tür oder beliebig definierbare, allgemeine Vorgänge signalisieren können.

Batterie
Offline-Türen (Schlösser) mit Batterieversorgung erzeugen bei zu niedrigem Batteriestand Warnungsmeldungen. Diese können in der GAT Mobile Access Management App angezeigt werden (siehe "5.2.5. Bereich "Batterien"").

Türe zu beladen
Offline-Türen, die noch beladen werden müssen, z. B. weil die Konfiguration oder Berechtigungseinstellungen für diese Türen in Matrix geändert wurden, können ebenfalls in der App direkt angezeigt werden (siehe "5.2.6. Bereich "Türen zu beladen"").

3 INSTALLATION

Beachten Sie die Systemvoraussetzungen für die Installation. Führen Sie dann die Installation schrittweise durch, indem Sie die in diesem Kapitel beschriebenen Abschnitte der Reihe nach ausführen.

3.1 GAT Mobile Access Server

3.1.1 Unterstützte Betriebssysteme

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

Bitte beachten Sie: Die Installationsoptionen Server Core, RT, Starter, Home, Small Business oder Web Editionen werden nicht unterstützt.

HINWEIS! Bitte beachten Sie, dass Gantner nur dann Support-Unterstützung anbieten kann, wenn GAT Mobile Access Server auf einer deutschen oder englischen Windows-Version installiert ist.
Ein Support durch Gantner kann weiter nur gewährleistet werden, wenn der Kunde im Supportfall alle Informationen bekanntgibt, um mit angemessenen Berechtigungen auf das System zugreifen zu können (z. B. Windows Account, Zugriff auf die SQL Datenbank, etc.).

HINWEIS! Der Kunden muss benötigte Lizenzen, z. B. für Betriebssystem oder Datenbanken zur Verfügung stellen.

3.1.2 Hardwareanforderungen

- Mind. Festplattenplatz 2 GB (System und erweiterte Protokollierung).
- Statische Server IP-Adresse für den Zugriff von mobilen Geräten
- Optional: Internetverbindung mit statischer IP-Adresse für externen Zugriff.
- Wenn eine Antivirussoftware verwendet wird, muss das Programmverzeichnis von GAT Mobile Access von den Anti-Virus-Scans ausgenommen werden, um Fehlalarme zu vermeiden.

3.1.3 Microsoft .NET Framework

Zur Verwendung der GAT Mobile Access Management Software muss das .NET Framework 4.7.2 vorinstalliert sein.

3.1.4 Weitere notwendige Software und Hardware

GAT Mobile Access Server benötigt neben der Hardware (Zutrittskontrollanlage mit den entsprechenden Türcontrollern und/oder Offline Türzylindern von Gantner) auch folgende weitere Software:

- GAT ACE 7000 oder GAT ACE 3000
  Konfigurationssoftware für die Türcontroller und Offline Türzylinder. Mit dieser Software werden die Geräte der Zutrittsanlage (Controller, Leser, Türzylinder) konfiguriert und GAT ACE 7000 bzw. GAT ACE 3000 regelt auch die Kommunikation in der Zutrittskontrollanlage sowie zwischen den Geräten und der Software.
- Matrix
  Bediensoftware für die Zutrittskontrollanlage. In Matrix werden die Berechtigungen der Benutzer vergeben, Buchungen und Türzustände ausgewertet, Betriebskalender und Zeitpläne festgelegt, etc.
  Es muss auch der GAT Matrix Synchronizer installiert, eingerichtet und gestartet sein.

Diese genannten Programme müssen nicht auf dem gleichen PC installiert werden, wie GAT Mobile Access Management, aber sie müssen im Netzwerk erreichbar sein.

HINWEIS! Bitte beachten Sie, dass eine instabile oder langsame Verbindung zu Problemen bei der Verwendung der mobilen Apps führen kann.

3.1.5 Installation des GAT Mobile Access Server

Starten Sie die Installation des GAT Mobile Access Servers wie folgt.

► Doppelklicken Sie auf die Datei "setup.exe" im GAT Mobile Access Management Installationspaket.
  - Der Installationsassistent wird geöffnet.

HINWEIS! Der Installationsassistent ist nur in englischer Sprache verfügbar.

***Bild 3.1** - GAT Mobile Access Server Installation - Schritt 1*

► Klicken Sie "Next".

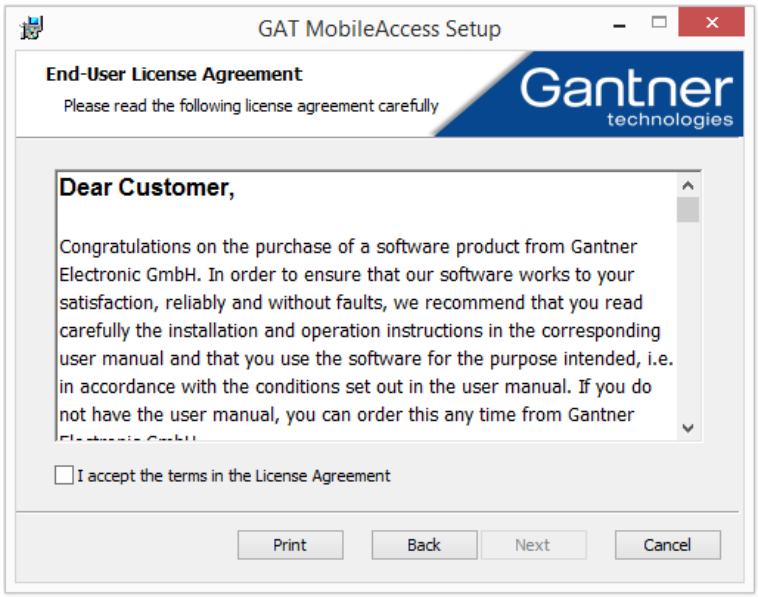


***Bild 3.2** - GAT Mobile Access Server Installation - Schritt 2*

► Lesen Sie die Lizenzinformation und markieren Sie dann das Feld "I accept the terms in the License Agreement", um die Lizenzinformationen zu bestätigen.

► Klicken Sie "Next".

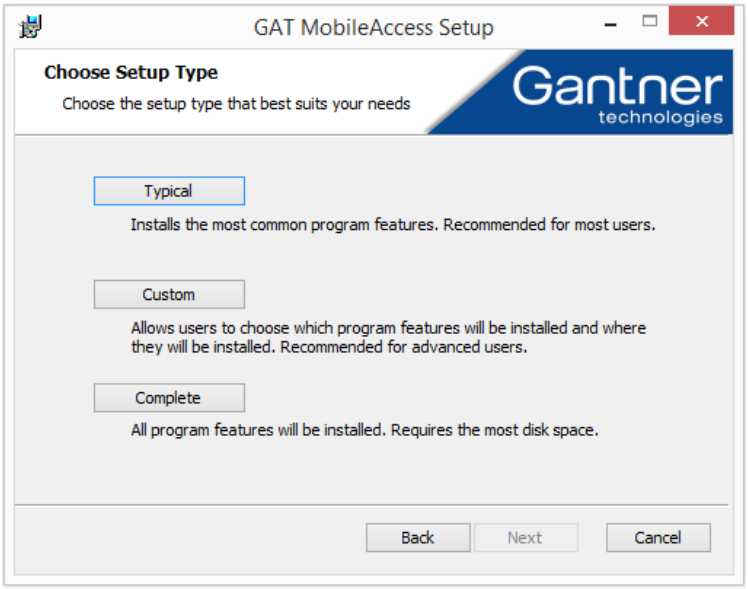


***Bild 3.3** - GAT Mobile Access Server Installation - Schritt 3*

► Wählen Sie die Art der Installation:

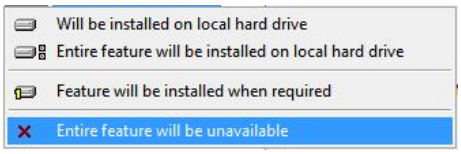
- Typical: Installiert GAT Mobile Access Management. Dies ist die Standardoption für die meisten Benutzer.

- Custom: Erlaubt eine Auswahl, welche Teile von GAT Mobile Access Management installiert werden sollen, sowie die Auswahl des Installationsortes. Folgendes Fenster wird angezeigt.

  ► Wählen Sie die Optionen, die installiert werden sollen.

    ○ Ein weißes Symbol vor einer Option bedeutet, dass diese Option installiert wird.

  ► Um die Installation einer Option zu ändern klicken Sie auf das Symbol vor der entsprechenden Option und wählen die gewünschte Aktion. Wenn z. B. der GAT Mobile Access Management Server bereits auf einem andere Server/PC installiert ist und Sie darum nur den Client installieren möchten, wählen Sie für den Server die Option "Entire feature will be unavailable".



  ► Wählen Sie nun noch das Verzeichnis, in dem GAT Mobile Access Management Server installiert werden soll. Möchten Sie nicht das vorgeschlagene Standard-Verzeichnis verwenden, können Sie durch Druck auf "Browse" ein anderes Verzeichnis wählen.

  ► Klicken Sie abschließend "Next".

- Complete: Diese Option installiert alle verfügbaren Teile von GAT Mobile Access Management. Diese Option benötigt den meisten Speicherplatz.

o Nach Auswahl der Installationsoption wird im nächsten Schritt folgende Fenster angezeigt.

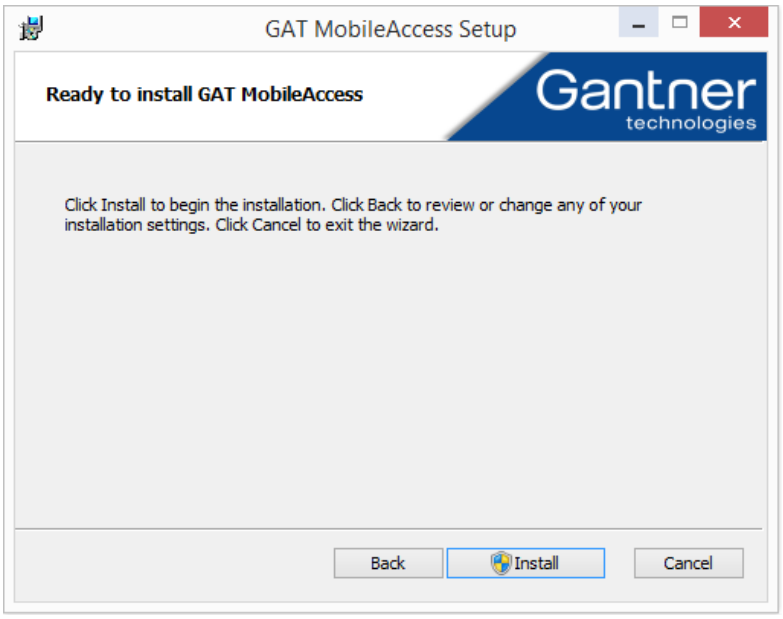


***Bild 3.4** - GAT Mobile Access Server Installation - Schritt 4*

► Klicken Sie "Install" und bestätigen Sie die folgende Berechtigungsabfrage mit "OK".

o Dadurch wird die Installation gestartet. Ein grüner Balken zeigt den Fortschritt der Installation.

► Nachdem die Installation beendet ist klicken Sie auf "Finish", um den Installationsassistenten zu beenden.

o Der GAT Mobile Access Server ist nun installiert und einsatzbereit.

HINWEIS! Einstellungen zu Anti-Virus Software:
Es ist sehr wichtig, dass die Installationsverzeichnisse von GAT Mobile Access Server von den Anti-Virus Prüfungen ausgenommen sind. In einer Standard-Installation betrifft dies die Verzeichnisse:
- Für 32 Bit Windows Versionen:
  "C:\Programme\GAT\GAT MobileAccess"
- Für 64 Bit Windows Versionen:
  "C:\Programme(x86)\GAT\GAT MobileAccess"

Außerdem muss in der Anti-Virus Software der GAT Mobile Access Service von einem Livescan ausgenommen werden, da es sonst zu Fehlermeldungen kommen kann.
Lesen und beachten Sie auch die Informationen von Microsoft über die Auswahl von Anti-Virus Software für Computer mit SQL Server (siehe in deutsch https://support.microsoft.com/de-de/kb/309422 bzw. in englisch https://support.microsoft.com/en-us/kb/309422).

3.2 GAT Mobile Access App

Für die Bedienung am Mobilgerät (Smartphone oder Tablet) muss die entsprechende App auf dem Mobilgerät installiert werden. Gantner bietet die App für die Android und iOS Betriebssysteme an.

Die App kann von dem für Ihr Gerät gültigen App-Store geladen werden (Google Play Store, Apple App Store).

HINWEIS! Bitte beachten Sie neben den nachfolgend angeführten Voraussetzungen auch die in den jeweiligen in den App-Stores beschriebenen aktuellen Systemvoraussetzungen.

3.2.1 Unterstützte Betriebssysteme

- Android (ab Version 6.0)
- Apple iOS (ab Version 12.2)

3.2.2 Hardwareanforderungen und Berechtigungen

Bitte beachten Sie die im jeweiligen App-Store angegbenen Hardware- und Softwareanforderungen zu der jeweiligen App. Hier finden Sie die jeweils gültigen Anforderungen entsprechend den App-Versionen.

3.2.3 Installation der GAT Mobile Access App

Der einfachste Weg, um die App zu installieren, besteht darin, sie in dem betreffenden App-Store zu laden.

► Öffnen Sie auf Ihrem Mobilgerät den App-Store.
► Suchen Sie im Store nach "GAT MobileAccess".
  ○ Die GAT Mobile Access App wird nach kurzer Suche angezeigt.
► Klicken Sie die gefundene App und im App-Fenster auf "Installieren".

Nach der Installation erscheint folgendes Symbol in ihrem App-Launcher.

4 KONFIGURATION

4.1 Konfiguration des GAT Mobile Access Servers

Nach der Installation wird der GAT Mobile Access Server nicht automatisch gestartet sondern muss zuerst konfiguriert werden.

► Starten Sie die Anwendung "GAT Mobile Access Configuration". Nach einer Standard-Installation finden Sie diese Anwendung im Pfad "Alle Programme" -> "GANTNER Electronic GmbH" -> "GAT MobileAccessService".

HINWEIS! Es wird empfohlen, diese Anwendung als Administrator auszuführen, da der GAT Mobile Access Dienst ansonsten nicht gestartet bzw. gestoppt werden kann.

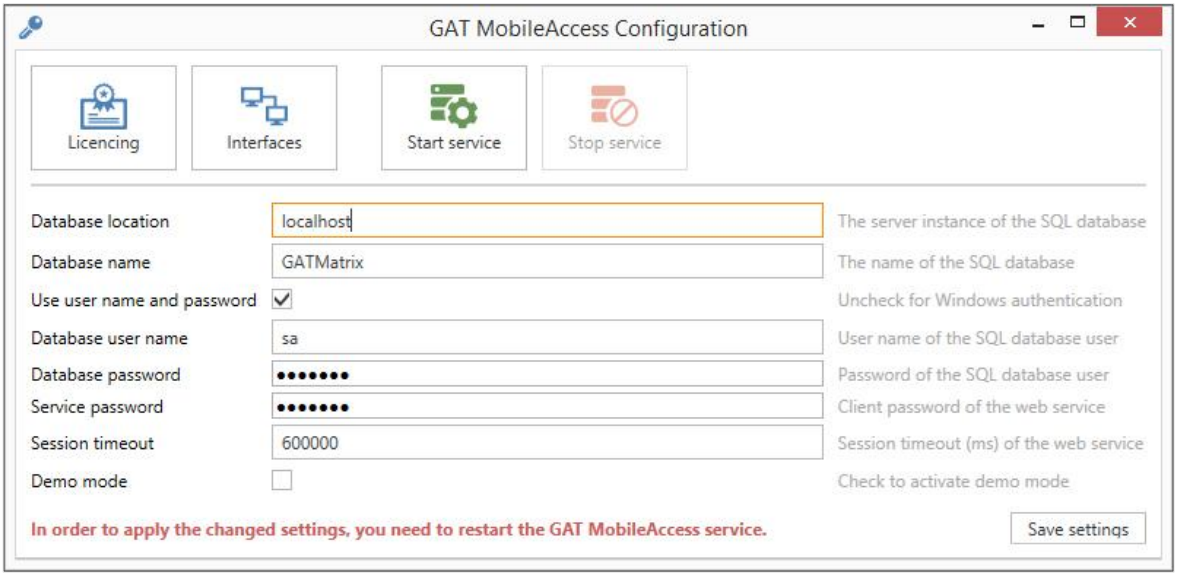


***Bild 4.1** - Benutzeroberfläche des Konfigurators "GAT Mobile Access Configuration"*

► Öffnen Sie zunächst alle verwendeten Ports.

Standardmäßig werden folgende Ports verwendet:

- TCP 8234: Zugriff von mobilen Endgeräten auf den GAT Mobile Access Server
- TCP 8701: Zugriff auf GAT ACE 7000
- TCP 8301: Zugriff auf GAT ACE 3000
- TCP 5228, 5229, 5230: Für Endgeräte via Firebase Cloud Messaging Platform (siehe Hinweis unten)

HINWEIS! Sollten Sie für eine der obigen Komponenten abweichende Ports verwenden, müssen natürlich die entsprechenden Ports freigegeben werden.

HINWEIS! Damit die mobilen Endgeräte Nachrichten (Push Notifications, siehe "4.5. Konfiguration der GAT Mobile Access App") über die verwendete Firebase Cloud Messaging Plattform erhalten können, müssen auf den Endgeräten die Ports 5228, 5229 und 5230 freigegeben bzw. offen sein. Auf der Serverseite werden dafür nur die Standard-Ports von http/https benötigt).

► Stellen Sie eine Verbindung zur Matrix Datenbank her. Dazu sind folgende Angaben notwendig:

- Database location: Der SQL Datenbank-Server, in dem die Matrix Datenbank gehostet wird.
- Database name: Der Name der Matrix Datenbank.
- Use user name and password: Aktivieren Sie das Kontrollkästchen, wenn für den Zugriff auf die Datenbank Benutzername und Passwort erforderlich sind.
- Database user name: Falls erforderlich, der Benutzername für den Zugriff auf die Datenbank.
- Database password: Falls erforderlich, das Passwort für den Zugriff auf die Datenbank.

► Legen Sie die weiteren Einstellungen des GAT Mobile Access Servers fest:

- Service password: Das Passwort, das ein mobiles Gerät verwenden muss, um sich mit dem Dienst zu verbinden (Standard: GAT0815).
- Session timeout: Ein inaktives mobiles Endgerät wird nach der eingestellten Inaktivität (in ms) automatisch abgemeldet. Es kann sich aber selbstverständlich wieder anmelden, sofern die Lizenz das erlaubt.
- Demo mode: Der GAT Mobile Access Service verfügt über einen Demonstrationsmodus. In diesem Modus wird zwar mit den Daten aus der Matrix Datenbank gearbeitet, es werden aber keine Kommandos an GAT ACE 7000 bzw. GAT ACE 3000 gesendet.
  HINWEIS! Bitte betreiben Sie den Demonstrationsmodus nie mit produktiven Daten!

