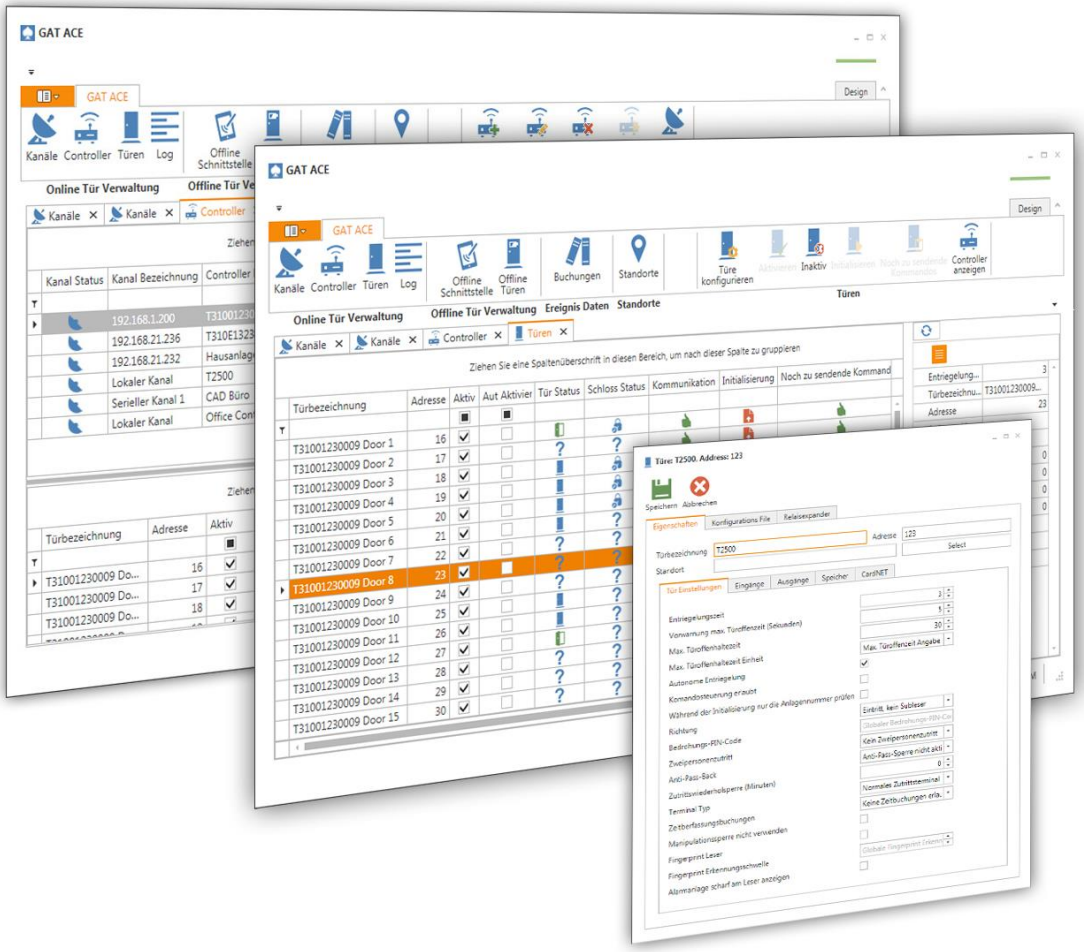
Gantner

GAT ACE 3000

Middleware für Zutrittskontrolle von GANTNER Electronic GmbH



Installation, Konfiguration, Bedienung
Dokumentversion 3.0.1
Softwareversion 3.0.0

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 der GAT ACE Software 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 unseres Produkts. Wir würden uns freuen, Sie alsbald wieder als Kunden begrüßen zu dürfen.

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Zu diesem Handbuch

Kapitel "1. EINLEITUNG" in diesem Handbuch enthält einen Überblick über die GAT ACE Software und beschreibt die wichtigsten Merkmale. Außerdem finden Sie hier eine Begriffsdefinition über die wichtigsten, in diesem Handbuch verwendeten Begriffe.

Kapitel "2. INSTALLATION" beschreibt die Systemanforderungen für die GAT ACE Software und die Konfiguration der Datenbank und zeigt einen Überblick über die Installationsvarianten. Danach wird im Detail die Installation von GAT ACE und der weiteren erforderlichen Komponenten wie das .NET Framework und die Datenbank beschrieben.

Kapitel "3. GAT ACE 3000 STARTEN" beschreibt den ersten Start von GAT ACE und die dabei notwendigen Einstellungen, die einmal durchgeführt werden müssen (z. B. für die Datenbankverbindung). Außerdem wird hier auch beschrieben, wie eine ältere Datenbank von einer bestehenden Zutrittsanlage mit GAT Manager in GAT ACE importiert werden kann.

Kapitel "4. KONFIGURATION" beschreibt die allgemeinen Konfigurationseinstellungen für GAT ACE wie z. B. die Datenbankkonfiguration, Definition der gültigen Ausweise oder Lizenz- und Rollendefinitionen. Diese müssen normalerweise nur einmal nach Installation von GAT ACE definiert werden, können aber auch nachträglich geändert werden.

Kapitel "5. BEDIENUNG" beschreibt den Aufbau und Anwendung der Benutzeroberfläche von GAT ACE und die wichtigsten, grundsätzlichen Schritte zur Konfiguration einer Zutrittskontrollanlage. Dieses Kapitel enthält außerdem eine detaillierte Beschreibung aller Funktionen von GAT ACE.

Kapitel "6. BERECHTIGUNGS-MANAGEMENT" beschreibt das Berechtigungsmanagement in GAT ACE. Es können verschiedene Benutzer mit verschiedenen Rechten in GAT ACE angelegt werden. Zum Beispiel kann einer Person die Rolle des Administrator (der alle Einstellungen und Funktionen in GAT ACE verwenden kann) und anderen Angestellten die Rolle der "Täglichen Benutzer" (die nur die für sie wichtigen Funktionen von GAT ACE verwenden aber nicht die Konfiguration ändern können) zugewiesen werden.

In Kapitel "7. UMSTIEG VON GAT MANAGER AUF GAT ACE" wird das Lizenzverfahren (Aktivierung/Lizensierung von GAT ACE) beschrieben.

Kapitel "8. DATENSCHUTZ" informiert Sie über die neue EU-Datenschutz-Grundverordnung und wie GAT ACE 3000 dabei unterstütz, die Vorgaben einzuhalten.

1.2 Formatierungen

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.

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.

1.3 Allgemeine Informationen

GAT ACE ist eine Middleware zur Konfiguration einer Zutrittskontrollanlage mit Controllern und Peripheriegeräten von GANTNER Electronic GmbH. Sie dient als Schnittstelle zur Verwendung der Controller mit anderen Softwarepaketen und regelt die gesamte Kommunikation zwischen den Controllern und der übergeordneten Software. GAT ACE läuft auf Microsoft Windows® Betriebssystemen (siehe "2.2.1 Unterstützte Betriebssysteme für GAT ACE").

In GAT ACE wird die Struktur der Zutrittskontrollanlage definiert. Dazu zählen die Einstellungen, Konfigurationen, Adressen und Kommunikationsparameter der einzelnen Controller. Außerdem bietet GAT ACE auch eine Möglichkeit zur Auswertung der Buchungen an den Controllern sowie der Ansicht der Kommunikations-Logdateien.

GAT ACE 3000 besteht aus einem Windows-Dienst, der im Hintergrund läuft und die gesamte Kommunikation regelt, und einer grafischen Benutzeroberfläche für die einfache Konfiguration und Steuerung des Dienstes. Da die Arbeit für die Benutzer normalerweise immer in der grafischen Benutzeroberfläche erfolgt, wird die Bezeichnung "GAT ACE" in dieser Anleitung allgemein für die Benutzeroberfläche der GAT ACE 3000 Software verwendet.

Die Vergabe und Verwaltung der Zutrittsberechtigungen an Personen bzw. Datenträgern erfolgt durch eine übergeordnete Zutrittskontrollsoftware, die nicht Teil von GAT ACE ist. Hier bietet GANTNER Electronic GmbH GAT Matrix als ideale Kombination mit GAT ACE an. Außerdem sind auch Gebäudeleitstände und -überwachungssysteme mit GAT ACE verwendbar.

Es ist entweder möglich GAT ACE auf demselben Computer wie GAT Matrix oder eine andere Zutrittskontrollsoftware zu installieren oder, wenn mehrere GAT Matrix Installationen verwendet werden, kann GAT ACE auch auf einem Server installiert werden und alle GAT Matrix Installationen (Clients), die sich auf anderen Computern befinden, greifen auf dieselben Informationen bzw. Datenbank von GAT ACE zu (siehe Kapitel 2.3.2. Installation der GAT ACE).

1.4 Merkmale von GAT ACE 3000

- Mehrsprachigkeit (deutsch, englisch)
- Läuft auf allen modernen Windows Betriebssystemen (32- und 64-Bit)
- Kommunikationskanäle nur durch die Hardware limitiert
- Kommunikation über TCP/IP und RS-485
- Insgesamt 999 Geräte pro System
- Hardware Konfiguration der Controller
    - Funktion der Controllereingänge
    - Funktion der Controllerausgänge
    - Konfiguration angeschlossener Peripherie-Geräte
    - Einstellung der Leser
- Schnittstelle zu GAT Matrix und anderen Zutrittsmanagementsystemen
- Sehr schnelle Kommunikation zu den Controllern (Parallelisierung) und der Managementsoftware
- Dienst läuft ohne Benutzeranmeldung
- Erkennung der Bewegungsrichtung
- Spezialfunktionen (Anti Pass Back Funktion, Zutrittswiederholsperre, Zweipersonenzutritt, etc.)
- Bedrohungs-PIN-Code
- Controller-Initialisierung
- Setzen von Controller-Adressen
- Speicheraufteilung
- Unterstützt sowohl Online als auch Offline-Controller
- Zutritts- und Zeitbuchungen lesen
- Direkte Controller-Steuerung mittels Kommandos
- Protokollierung von Ereignissen und Kommunikation

1.5 Unterstützte Geräte

Die Geräte, die mit GAT ACE verbunden und konfiguriert werden sollen, müssen das FLEX-Protokoll von GANTNER Electronic GmbH unterstützen. Es ist möglich, sowohl Online- als auch Offline-Terminals zu verwenden.

Aktuell unterstützt GAT ACE die folgenden Geräte von GANTNER Electronic GmbH:

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

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

Die Unterstützung der Geräte wurde jeweils mit der letzten Firmware-Version der Geräte geprüft. Ältere Firmwarestände der Geräte müssen unter Umständen aktualisiert werden, damit das Zusammenspiel zwischen GAT ACE und den Geräten möglich ist.

Die Datenübertragung an Offline Geräte kann mit folgenden Geräten erfolgen. Teilweise ist dazu noch zusätzlich die PC-Software GAT Config Manager oder einSD Kartenleser erforderlich.

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

Aktuell unterstützt GAT ACE mit Einschränkungen die folgenden Geräte von GANTNER Electronic GmbH:

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

1.6 Begriffsdefinitionen

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

Zutrittskontrollsoftware
Damit wird in diesem Handbuch eine GAT ACE übergeordnete Software für die Vergabe und Verwaltung der Personenberechtigungen bezeichnet. GANTNER Electronic GmbH bietet z. B. das GAT Matrix Softwarepaket für diesen Zweck an.

Benutzer
Der Begriff "Benutzer" bezeichnet in diesem Handbuch die Person, die GAT ACE 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. GAT 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).

Controller / Terminal
Die Begriffe Controller und Terminal sind in dieser Anleitung gleichbedeutend und bezeichnen 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 Controller mit integrierten oder abgesetzten Lesern verfügbar. Controller werden in GAT ACE konfiguriert und verwaltet.
Es ist zwischen Online- und Offline-Controllern zu unterscheiden. Online-Controller besitzen eine Netzwerkschnittstelle, über die sie an ein lokales Netzwerk angeschlossen sind. Dabei ist je nach Controllertyp sowohl ein LAN-Netzwerk (Ethernet) als auch ein serielles RS 485 Netzwerk möglich. Mit Online-Controllern ist eine direkte Verbindung möglich was eine direkte Konfiguration sowie eine aktuelle Statusanzeige ermöglicht.
Offline-Controller haben keine Netzwerkschnittstelle und die Konfiguration und Kommunikation mit diesen Controllern erfolgt hier vor Ort durch ein Programmiergerät oder mittels entsprechenden Datenträgern oder auch über Funk.

Ein-/Ausgänge
Die meisten Controller besitzt ein oder mehrere digitale Optokopplereingänge zur Statuserkennung und Relaisausgänge, um Einrichtungen wie das Entriegelungsrelais einer Tür zu schalten. Die Funktion dieser Ein- und Ausgänge kann bei der Controllerkonfiguration genau festgelegt werden.

Tür
Der Begriff Tür wird in diesem Handbuch allgemein für das zu kontrollierende Objekt verwendet. Meistens handelt es sich dabei um die Tür zu einem Raum, dessen Zutritt überwacht werden soll. Es ist aber auch möglich anstelle der Tür z. B. ein Rolltor oder eine Schrankenzufahrt zu kontrollieren und überwachen. Das Prinzip der Zutrittskontrolle, d.h. die Konfiguration in GAT ACE ist aber jeweils identisch.
Es ist zu beachten, dass eine Türe nicht mit einem Controller gleichzusetzen ist, da ein Controller je nach Typ z. B. auch mehrere Türen kontrollieren kann.

Leser
An jedem Controller sind ein oder mehrere Leser angeschlossen oder fix eingebaut. An den Lesern erfolgt die Identifikation mittels Datenträger statt und die gelesenen Daten werden an den Controller übertragen, wo die Auswertung erfolgt. Außerdem können je nach Ausführung auch Datenträger an Lesern beschrieben werden.
Es gibt die verschiedensten Ausführungsvarianten von Lesern, z. B. abgesetzte Leseeinheiten die mittels Leser- oder RS-485 Schnittstelle mit dem Controller verbunden sind oder auch in den Controllern integrierte Lesereinheiten, wo also die Identifikation direkt am Controller erfolgt. Weiter wird zwischen Lesern für den Nahbereich oder Weitbereichsleser, mit denen die Identifikation im Abstand von einigen Metern möglich ist, unterschieden.

Kanal
GAT ACE kommuniziert mit den Controllern über sogenannte Kanäle. Für jede Schnittstellenverbindung wird ein Kanal definiert. So ist z. B. bei einer TCP/IP Verbindung jeder Controller (jede IP-Adresse) über einen eigenen Kanal mit einstellbaren Parametern verbunden. Bei einer seriellen RS 485 Verbindung können an einer Schnittstelle (einem Kanal) mehrere Controller angeschlossen sein, die dann dieselben Kommunikationsparameter verwenden.

CardNET
Dieser Begriff bezeichnet eine Betriebsart bei Offline-Controllern.
CardNET bedeutet, dass für die Konfiguration der Terminals ein Programmiergerät verwendet wird, um die Controller vor Ort zu konfigurieren. Die Berechtigungen der Personen werden mit den Ausweisen übertragen.
Die Berechtigungsdaten der Personen für Offline Türen (Controller) können von der Zutrittskontrollsoftware (z. B. GAT Matrix) an bestimmte Controller in der Zutrittsanlage gesendet werden. An diesen Controllern können dann die Datenträger der Personen direkt programmiert werden. Die Controller müssen die Schreib-/Lesefunktion (Read/Write oder CardNET Funktion) unterstützen. Die Datenträger müssen dafür geeignet und vorbereitet sein.

WiNET
Dieser Begriff bezeichnet eine Betriebsart bei Offline-Controllern.
WiNET bedeutet, dass die Offline-Terminals über eine Funkverbindung verfügen, über die sie mit einem Controller verbunden sind. Die Konfiguration und Berechtigungen werden über das Funknetzwerk verwaltet.

Zeitplan
Ein Zeitplan definiert Zutrittsberechtigungen und Controller-Funktionen und kann für einen Controller (Generell-Offen Plan oder Türzeitplan) oder für Personen (Personalzeitplan) erstellt werden.

Generell-Offen Plan oder Türzeitplan
Ein Generell-Offen Plan kann einem Controller zugewiesen werden und bestimmt, welche Controllerfunktionen an bestimmten Zeiten aktiv sein sollen. Mit einem Generell-Offen Plan 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.

Personalzeitplan
Ein Personalzeitplan enthält die Definition einer Zutrittsberechtigung für alle Tage einer Woche sowie für 5 Sondertagetypen. Personalzeitpläne werden den Personen und Controllern in der Zutrittskontrollsoftware zugewiesen und bestimmen so die Art der Zutrittsberechtigung für die Personen an den einzelnen Controllern.

Sonderberechtigung
In den Personaldaten kann jeder Person eine Sonderberechtigung zugewiesen werden. Durch die entsprechende Konfiguration der Ein- und Ausgänge der Controller kann so abhängig davon, ob eine Person die Sonderberechtigung besitzt oder nicht, unterschiedliche Funktionen durchgeführt werden.
Mögliche Funktionen für die Sonderberechtigung sind:

- Das Sonderrelais wird bei Identifikation mit Sonderberechtigung zusätzlich aktiviert. Dies kann z.B. zur Ansteuerung einer zweiten Parkschranke verwendet werden.
- Autorisation für den Zweipersonenzutritt mit Masterfunktion.
- Zutrittsberechtigung bei einem Controller durch Benutzung der Tastatur am Controller.
- Möglichkeit zur Aktivierung oder Deaktivierung der Alarmanlage bei einem Controller mit Schaltrelais.

4-Augen-Prinzip
Diese Funktion wird auch "Zweipersonenzutritt" genannt. Um Zutritt zu erhalten sind hier zwei verschiedene, gültige Identifikationen hintereinander erforderlich.

Anti-Pass-Back-Funktion
Ist die Option "Anti-Pass-Back" aktiviert, so ist es immer notwendig, Ein- und Austritte in einer logischen Kombination durchzuführen. Es ist dann nicht möglich, zwei Eintrittsbuchungen ohne dazwischenliegender Austrittsbuchung durchzuführen.

Zutrittswiederholsperre
Ist die Option "Zutrittswiederholsperre" aktiviert, so ist es nicht möglich, während einer gewissen Zeitspanne einen erneuten Eintritt an einer Türe mit demselben Datenträger zu erlangen. Nach Ablauf der Zeitspanne ist ein Zutritt mit dem Datenträger wieder möglich.

Bedrohungs-PIN-Code
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 Controller auftritt, generiert der Controller eine Buchung im internen Buchungsspeicher. Diese Buchungen können mit GAT ACE ausgelesen, gespeichert und ausgewertet werden.

2 INSTALLATION

2.1 Hardwareanforderungen

Abhängig von der Art der Installation sind für die PCs/Server, auf denen GAT ACE und die Zutrittskontrollsoftware wie z. B. GAT Matrix installiert ist, verschiedene Anforderungen zu beachten.

2.1.1 Konfigurationsbeispiel 1

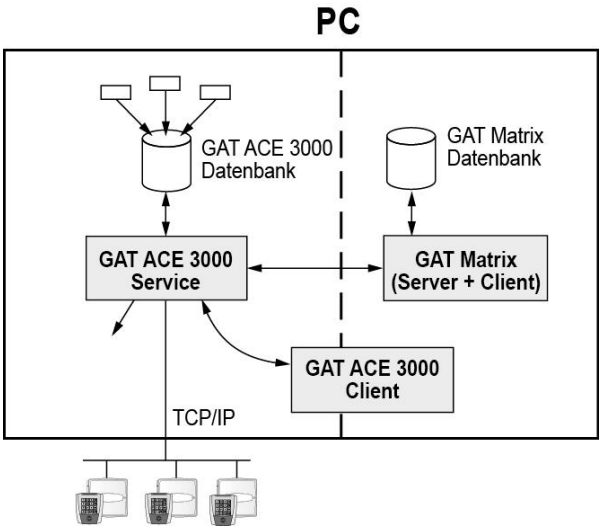


Bild 2.1 *- Installation von GAT ACE und GAT Matrix auf demselben PC*

2.1.2 Konfigurationsbeispiel 2

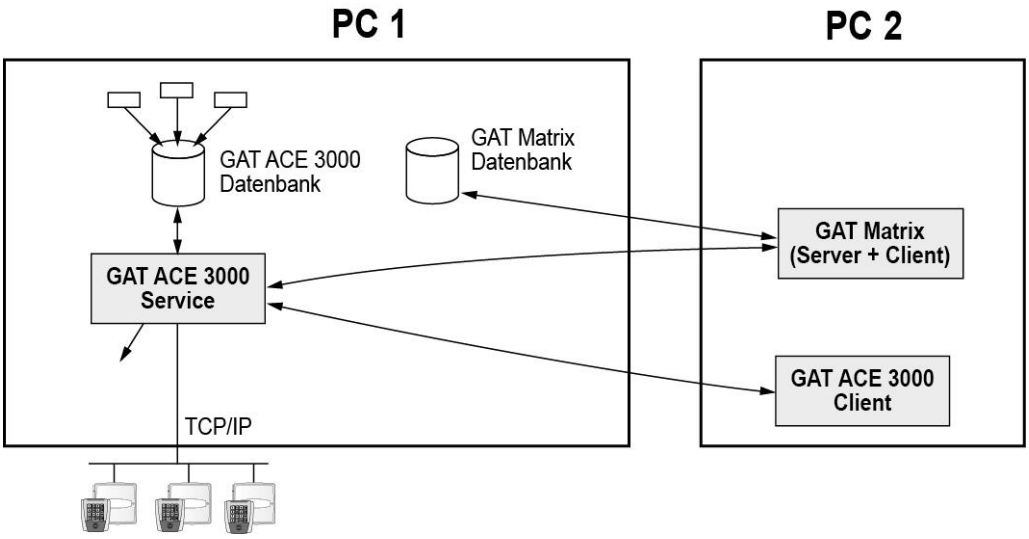


Bild 2.2 *– Installation von GAT ACE und GAT Matrix auf versch. PCs, Datenbank von GAT Matrix auf GAT* ACE PC

2.1.3 Konfiguration 3

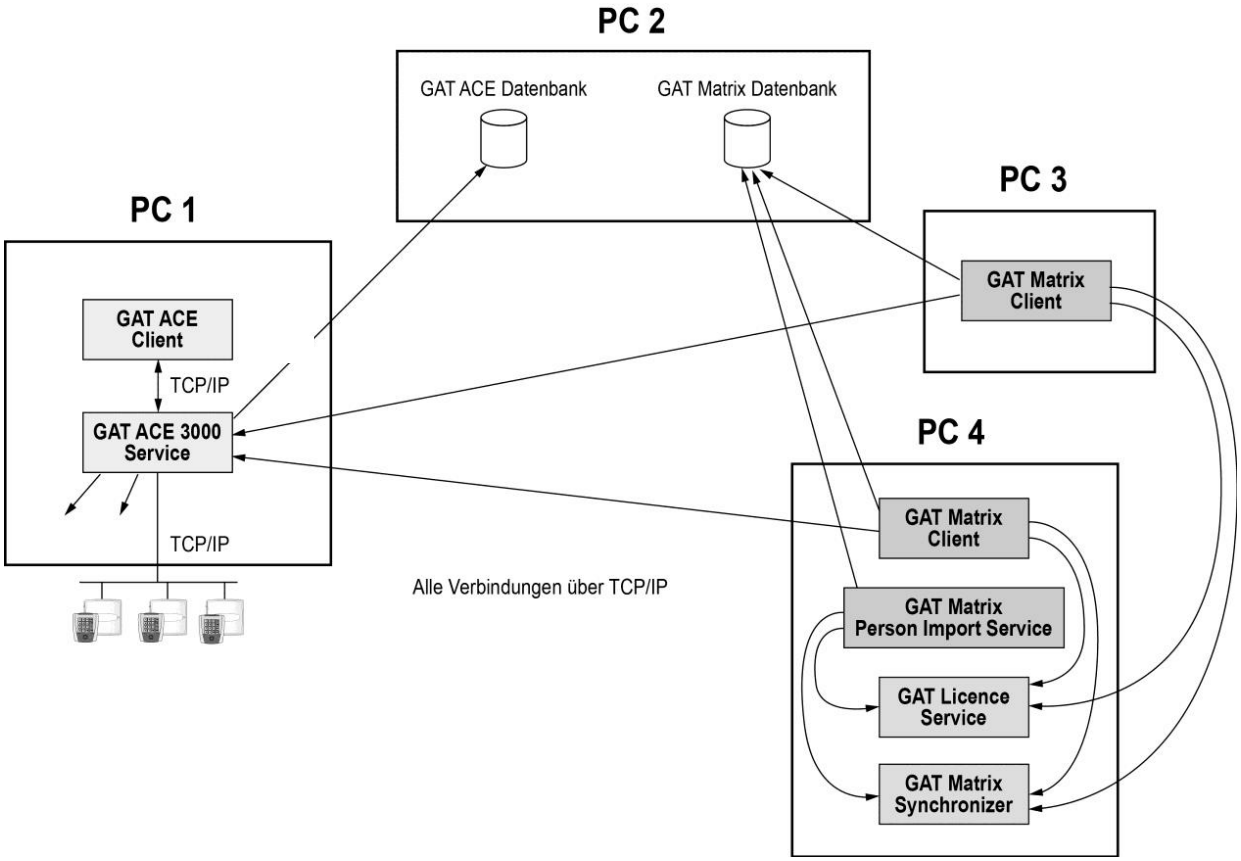


***Bild 2.3** – Installation von GAT ACE und GAT Matrix auf versch. PCs, Datenbank von GAT Matrix auf eigenem PC*

Hardware – Empfohlene Anforderungen für die PCs:

- IBM-kompatibler PC, z. B. Core i5, 3 GHz oder vergleichbare CPU
- CD ROM Laufwerk
- Netzwerkkarte (TCP/IP)
- PC-Schnittstellen: Ethernet (TCP/IP) und USB
- Internetzugang für Updates
- Monitor (min. 1024 x 768 Auflösung)
- Internetbrowser ab Internet Explorer 7.0

Benötigter Festplatten- und Arbeitsspeicherplatz für die einzelnen Programme:

- Freier Arbeitsspeicher: ca. 2 GByte für GAT ACE 3000
  Zusätzlich ca. 2 GB für den Microsoft SQL Server Express
- Freier Festplattenplatz: 20 GB (für Protokoll- und Konfigurationsdaten)

Die Mindestanforderungen für den Rechner summieren sich, wenn weitere Programme wie z. B. GAT Matrix, GAT Mobile Access Management, GAT ACE 7000 usw. installiert werden. Weitere Informationen dazu finden Sie im Handbuch der GAT Matrix.