Als nächstes stellen Sie eine Verbindung zu GAT ACE 7000 oder zu GAT ACE 3000 her.

► Klicken Sie auf die Schaltfläche "Interfaces".

○ Das Fenster "Interface definitions" wird geöffnet.

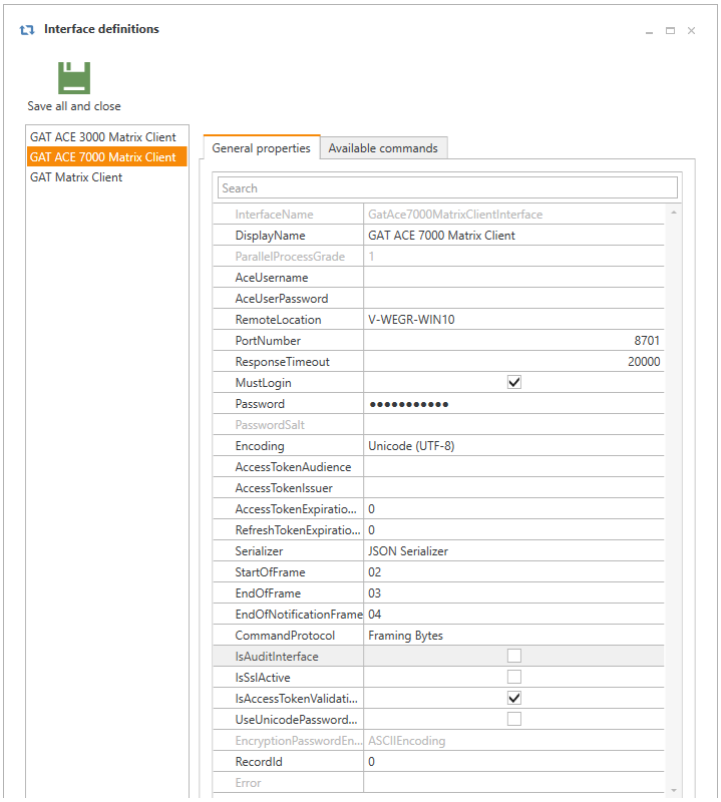
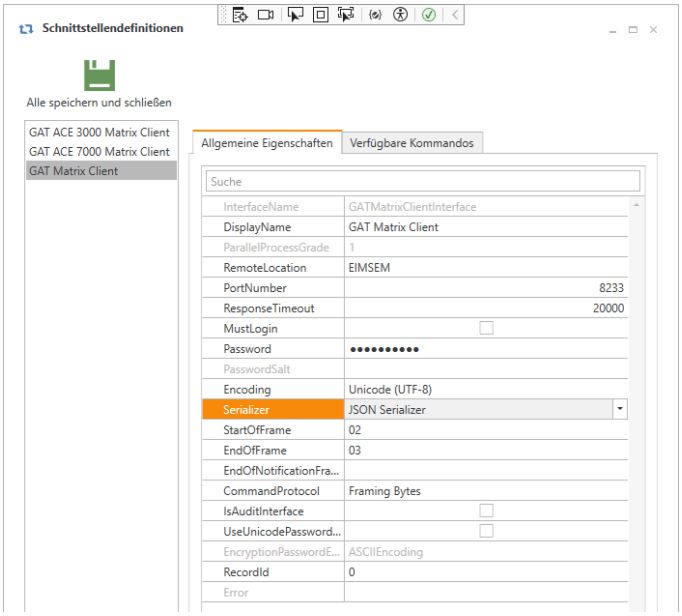


***Bild 4.2** - Einstellen der Schnittstellenparameter*

► Klicken Sie in der linken Spalte auf "GAT Matrix Client".

  o Die Schnittstellenparameter für die Kommunikation mit Matrix werden angezeigt.



► Geben Sie hier folgende Daten ein:

- RemoteLocation: Geben Sie den Servernamen ein, auf dem Matrix installiert ist. Sollte es derselbe Server sein, auf dem auch der GAT Mobile Access Management Server installiert ist, verwenden Sie bitte "localhost".
- PortNumber: Sollten Sie für Matrix nicht den standardmäßigen Port 8233 verwenden, geben Sie den entsprechenden Port bitte hier an.
- Serializer: Diese Einstellung ist abhängig von der verwendeten Matrix Version:
  - Für Matrix Version 4 und älter wählen Sie "Binary Matrix Serializer".
  - Für Matrix Version 5 oder 6 ist "JSON Serializer" oder "Binary Matrix Serializer" möglich.
  - Ab Matrix Version 7 ist nur "JSON Serializer" möglich.

► Alle anderen Werte können auf den Standardeinstellungen belassen werden, solange in Matrix die entsprechenden Werte nicht geändert wurden.

► Klicken Sie in der linken Spalte auf "GAT ACE 7000 Matrix Client“ oder "GAT ACE 3000 Matrix Client“, je nach dem, welche GAT ACE Version Sie verwenden.

  o Die Schnittstellenparameter für die Kommunikation mit GAT ACE 7000 bzw. 3000 werden angezeigt.

► Geben Sie hier folgende Daten ein:

- RemoteLocation: Geben Sie den Servernamen ein, auf dem GAT ACE 7000 bzw. 3000 (der Windows Dienst) installiert ist. Sollte es derselbe Server sein, auf dem auch der GAT Mobile Access Server installiert ist, verwenden Sie bitte "localhost".
- PortNumber: Sollten Sie für GAT ACE 7000 nicht den Standard-Port 8701 bzw. für GAT ACE 3000 nicht den Standard-Port 8301 verwenden, geben Sie den entsprechenden Port bitte hier an.
- Passwort: Sollten Sie für GAT ACE 7000 bzw. 3000 ein anderes Interface-Passwort vergeben haben, geben Sie es bitte hier ebenfalls an.
- IsSslActive: Wenn für die Verbindung zu GAT ACE 7000 oder 3000 die gesicherte Verbindung über TLS verwendet werden soll, markieren Sie die Option "IsSslActive". Die TLS Verbindung muss dann auch in GAT ACE 7000 bzw. 3000 aktiviert sein. Weitere Verbindung zu TLS siehe "4.4. Einrichtung einer TLS Verbindung zu GAT ACE").

- IsAccessTokenValidationActive:
  Mit dieser Einstellung kann die Authentifizierung mittels JWT Token aktiviert werden, was im Zusammenhang mit TLS immer aktiv sein sollte (siehe "4.4. Einrichtung einer TLS Verbindung zu GAT ACE").
- AceUsername, AceUserPassword:
  Bei der Benutzung der Validierung über Access Token muss hier ein gültiger GAT ACE 7000 Benutzer mit Passwort eingetragen sein.

► Alle anderen Werte können auf den Standardeinstellungen belassen werden, solange in GAT ACE 7000 bzw. 3000 die entsprechenden Werte nicht geändert wurden.

► Klicken Sie auf die Schaltfläche "Save all and close".

GAT Mobile Access Management läuft 14 Tage im Demomodus und nach Eingabe einer Lizenz weitere 14 Tage ohne Aktivierung. Deshalb müssen Sie eine Lizenz für GAT Mobile Access Management erwerben und diese wie folgt eingeben.

► Klicken Sie in der Benutzeroberfläche des Konfigurators auf die Schaltfläche "Licencing".

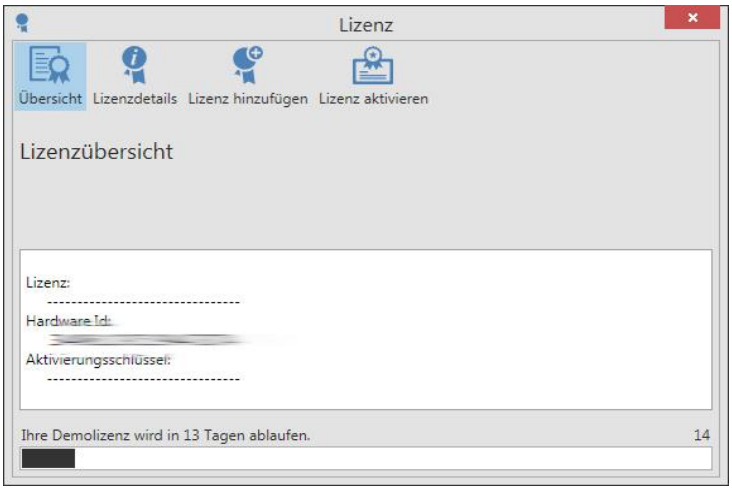


***Bild 4.3** – Lizenzverwaltung*

► Auf der Registerkarte "Übersicht" sehen Sie die Lizenz, Hardware-ID und Information über die Dauer der Lizenz bzw. bis wann Sie eine Lizenz eingeben müssen.

► Klicken Sie auf das Symbol "Lizenz hinzufügen", um eine Lizenz hinzuzufügen.

HINWEIS! Den Lizenzcode können Sie entweder manuell eintippen oder aus einer Datei importieren. Kontaktieren Sie bitte Ihren lokalen Vertriebspartner oder die entsprechende Gantner Niederlassung, um eine Lizenz zu erhalten.

► Klicken Sie auf "Lizenz aktivieren", um Ihre Lizoenz mittels Aktivierungscode zu aktivieren.

HINWEIS! Den Aktivierungscode erhalten Sie wiederum von Ihrem lokalen Vertriebspartner oder der entsprechenden Gantner Niederlassung. Für den Aktivierungscode benötigen Sie Ihren Lizenzcode und die Hardware-ID des PC/Servers, auf dem GAT Mobile Access Management Server installiert ist.

► Klicken Sie nun in der Benutzeroberfläche des Konfigurators auf die Schaltfläche "Save settings“, um alle Einstellungen zu speichern.

► Drücken sie in der Benutzeroberfläche des Konfigurators auf die Schaltfläche "Start service“, um den GAT Mobile Access Management Dienst zu starten.

► Warten Sie solange, bis eine Mitteilung zum erfolgreichen Start des Diensts erscheint.

► Öffnen Sie einen Browser (am besten auf einem anderen PC) und geben Sie folgende URL ein:
http://<*Server*>:8234/MobileAccessService/TestService/wp=<*WebservicePasswort*>
Ersetzen Sie <*Server*> und <*WebservicePasswort*> durch Ihre Konfiguration. Für <*Server*> können Sie den Namen oder die IP-Adresse eingeben.
Beispiel: http://mademo.gantner.com:8234/MobileAccessService/TestService/wp=GAT0815

- Die Antwort wird im JSON Format ausgegeben und sollte im Erfolgsfall wie nachfolgend aussehen:
{"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}

HINWEIS! Löschen Sie aus Sicherheitsgründen den Cache des Browsers nach dem Test der Verbindung, da beim Test das Passwort des Webservice mitgesendet wird.

4.2 Starteinstellungen des GAT Mobile Access Dienstes

Wenn der GAT Mobile Access Server und die Matrix Datenbank auf demselben PC installiert sind, besteht die Möglichkeit, dass der GAT Mobile Access Server vor dem SQL Dienst für die Datenbank startet. In diesem Fall kann keine Verbindung mit der Datenbank hergestellt werden und GAT Mobile Access Server wird keine Daten bereitstellen können. Dieses Problem ist leicht zu beheben.

► Öffnen Sie den "Ausführen"-Dialog von Windows mit der Tastenkombination "Windows"+"R".

► Geben Sie "services.msc" ein, gefolgt von Enter.

- Das Dienst-Fenster von Windows wird geöffnet.

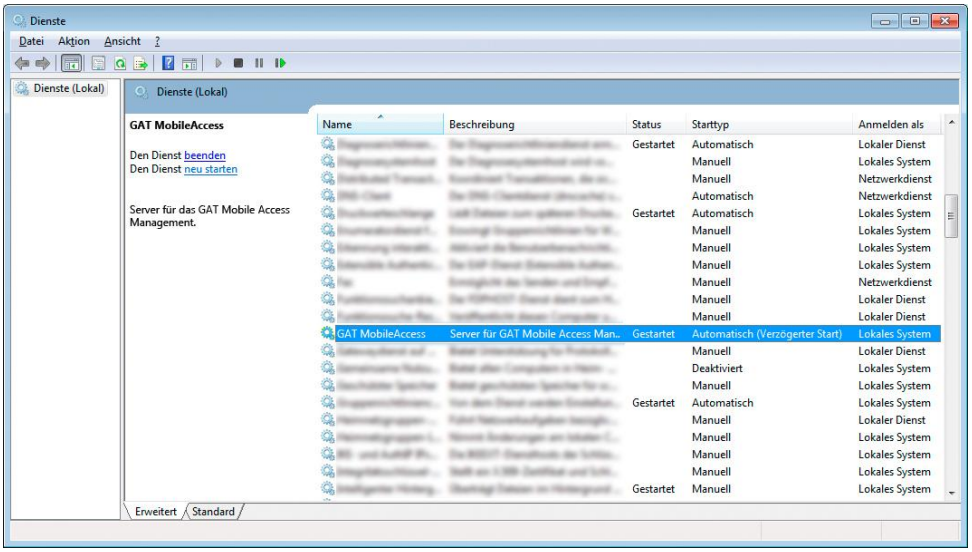


Bild 4.4 *- Windows Dienste*

► Hier muss der "GAT Mobile Access" Dienst gestartet sein (siehe Spalte "Status"). Sie können den Eintrag markieren und links neben der Liste auf "starten" klicken oder den Dienst mit "neu starten" beenden und automatisch neu starten lassen.

4.3 Einrichten von HTTPS für Mobile Access Management

Mit den folgenden Schritten kann die HTTPS Verbindung aktiviert werden. Damit wird die Verbindung zwischen der GAT Mobile Access App auf dem mobilen Gerät und dem GAT Mobile Access Server verschlüsselt. Es wird empfohlen, die HTTPS-Verbindung zu aktivieren, um eine sichere Kommunikation zu gewährleisten. Die folgenden Voraussetzungen müssen erfüllt sein, bevor Sie HTTPS für Mobile Access Management einrichten:

- Mobile Access Management installiert (siehe Kapitel „3 INSTALLATION“).
- HTTPS-Zertifikat verfügbar.
- DNS und Portweiterleitung abgeschlossen.

Installieren des IIS-Webservers (Internet Information Service)

► Öffnen Sie den "Server Manager".

► Klicken Sie auf "Rollen und Features hinzufügen".

► Fügen Sie in der Liste "Rollen" die Rolle "Webserver (IIS)" hinzu und klicken Sie auf "Installieren".

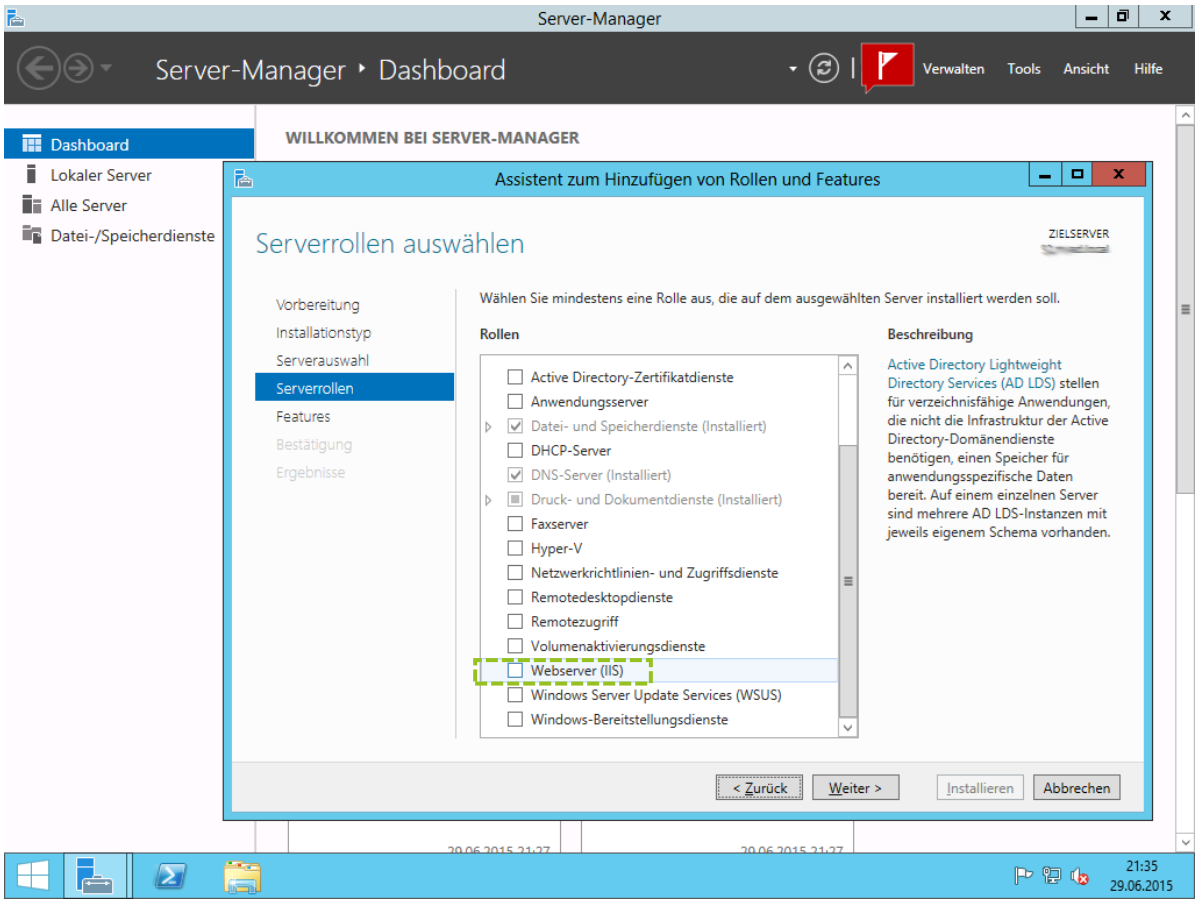


***Bild 4.5** – Server Manager, "Web Server (IIS)" Rolle hinzufügen*

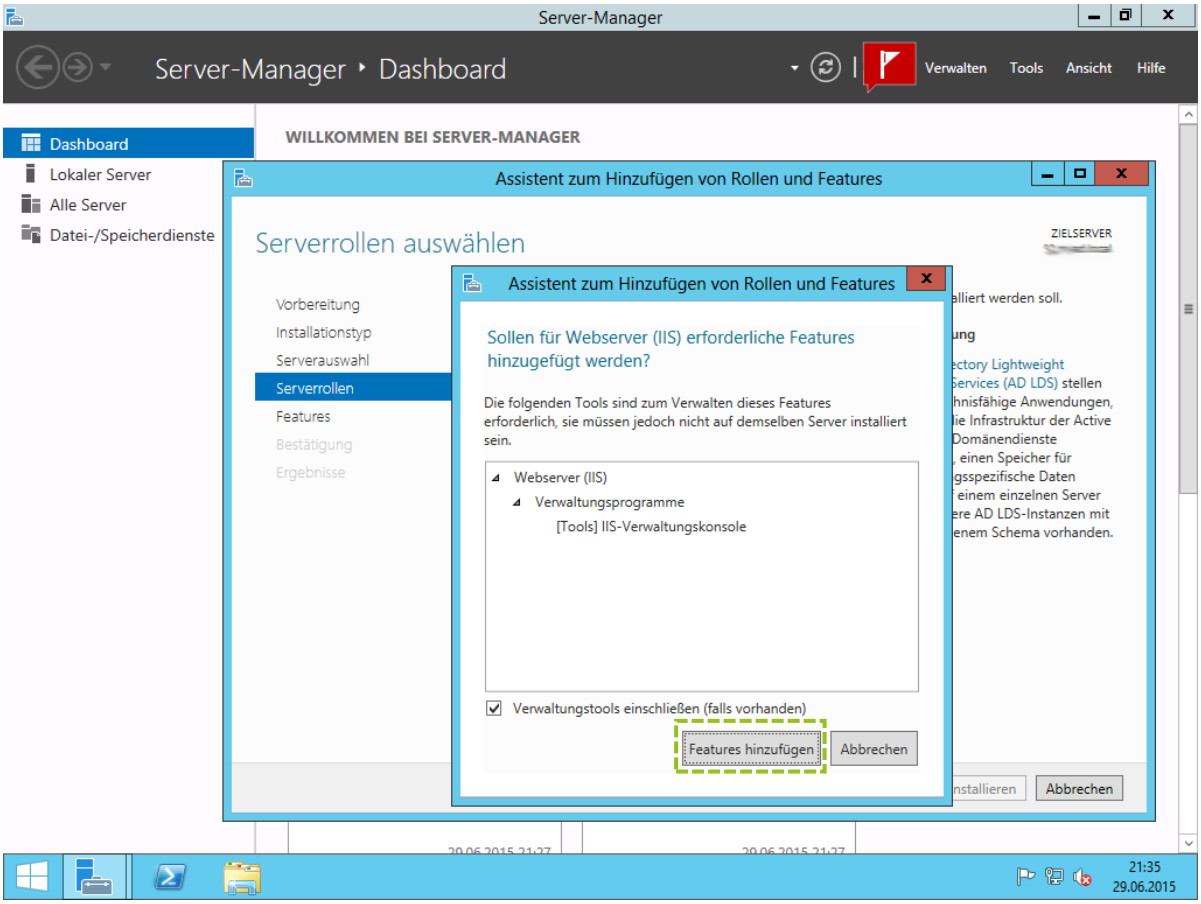


***Bild 4.6** – Server Manager, "Web Server (IIS)" Rolle*

- Der Installationsassistent "Assistent zum Hinzufügen von Rollen und Features" wird geöffnet.

► Übernehmen Sie diese Einstellungen als Standard und klicken Sie auf "Features hinzufügen".

- Der Installationsassistent installiert den IIS-Webserver, was einige Minuten dauern kann.

Installieren des ARR (Application Request Routing)

► Um "Application Request Routing" zu installieren, rufen Sie in einem Browser folgende Seite auf: https://www.microsoft.com/web/downloads/platform.aspx.

► Klicken Sie auf der Webseite auf "Install this extension" und dann auf "Save file".

- Der Download für Microsoft Web Platform Installer 5.0 wird gestartet.

► Installieren Sie die Erweiterung nach dem Download.

► Klicken Sie nach der Installation oben rechts im Fenster auf "Application Request Routing".

- Das folgende Fenster wird angezeigt.

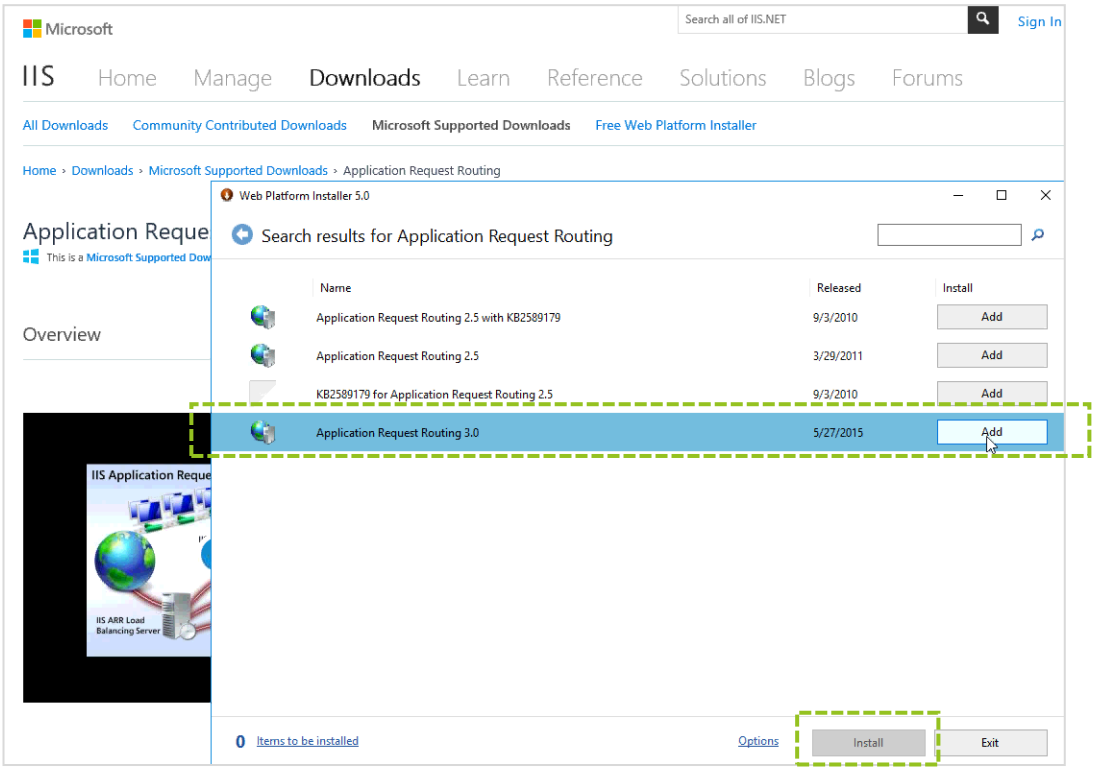


***Bild 4.7** – Microsoft Web Platform 5.0, Application Request Routing*

► Klicken Sie in der Zeilte "Application Request Routing 3.0" auf "Add" und dann unten im Fenster auf "Install".

Konfigurieren des IIS-Webservers

► Öffnen Sie den "Internet Information Service (IIS) Manager" über die Windows-Verwaltung (in der Systemsteuerung unter "Systemsteuerung -> Alle Systemsteuerungselemente -> Verwaltung").

► Um das Application Request Routing zu aktivieren, öffnen Sie die IIS-Server-Homepage und klicken Sie auf "Application Request Routing".

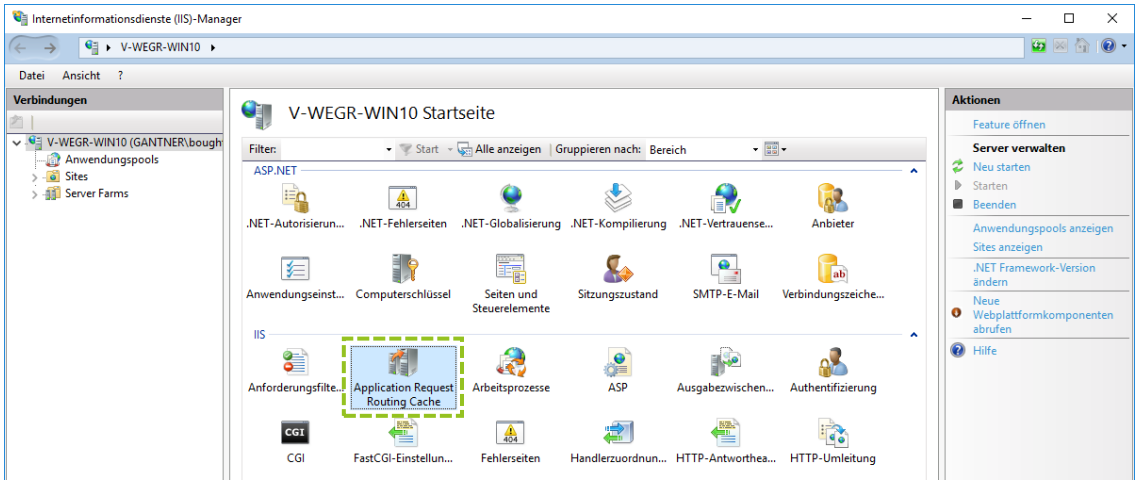


***Bild 4.8** – IIS Manager, Application Request Routing*

► Klicken Sie in der rechten Spalte "Aktionen" auf "Server Proxy Settings…".

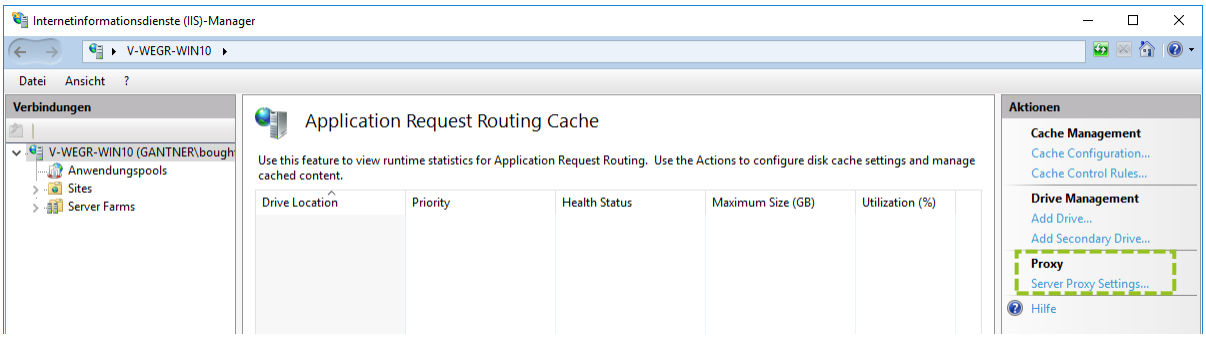


***Bild 4.9** – IIS Manager, Einstellungen für Server Proxy aufrufen*

► Wählen Sie die Option "Enable proxy" (lassen Sie die anderen Einstellungen unverändert) und klicken Sie dann rechts in der Spalte "Aktionen" auf "Übernehmen".

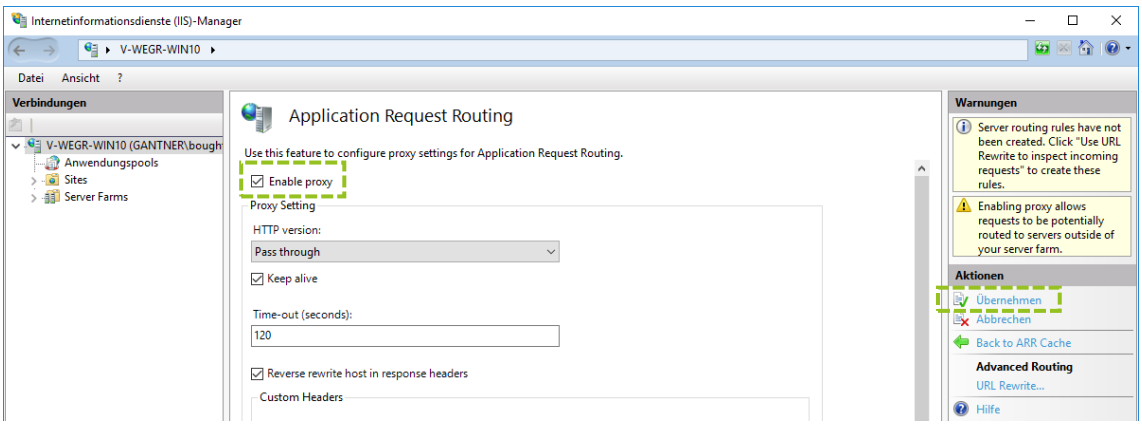


***Bild 4.10** – IIS Manager, Proxy aktivieren*

► Kehren Sie zur Strartseite des IIS-Servers zurück und klicken Sie auf "Serverzertifikate", um das Zertifikat für HTTPS zu importieren.

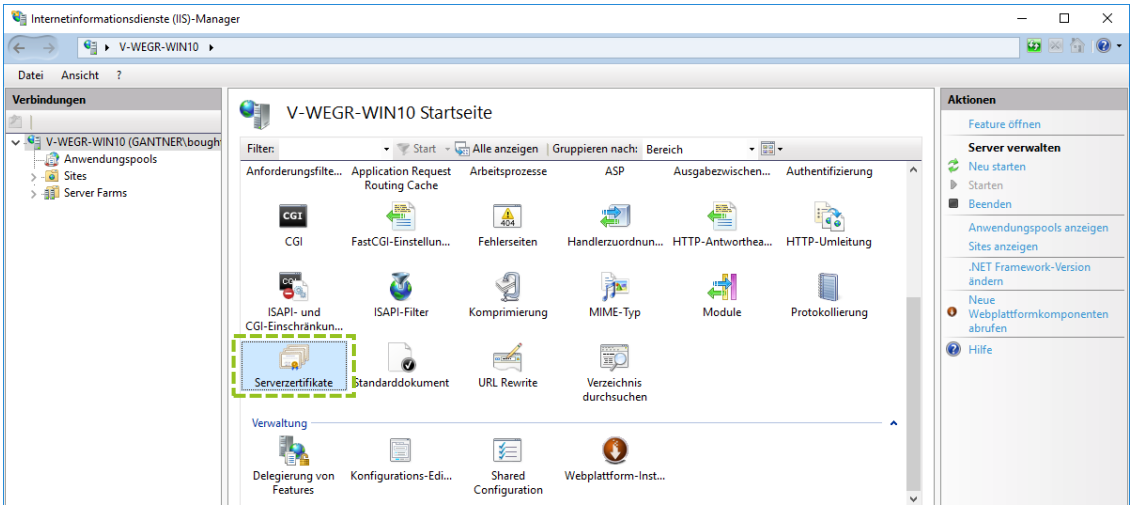


***Bild 4.11** – IIS Manager, Serverzertifikate*

► Klicken Sie in der rechten Spalte "Aktionen" auf "Importieren…".

► Geben Sie im Fenster "Zertifikat importieren" den Speicherort und das Kennwort des Zertifikats ein und klicken Sie dann auf "OK".

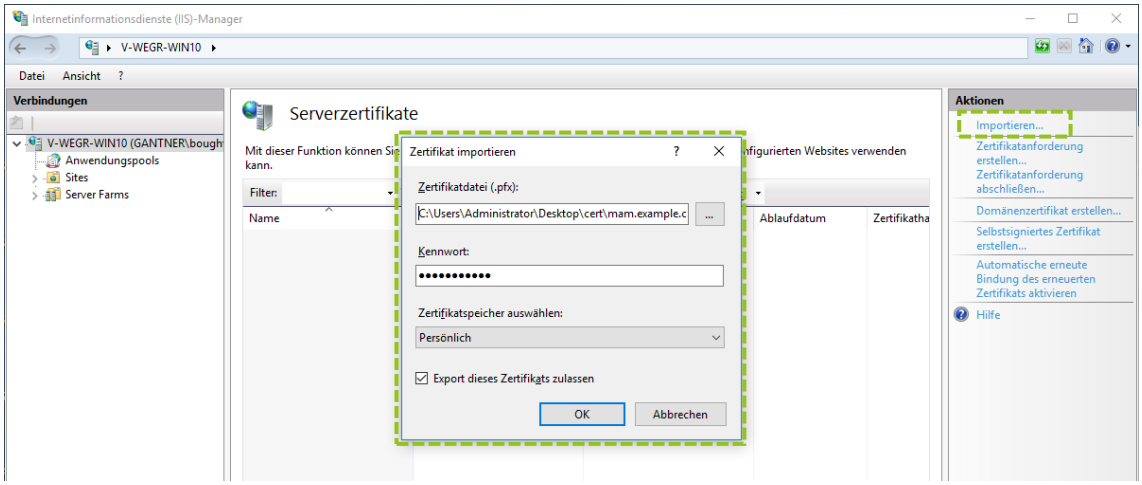


***Bild 4.12** – IIS Manager, Zertifikat importieren*

► Öffnen Sie in der linken Spalte "Verbindungen" den Ordner "Sites", klicken Sie mit der rechten Maustaste auf "Default Website" und wählen Sie im Menü "Entfernen".

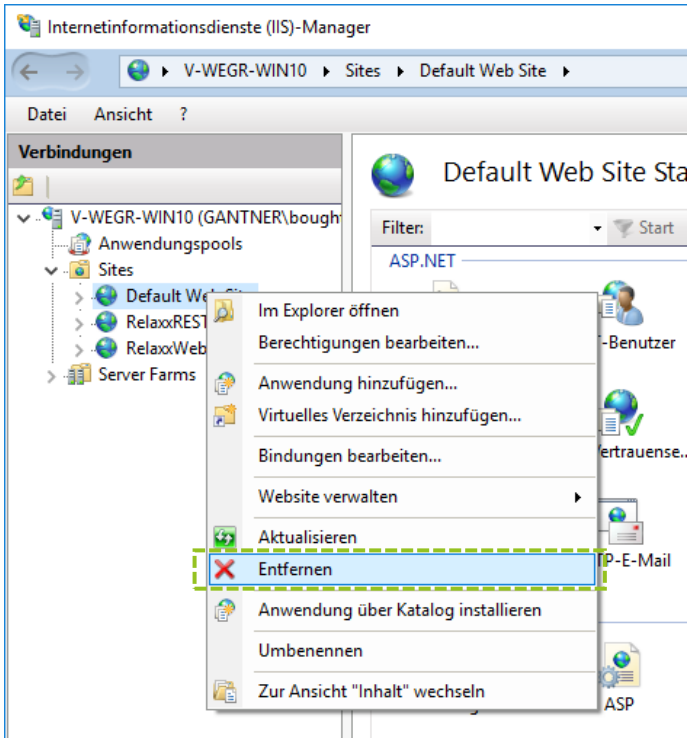


***Bild 4.13** – IIS Manager, Standard Webseite entfernen*

► Klicken Sie links in der Spalte "Verbindungen" mit der rechten Maustaste auf den Ordner "Sites" und wählen Sie dann im Menü die Option "Website hinzufügen".