2.2 Softwareanforderungen

2.2.1 Unterstützte Betriebssysteme für GAT ACE

- Microsoft® Windows® 7 (alle außer Home-Edition), 32- und 64-Bit
- Microsoft® Windows® 8 (alle außer RT), 64-Bit
- Microsoft® Windows® 10 (Pro, Enterprise), 64-Bit
- Microsoft® Windows Server® 2008 R2, 64-Bit
- Microsoft® Windows Server® 2012, 64-Bit
- Microsoft® Windows Server® 2012 R2, 64-Bit
- Microsoft® Windows Server® 2016 (Essentials, Standard, Datacenter), 64-Bit
- Microsoft® Windows Server® 2019 (Essentials, Standard, Datacenter), 64-Bit

Die Server Core Installationsoption von Windows Server® 2008 R2 und Windows Server® 2012 werden von GAT ACE nicht unterstützt. Außerdem werden RT, Starter, Home, Small Business oder Web Editionen ebenfalls nicht unterstützt.

HINWEIS! Bitte beachten Sie, dass GANTNER Electronic GmbH nur dann Support-Unterstützung anbieten kann, wenn GAT ACE auf einer deutschen oder englischen Windows-Version installiert ist.
Ein Support durch GANTNER Electronic GmbH 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.

2.2.2 Datenbankserver

Unterstützte Datenbanken:

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

Die Microsoft® SQL Server® 2016 Express Datenbank kann im Partnerbereich der GANTNER Homepage heruntergeladen werden. Die aktualisierten Systemanforderungen des Microsoft® SQL Server® 2016 Express sind unter folgender Seite zu finden: https://technet.microsoft.com/de-de/library/ms143506.aspx
Ab Version 2016 ist der Microsoft® SQL Server® nur noch als 64-Bit Variente erhältlich.

HINWEIS! Bitte beachten Sie, dass der Partnerberiech nur die freie Microsoft® SQL Server® Express Datenbank enthält. Wenn eine vollwertige SQL Datenbank benötigt wird, muss diese von der IT des Anlagenbetreibers mit den erforderlichen Microsoft Lizenzen bereitgestellt werden.
Es wird empfohlen, das Microsoft SQL Server Management Studio Express zu installieren. Diese Anwendung ist im SQL-Download-Archiv, das Sie im GANTNER Partnerbereich finden, enthalten.

Wenn die Express-Version des Microsoft® SQL Server® verwendet wird achten Sie bitte darauf, dass die Datenbankbereinigung aktiviert ist, um die Datenbank klein zu halten.

Für den Ordner, in dem die Datenbank liegt, müssen folgende Punkte beachtet werden:

- Keine Antivirus Software ist erlaubt, um den Ordner zu scannen. Siehe dazu die Empfehlungen von Microsoft (https://technet.microsoft.com/de-de/library/ms144228.aspx).
- Von diesem Ordner darf kein automatisches Backup gemacht werden.

2.2.3 Microsoft .NET Framework

Für die Funktion der GAT ACE 3000 muss das .NET Framework 4.6.1 vorinstalliert sein.

2.3 Installation von GAT ACE 3000

Dieser Abschnitt beschreibt die Installation von GAT ACE 3000 für den Fall, dass Sie noch keine ältere Zutrittskontrollsoftware von GANTNER Electronic GmbH zuvor in Verwendung hatten.

► Starten Sie die Installation von GAT ACE 3000 durch doppelklick auf die Datei "Setup.exe" im Installationspaket.

2.3.1 Installation des Microsoft SQL Server 2016 Express

Für GAT ACE 3000 ist eine SQL Datenbank erforderlich. Wenn bereits ein bestehender SQL-Server zu Verfügung steht, kann die Datenbank in diesem Server erstellt und dieser Abschnitt übersprungen werden. Ist dies nicht der Fall, installieren Sie zuerst den Microsoft SQL Server 2016 Express wie im Folgende beschrieben.
Im Partnerbereich der GANTNER Homepage finden Sie den Microsoft SQL Server 2016 Express für 64-Bit Betriebssysteme.

HINWEISE!

- Im Download ist ebenfalls das Microsoft SQL Server Management Studio enthalten. Es wird empfohlen, dieses ebenfalls zu installieren, damit eine optimale Voraussetzung für Wartung und Service von GAT ACE gegeben ist.
- Dieser Abschnitt beschreibt die wichtigsten Punkte für die Installation von Microsoft SQL Server 2016 Express. MS SQL Server haben noch viele weitere Einstellungen. Um diese zu definieren kann das MS SQL Server Management Studio Express verwendet werden. Kontaktieren Sie Ihren Datenbank-Administrator bezüglich Fragen zu den erweiterten Einstellungen.
- Das Installationsprogramm für den Microsoft SQL Server 2016 Express ist nur in englischer Sprache verfügbar.

- ► Loggen Sie sich mit Ihren Zugangsdaten im Partnerbereich der GANTNER-Homepage ein und laden Sie die Microsoft SQL Express herunter (Menü "Produkte" -> "Software" -> "GAT ACE 3000").
- ► Entpacken Sie die geladene Datei in einem Verzeichnis.
- ► Starten Sie das Setup indem Sie die entpackte Datei "Setup_x64.bat" als "Administrator" aufrufen.
  Achtung: Die Setup_x64.bat beinhaltet alle notwendigen Voreinstellungen und Parameter für die Installation. Wird die Setup_x64.bat Datei nicht verwendet, werden die benötigten Voreinstellungen und Parameter nicht automatisch beim Installationsassistenten in der geführten Oberfläche erweitert.
  - ○ Das Installationsprogramm prüft, ob alle Voraussetzungen zur Installation des SQL Servers erfüllt sind:
    1. Das .NET Framework 3.5 muss installiert sein.
    2. Microsoft Visual C++ 2015 x86 Redistributable
  - ○ Fehlt eine dieser Softwarekomponenten, wird eine entsprechende Meldung angezeigt und diese kann im Installationsprogramm automatisch mit installiert werden.
  - ○ Sind die Voraussetzungen erfüllt, wird der Installationsassistent für den SQL Server 2016 Express gestartet. Dieser führt Sie schrittweise durch den Installationsprozess.
- ► Bestätigen Sie die angezeigten Lizenzbedingungen, indem Sie die Option "I accept the license terms" markieren und auf "Next >" klicken.
  - ○ Anschließend gelangen Sie zum folgenden Dialog. Links werden die einzelnen Installationsschritte dargestellt und in der Mitte können die Einstellungen für die Installation vorgenommen werden.

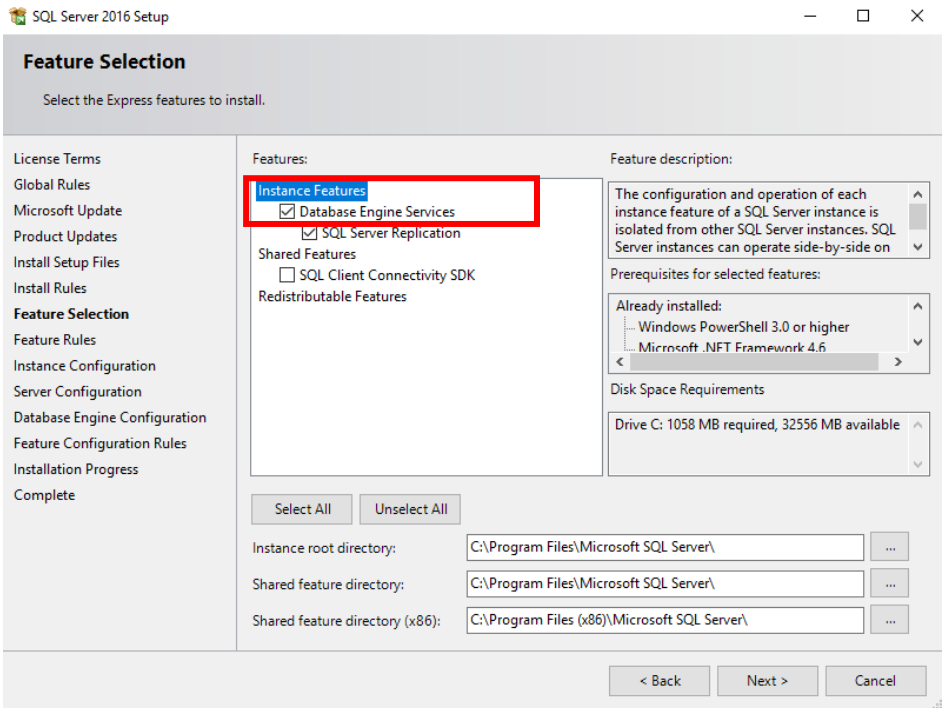


Bild 2.4 *- Microsoft SQL Server 2016 Express - Optionsauswahl*

- ► Die benötigten Optionen sind bereits ausgewählt (siehe Bild 2.4).
- ► Klicken Sie auf "Next >", bis folgendes Fenster angezeigt wird ("Server Configuration").

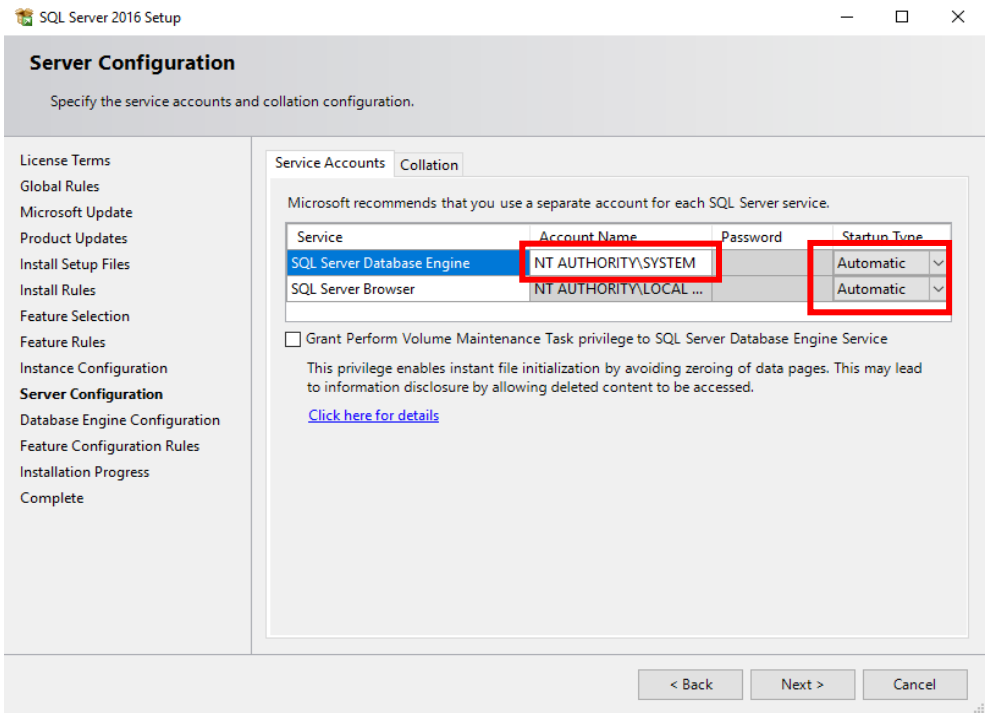


Bild 2.5 *- Microsoft SQL Server 2016 Express - Serverkonfiguration*

- Spezifizieren Sie hier das Benutzerkonto, unter welchem der SQL Server laufen soll. Sollten Sie ein spezielles Benutzerkonto erstellt haben, unter welchem der SQL Server laufen soll, kann dies hier angegeben werden. Ansonsten sollte das Konto "NT-AUTORITÄT\SYSTEM" verwendet werden.
- Als Startup Typ sollte immer "Automatic" gesetzt werden, damit die Dienste beim Start von Windows automatisch gestartet werden.
- Mit "Next >" gelangen Sie zum nächsten Dialog "Database Engine Configuration".
  - Hier wird die Anmeldemethode sowie die Administratoren des SQL Servers festgelegt.