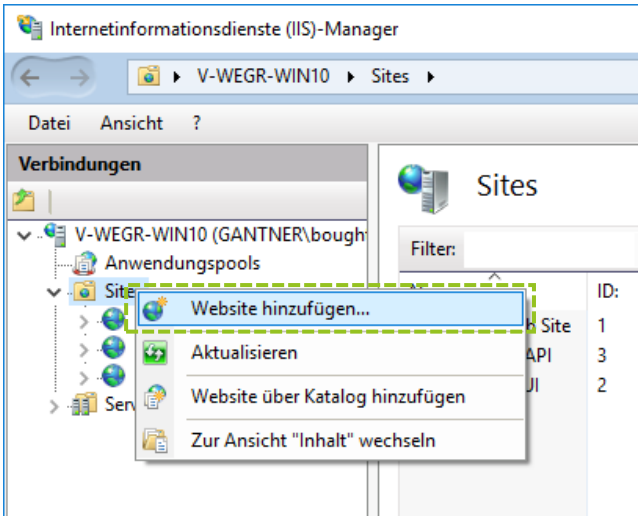


***Bild 4.14** – IIS Manager, Website hinzufügen*

- Das Fenster "Website hinzufügen" wird geöffnet.

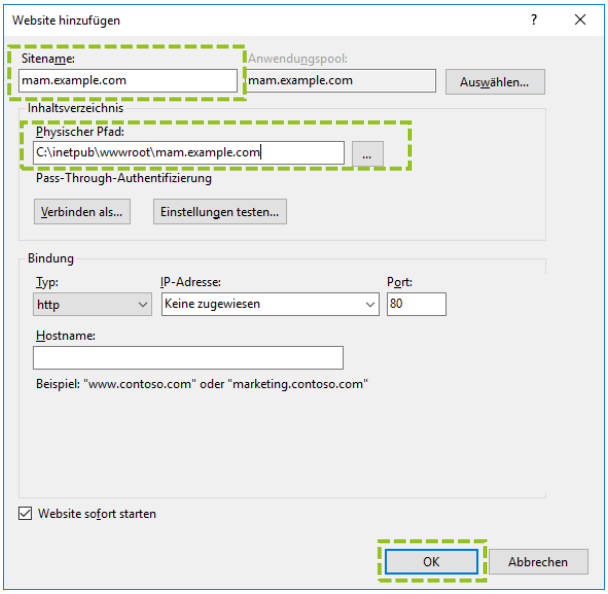


***Bild 4.15** – IIS Manager, Einstellungen für neue Website*

► Geben Sie folgende Informationen ein:

- Sitename: Geben Sie den Domain-Namen ein, der für Mobile Access Management verwendet werden soll, z. B. `mam.example.com`
- Physischer Pfad: Geben Sie den Pfad zu dem Ordner ein, in dem die Website installiert ist, z. B. `C:\inetpub\wwwroot\mam.example.com`

► Klicken Sie auf "OK", um die Einstellungen zu speichern.

► Öffnen Sie die erstellte Website und klicken Sie rechts in der Spalte "Aktionen" auf "Bindungen…".

► Klicken Sie auf "Hinzufügen", um eine weitere Bindung für diese Site hinzuzufügen, und konfigurieren Sie dann die folgenden Einstellungen im Fenster "Sitebindung hinzufügen":

- Typ: Wählen Sie "`https`" aus dem Menü.
- Hostname: Geben Sie den DNS-Namen der Website ein, z. B. „`mam.example.com`“.
- SSL-Zertifikat: Wählen Sie das importierte Zertifikat aus (wie über "Serverzertifikate" auf der IIS-Homepage importiert).

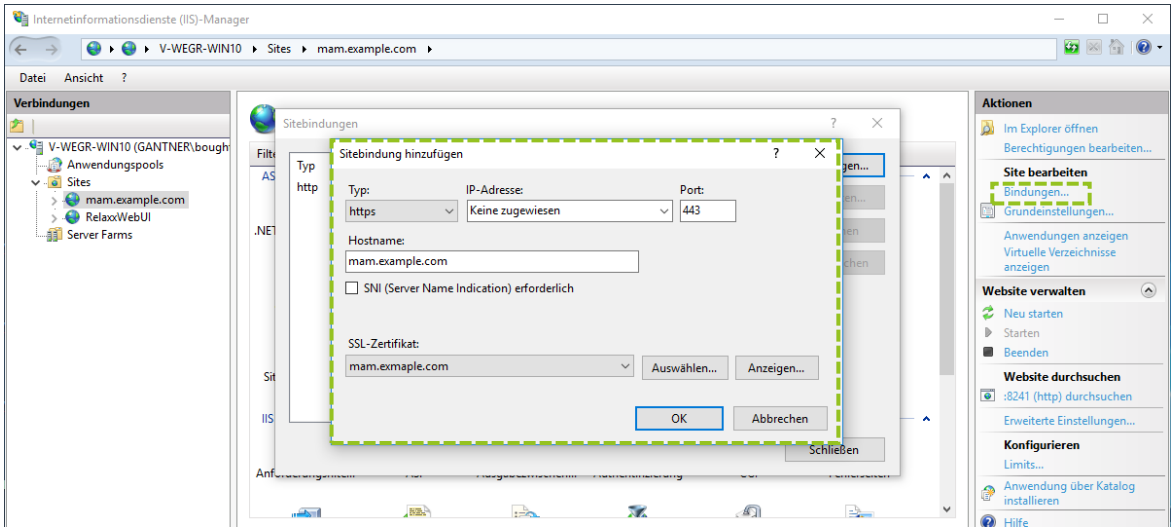


***Bild 4.16** – IIS Manager, Sitebindung hinzufügen*

► Klicken Sie auf "OK", um die Einstellungen zu speichern und klicken Sie dann im Fenster "Sitebindungen" auf "Schließen".

► Klicken Sie auf der Homepage der aktuellen Site auf "URL Rewrite".

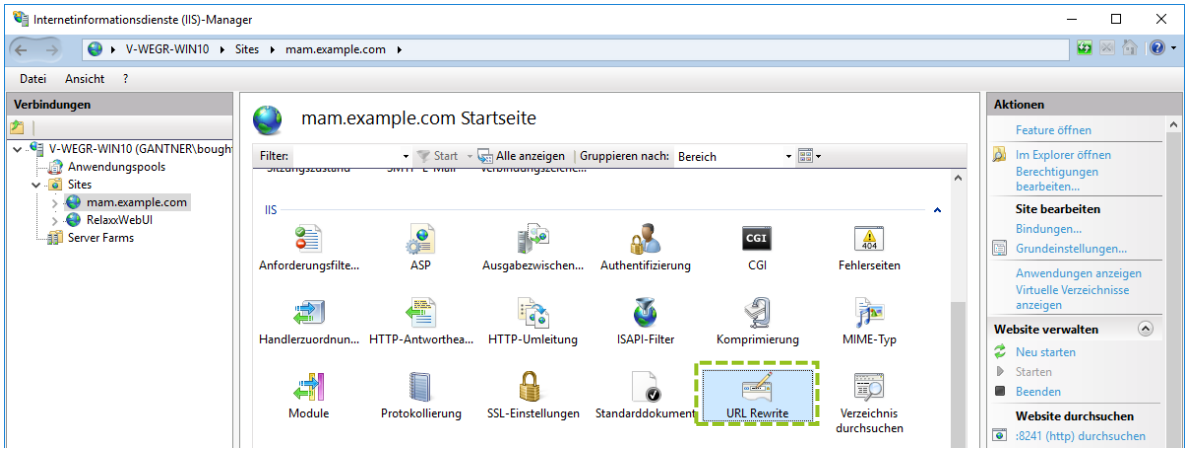


***Bild 4.17** – IIS Manager, Umleitung für URL festlegen*

► Klicken Sie rechts in der Spalte "Aktionen" auf "Add Rule(s)…".

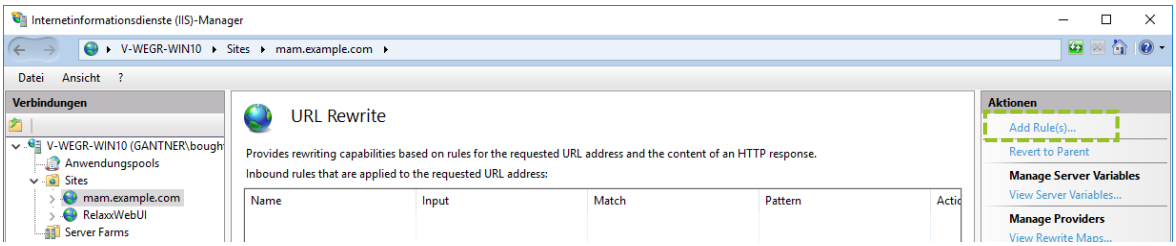


***Bild 4.18** – IIS Manager, Regel hinzufügen*

► Wählen Sie im Fenster "Add Rule(s)" die Option "Blank rule" und klicken Sie auf "OK".

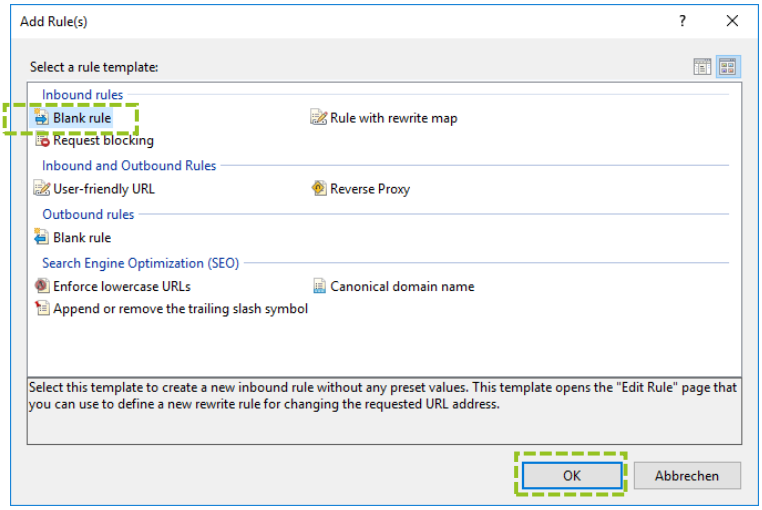


***Bild 4.19** – IIS Manager, Auswahl einer leeren Regelvorlage*

► Konfigurieren Sie im Fenster "Edit Inbound Rule" die folgenden Einstellungen:

- Name: Geben Sie "`HTTP to HTTPS`" in das Feld ein.
- Pattern: Geben Sie "`(.*)`" in das Feld ein.

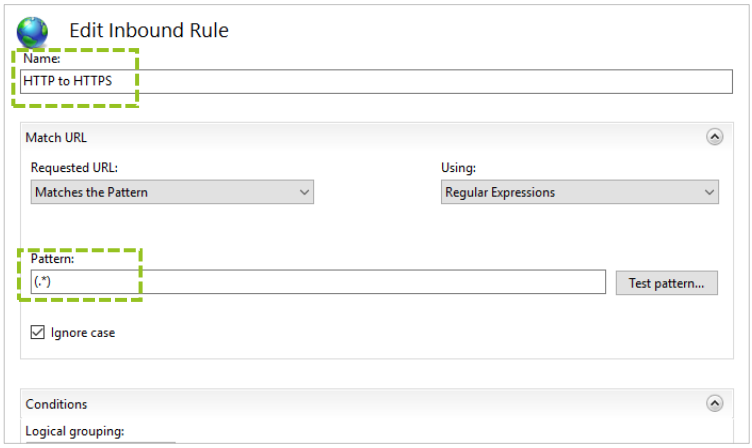


***Bild 4.20** – IIS Manager, Eingangsregel bearbeiten*

► Klappen Sie den Bereich "Conditions" auf und klicken Sie dann auf "Add…".

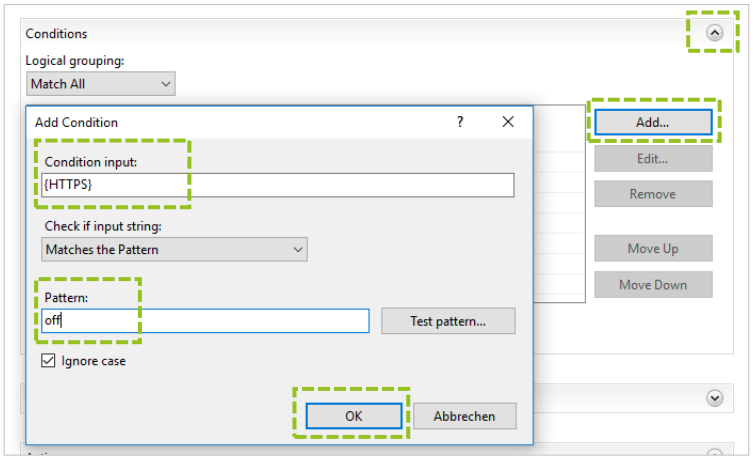


***Bild 4.21** – IIS Manager, Bedingung hinzufügen* (Conditions)

► Konfigurieren Sie im Fenster "Add Condition" die folgenden Einstellungen und klicken Sie dann auf "OK".

- Condition input: Geben Sie "`{HTTPS}`" in das Feld ein.
- Pattern: Geben Sie "`off`" in das Feld ein.

► Klappen Sie den Bereich "Action" auf und konfigurieren Sie folgende Einstellungen:

- Action type: Wählen Sie im Menü die Option "Redirect".
- Redirect URL: Geben Sie "`https://<domain name>/{R:1}`" ein (z. B. `https://mam.example.com/{R:1}`
- Redirect type: Wählen Sie im Menü die Option "Permanent (301)".

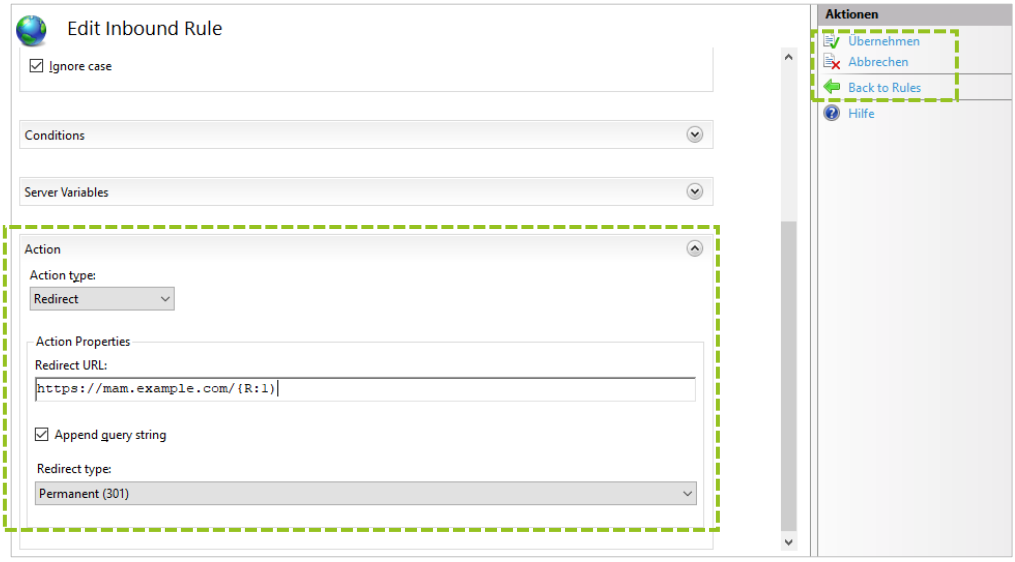


***Bild 4.22** – IIS Manager, Aktionen festlegen (Actions)*

► Klicken Sie in der rechten Spalte "Aktionen" auf "Übernehmen" und dann auf "Back to Rules".

► Fügen Sie eine weitere Regel hinzu, indem Sie im IIS Manager unter "URL Rewrite" auf "Add Rule(s)…" and "Blank rule" klicken (siehe vorige Schritte). Konfigurieren Sie die folgenden Einstellungen:

- Name: Geben Sie "`HTTP Rewrite`" in das Feld ein.
- Pattern: Geben Sie "`(.*)`" in das Feld ein.

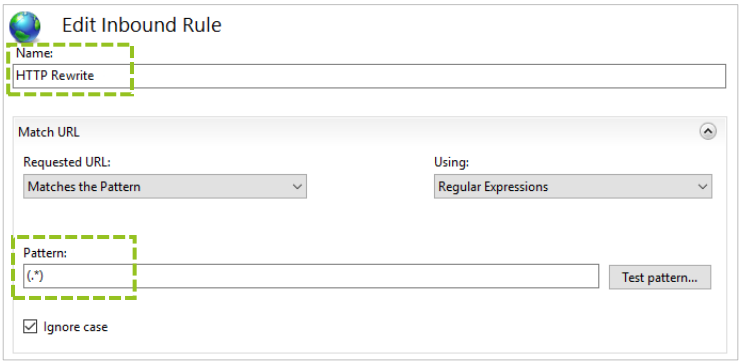


***Bild 4.23** – IIS Manager, Eingangsregel bearbeiten*

► Klappen Sie den Bereich "Conditions" auf und klicken Sie dann auf "Add…"

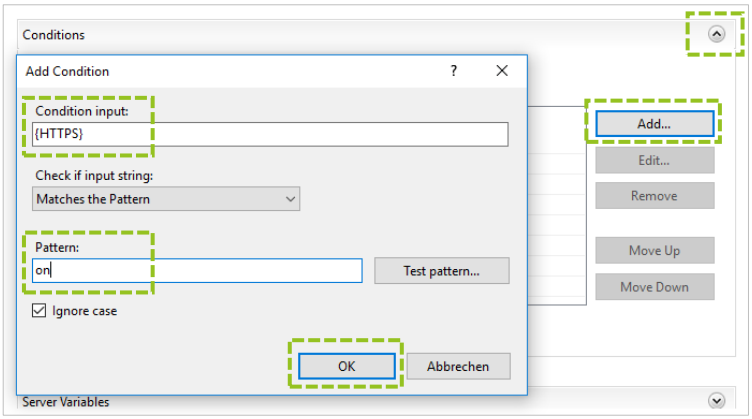


***Bild 4.24** – IIS Manager, Bedingung hinzufügen (Conditions)*

► Konfigurieren Sie im Fenster "Add Condition" die folgenden Einstellungen und klicken Sie dann auf "OK".

- Condition input: Geben Sie "`{HTTPS}`" in das Feld ein.
- Pattern: Geben Sie "`on`" in das Feld ein.

► Klappen Sie den Bereich "Action" auf und konfigurieren Sie folgende Einstellungen:

- Action type: Wählen Sie "Rewrite" aus dem Menü.
- Rewrite URL: Geben Sie "`http://<interner Pfad zum Mobile Access Management Dienst>:8234/{R:1}`" ein. z. B. `http://localhost:8234/{R:1}`
- Markieren Sie die Option "Stop processing of subsequent rules".

***Bild 4.25** – IIS Manager, Aktionen festlegen (Actions)*

► Klicken Sie in der rechten Spalte "Aktionen" auf "Übernehmen".

- Die Einrichtung für HTPPS ist jetzt abgeschlossen.

► Um zu überprüfen, ob die HTTPS Verbindung funktioniert, öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

`http://<Ihr Domainname>/MobileAccessService`

(z. B. `http://mam.example.com/MobileAccessService`)

- Eine Seite, wie in folgendem Bild gezeigt, sollte angezeigt werden. Vergewissern Sie sich, dass die URL von "`http://...`" auf "`https://...`" geändert wurde.

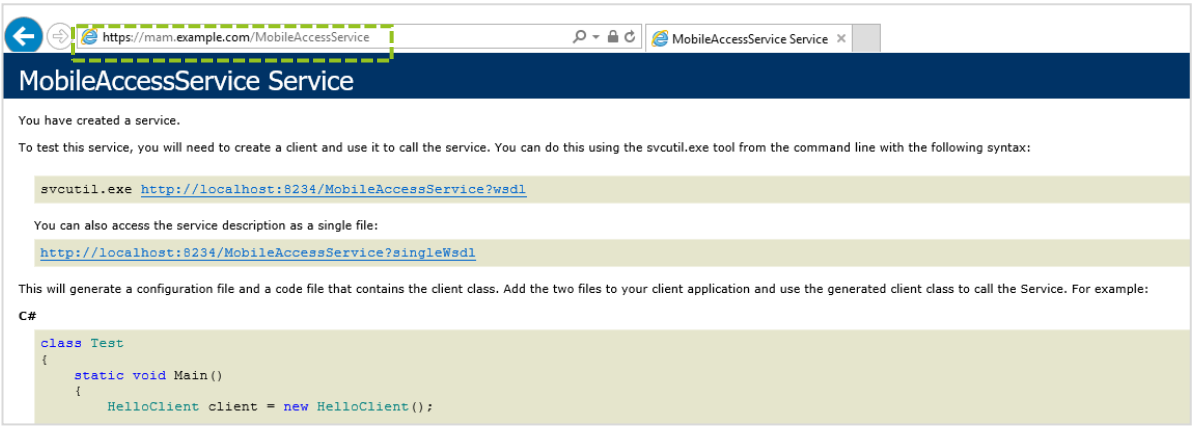


***Bild 4.26** – Testen der HTTPS-Verbindung*

4.4 Einrichtung einer TLS Verbindung zu GAT ACE

Die Kommunikation zwischen dem GAT Mobile Access Server und GAT ACE 3000 oder 7000 kann optional über das TLS Protokoll (früher SSL genannt) verschlüsselt erfolgen. Dazu kann ein Zertifikat verwendet werden, das vom Kunden bereitgestellt wird, oder es kann ein selbst signiertes Zertifikat erzeugt werden.

TLS muss sowohl für den GAT Mobile Access Server als auch in der Konfigurationsdatei von GAT ACE 3000 bzw. 7000 aktiviert werden.

Lesen Sie auch die detailierten Informationen zur TLS Verbindung im GAT ACE Handbuch.

4.4.1 GAT Mobile Access Configuration

Aktivieren Sie die TLS Verschlüsselung für GAT ACE wie folgt.

► Klicken Sie im GAT Mobile Access Configuration auf "Interfaces".
  - Es öffnet sich folgendes Fenster.

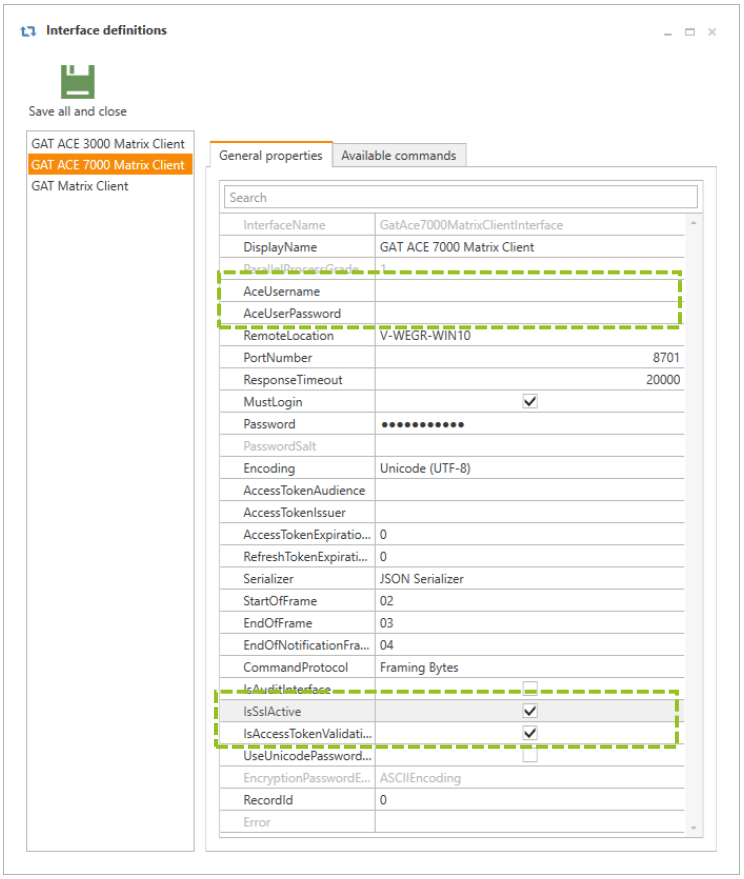


***Bild 4.27** - Einstellen der Schnittstellenparameter*

► Wechseln Sie links zu dem GAT ACE Client, den Sie konfigurieren wollen (im Beispiel GAT ACE 7000).
► Markieren Sie "IsSslActive".

► Markieren Sie, wenn gewünscht, auch "IsAccessTokenValidationActive". Der Parameter gibt an, ob die Authentifizierung mittels JWT Token aktiviert ist, was im Zusammenhang mit TLS immer aktiv sein sollte. Geben Sie bei Aktivierung dann auch noch folgende Informationen ein :

- AceUsername: Benutzername für die Anmeldung an GAT ACE.
- AceUserPassword: Passwort für die Anmeldung an GAT ACE.

► Bestätigen Sie mit Klick auf "Save".

4.4.2 GAT ACE 3000 und 7000

In GAT ACE 3000 bzw. 7000 muss TLS in der Konfigurationsdatei aktiviert werden. Dazu ist ein Eintrag in dieser Datei notwendig. Es handelt sich um eine Textdatei, die Sie in einem Texteditor öffnen können. Für GAT ACE 7000 gehen Sie wie folgt vor:

► Öffnen Sie die Datei "`GATAce7000.cfg`" im Standardpfad der GAT ACE 7000 Software.

***Bild 4.28** - Konfigurationsdatei für GAT ACE 7000*

► Setzen Sie im Abschnitt "`MatrixInterface`" den Wert von "`issslactive`" auf "True".

► Zur Authentifizierung mittels JWT Token setzen Sie auch die Option "`isaccesstokenvalidationactive`" auf "True".

► Starten Sie den Dienst von GAT ACE 7000 neu.

Bei GAT ACE 3000 ist die selbe Einstellung notwendig. Der Name der Konfigurationsdatei ist dort "`GATAce3000.cfg`", und die Einstellung findet sich dort beim Feld "`issslactive`" im Abschnitt "`GatAceMatrixServerInterface`".

Im Handbuch zu GAT ACE 7000 und 3000 finden Sie weitere Informationen zur Aktivierung der TLS Verschlüsselung und wie das notwendige Zertifkat installiert wird.

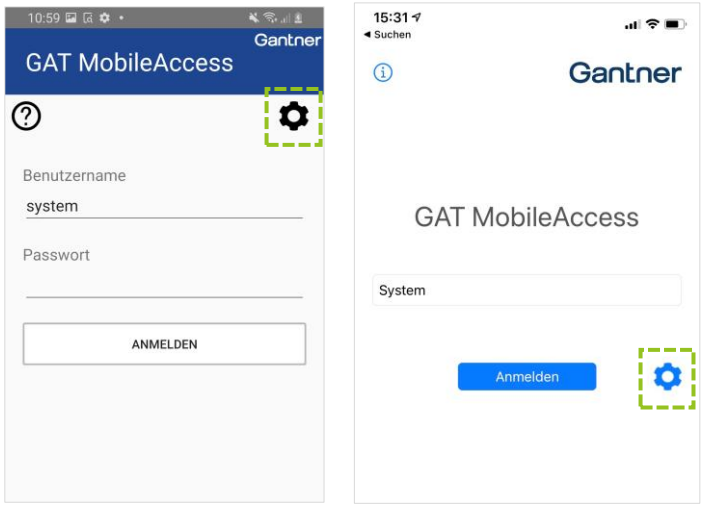
4.5 Konfiguration der GAT Mobile Access App

Nach der Installation der GAT Mobile Access App können Sie grundsätzliche Einstellungen, die die gesamte App betreffen, einstellen. Es können mehrere Konfigurationen mit jeweils unterschiedlichen Login Daten gespeichert werden. GAT Mobile Access merkt sich die ausgewählte Konfiguration, so dass diese für jeden zukünftigen Login verwendet wird, sofern nicht manuell eine andere Konfiguration ausgewählt wird.

HINWEIS! Die folgende Beschreibung zeigt die Einstellungen in der Android-App. Die Einstellungen sind bei der iPhone App gleich.

► Starten Sie die App.

► Klicken Sie im Anmeldebildschirm auf das "Einstellungen"-Symbol. Dies sieht je nach Betriebssystem wie folgt aus:



Android iPhone

***Bild 4.29** - Einstellungsseite aufrufen*

- Es öffnet sich die Liste der definierten Konfigurationen. Die gerade aktive Konfiguration ist mit einem Haken markiert (hier "GAT Mobile Access Server"). Diese wird für die Anmeldung in der App verwendet.

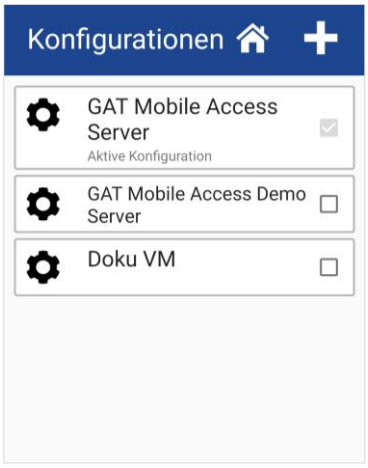


***Bild 4.30** - App-Einstellungen bei Android*

- ► Um eine andere Konfiguration zu aktivieren, klicken sie auf das Markierungsfeld rechts neben der gewünschte Konfiguration oder klicken Sie länger auf eine inaktive Konfiguration und wählen Sie dann aus dem angezeigten Menü "Als aktive Konfiguration setzen".
  - o Die Konfiguration wird mit Haken markiert und an erster Stelle angezeigt.
- ► Mit dem Symbol " " gelangen Sie zurück zum Anmeldebildschirm.
- ► Mit dem Symbol " " können Sie eine neue Konfiguration anlegen.
- ► Mit Klick auf eine Konfiguration können Sie die Einstellungen der Konfiguration ändern.
  - o In beiden Fällen gelangen Sie zur Einstellungsseite der Konfiguration.
  - o Die Konfiguration ist in die beiden Tabs "Server" und "Inhalt" unterteilt (bei Android nebeneinander, bei iPhone untereinander angeordnet).

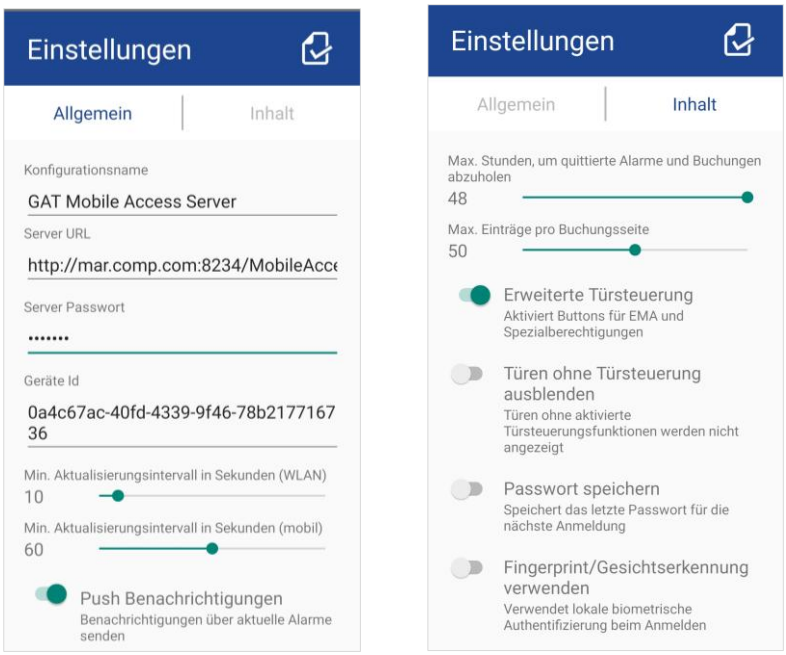


***Bild 4.31** - App-Einstellungen bei Android*

- ► Definieren Sie in der Einstellungsseite "Server" folgende Einstellungen:
  - Konfigurationsname: Hier können Sie für die Konfiguration einen Namen eintragen.
  - Server URL: Dies ist die URL, mit der Ihr installierter GAT Mobile Access Management Server erreichbar ist. Geben Sie diese in folgender Form ein:
    `http://<Server>:8234/MobileAccessService`
    Das Feld `<Server>` in den spitzen Klammen muss durch den richtigen Namen des Servers oder die richtige IP-Adresse ersetzt werden (der Demoserver hat den Namen `mademo.gantner.com`). Der Port 8234 und "/MobileAccessServcie" sind die Standardwerte, die bei einer Standardinstallation ohne manuelle Änderungen verwendet werden.
  - Server Passwort: Das Passwort des GAT Mobile Access Management Service, so wie es bei der Installation hinterlegt wurde (Standard = GAT0815).
  - Geräte Id: Hier wird die ID ihres Mobilgeräts angezeit. Sie müssen diese ID in Matrix eintragen, um das Mobilgerät zu registrieren (siehe unten).
  - Min. Aktualisierungsintervall in Sekunden (WLAN):
    Hat das mobile Endgerät Zugriff auf ein LAN, wird der Inhalt der App jeweils automatisch nach dem eingetragenen Intervall (Angabe in Sekunden) aktualisiert.

Beachten Sie, dass es für verschiedene Bereiche der App Abweichungen von dieser Einstellung geben kann.

- Min. Aktualisierungsintervall in Sekunden (mobile):
  Verfügt das mobile Endgerät nur über eine GSM Verbindung, wird der Inhalt der App jeweils automatisch nach dem eingetragenen Intervall (Angabe in Sekunden) aktualisiert. Beachten Sie, dass es für verschiedene Bereiche der App Abweichungen von dieser Einstellung geben kann.
- Push Benachrichtigungen: Geben Sie hier an, ob Sie Push-Benachrichtigungen ("Push Notifications") vom Server erhalten wollen. Bitte beachten Sie, dass sowohl das mobile Endgerät als auch der GAT Mobile Access Management Service Zugriff auf den verwendeten Push-Benachrichtigungsdienst Firebase Cloud Messaging haben müssen. Möglicherweise unterstützen nicht alle mobilen Endgeräte Push-Benachrichtigungen. Eine Änderung dieser Einstellung wird erst nach einem erfolgreichen Login aktiv.
  HINWEIS! Bitte beachten Sie die Angaben zum Thema Verfügbarkeit und Performance der jeweiligen Push-Benachrichtigungsdienste.

► Definieren Sie in der Einstellungsseite "Inhalt" folgende Einstellungen:

- Max. Stunden um quittierte Alarme und Buchungen abzuholen:
  Buchungen und quittierte Alarme werden nur für die hier angegeben Stunden angezeigt. Buchungen und quittierte Alarme, die weiter in der Vergangenheit liegen, werden nicht angezeigt.
- Max. Einträge pro Buchungsseite:
  Anzahl der Buchungen die pro Buchungsseite angezeigt werden. Sollte es zu starken Verzögerungen bei der Darstellung der Buchungsliste kommen, verringern Sie bitte diesen Wert.
- Erweiterte Türsteuerung: Aktiviert die Steuerelemente für die Überwachung und spezielle Rechte in der Detailansicht der Türen.
- Türen ohne Türsteuerung ausblenden:
  Wenn diese Funktion aktiviert ist, werden nur Türen angezeigt, für die die Türsteuerungsfunktion in Matrix aktiviert ist.
- Passwort speichern: Speichert das zuletzt verwendete Passwort ab und stellt es beim Login automatisch zur Verfügung.
  ACHTUNG! Beachten Sie, dass durch das Speichern ein erhöhtes Sicherheitsrisiko bei Verlust oder Diebstahl Ihres Geräts entsteht.
- Fingerprint/Gesichtserkennung verwenden:
  Ist diese Option markiert, kann für die Anmeldung in der App anstelle eines Passworts die Biometrieerkennung des Mobilegeräts (Fingerabdruck oder Gesichtserkennung) verwendet werden (siehe "5.1. Erster Start und Login").

► Zum Speichern der Änderungen an der Konfiguration klicken Sie auf das Symbol " ".

► Wollen Sie eine Konfiguration löschen, klicken Sie länger auf eine Konfiguration (nur inaktive Konfiguationen) und wählen Sie aus dem angezeigten Menü den Menüpunkt "Konfiguration löschen".

4.5.1 Sprache

Die GAT Mobile Access Management Apps unterstützen die Sprachen Englisch und Deutsch. Wird die App auf einem deutschen Endgerät installiert, wird automatisch Deutsch verwendet, ansonsten immer Englisch

4.6 Registrieren eines mobilen Geräts in Matrix

Um ein mobiles Endgerät mit GAT Mobile Access Management verwenden zu können, muss es zunächst in der Matrix Software einem Matrix Benutzer zugeordnet werden. Gehen Sie dazu wie folgt vor:

- ► Öffnen Sie die Software Matrix und wechseln Sie in die Benutzerverwaltung (Menü "Datei" -> Menüpunkt "Benutzerverwaltung").
- ► Öffnen Sie den gewünschten Benutzer, durch markieren und Auswahl des Symbols "Benutzer editieren".
  - o Folgendes Fenster wird angezeigt.

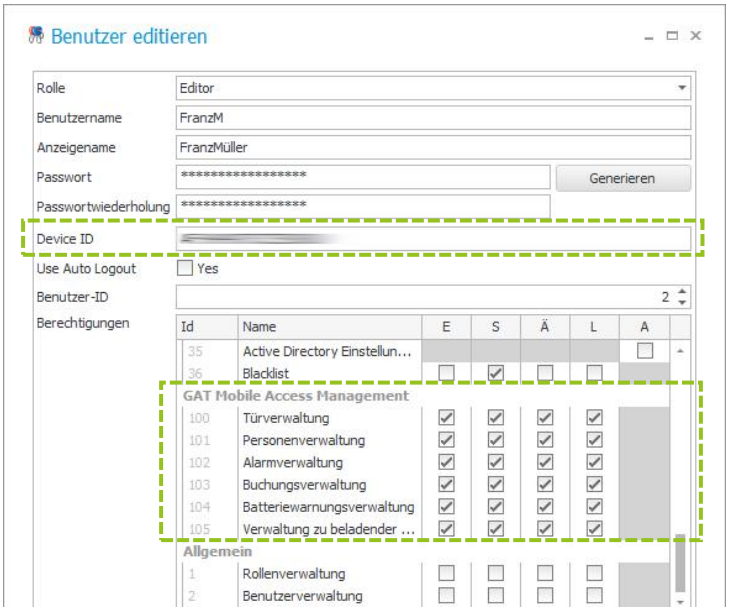


***Bild 4.32** - Bearbeiten eines Benutzers in Matrix*

- ► Tragen Sie die Geräte IDs der mobilen Endgeräte des Benutzers getrennt durch ein Semikolon ";" in das Feld "Device ID" ein. Die Geräte IDs finden Sie in den Einstellungen des mobilen Endgeräts unter "Geräte Id" (siehe vorigen Abschnitt).