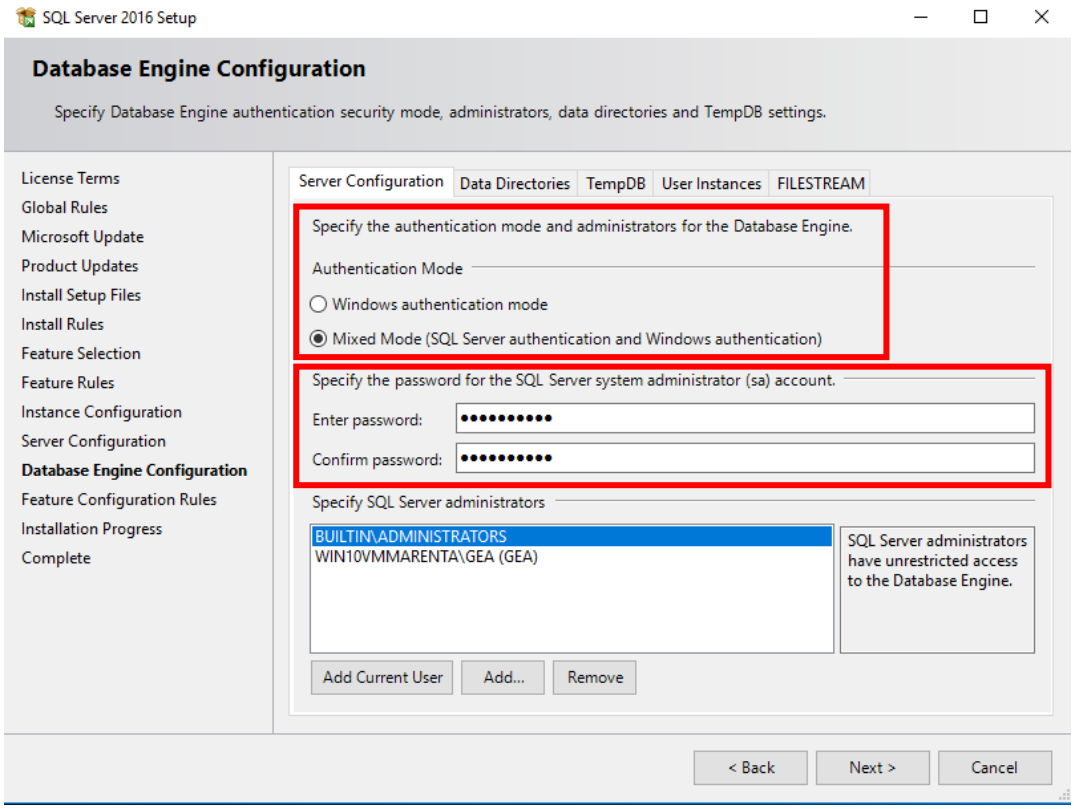


Bild 2.6 *- Microsoft SQL Server 2016 Express - Datenbankverbindung*

► Die benötigten Optionen sind hier bereits vorkonfiguriert.

- Das Passwort für den SQL Administrator "sa" wird vom Setup-Programm automatisch vergeben (Info Passwort "GATMatrix1").
- Es wird empfohlen, das Standard-Passwort beizubehalten. Sollten Sie das Passwort ändern, wählen Sie ein starkes Passwort, d.h. mindestens 10 Zeichen, Großbuchstaben, Kleinbuchstaben sowie Ziffern. Richten Sie sich hier bitte die für Sie vorgegebenen IT-Richtlinien. Merken Sie sich das Passwort und bewahren Sie dieses an einem sicheren Ort auf, da ohne diesem kein Service-Zugriff auf die GAT ACE 3000 Datenbank möglich ist.

► Klicken Sie anschließend mehrmals auf "Next >", bis die Installation abgeschlossen ist.

- Die erfolgreich ausgeführten Insatallationsschritte werden im letzten Fenster mit grünen Symbolen und dem Status "Succeeded" signalisiert.

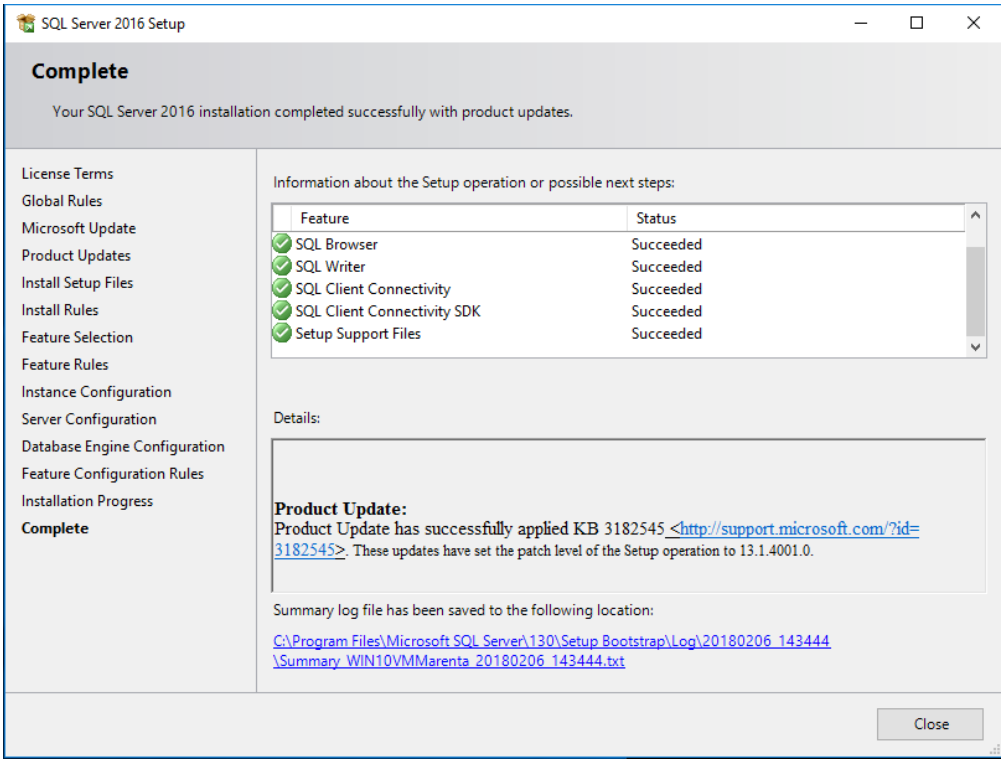


Bild 2.7 *- Microsoft SQL Server 2016 Express - Installationsvorgang abgeschlossen*

► Klicken Sie auf "Close".

○ Anschließend wird der Setup-Assisten für das Microsoft SQL Server Management Studio gestartet.

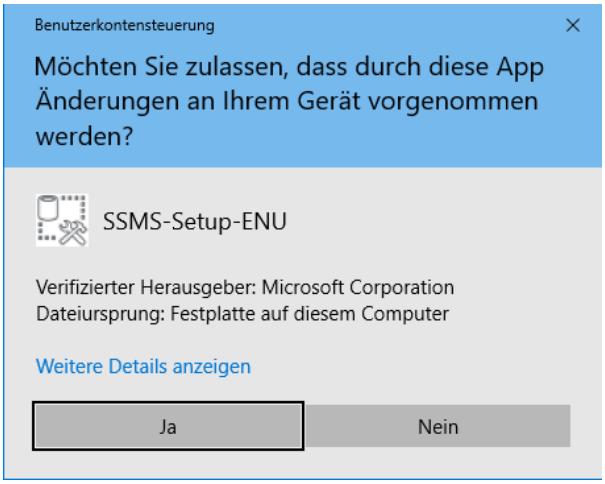


Bild 2.8 - Microsoft SQL Server Management Studio installieren

► Sie sollten dieses Management Studio unbedingt installieren, um eventuell notwendige Wartungsarbeiten an der Datenbank zu erleichtern.

► Klicken Sie auf "Ja" und warten Sie, bis die Installationsschritte abgeschlossen sind. Die Installation erfolgt automatisch.

2.3.2 Installation der GAT ACE

Sind alle benötigten Komponenten für GAT ACE installiert, wird die Installation von GAT ACE gestartet.

HINWEIS! GAT ACE muss durch einen Administrator mit allen Nutzerrechten installiert werden.

► Legen Sie die Installations-CD von GAT ACE ein, um das Setup zu starten.
► Doppelklicken Sie auf die Datei "setup.exe".
  ○ Der Installationsassistent wird geöffnet.

Bild 2.9 *- GAT ACE Installation - Schritt 1*

Hinweis: Der Installationsassistent ist nur in englischer Sprache verfügbar.

► Klicken Sie "Next".

Bild 2.10 *- GAT ACE 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 akzeptieren und fortfahren zu können.

► Klicken Sie "Next".

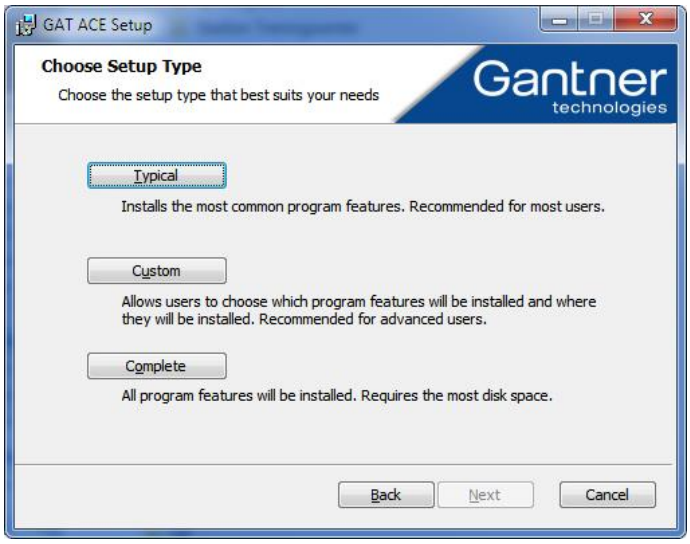


Bild 2.11 *- GAT ACE Installation - Schritt 3*

► Wählen Sie die Art der Installation (Standard = "Typical"):

- Typical: Installiert GAT ACE (Service und Client) und die wichtigsten Programmteile. Dies ist die Standardoption für die meisten Benutzer.

- Custom: Erlaubt eine Auswahl, welche Teile von GAT ACE installiert werden sollen, und an welchen Ort diese Komponenten installiert werden sollen. Folgendes Fenster wird angezeigt. Dabei steht GAT ACE für die grafische Benutzeroberfläche und GAT ACE 3000 für den Dienst.

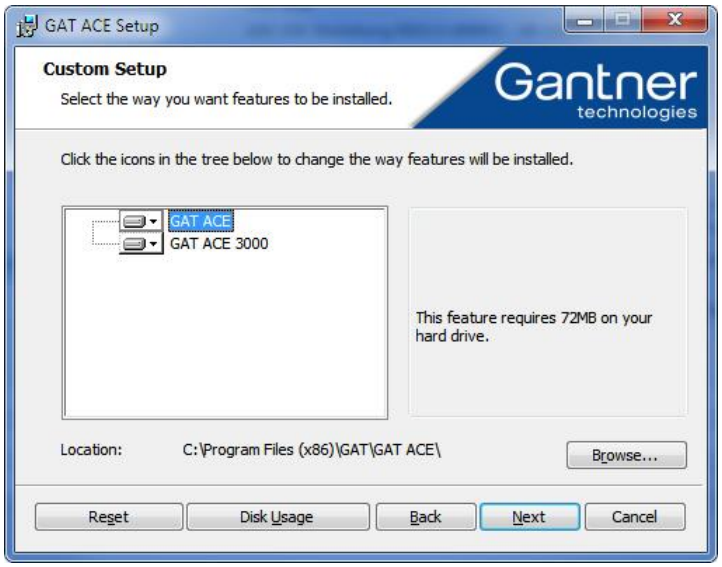


Bild 2.12 *- GAT ACE Installation - Custom Setup*

► 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. nur der Client und nicht der Server installiert werden soll (z. B. Dienst läuft auf einem anderen Server), wählen Sie für GAT ACE 3000 die Option "Entire feature will be unavailable".

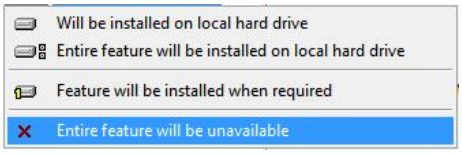


Bild 2.13 *- GAT ACE Installation - Schritt 4*

► Wählen Sie nun noch das Verzeichnis, in dem GAT ACE 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 ACE. Diese Option benötigt den meisten Speicherplatz.

○ Nach Wahl der Installationsart und Durchführung der vorigen Schritte wird folgendes Fenster angezeigt.

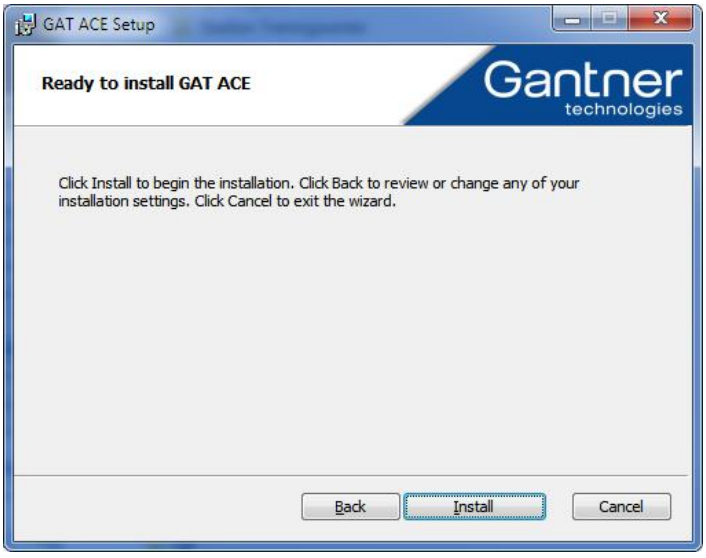


Bild 2.14 *- GAT ACE Installation - Schritt 4*

► Klicken Sie "Install" und bestätigen Sie die folgende Berechtigungsabfrage mit "OK".
  ○ 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.
  ○ GAT ACE ist nun installiert und einsatzbereit.