  HINWEIS! Beachten Sie bei der Eingabe der Geräte-Id unbedingt die Groß- und Kleinschreibung.
- ► Stellen Sie in den Berechtigungen unter "GAT Mobile Access Management" die gewünschten Rechte ein.

HINWEIS! Die Geräte ID eines mobilen Endgeräts bleibt so lange erhalten wie die App installiert ist und überdauert auch Updates. Es kann allerdings möglich sein, dass auf Grund geänderter Anforderungen der einzelnen Plattformen die Geräte IDs erneuert werden müssen.

Falls die mobile App in einem Zutrittssystem registriert ist und Sie die App in einem anderen System verwenden möchten, muss die App deinstalliert und neu installiert werden, damit die Push Notifications im neuen System ordnungsgemäß funktionieren. Durch diesen Vorgang wird eine neue Device-ID generiert, welche im neuen System (Matrix) wie beschrieben eingetragen werden muss.

5 BEDIENUNG

In diesem Kapitel finden Sie einen Funktionsüberblick der mobilen GAT Mobile Access App (kurz: GAT Mobile Access). Die Bedienung wird hier für das Android Betriebssystem beschrieben. Grundsätzlich ist die Bedienung auf den anderen Betriebssystemen identisch. Bei eventuellen Abweichungen wird speziell darauf hingewiesen.

5.1 Erster Start und Login

Nachdem sowohl der GAT Mobile Access Service als auch die App GAT Mobile Access konfiguriert sind, können Sie die App starten. Für die Verwendung müssen Sie sich mit Ihrem Benutzer anmelden.

Für die Anmeldung kann die Kombination aus Benutzername oder die vom mobilen Gerät unterstützte Biometrie-Erkennung mittels Fingerabdruck oder Gesichtserkennung verwendet werden. Zur Verwendung der Biometrie-Erkennung muss diese in der Konfiguration aktiviert sein (Option "Fingerprint/Gesichtserkennung verwenden" in den Einstellungen -> siehe "4.5. Konfiguration der GAT Mobile Access App").

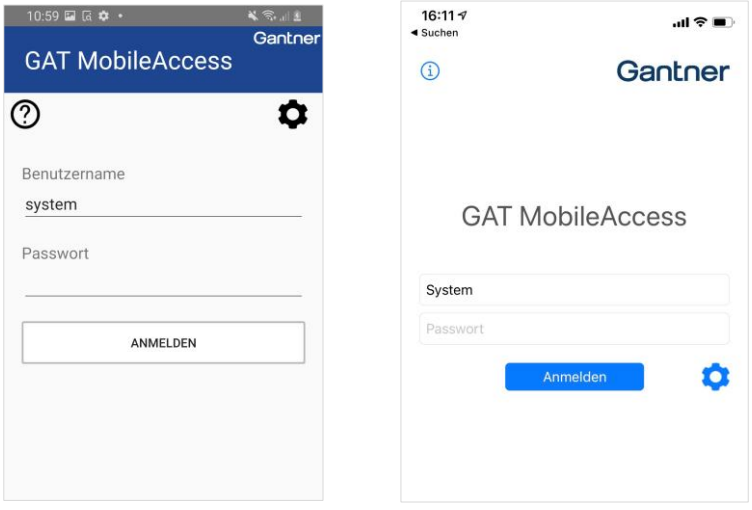
ACHTUNG! Wenn Sie die Arbeit in der App beendet haben, melden Sie sich bitte aus Sicherheitsgründen immer mit dem Symbol ⏻ ab. Sie gelangen dann zurück in den Login-Bildschrim.

5.1.1 Login mittels Benutzername und Passwort

Diese Anmeldemöglichkeit kann immer verwendet werden, auch wenn die Biometrie-Erkennung aktiviert ist.

► Starten Sie die App.

- Ist die Biometrie-Erkennung deaktiviert, werden die Eingabefelder für Benutzername und Passwort angezeigt.



Android iPhone

***Bild 5.1** – Anmeldebildschirm für Benutzername und Passwort auf den verschiedenen Betriebssystemen*

- Ist die Biometrie-Erkennung aktiviert, wird zuerst nur der Benutzername angezeigt. Mit Klick auf "ANMELDEN" haben Sie die Möglichkeit zur Biometrie-Erkennung (siehe nächste Seite). Klicken Sie hier auf "ABBRECHEN". Die Biometrie-Erkennung wird abgebrochen und es wird Bild 5.1 angezeigt.

► Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
HINWEIS! Da in Matrix Ihr Mobilgerät Ihrem Matrix Benutzer zugewiesen wurde (siehe "4.6. Registrieren eines mobilen Geräts in Matrix") können Sie für den Login denselben Benutzername und das gleiche Passwort wie für den Login in Matrix verwenden.

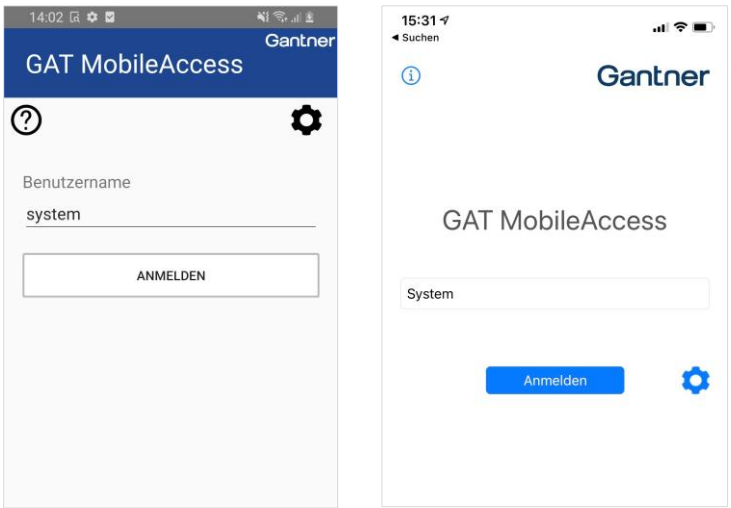
► Drücken Sie anschließend auf “ANMELDEN“.
  - Der Startbildschirm von GAT Mobile Access wird angezeigt.

HINWEIS! Wird GAT Mobile Access im Demomodus betrieben, verwenden Sie bitte jeweils „Demo“ als Benutzername und Passwort.

5.1.2 Login mittels Biometrie-Erkennung

Die Biometrie-Erkennung kann mit der Option "Fingerprint/Gesichtserkennung verwenden" in den Einstellungen aktiviert werden. Es wird dabei die Biometriefunktion des Mobilegeräts verwendet. Für die Identifkation mittels Fingerabdruck muss das Mobilegerät deshalb über einen Fingerabdrucksensor verfügen und Sie müssen einen Fingerabdruck berechtigt haben. Das selbe gilt für die Gesichtserkennung mittels eingebauter Kamera und zuvor am Mobilgerät berechtigtem Gesicht.

► Starten Sie die App.
  - Wenn die Biometrie-Erkennung aktiviert ist, wird beim Start von GAT Mobile Access nur das Feld für den Benutzernamen angezeigt.



Android iPhone

***Bild 5.2** - Anmeldebildschirm für Biometrie auf den verschiedenen Betriebssystemen*

► Klicken Sie auf "ANMELDEN".
  - Es werden folgende Auswahloptionen für die die Biometrie-Erkennung angezeigt.

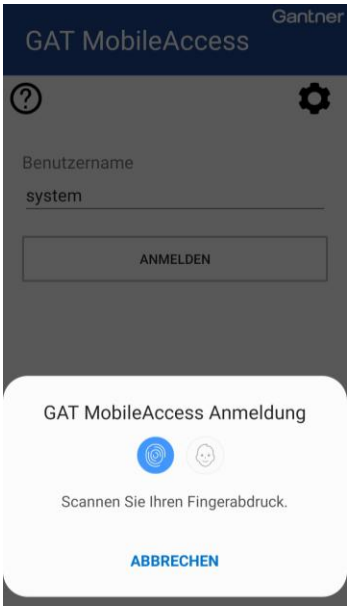


***Bild 5.3** - Biometrie-Erkennung Auswahl*

- ► Wählen Sie den Typ der Biometrie-Erkennung aus (linkes Symbol = Fingerabdruck oder rechtes Symbol = Gesichtserkennung).
- ► Identifizieren Sie sich nun je nach Auswahl mit Ihrem Fingerabdruck oder Ihrem Gesicht am Mobilgerät.

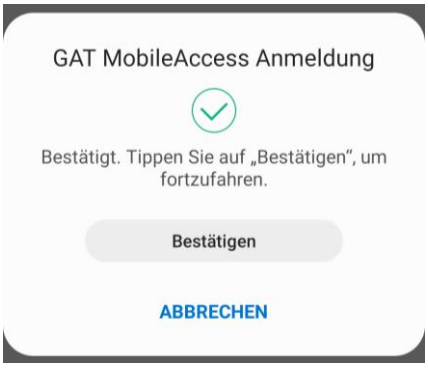


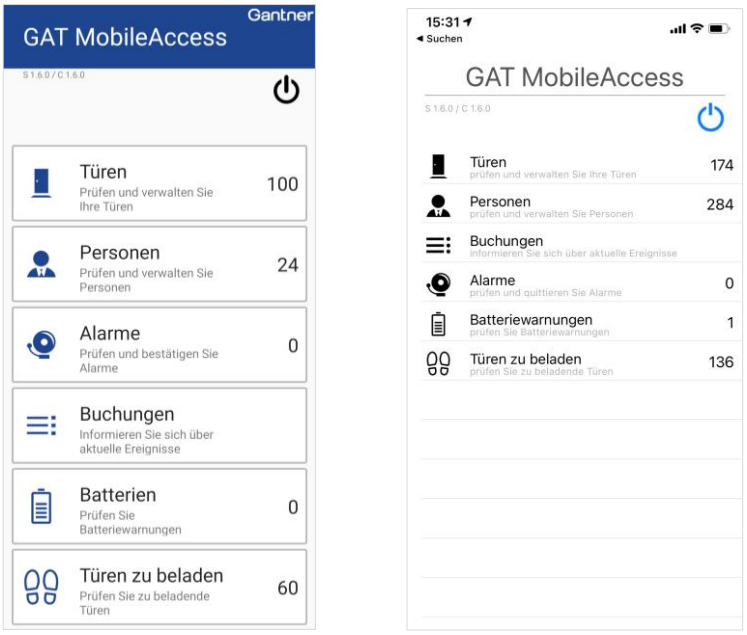
***Bild 5.4** - Biometrie-Erkennung erfolgreich*

- ► Klicken Sie auf "Bestätigen".
- ► Mit "ABBRECHEN" können Sie die Biometrie-Erkennung auch abbrechen und sich mit ihrem Benutzernamen und Passwort anmelden.

  - o Bei der ersten Benutzung der Biometrie-Erkennung ist noch einmal die Passworteingabe notwendig.
  - o Bei weiteren Logins werden Sie direkt nach erkanntem Fingerabdruck bzw. Gesicht, ohne Passworteingabe, in GAT Mobile Access angemeldet.

5.2 Funktionen

Nach dem Einloggen wird der Startbildschirm von GAT Mobile Access angezeigt.



Android iPhone

***Bild 5.5** - Startbildschirme von GAT Mobile Access auf den verschiedenen Betriebssystemen*

Für die Bedienung von GAT Mobile Access finden Sie im Startbildschirm mehrere Bereiche:

- Türen: Hier können Sie den Status jeder Tür anzeigen und die Tür steuern (sperren, öffnen, generell sperren oder öffnen).
- Personen: Personen bezeichnet hier die Benutzer der Zutrittsanlage. In diesem Bereich können Sie die den Personen zugewiesenen Datenträger anzeigen und sperren, die Personen blockieren oder freigeben sowie die Buchungen und Alarme der Personen anzeigen lassen.
- Alarme: In diesem Bereich können Sie die in der Zutrittsanlage aufgetretenen Alarme anzeigen, bearbeiten und löschen.
- Buchungen: Hier werden alle Buchungen, d.h. Aktionen wie Eintritte, Austritte und Zeitbuchungen an den Türcontrollern, die in der Zutrittsanlage aufgetreten sind, angezeigt. Bei jeder Buchung sehen Sie die Person, die die Buchung erstellt hat.
- Batterien: Hier sehen Sie Batteriewarnungen von Offline-Türen, bei denen der Ladestand der Batterien unter einen bestimmten Wert gefallen ist oder bei denen die Batterien ganz leer sind.
- Türen zu beladen: In diesem Bereich wird angezeigt, welche Offline-Türen noch beladen werden müssen.

► Zum Öffnen eines Bereichs klicken Sie im Startbildschirm auf den gewünschten Bereich.

► Ist einer der Bereiche Türen, Personen, Alarme oder Buchungen geöffnet, können Sie auf iPhone auch direkt zu einem anderen dieser Bereich wechseln. Klicken Sie dazu am unteren Rand des Arbeitsbereichs von GAT Mobile Access auf das Symbol des gewünschten Bereichs.

5.2.1 Bereich "Türen"

Dieser Bereich zeigt zunächst alle definierten und sichtbaren Türgruppen, so wie sie in Matrix definiert wurden, an.

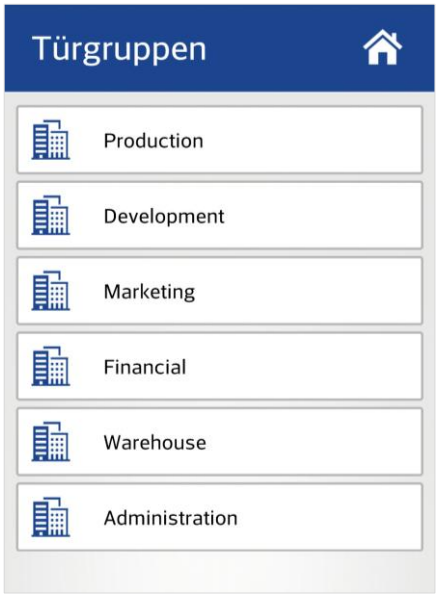


***Bild 5.6** - Türgruppen*

► Wählen sie eine Türgruppe.

- Es werden die in der Türgruppe enthaltenen Türen angezeigt.

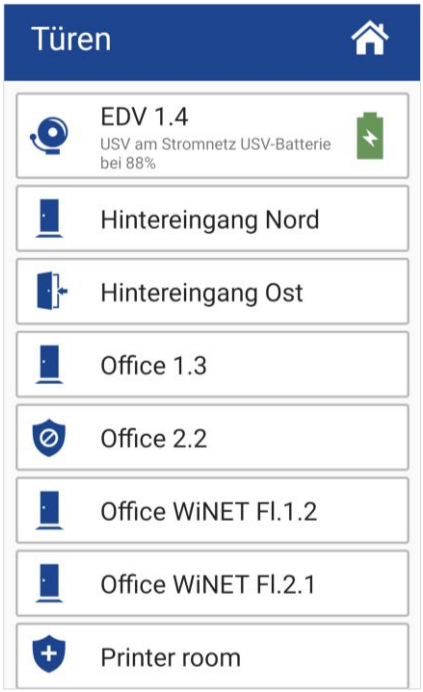


***Bild 5.7** - Türen in der gewählten Türgruppe*

- Sie sehen hier anhand der Icons vor den Türen den jeweils aktuellen Türstatus.
  - Türe ist offen/entriegelt.
  - Türe ist geschlossen/verriegelt.
  - Türe ist generell offen.
  - Türe ist generell versperrt.
  - An der Türe ist ein Alarm aufgetreten (siehe "5.2.3. Bereich "Alarme" ").
  - Für die Versorgung des Türcontrollers wird eine USV verwendet. Dieses Symbol mit Text "USV am Stromnetz" zeigt an, dass das Hauptstromnetz in Ordnung ist und die USV sowie der Türcontroller über das reguläre Stromnetz versorgt werden. Sie sehen auch die Ladung des Akkus der USV.
  - Für die Versorgung des Türcontrollers wird eine USV verwendet. Das Stromnetz zur Versorgung der USV ist ausgefallen und der Türcontroller wird aktuell von der USV versorgt. Die Ladung des Akkus der USV wird mittels Zahlenwert und Symbol angezeigt:
    - … Akku noch über 50% geladen
    - … Akku zwischen 50% und 20% geladen
    - … Akku unter 20% geladen

► Wählen Sie eine Tür.

- Die Türdetails der Tür werden angezeigt. Die Türdetails sind in die 3 Unterbereiche "Türsteuerung", "Alarme" und "Buchungen" unterteilt.

HINWEIS: Damit der Türstatus angezeigt werden kann, muss dies in Matrix bei der Türsteuerung aktiviert sein (Rechtsklick auf die Tür und Auswahl von "Türe editieren" -> Registerkarte "Datenpunkte" -> Einstellung "Türstatus anzeigen".

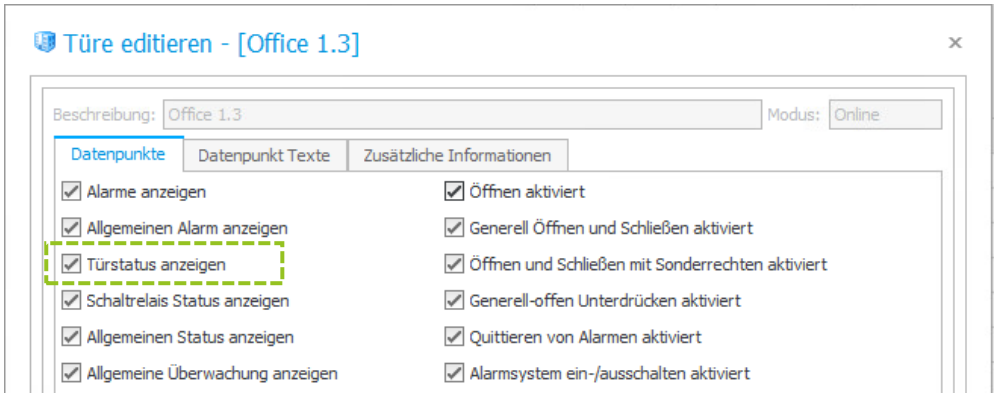


***Bild 5.8** - Türstatus in Matrix aktivieren*

Unterbereich "Türsteuerung"

In diesem Unterbereich sehen Sie den aktuellen Status der Türe und können verschiedene Steuerkommandos an die Türe verschicken.