Anti-Virus Software:
Bei einer verwendeten Anti-Virus Software sind folgende Punkte zu beachten:
- Es ist sehr wichtig, dass die Installationsverzeichnisse von GAT ACE und GAT ACE 3000 von den Anti-Virus Prüfungen ausgenommen sind. In einer Standard-Installation betrifft dies die Verzeichnisse:
  - Für 32 Bit Windows Versionen:
    "C:\Programme\GAT\GAT ACE"
    "C:\Programme\GAT\GAT ACE 3000"
  - Für 64 Bit Windows Versionen:
    "C:\Programme(x86)\GAT\GAT ACE"
    "C:\Programme(x86)\GAT\GAT ACE 3000"
- Außerdem müssen die Komponenten der GAT ACE Software von Live-Scan einer Virusprüfung ausgenommen werden, um Virus-Fehlmeldungen zu vermeiden.

2.3.3 Einstellungen Windows-Dienst

Wenn der GAT ACE Windows-Dienst und die Datenbank auf demselben PC installiert sind besteht die Möglichkeit, dass der GAT ACE Dienst vor dem SQL Dienst startet. In diesem Fall kann keine Verbindung mit der Datenbank hergestellt werden und GAT ACE startet nicht.

Für Windows 7 und Windows Server 2008 ist dieses Problem 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.

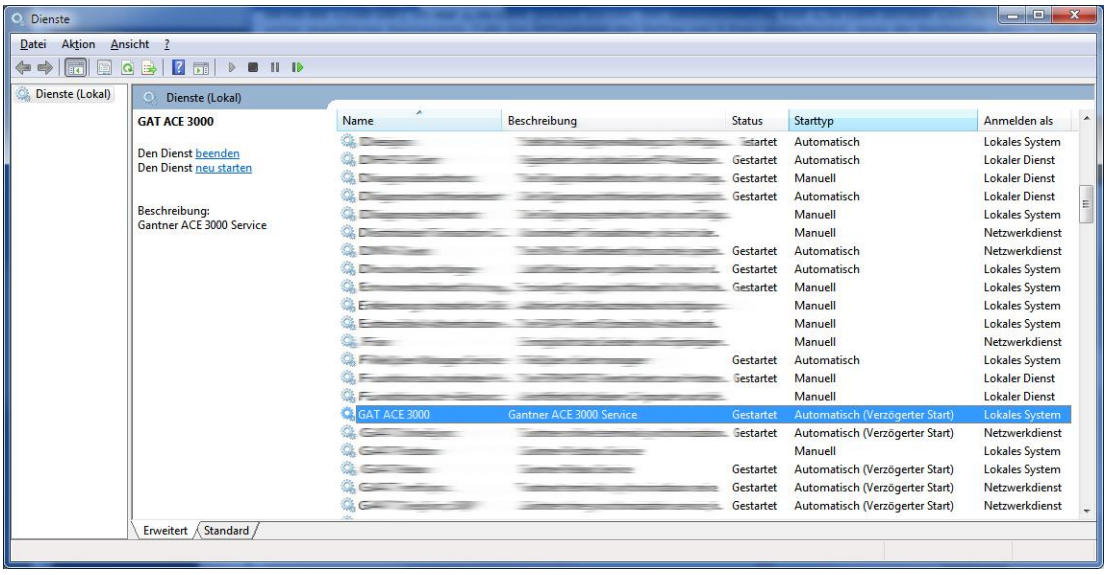


Bild 2.15 *- Windows Dienste*

► Hier muss der "Starttyp" auf "Automatisch (Verzögerter Start)" gesetzt werden. Klicken Sie dazu mit der rechte Maustaste auf den GAT ACE 3000 Dienst und wählen Sie den Menüpunkt "Eigenschaften" aus dem Pop-Up Menü.
  ○ Das Eigenschaftenfenster des GAT ACE 3000 Diensts wird geöffnet.

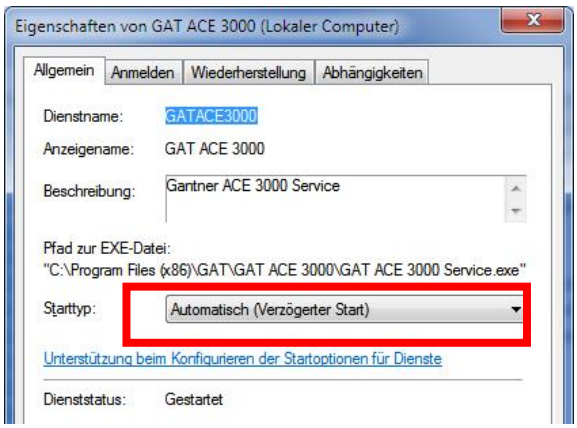


Bild 2.16 *- Windows Dienst*

- ► Für den "Starttyp" wählen Sie hier "Automatisch (Verzögerter Start)".
- ► Drücken Sie "OK"
  - ○ Diese Einstellung sorgt dafür, dass der GAT ACE 3000 Dienst automatisch, aber verzögert, startet.

2.4 Umstieg von GAT Manager auf GAT ACE

Beim Umstieg von einer bestehenden Zutrittskontrollanlage mit GAT Manager Software von GANTNER Electronic GmbH auf die neue GAT ACE Software können die bestehenden Controller-Konfigurationen übernommen werden.

Um einen einwandfreien Umstieg zu gewährleisten, müssen bestimmte Schritte ausgeführt werden. Die genaue Beschreibung dafür finden Sie im "7. UMSTIEG VON GAT MANAGER AUF GAT ACE".

2.5 Update von GAT ACE

In GAT ACE haben Sie die Möglichkeit, automatisch auf eine neue Version von GAT ACE zu prüfen. Dazu ist lediglich eine Internetverbindung notwendig. Wird eine neuere Version von GAT ACE gefunden, haben Sie die Möglichkeit, das Update zu laden und zu installieren. Sollte dies nicht funktionieren, kontaktieren Sie bitte Ihren IT-Betreuer.

Nach dem Update kann dieselbe Lizenz wie vor dem Update verwendet werden. Es ist möglich, dass durch das Update Zusatzpakete (wie z. B. die Anti-Pass-Back oder andere Funktionen) neu hinzukommen. Diese können mit der bestehenden Lizenz dann nicht genutzt werden. Für deren Nutzung muss die entsprechende Erweiterungslizenz erworben werden.

Eventuell muss die Datenbank nach dem Update aktualisiert werden, weil durch das Update neue Datenbankfelder hinzukommen sind. Die bestehenden Daten werden dadurch aber nicht verändert oder gelöscht.

HINWEIS Es wird empfohlen, vor einem Update immer ein Backup der Datenbank zu erstellen. Nähre Informationen, wie Sie ein Backup einer SQL-Datenbank erstellen können, finden Sie im Internet z.B. auf der Seite https://msdn.microsoft.com/de-de/library/ms187510%28v=sql.120%29.aspx.

3 GAT ACE 3000 STARTEN

Beim ersten Starten von GAT ACE 3000 nach der Installation müssen eventuell noch Einstellungen wie z. B. die Datenbankverbindung vorgenommen werden. Bei weiteren Starts sollten Sie dann direkt zum Anmeldebildschirm gelangen.

3.1 Startvorgang

► Starten Sie GAT ACE durch Auswahl des Startmenü-Eintrags "GAT Ace".

HINWEIS! Nach der Installation ist standardmäßig ein Programmeintrag für GAT ACE im Windows-Startmenü unter folgendem Pfad eingetragen: Start -> Alle Programme -> GANTNER Electronic GmbH -> GAT Ace.

- Der Ladebildschirm von GAT ACE wird angezeigt.

Beim Start prüft GAT ACE die Verbindung zum GAT ACE Dienst und zur Datenbank. Wenn der Dienst nicht läuft bzw. die Verbindung zu dem Dienst noch nicht richtig eingestellt ist, erhalten Sie eine entsprechende Information am Bildschirm. Ebenso wenn die Datenbank noch nicht existiert oder keine Verbindung zur Datenbank aufgebaut ist.

3.1.1 GAT ACE 3000 Dienst

Der GAT ACE 3000 Dienst ist ein Windows Dienst, der im Hintergrund läuft und die Kommunikation und Datenverarbeitung zischen einem oder auch mehreren GAT ACE Clients, der Datenbank und den zu konfigurierenden Geräten herstellt. Dieser Dienst muss deshalb gestartet sein, damit GAT ACE benutzt werden kann.
GAT ACE prüft beim Starten die Verbindung zum GAT ACE 3000 Dienst. Ist dieser nicht erreichbar, wird eine Fehlermeldung angezeigt.

HINWEIS! Normalerweise wird der Dienst beim Start von GAT ACE automatisch gestartet.

Bild 3.1 *- GAT ACE 3000 Dienst starten*

► Wenn der GAT ACE 3000 Dienst ausf einem anderen PC/Server installiert ist konfigurieren Sie hier die Adresse des Servers und die Portnummer.

HINWEIS Wenn der Dienst auf demselben PC/Server läuft wie die aktuell gestartete GAT ACE geben Sie im Feld "Remote Location" "localhost" ein.

3.1.2 Datenbankeinstellungen

Nach der Installation von GAT ACE muss einmal eine Datenbank für GAT ACE erstellt und die Verbindung zur Datenbank konfiguriert werden. Bei weiteren Starts der GAT ACE erkennt die Software automatisch, ob eine Verbindung zur Datenbank besteht oder diese bei Änderungen eventuell neu konfiguriert werden muss.

Um die Datenbank zu erstellen und die Verbindung zur Datenbank zu konfigurieren, führen Sie folgende Schritte aus:

► Folgendes Fenster wird beim Start angezeigt, wenn die Verbindungseinstellungen zur Datenbank nicht richtig konfiguriert sind.

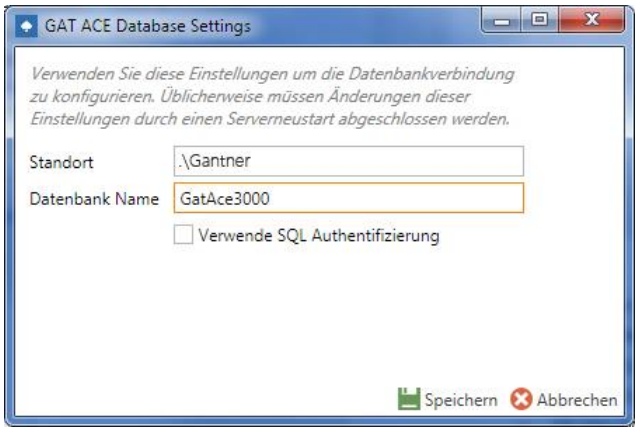


Bild 3.2 *- Verbindungseinstellung für Datenbank*

► Geben Sie im Feld "Standort" den Serverstandort der Datenbank ein.
  - Wird die Datenbank auf demselben PC wie GAT ACE und mit den Standardeinstellungen installiert, so geben Sie als Standort "`.\Gantner`" ein. Wurden die Werte bei der Installation geändert, geben Sie hier den genauen Serverstandort der Datenbank an (d.h. Netzwerkname oder IP-Adresse und SQL Server-Instanzname).

► Im Feld "Datenbank Name" muss der Name der Datenbank eingegeben werden (Standard = "`GatAce3000`").

► Mit dem Feld "Verwende SQL Authentifizierung" kann ausgewählt werden, ob GAT ACE für die Anmeldung an der Datenbank die Windows-Authentifizierung des jeweiligen Benutzerkontos oder die SQL-Authentifizierung mit Benutzername und Passwort verwendet werden soll.
  - Ist das Feld nicht markiert, wird die Windows Authentifizierung verwendet (= Standard).
  - Ist das Feld markiert geben Sie bitte den Benutzernamen und das Passwort ein, das für die Datenbankanmeldung verwendet werden soll.

HINWEIS! Bitte berücksichtigen Sie, dass eine Datenbank nur dann anhand der Standardeinstellungen generiert werden kann, wenn eine SQL Server-Instanz namens „SQLEXPRESS“ auf dem Gerät installiert ist und eine Windows-Authentifizierung zulässt. Dies ist der Fall, wenn Sie SQL Server Express zusammen mit GAT ACE installiert haben.

HINWEIS! Der Zugriff auf die GAT ACE Datenbankeinstellungen ist auch später in GAT ACE jederzeit über die Programmeinstellungen möglich (Symbol -> Menüpunkt "Datenbank-Einstellungen").

► Speichern Sie die Einstellungen mit der Schaltfläche "Speichern".

- GAT ACE 3000 startet neu und versucht, sich mit dem Datenbankserver zu verbinden. Existiert noch keine Datenbank mit dem eingetragenen Namen, so werden Sie gefragt, ob die Datenbank jetzt erstellt werden soll.

***Bild 3.3** - Neue Datenbank erstellen*

► Klicken Sie auf "Ja", um die Datenbank zu erstellen und fortzufahren.

3.1.3 Anmeldebildschirm

Wenn GAT ACE mit dem GAT ACE 3000 Dienst verbunden ist und die Datenbankverbindung aufgebaut ist erscheint nach wenigen Sekunden der Anmeldebildschirm. Hier muss sich der Benutzer mit Benutzername und Passwort anmelden, um Zugriff auf die GAT ACE 3000 Funktionen zu haben.

HINWEIS! Es können verschiedene Benutzer mit unterschiedlichen Berechtigungen angelegt werden. Näheres dazu finden Sie in Kapitel "6. BERECHTIGUNGS-MANAGEMENT".

***Bild 3.4** - Anmeldebildschirm von GAT ACE 3000*

► Geben Sie im Feld "Benutzername" Ihren Benutzernamen ein.

- ► Geben Sie im Feld "Passwort" Ihr Passwort ein. Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden.
- ► Bestätigen Sie die Eingaben mit Klick auf "Anmeldung".
  - ○ Bei Korrekter Eingabe gelangen Sie in den Hauptbildschirm von GAT ACE 3000 (siehe "5.1. Funktionsübersicht von GAT ACE"). Ansonsten haben Sie die Möglichkeit, den Benutzernamen und das Passwort erneut einzugeben.

Ändern Sie nach der Installation die Standard Passwörter.
Nach der Installation von GAT ACE sind die Standard Benutzer "SYSTEM" und "Administrator" mit Standard Passwörtern eingerichtet. Ändern Sie unbedingt nach der Installation von GAT ACE diese Standard Passwörter auf sichere, geheime Passwörter. Siehe dazu Kapitel "6. BERECHTIGUNGS-MANAGEMENT".

4 KONFIGURATION

In den Programmeinstellungen können alle grundlegenden Funktionalitäten von GAT ACE eingestellt werden. Die konfigurierbaren Einstellungen sind auf verschiedene Seiten, im folgenden "Einstellungsseiten" genannt, aufgeteilt. Diese Einstellungsseiten können wie folgt aufgerufen werden.

► Klicken Sie auf das Symbol oberhalb der Hauptmenüleiste.

- Die Liste der Einstellungsseiten für die Programmeinstellungen wird angezeigt.

► Wählen Sie die gewünschte Einstellungsseite aus.

- Die Einstellungen werden rechts neben der Liste angezeigt.

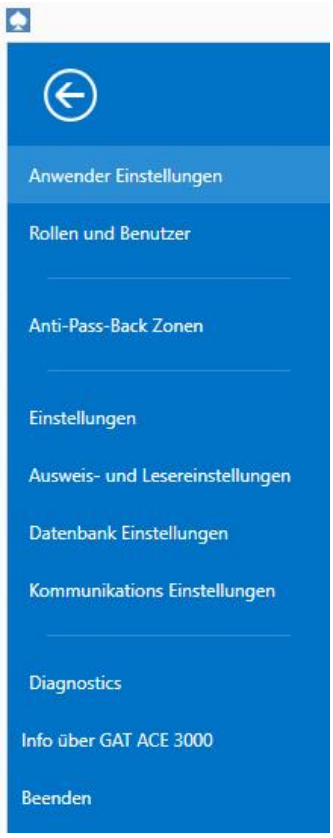


***Bild 4.1** - Programmeinstellungen*

Die verschiedenen Einstellungsseiten werden auf den folgenden Seiten beschrieben.

HINWEIS! Wenn auf einer Einstellungsseite Änderungen vorgenommen werden, müssen diese mit der Schaltfläche "Speichern" gespeichert werden. Diese Schaltfläche wird erst angezeigt, nachdem eine Änderung auf einer Seite gemacht wurde. Einstellungsseiten mit geänderten aber noch nicht gespeicherten Einstellungen werden rot markiert.

***Bild 4.2** - Einstellungsseiten mit noch nicht gespeicherten Änderungen*

4.1 Einstellungsseite "Anwender Einstellungen"

***Bild 4.3** - Programmeinstellungen - Sprachauswahl*

Hier können Sie die Sprache auswählen. Sobald eine andere Sprache gewählt wird schließt GAT ACE das Programmfenster und öffnet es gleich wieder. Die Sprache ist dann umgestellt, ein Neustart ist nicht notwendig.

HINWEIS! Beim Umstellen der Sprache werden alle zu dem Zeitpunkt geöffneten Ansichten in GAT ACE geschlossen.

4.2 Einstellungsseite "Rollen und Benutzer"

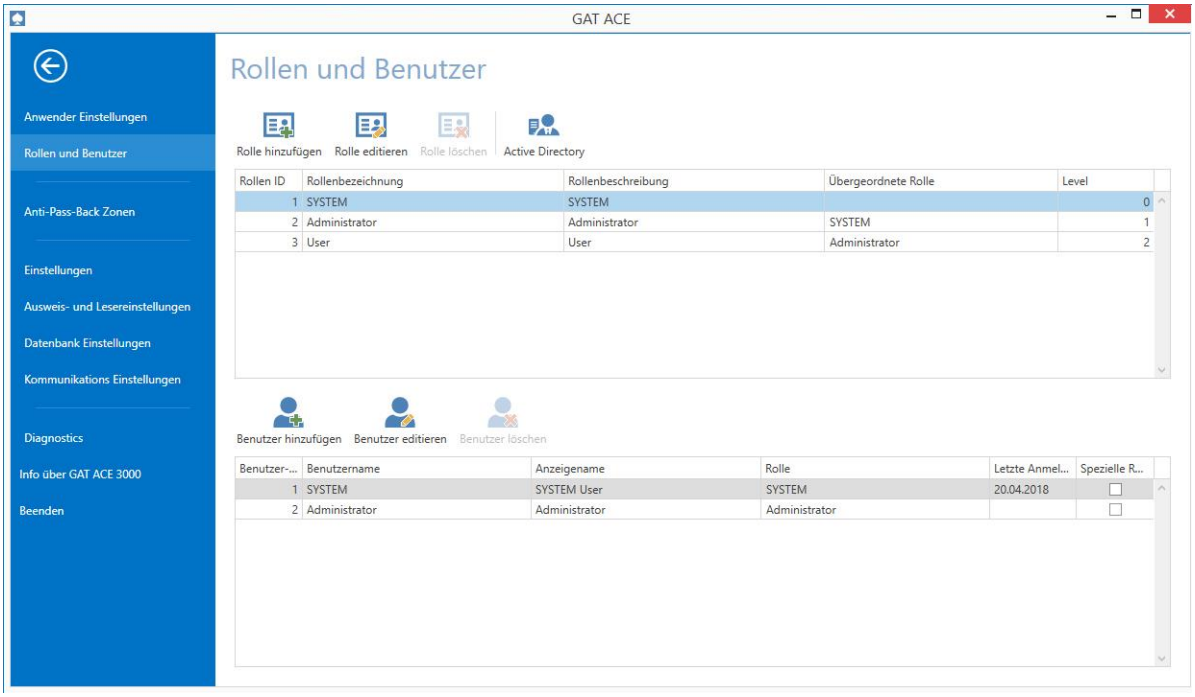


***Bild 4.4** - Programmeinstellungen - Rollen und Benutzereinstellunegn*

Um mit GAT ACE arbeiten zu können ist aus Sicherheitsgründen die Eingabe eines Benutzernamens und zugehörigem Passwort notwendig. Das Benutzersystem ist hierarchisch aufgebaut, so dass verschiedene Benutzer unterschiedliche Berechtigungen haben können. Die Definition dieser Berechtigungen erfolgt mittels Rollen, die in GAT ACE eingestellt und gespeichert werden.

In diesem Einstellungsfenster werden die Rollen und die Benutzer erstellt und die Rollen den Benutzern zugewiesen. Die Rollen und Benutzerverwaltung ist im Detail in Kapitel "6. BERECHTIGUNGS-MANAGEMENT" beschrieben.

4.3 Einstellungsseite "Anti-Pass-Back Zonen"

Mit der Anti-Pass-Back-Funktion kann verhindert werden, dass mehrere Personen durch Weitergabe des Datenträgers mit demselben Datenträger Zutritt erlangen. Das bedeutet, dass sich bei Aktivierung dieser Funktion jede Person nach einem Zutritt auch beim Verlasen wieder identifizieren muss, um erneut einen Zutritt durchführen zu können. Dafür werden an einem Zugang sowohl ein Eintritts- als auch ein Austrittsleser benötigt, mit dem die Bewegungen überwacht werden.

Für die Anti-Pass-Back-Funktion können Zonen definiert werden. In jeder Zone wird diese Funktion dann getrennt verarbeitet. Das bedeutet, dass mit einem Datenträger nicht zweimal hintereinander Zutritt zur selben Zone möglich ist, bevor nicht ein Austritt mit dem Datenträger aus dieser Zone erfolgte.

Die Anti-Pass-Back Funktion ist eine lizenzpflichtige Erweiterung der GAT ACE 3000. Ohne Lizenz sind die Funktionen nicht verfügbar.

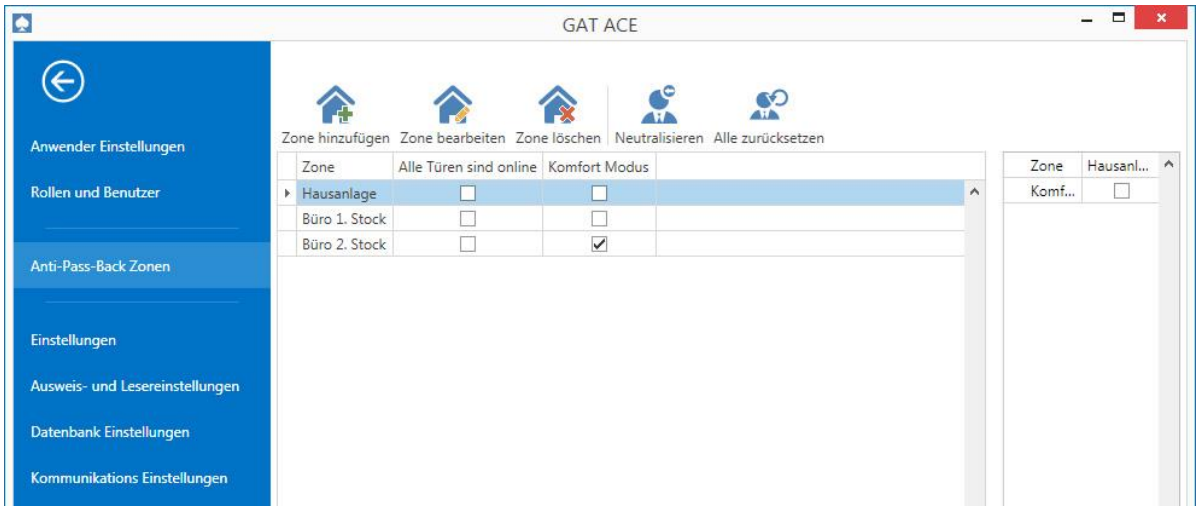


Bild 4.5 *- Programmeinstellungen - Anti-Pass-Back-Funktion*

In dieser Ansicht werden alle bereits definierten Zonen aufgelistet.

Wenn das Feld in der Spalte "Alle Türen sind online" markiert ist bedeutet das, dass GAT ACE Verbindung zu allen Türen in der jeweiligen Zone hat. Dies ist für die Anti-Pass-Back Funktion wichtig, da bei dieser Funktion laufend geprüft werden muss, an welchen Türen ein Ein- oder Austritt mit welchem Datenträger stattgefunden haben, um feststellen zu können, in welcher Zone sich die Personen befinden.

Wird für eine Zone der Komfort Modus aktiviert, wird bei einer Verbindungsunterbrechung zu einer Türe die Anti-Pass-Back- Funktion der Zone ausgeschaltet damit ein möglichst störungsfreier Betrieb des Zutrittskontrollsystems gewährleistet ist. Für sicherheitskritische Zonen soll der Komfortmode nicht verwendet werden. Für die optimale Umsetzung des Komfort Modes ist auch eine entsprechende Konfiguration der Türe erforderlich.

HINWEIS! Zusätzlich zur Einstellung des Komfortmodus sollte bei den Controllern der Anlage auch die Einstellung "Anti-Pass-Back aktiviert wenn die Türe online ist" gesetzt sein (siehe "5.2.9. Türen konfigurieren"). Dadurch wird bei Ausfall der Verbindung zu einer Tür eine normale Zutrittsprüfung durchführen, ohne die Anti-Pass-Back Einstellungen zu berücksichtigen. Das Deaktivieren des Anti-Pass-Back erfolgt mit einer Verzögerung von bis zu einer Minute. Die Anti-Pass-Back Prüfung wird wieder aktiviert sobald die Verbindung wieder online ist.