HINWEIS: Abhängig von den in Matrix aktivierten Datenpunkte für die Tür werden hier unterschiedlich viele Optionen angezeigt. Die Datenpunkte sind rechts im Fenster "Tür editieren" aufgelistet. Zum Öffnen des Fensters klicnen Sie in Matrix mit rechter Maustaste auf die Tür, wählen Sie "Türe editieren" und hier die Registerkarte "Datenpunkte".

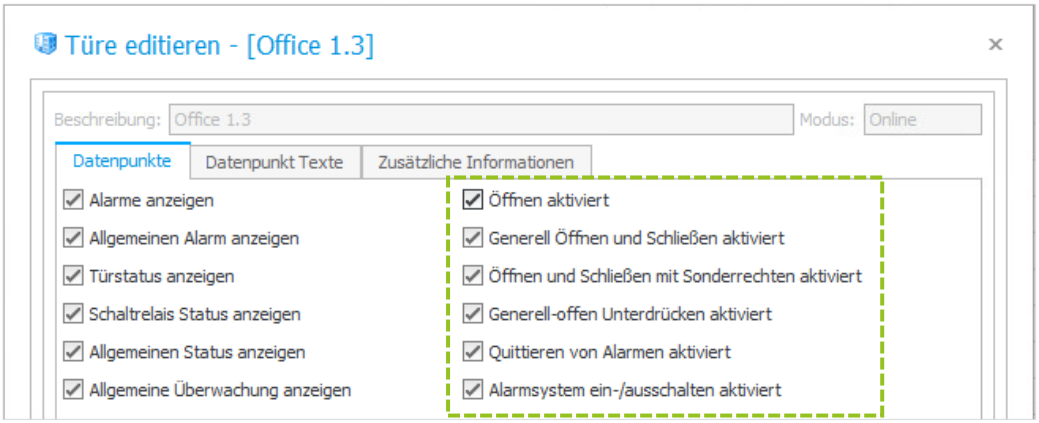
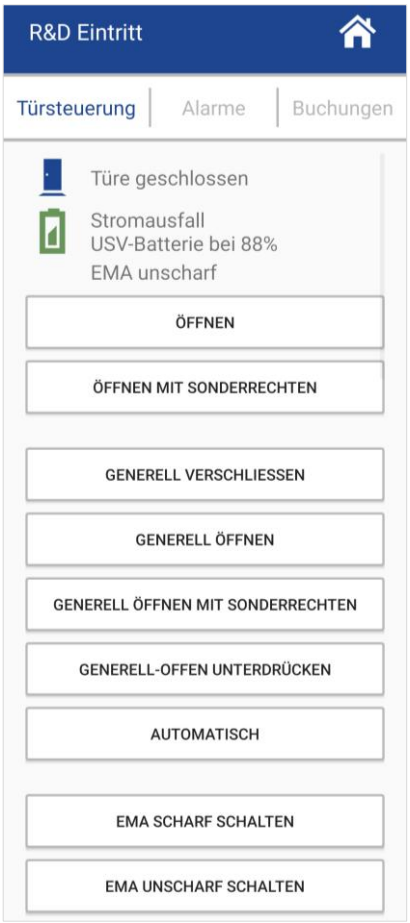


***Bild 5.9** – Datenpunkte für die Türsteueurng in Matrix aktivieren*

Folgendes Bild zeigt hinter allen möglichen Optionen zur Steuerung die dazu notwendigen Datenpunkte.



"Türstatus anzeigen" + "Öffnen aktiviert"

"Türstatus anzeigen" + "Öffnen und Schließen mit Sonderrechten aktiviert"

"Türstatus anzeigen" + "Generell Öffnen und Schließen aktiviert"

"Türstatus anzeigen" + "Generell Öffnen und Schließen aktiviert"

"Türstatus anzeigen" + "Generell Öffnen und Schließen aktiviert" + "Öffnen und Schließen mit Sonderrechten aktiviert"

"Türstatus anzeigen" + "Generell-offen Unterdrücken aktiviert"

"Türstatus anzeigen" + "Generell Öffnen und Schließen aktiviert"

"Schaltrelais Status anzeigen" + "Alarmsystem ein-/ausschalten aktiviert"

"Schaltrelais Status anzeigen" + "Alarmsystem ein-/ausschalten aktiviert"

***Bild 5.10** - Bereich "Türen" - Unterbereich "Türsteuerung"*

Der Türstatus wird im oberen Bereich mit Text und entsprechendem Symbol angezeigt. Hier sehen Sie auch, ob eine EMA (Überwachung durch Alarmanlage) aktiviert oder deaktiviert ist.
Außerdem wird hier der Status einer Notstromversorgung USV angezeigt, falls eine USV verwendet wird. Das Symbol zeigt Informationen über den Ladezustand der USV und ob das Stromnetz ausgefallen ist oder nicht:

Dieses Symbol mit Text "USV am Stromnetz" zeigt an, dass das Hauptstromnetz in Ordnung ist und die USV sowie der Türcontroller über das reguläre Stromnetz versorgt werden. Sie sehen auch die Ladung des Akkus der USV.

Das Stromnetz zur Versorgung der USV ist ausgefallen und der Türcontroller wird aktuell von der USV versorgt. Die Ladung des Akkus der USV wird mittels Zahlenwert und Symbol angezeigt:

… Akku noch über 50% geladen

… Akku zwischen 50% und 20% geladen

… Akku unter 20% geladen

Mit den Schaltflächen darunter können Sie die Türe steuern. Folgende Aktionen sind möglich:

- ÖFFNEN: Tür wird für die konfigurierte Entriegelungszeit geöffnet und danach wieder in den vorherigen Status zurückgesetzt (z. B. verschlossen oder generell offen/verschlossen).
- ÖFFNEN MIT SONDERRECHTEN: Tür wird für die konfigurierte Entriegelungszeit geöffnet und zusätzlich wird, falls definiert, das Relais mit der Funktion "Sonderrelais" mit angezogen. Dadurch kann z. B. ein Tor auf Autobreite statt nur auf Fußgängerbreite geöffnet werden.
- GENERELL VERSCHLIESSEN: Die Tür wird versperrt und kann auch mit gültigem Datenträger nicht geöffnet werden.
- GENERELL ÖFFNEN: Die Tür wird generell entriegelt und kann somit ohne Datenträger geöffnet werden (z. B. für Bürofunktion).
- GENERELL ÖFFNEN MIT SONDERRECHTEN: Die Tür wird generell entriegelt und das Relais mit der Funktion "Sonderrelais" wird zusätzlich angezogen.
- GENERELL-OFFEN UNTERDRÜCKEN: Diese Funktion unterdrückt die Generell-Offen und Generell Verschließen Funktion sowie den Generell-Offen Zeitplan an der Tür. Es gelten also nur die Personalzeitpläne und die Tür kann laut den hinterlegten Berechtigungsplänen ent- und verriegelt werden.
- AUTOMATISCH: Die Tür wird von generell verschlossen oder generell geöffnet auf den "normalen" Betriebsmodus zurückgesetzt, in dem die Entriegelungsentscheidung anhand der hinterlegten Zeitpläne und Personaldaten erfolgt.
- EMA SCHARF / UNSCHARF SCHALTEN: Mit diesen beiden Funktionen kann die Alarmanlage scharf oder unscharf geschaltet werden.

HINWEIS! Einige Funktionen sind nur wählbar, wenn die "Erweiterte Türsteuerung" in den Einstellungen (siehe "4.5. Konfiguration der GAT Mobile Access App") aktiviert ist.

Unterbereich "Alarme"

Hier sehen Sie alle aktuellen Alarme zu der Türe:

***Bild 5.11** - Bereich "Türen" - Unterbereich "Alarme"*

► Drücken Sie auf einen Alarm, um die Alarmdetails aufzurufen.
  - Sie gelangen in die Alarmanzeige. Nähere Informationen dazu siehe "5.2.3. Bereich "Alarme"".

Unterbereich "Buchungen"

Hier sehen Sie die letzten 5 Buchungen zu dieser Türe im konfigurierten Zeitraum.

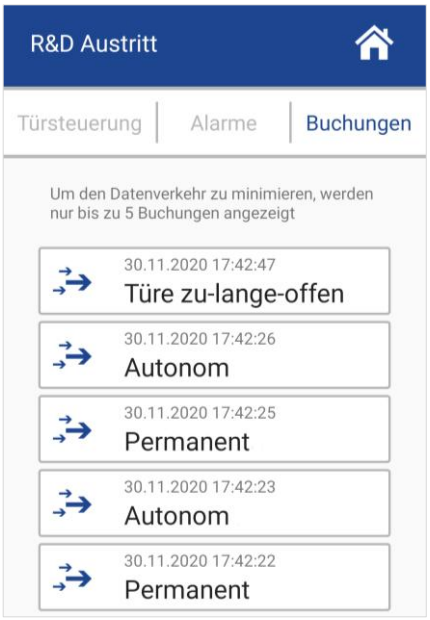


***Bild 5.12** - Bereich "Türen" - Unterbereich "Buchungen"*

► Drücken Sie auf eine Buchung um die Buchungsdetails anzuzeigen.
  - Sie gelangen in die Buchungsanzeige. Nähere Informationen dazu siehe "5.2.4. Bereich "Buchungen"".

5.2.2 Bereich "Personen"

Dieser Bereich zeigt zunächst alle definierten und sichtbaren Personengruppen, so wie sie in der Matrix definiert wurden, an.

***Bild 5.13** – Personengruppen*

► Wählen sie eine Personengruppe.

- Es werden die in der Personengruppe enthaltenen Personen angezeigt.

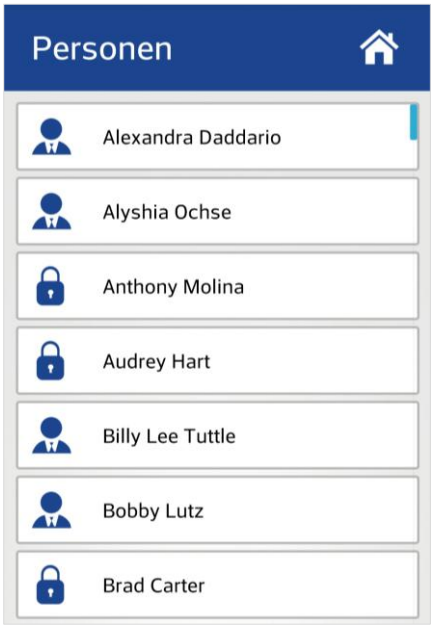


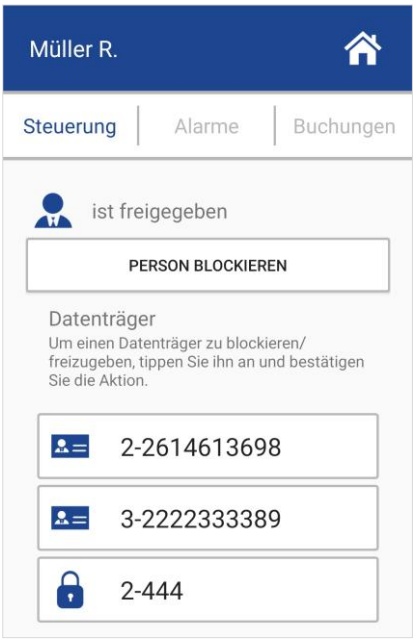
***Bild 5.14** - Person in einer Personenengruppe*

- Sie sehen hier anhand der Icons vor den Personen den jeweils aktuellen Status der Person.
  Person ist freigegeben und hat somit Zutrittsberechtigung entsprechend ihrer Berechtigungseinstellungen.
  Person ist blockiert und hat somit keine Zutrittsberechtigung.

► Wählen Sie eine Person.
- Die Personendetails der Person werden angezeigt. Die Personendetails sind in die 3 Unterbereiche "Steuerung", "Alarme" und "Buchungen" unterteilt.

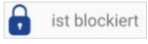
Unterbereich "Steuerung"

In diesem Unterbereich sehen Sie den aktuellen Status der Person und können die Person und die zugewiesenen Datenträger der Person blockieren oder freigeben.

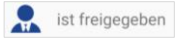


Der Personalstatus zeigt an, ob die Person freigegeben oder blockiert ist. Freigegeben bedeutet, dass die Person laut den für sie definierten Berechtigungsdaten und den Türkonfigurationen und Zeitplänen zutrittsberechtigt ist. Blockiert bedeutet, dass die Person an keiner Tür der Anlage zutrittsberechtigt ist. Diese Informationen werden im oberen Bereich mit entsprechendem Text und Symbol angezeigt.

***Bild 5.15** - Bereich "Personen" - Unterbereich "Steuerung"*

► Wollen Sie eine freigegebene Person blockieren, berühren Sie die Schaltfläche "PERSON BLOCKIEREN".
- Das Symbol der Person mit Text ändert sich zu 

.

► Wollen Sie eine blockierte Person freigeben, drücken Sie die Schaltfläche "PERSON FREIGEBEN".
- Das Symbol der Person mit Text ändert sich zu 

.

Nach dem Auswählen einer der beiden Funktionen wird ein Löschkommando an die GAT ACE Software gesendet, das die entsprechenden Daten in allen Türcontrollern aktualisiert. Bitte beachten Sie, dass das einige Zeit in Anspruch nehmen kann und bei Offline-Türen eine Vor-Ort-Beladung der Türe erfordern machen kann.

HINWEIS! Ab Matrix Version 7.1.2 und GAT ACE 7 wird die Aktualisierung der Türcontroller autmoatisch im Hintergrund durchgeführt. Bei älteren Matrix Versionen ist eine manuelle Beladung der Controller notwendig.

HINWEIS! Beim Personenimport in Matrix werden die Türcontroller ebenfalls neu beladen. Deshalb kann das manuelle Beladen eventuell entfallen, wenn Sie z. B. einen regelmäßigen, automatischen Personenimport in kurzen Zeitabständen eingestellt haben.

- ► Mit der aktuellsten App und Matrix Version werden die Personen-Änderungen live angezeigt. Bei älteren Versionen vor App Version 1.7.1 und Matrix Version 7.1.2 war es oft nötig, die Ansicht der Matrix durch Drücken von F5 zu aktualisieren um die Änderung anzuzeigen.
- ► Um einen Datenträger der Person zu blockieren oder freizugeben klicken Sie auf den gewünschten Datenträger. Die Symbole zeigen an, welche Datenträger blockiert oder freigegeben sind. Ein blockierter Datenträger hat keine Zutrittsberechtigung mehr.

… freigegebener Datenträger

… blockierter Datenträger

Unterbereich "Alarme"

Hier sehen Sie alle aktuellen Alarme, die eine Person betreffen. Ein typischer Alarm kann z. B. auftreten, wenn die Person die Tür nach einer gültigen Entriegelung mit ihrem Datenträger länger als die definierte max. Türoffenzeit geöffnet hält.

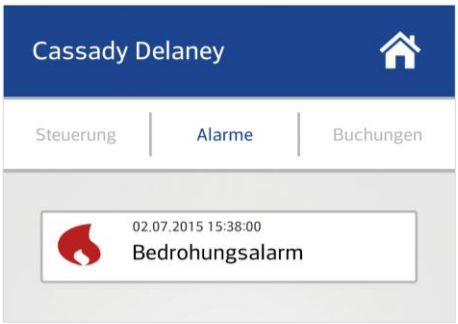


***Bild 5.16** - Bereich "Personen" - Unterbereich "Alarme"*

- ► Drücken Sie auf einen Alarm, um die Alarmdetails aufzurufen.
  - o Sie gelangen in die Alarmanzeige. Nähere Informationen dazu siehe "5.2.3. Bereich "Alarme"".

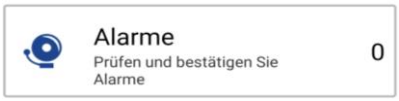
Unterbereich "Buchungen"

Hier sehen Sie die letzten 5 Buchungen zu der aktuellen Person im konfigurierten Zeitraum.

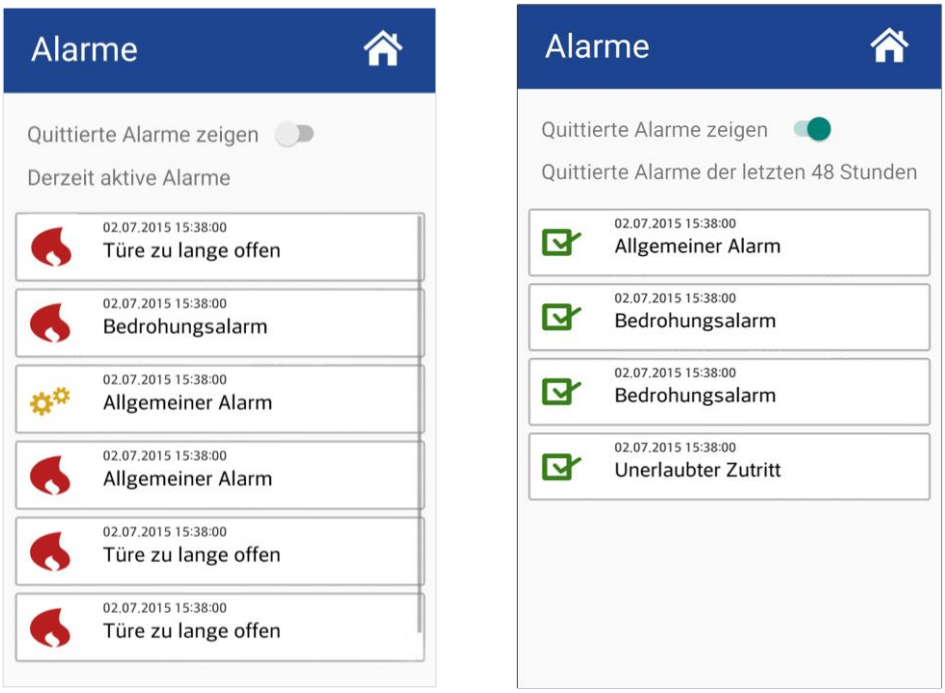
***Bild 5.17** - Bereich "Personen" - Unterbereich "Buchungen"*

► Drücken Sie auf eine Buchung um die Buchungsdetails anzuzeigen.
  - Sie gelangen in die Buchungsanzeige. Nähere Informationen dazu siehe "5.2.4. Bereich "Buchungen"".

5.2.3 Bereich "Alarme"



Dieser Bereich zeigt alle Alarme, die in der Zutrittskontrollanlage aufgetreten sind. Es kann zwischen einer Ansicht aller aktiven Alarme und der bereits quittierter Alarme umgeschaltet werden.



Aktive Alarme **bereits quittierte Alarme**

***Bild 5.18** - Anzeige der aufgetretenen Alarme in der Zutrittskontrollanlage*

- ► Wählen Sie das Feld neben "Quittierte Alarme zeigen".
  - Das Feld wechselt bei jeder Auswahl den Zustand zwischen "Aus" und "Ein".
  - Ist das Feld auf "Aus", werden nur die aktiven Alarme aufgelistet. Alarme, die noch aktiv aber gerade in Bearbeitung sind, werden mit dem Symbol dargestellt.
  - Ist das Feld auf "Ein" werden nur die bereits quittierten Alarme im konfigurierten Zeitraum (siehe "4.3. Konfiguration der GAT Mobile Access App4.5") aufgelistet.
- ► Wählen Sie einen Alarm aus.
  - Eine Detailansicht des Alarms wird angezeigt.

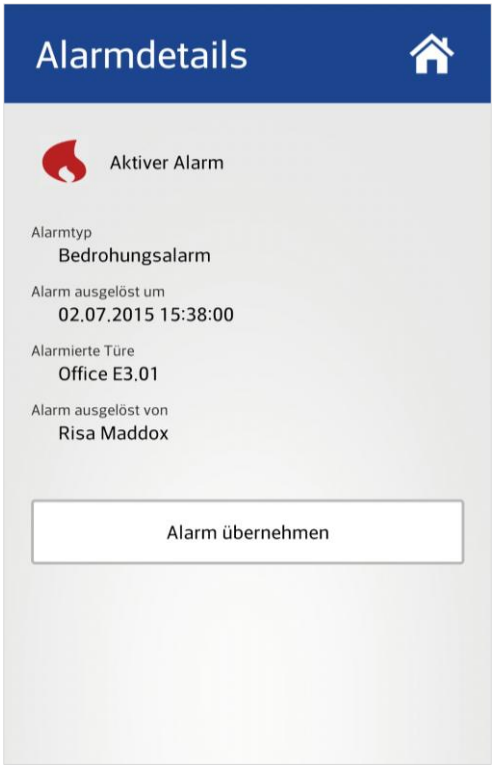


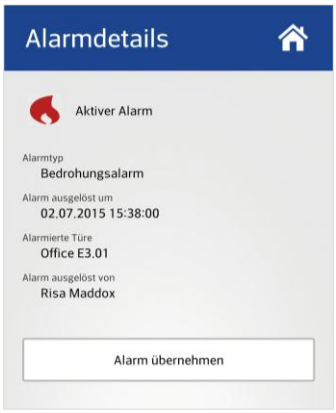
***Bild 5.19** - Alarmdetails eines aktiven Alarms*

- In dieser Ansicht sehen Sie folgende Details für den Alarm:
  - Alarmstatus: "Aktiver Alarm", "In Bearbeitung", "Quittiert"
  - Alarmtyp: Hier wird der Typ des Alarms angezeigt. Es sind verschiedene Alarme möglich.
    - Türe zu lange offen: Dieser Alarm wird ausgelöst, wenn die Türe nach gültiger Entriegelung länger als die definierte max. Türoffenzeit geöffnet bleibt.
    - Bedrohungsalarm: Wird durch Eingabe eines Bedrohungs-PIN-Codes ausgelöst.
    - Allgemeiner Alarm: Dieser Alarm wird bei der Aktivierung des Relais mit der Einstellung "Allgemeiner Alarm" ausgelöst.
    - Zutritt ohne Berechtigung: Die Türe wurde ohne Berechtigung geöffnet. Das kann z. B. auf einen Einbruch hinweisen.
  - Alarm ausgelöst um: Datum und Uhrzeit, an dem der Alarm ausgelöst wurde.
  - Alarmierte Türe: Name der Tür, an dem der Alarm ausgelöst wurde.
  - Alarm ausgelöst von: Name der Person, die den Alarm ausgelöst hat.

Alarme quittieren

Das Quittieren eines Alarms erfolgt in folgenden 3 Schritten. Der jeweilige Schritt wird als Statusinformation bei jedem Alarm angezeigt.

1. Aktiver Alarm:

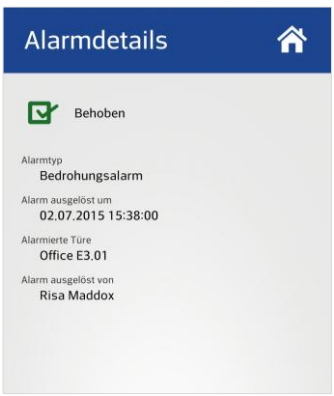


Der Alarm ist neu aufgetreten und wurde noch nicht bearbeitet. Ein zuständiger Benutzer muss sich darum kümmern, dass die Ursache des Alarms behoben wird. Dazu muss der Benutzer in den Alarmdetails die Schaltfläche "Alarm übernehmen" wählen. Dadurch wechselt der Alarmstatus zu "In Bearbeitung".

2. In Bearbeitung:

Der Alarm ist gerade von einem Benutzer in Bearbeitung. Das bedeutet, der Benutzer muss sich darum kümmern, dass die Ursache des Alarms behoben wird und eventuell notwendige, weitere Maßnahmen durchgeführt werden, damit der Alarm nicht wieder auftritt. Ist dies erledigt, wählt der Benutzer die Schaltfläche "Alarm quittieren".

3. Quittiert:



Der Alarm wurde bearbeitet und die Ursache des Alarms ist behoben worden. Quittierte Alarme werden in einer separaten Ansicht in der Alarmanzeige dargestellt und können für die in den Einstellungen (siehe "4.5. Konfiguration der GAT Mobile Access App") definierte Zeit noch weiters wieder angezeigt werden.

5.2.4 Bereich "Buchungen"

Dieser Bereich zeigt alle Buchungen an, die während dem in den App-Einstellungen konfigurierten Zeitraum erstellt wurden. Die Anzeige ist auf mehrere Seiten aufgeteilt und die Anzahl der Buchungen, die pro Seite angezeigt werden, kann ebenfalls in den App-Einstellungen defniert werden (siehe "4.5. Konfiguration der GAT Mobile Access App").

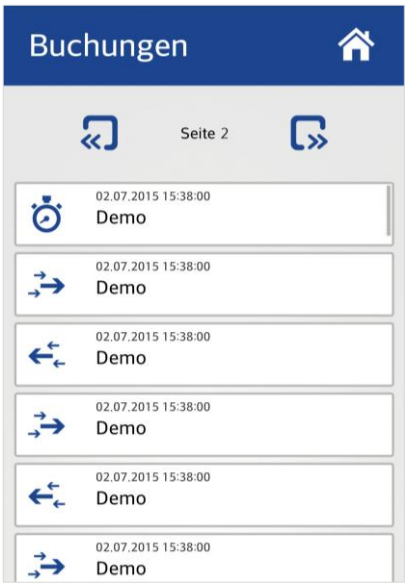


***Bild 5.20** - Buchungsanzeige*

- ► Mit den Symbolen « und » können Sie in den Seiten der Buchungsanzeige blättern.
- ► Wählen Sie eine Buchung aus, um die Details der Buchung anzuzeigen.
  - ○ Die Buchungsdetails werden geöffnet.

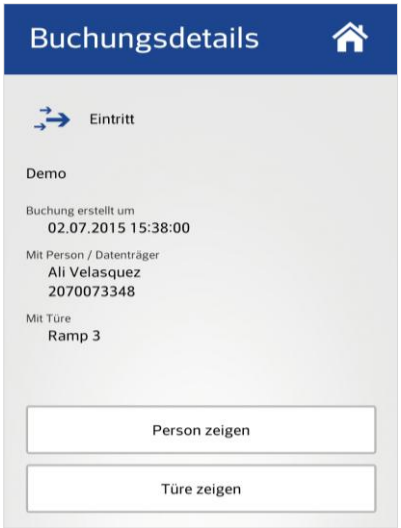


***Bild 5.21** - Buchungsdetails*

- In dieser Ansicht sehen Sie folgende Details für die geöffnete Buchung:
  - Buchungstyp: In der ersten Zeile sehen Sie den Typ der Buchung. Der Typ wird mittels Symbol und Text angezeigt.
    - Eintritt: Diese Buchung zeigt einen durchgeführten Eintritt einer Person an einem Türcontroller.
    - Austritt: Diese Buchung zeigt einen durchgeführten Austritt einer Person an einem Türcontroller.
    - Zeitbuchung: Diese Buchung zeigt eine durchgeführte Zeitbuchung an einem Zeiterfassungsterminal.
  - Buchung erstellt um: Datum und Uhrzeit, an dem die Buchung im Türcontroller erstellt wurde.
  - Mit Person / Datenträger: Name der Person, die die Buchung erstellt hat. Außerdem wird auch die Nummer des Datenträgers angezeigt, mit dem die Buchung erstellt wurde.
  - Mit Türe: Name der Türe, an dem die Buchung erstellt wurde.

► Wählen Sie die Schaltfläche "Person zeigen", um die Person, die die Buchung erstellt hat, anzuzeigen.

- Die Anzeige ändert sich und es wird die Detailansicht der Person angezeigt.

► Wählen Sie die Schaltfläche "Türe zeigen", um die Tür, an der die Buchung erstellt wurde, anzuzeigen.

- Die Anzeige ändert sich und es wird die Detailansicht der Tür angezeigt.

5.2.5 Bereich "Batterien"

Hier werden die Batteriewarnungen angezeigt, die von Offline-Türen (Schlössern) erzeugt werden. Die Anzahl der aktuellen Batteriewarnungen wird im Feld "Batterien" angezeigt.

Die Batteriewarnungen werden über Datenträger, ein Transportgerät oder über eine Funkschnittstelle übertragen und die Batteriewarnungen zeigen deshalb nicht immer den gerade aktuellen Stand sondern den Stand bei der letzten Auslesung. Wechseln Sie deshalb die Batterien früh genug, so dass die betreffenden Schlösser noch bedient werden können.

► Wählen Sie im Startbildschirm den Bereich "Batterien".
  - Die gerade aktiven Batteriewarnungen werden mit dem Namen des betreffenden Schlosses und einem Symbol angezeigt.

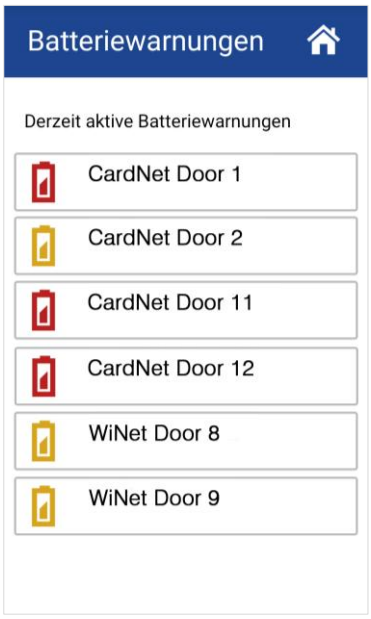


***Bild 5.22** - Batteriewarnungen*

  - Es werden 2 verschiedene Symbole für die Anzeige der Batteriewarnungen verwendet:
    - Batterieladung niedrig: Das Offline-Schloss ist noch einsatzbereit, aber die Batterie ist fast leer und muss getauscht werden.
    - Batterie ist leer: Die Batterie ist leer und muss getauscht werden. Das Offline-Schloss ist nicht mehr einsatzbereit.

► Um Details zu einer Batteriewarnung zu erhalten klicken Sie auf die Warnung.
  - Es wird ein Fenster mit Details zu der Batteriewarnung angezeigt.

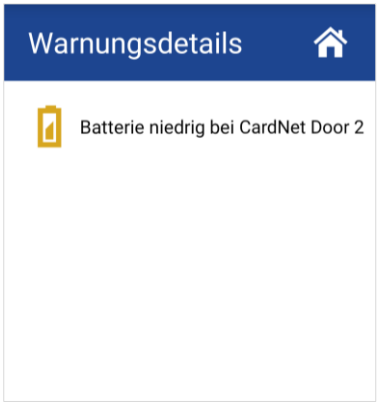


***Bild 5.23** - Details einer Batteriewarnung*

► Führen sie an den angezeigten Offline-Türen ein Batterietausch laut der Beschreibung der dort verwendeten Offline-Schlösser durch. Dieser Prozess umfasst im Regelfall folgende Schritte:

1. Alte Batterie gegen eine neue, voll geladene Batterie tauschen.
2. Offline-Schloss mit der zugehörigen Batteriekarte zurücksetzen (=Batteriewarnung löschen).
3. Offline-Schloss neu beladen.
4. Das Transportgerät für die Offline-Konfigurationen mit dem PC bzw. mit GAT Mobile Access Management synchronisieren.

Erst nach Schritt 4 verschwinden auch die Batteriewarnungen in der App.

5.2.6 Bereich "Türen zu beladen"

In diesem Bereich sehen Sie die Offline-Türen, die noch beladen werden müssen, z. B. weil die Konfiguration oder Berechtigungseinstellungen für diese Türen in Matrix geändert wurden. Die Anzahl der noch nicht beladenen Offline-Türen wird im Feld "Türen zu beladen" angezeigt.

Beachten Sie, dass erst nach dem Beladen der Offline-Türen mit einem Programmiergerät oder über Funk, die Konfigurationen in den Türen/Schlössern aktuell sind und somit die gewünschte Funktion aktiv ist.

► Wählen Sie im Startbildschirm den Bereich "Türen zu beladen".

- Alle noch nicht beladenen Türen werden angezeigt.

***Bild 5.24** – Offline-Türen, die noch beladen werden müssen.*

- ► Wählen Sie eine Offline-Tür aus, um Details anzuzeigen.
  - o Die Beladedetails (z. B. die Adresse der Offline-Tür) werden angezeigt.

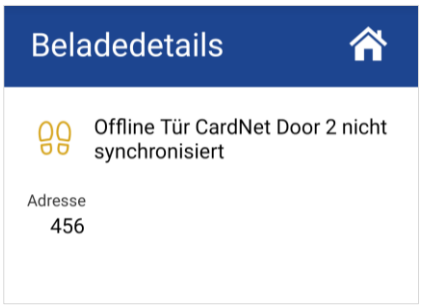
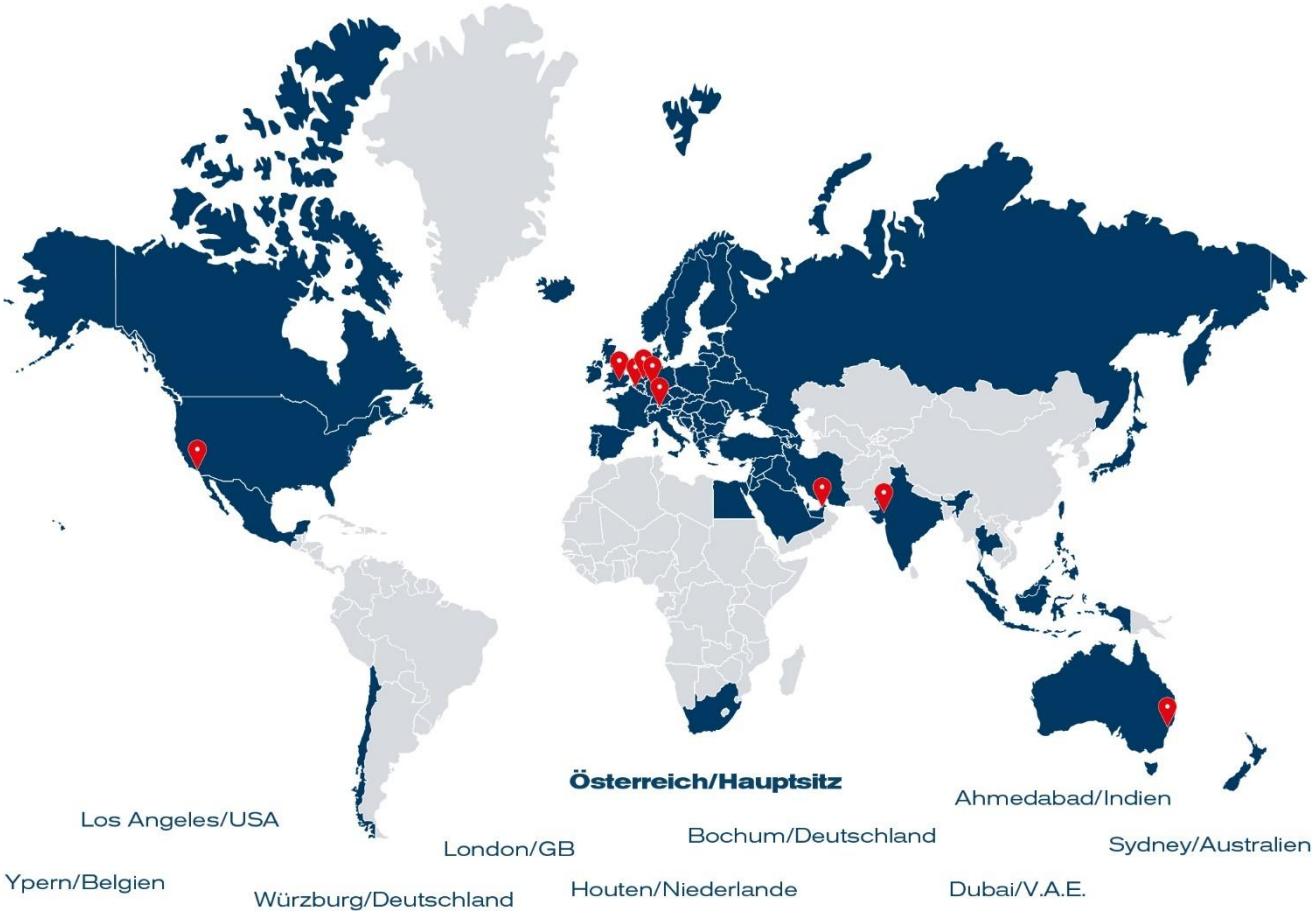


***Bild 5.25** – Details über eine zu beladende Offline-Tür*

- ► Beladen Sie Die angezeigten Offline Türen je nach Typ mit dem Programmiergerät oder über Funk.
- ► Nach Beladen mit einem Programmiergerät synchronisieren Sie dieses nocheinmal mit dem PC bzw. GAT Mobile Access Management. Erst durch diesen Schritt verschwinden die Beladeмarkierungen in der App.

Hinweis:
Dieses Handbuch ist gültig ab 17. März 2026. Änderungen und Ergänzungen dieses Handbuchs sind jederzeit ohne Vorankündigung möglich!
Informationen in diesem Handbuch beziehen sich auf die GAT Mobile Access Management Version 1.7.1 oder neuer.



Gantner ist in über 60 Ländern weltweit tätig. **Besuchen Sie uns unter: www.gantner.com**

Nüziders, Österreich
info@gantner.com

Houten, Niederlande
info@gantner.nl

Sydney, Australien
info-aus@gantner.com

London, GB
info-uk@gantner.com

Bochum, Deutschland
info-de@gantner.com

Los Angeles, USA
info-us@gantner.com

Ypern, Belgien
info@gantner.be

Dubai, Mittler Osten
info-me@gantner.com

Ahmedabad, Indien
info@gantnerticketing.com

Aktuelle Kontaktdaten: www.gantner.com/locations

Artikel-Nr.: 534828