► Um eine neue Zone hinzuzufügen, klicken Sie auf das Symbol "Zone hinzufügen".
  ○ Es wird das Fenster "Zone Konfiguration" geöffnet (siehe nächster Punkt).
► Um eine bestehende Zone zu löschen markieren Sie diese in der Liste und wählen Sie "Zone löschen".
► Um eine bestehende Zone zu bearbeiten markieren Sie diese in der Liste und wählen Sie "Zone bearbeiten".
  ○ Es wird das Fenster " Zone Konfiguration" geöffnet.

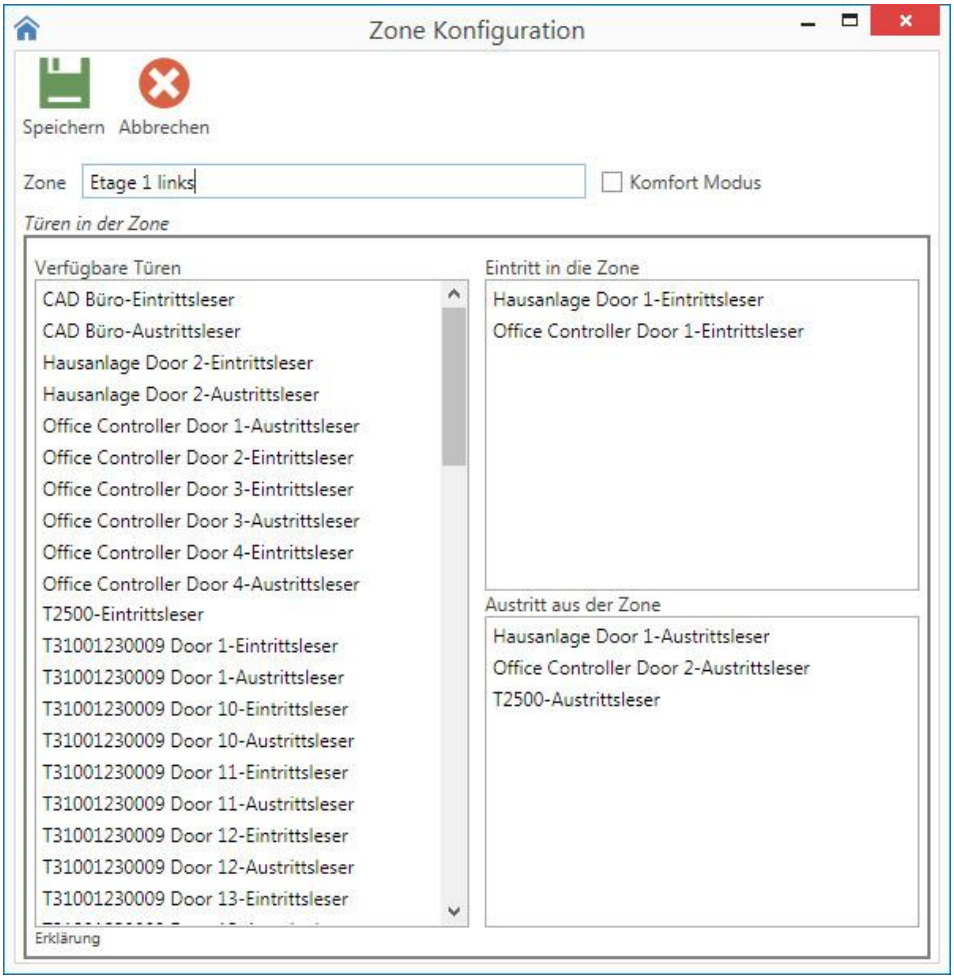


Bild 4.6 *- Konfiguration der Zonen für die Anti-Pass-Back-Funktion*

Hier wird die aktuelle Zone bearbeitet und die Türen bzw. Leser festgelegt, die für die Kontrolle des Eintritts und Austritts in die Zone verwendet werden sollen. In der Liste "Türen in der Zone" sind alle verfügbaren Türen, d.h. Controller bzw. Leser die für die Anti-Pass-Back-Funktion verwendet werden können, aufgelistet.

► Geben Sie im Feld "Zone" die Bezeichnung für die Zone ein.
► Markieren Sie das Optionsfeld "Komfortmodus", wenn Sie diesen Modus für die Zone aktivieren möchten (Erklärung siehe vorige Seite).
► Ziehen Sie mit der Maus eine Tür aus der Liste in das Feld "Eintritt in die Zone", um diese Tür als Eintritts-kontrolle in die Zone zu verwenden.
► Wiederholen Sie diesen Schritt mit dem Feld "Austritt aus der Zone", um eine Tür als Austrittskontrolle zu verwenden.

► Um eine Tür wieder vom Eintritts- bzw. Austrittsfeld zu entfernen ziehen Sie diese mit der Maus zurück in die Türliste links.

► Um die Einstellungen zu speichern klicken Sie auf "Speichern".

  ○ Sie gelangen zurück in die Einstellungsseite für die Anti-Pass-Back-Funktion und die Zonenliste wird entsprechend aktualisiert.

Anti-Pass-Back-Funktion neutralisieren und zurücksetzen

Für jede Zone kann der Anti-Pass-Back-Status getrennt neutralisiert werden oder es kann der Status für alle Türen im System zurückgesetzt werden. Dadurch ist es dann für alle Personen an Türen der gewählten Zone oder an allen Türen im System möglich eine Bewegung in eine beliebige Richtung zu machen. Durch eine erstellte Buchung wird der Anti-Pass-Back-Status der Person entsprechend gesetzt und in weiterer Folge auch wieder geprüft.

► Markieren Sie eine Zone und wählen Sie das Symbol "Neutralisieren", um die Anti-Pass-Back-Status für alle Personen an den Türen der gewählten Zone zu neutralisieren.

► Markieren Sie eine Zone und wählen Sie das Symbol "Alle zurücksetzen", um den Anti-Pass-Back-Status für alle Personen an allen Türen des Systems zu neutralisieren.

Möchten Sie den Anti-Pass-Back-Status einer einzelnen Person oder Türe zurücksetzen, so erfolgt dies durch eine Beladung aus der Zutrittskontrollsoftware.

4.4 Einstellungsseite "Einstellungen"

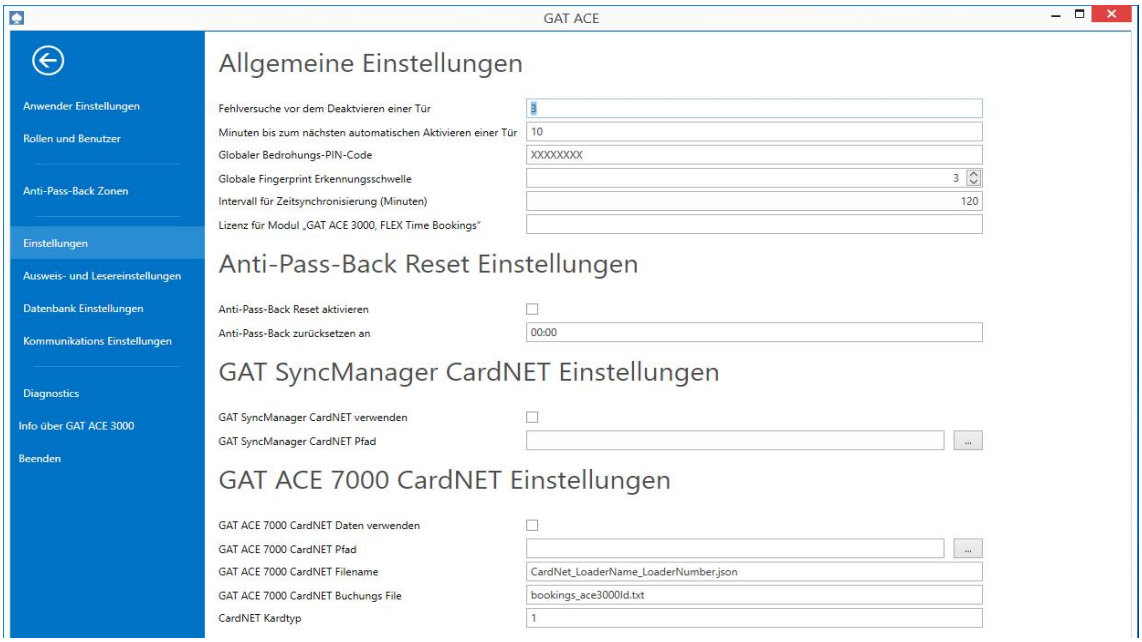


Bild 4.7 *- Programmeinstellungen - Allgemeine Einstellungen*

Auf dieser Einstellungsseite können generelle Zeit- und Timeouteinstellungen erfolgen.

- Fehlversuche vor dem Deaktivieren einer Tür:

  Dieser Wert legt fest, wie oft GAT ACE im Fehlerfall versucht, die Verbindung zu einer Tür (d.h. mit dem Controller, der die Tür kontrolliert), die eigentlich aktiviert und erreichbar sein sollte, herzustellen. Nach der eingestellten Anzahl Fehlversuchen wird die Tür deaktiviert. Dadurch wird verhindert, dass die Kommunikation verzögert wird und die Systemperformance sinkt.

- Minuten bis zum nächsten automatischen Aktivieren einer Tür:

  Dieser Wert legt die Wartezeit (in Minuten) nach dem deaktivieren einer Tür (siehe voriger Punkt) fest, nach der GAT ACE erneut versucht, eine Verbindung mit der Türe zu erhalten. Ist die Verbindung möglich, wird die Tür wieder aktiviert.

- Globaler Bedrohungs-PIN-Code:

  Hier kann ein Bedrohungs-PIN-Code eingetragen werden, der für alle Personen bei allen Controllern der Zutrittskontrollanlage gültig ist. Bei jedem Controller kann auch ein individueller Bedrohungs-PIN-Code definiert werden, der dann Vorrang vor dem globalen Bedrohungs-PIN-Code hat.
  Im Bedrohungs-PIN-Code werden nur für einige Stellen des Codes, die an diesen Stellen einzugebenden Zahlen definiert. Die restlichen Stellen werden mit "X" angegeben. An diesen Stellen muss die jeweilige Stelle des persönlichen PIN-Codes eingegeben werden.

  Beispiel:

  X X 1 X X X X 0 ← Bedrohungs PIN-Code
  - - - 2 4 8 8 2 ← persönlicher PIN-Code
  - - 1 2 4 4 8 0 ← PIN-Code, der eingegeben werden muss, um den Bedrohungs-Alarm auszulösen.

Es ist darauf zu achten, dass für Personen der persönliche PIN-Code nicht gleich dem Bedrohungs-PIN-Code ist, da in diesem Fall bei jeder gültigen Eingabe des PIN-Codes ein Bedrohungsalarm ausgelöst würde.
Der Bedrohungs PIN-Code kann nur dann eingegeben werden, wenn auch für den normalen Zutritt eine PIN-Code Eingabe erforderlich ist.

- Globale Fingerprint Erkennungsschwelle:

  Geben Sie hier die global zu verwendende Toleranzschwelle für die Fingerabdruck-leser ein. Dieser Wert wird standardmäßig für alle Controller mit Fingerabdruckleser verwendet, kann aber bei der Konfiguration der einzelnen Controller auch individuell eingegeben werden.
  Die Erkennungsschwelle definiert für einen Fingerabdruckleser wie genau die gelesenen Fingerabdrücke mit den gespeicherten Daten übereinstimmen müssen. Niedrigere Werte bedeuten hier, dass die Überprüfung der Fingerabdrücke anhand von weniger Merkmalen und mit höherer Toleranz erfolgt, wodurch die Fingerabdrücke häufiger akzeptiert werden. Höherer Werte bedeuten, dass die gelesenen Finger-abdrücke exakter mit den gespeicherten Fingerabdrücken übereinstimmen müssen, was die Sicherheit erhöht, aber öfters zu Abweisungen und dadurch in mehrfachem Auflegen der Finger resultieren kann. Die Erkennungsschwelle sollte passend den Sicherheitsbedürfnissen gewählt werden. Der Standardwert ist 3.

- Intervall für Zeitsynchronisierung (Minuten):

  Hier kann ein Zeitintervall eingegeben werden, zu dem regelmäßig die Uhrzeit der Controller durch den PC synchronisiert werden soll.

- Lizenz für Modul "GAT ACE 3000 FLEX Time Bookings":

  Um in GAT ACE die Funktion zur Behandlung von Zeitbuchungen der GANTNER Zeiterfassungsterminals zu verwenden, benötigen Sie den Lizenzcode für das "FLEX Time Booking" Modul (Einstellungen siehe "4.8. Einstellungsseite "Exporteinstellungen der Zeitbuchungen""). Geben Sie den Lizenzcode hier ein.

- Anti-Pass-Back Reset aktivieren:

  Wenn diese Option markiert ist, wird der Anti-Pass-Back Status automatisch an den eingestellten Zeiten (siehe nächster Punkt) zurückgesetzt, was den Personen den Eintritt und Austritt ermöglicht. Für Hinweise zur Anti-Pass-Back Funktion siehe "4.3. Einstellungsseite "Anti-Pass-Back Zonen"".

- Anti-Pass-Back zurücksetzen an:

  Wenn der automatische Reset der Anti-Pass-Back-Funktion aktiviert ist (siehe vorige Option) dann kann hier die Uhrzeit eingegeben werden, an denen täglich die Anti-Pass-Back-Status zurückgesetzt wird.

- GAT SyncManager CardNET Einstellungen:

  Ist in diesem Bereich das Optionsfeld "GAT SyncManager CardNET verwenden" aktiviert, so werden an den Zeiterfassungsgeräten GAT p.time ST380 / ST381 / ST390 / ST380 EVO / ST381 EVO und ST390 EVO Zutrittsberechtigungen für Offline-Schlösser im CardNET Mode auf die Datenträger geschrieben, die an den Geräten gelesen werden. Die Einstellungen, bei welchen Buchungen die Berechtigungen auf den Datenträgern verändert werden, kann in der Konfiguration der Zeiterfassungsgeräte festgelegt werden. So können zum Beispiel bei Kommen Buchungen die Berechtigungen erteilt und bei Gehen Buchungen die Berechtigungen gelöscht werden.
  Im Feld „GAT SyncManager CardNET Pfad“ kann der Ordner für den Datenaustausch gewählt werden. In diesem Ordner werden von der GAT ACE 3000 die Berechtigungsdaten

in der Datei "cardnet.dat" zur Verfügung gestellt. Der GAT SyncManager stellt in diesem Ordner Buchungsdaten zur Verfügung, die von GAT ACE 3000 periodisch im Minutenintervall übernommen werden. Die Datei für die Buchungen muss die Bezeichnung "accessbookings.exp" haben. Durch die Übernahme der Buchungen können Veränderungen der Berechtigungen auf Ausweisen sowie Batteriewarnungen in der GAT ACE 3000 und GAT Matrix nachvollzogen werden.
HINWEIS! Achten Sie beim Einrichten der Systeme darauf, dass im ausgewählten Ordner sowohl die GAT ACE 3000 als auch der GAT SyncManager Schreib- und Leserechte haben, damit die Funktion korrekt gegeben ist! Beachten Sie, dass die Schreib- und Leserechte für die beiden Programme für den Benutzer, unter dem sie ausgeführt werden (z. B. Networkservice), vorhanden sein müssen!

- GAT ACE 7000 CardNET Einstellungen:

Diese Einstellungen haben die selbe Funktion wie die vorher beschriebenen "GAT SyncManager CardNET Einstellungen", mit dem Unterschied dass hier GAT ACE 7000 und nicht die GAT SyncManager Software für die Verarbeitung der Offlinedaten (Berechtigungsdaten für Benutzerdatenträger und Offline-Buchungen) verwendet wird.
Mit dem Optionsfeld "GAT ACE 7000 CardNET Daten verwenden" können Sie diese Funktion ein- und ausschalten.
Im Feld "GAT ACE 7000 CardNET Pfad" wählen Sie den Ordner, in dem die Dateien mit den Offline-Berechtigungsdaten und Buchungen gespeichert werden sollen.
HINWEIS! Achten Sie beim Einrichten der Systeme darauf, dass im ausgewählten Ordner sowohl die GAT ACE 3000 als auch die GAT ACE 7000 Schreib- und Leserechte haben, damit die Funktion korrekt gegeben ist! Beachten Sie, dass die Schreib- und Leserechte für die beiden Programme für den Benutzer, unter dem sie ausgeführt werden (z. B. Networkservice), vorhanden sein müssen.
In den Feldern "GAT ACE 7000 CardNET Filename" and "GAT ACE 7000 CardNET Buchungs File" können Sie die Namen der Dateien eingeben, in denen die Offline-Berechtigungen und Buchungen gespeichert werden.
Im Feld "CardNET Card Type" geben Sie die Nummer des Kartentyps ein, der für die CardNET Funktion verwendet werden soll. GAT ACE 7000 kann verschiedene Kartentypen verwalten aber GAT ACE 3000 und CardNET können nur einen Kartentyp verwenden. Mehr Informationen zu den Kartentypen finden Sie im GAT ACE 7000 Handbuch.

4.5 Einstellungsseite "Ausweis- und Lesereinstellungen"

In dieser Einstellungsseite legen Sie die Einstellungen für die, in der Anlage verwendeten Datenträger und die dazu passenden Einstellungen für die Leser, fest. Dazu gehören die grundlegenden Datenstrukturen, Anlagennummern, etc.. Die Einstellungen in der Konfiguration eines Lesers müssen mit den, an diesem Leser verwendeten Datenträger übereinstimmen, damit die Datenträger verwendet werden können.

Da in einer Anlage teilweise verschiedene Datenträger verwendet werden, ist es möglich, mehrere Konfigurationen zu erstellen.

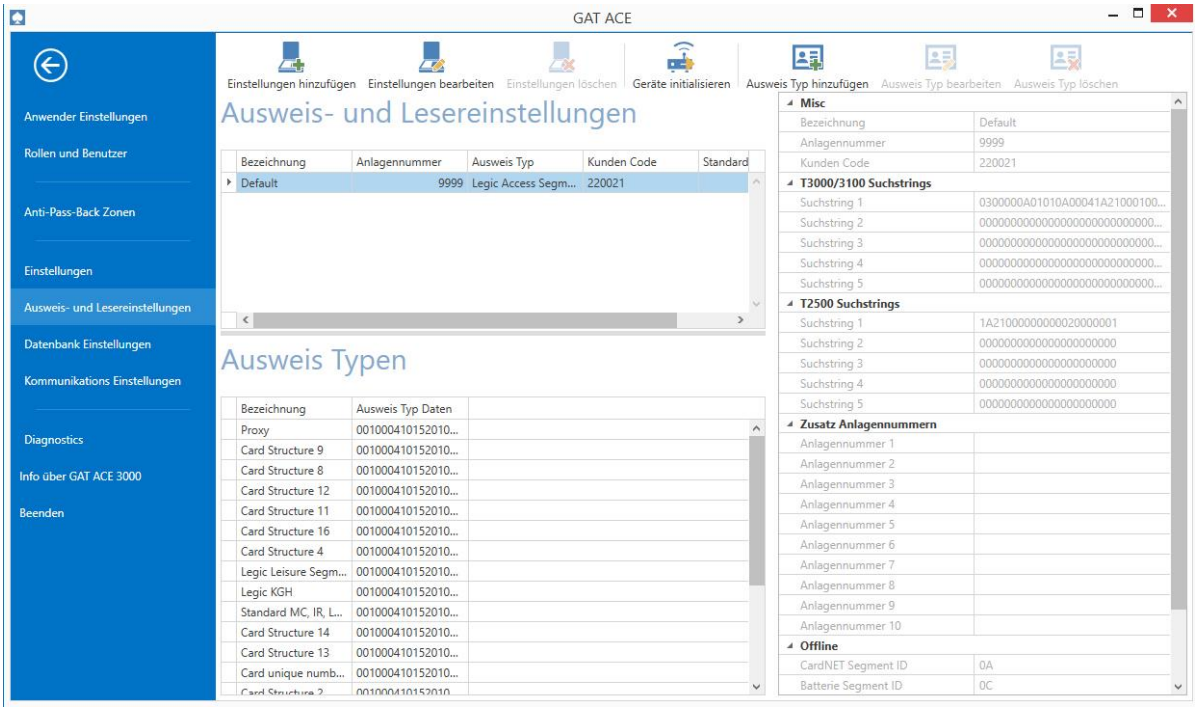


Bild 4.8 *- Programmeinstellungen - Ausweiseinstellungen*

Diese Einstellungsseite ist in 3 Bereiche eingeteilt.

Im Bereich "Ausweis- und Lesereinstellungen" werden unterschiedliche Ausweise und die dazu gehörigen Leserkonfigurationen verwaltet. Üblicherweise sind in einer Anlage nicht mehrere unterschiedliche Ausweiseinstellungen erforderlich. Sind jedoch Ausweise aus unterschiedlichen Generationen oder Technologien in Verwendung (z. B. bei zusätzlichem Einsatz von Longrange Tags), können diese hier erfasst werden. Es empfiehlt sich, die Einstellungen gleich nach der Installation der GAT ACE und vor der Definition von Controllern richtig festzulegen. Dadurch werden die Einstellungen wenn möglich, bereits automatisch auf die Leser übernommen.

Im rechten Bereich werden die Details der ausgewählten Ausweis Einstellung angezeigt.

Im Bereich "Ausweis Typen" sind bereits einige Arten von Technologien und speziellen Ausweis Codierungen definiert. Sollte die von Ihnen verwendete Technologie oder Codierung noch nicht verfügbar sein, kann diese als kundenspezifischer Kartentyp angelegt werden.

Näheres zu diesen Bereichen und wie die Leserkonfigurationen bearbeitet werden finden Sie auf den folgenden Seiten.

Ausweis Einstellungen

► Um eine neue Konfiguration für die Leser anzulegen klicken Sie auf das Symbol "Einstellungen hinzufügen".
  ○ Das Fenster "Ausweis und Lesereinstellungen" wird geöffnet (weiter nach dem nächsten Schritt).

► Um eine bestehende Konfiguration zu bearbeiten markieren Sie die Konfiguration in der Liste und wählen Sie "Ausweis Einstellungen bearbeiten".
  ○ Das Fenster "Ausweis und Lesereinstellungen" wird geöffnet.

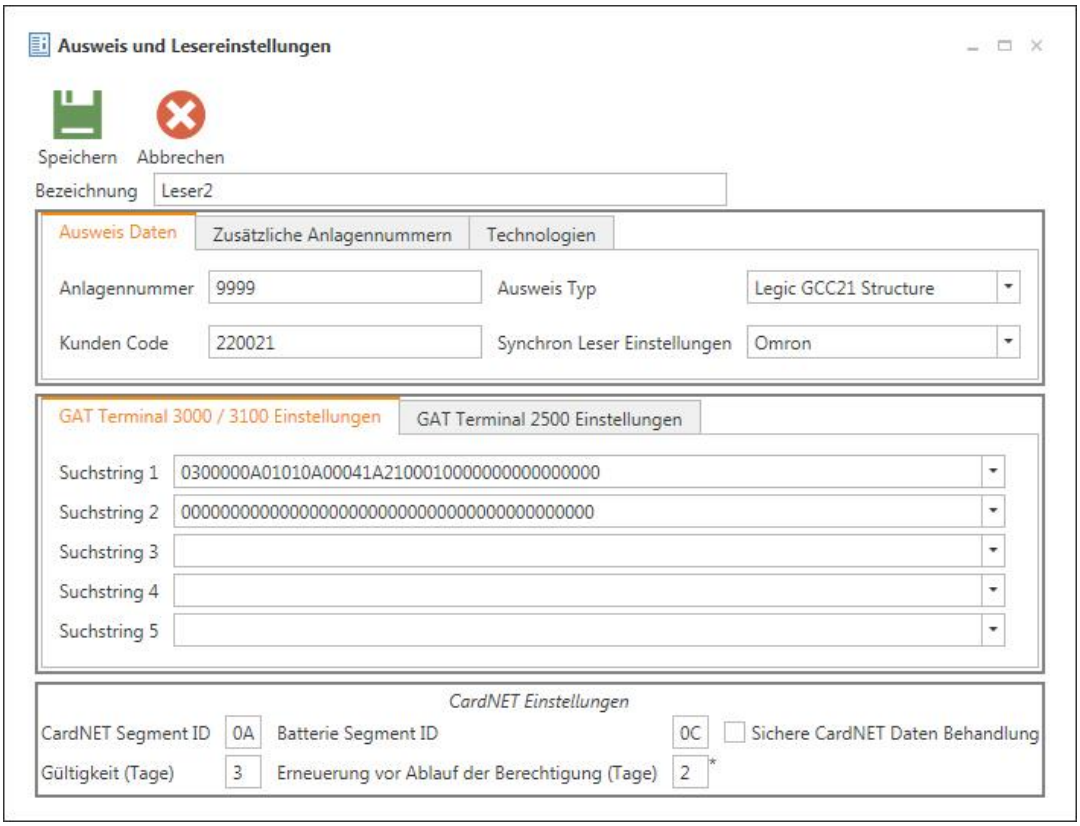


Bild 4.9 *- Programmeinstellungen - Ausweis- und Lesereinstellungen*

► Geben Sie eine eindeutige Bezeichnung für die Ausweise ein.
  ○ Unter diesem Namen kann diese Leserkonfiguration bei der Controller-Konfiguration ausgewählt und den Lesern zugewiesen werden.

► Legen Sie im oberen Bereich "Ausweis Daten" die folgenden Informationen fest.

- Anlagennummer: Die Anlagennummer (FID) ist eine eindeutige Nummer für Ihre Ausweiscodierung. Bei einigen Ausweis Typen ist keine Anlagennummer verfügbar. Lassen Sie in diesem Fall den Default Wert 9999.
  Für andere Ausweis Typen, die eine solche Anlagennummer haben, muss der korrekte Wert eingestellt werden. Dadurch wird sichergestellt, dass Fremddatenträger in ihrer Anlage keinen Zutritt erlangen können! Ihre Anlagennummer finden Sie auf den Auftragspapieren bei der Ausweislieferung oder sie bekommen sie von Ihrem Errichter genannt.
- Ausweis Typ: Wählen Sie aus der vordefinierten Liste von Ausweistypen den in Ihrer Anlage verwendete Typ von Ausweis. Ist dieser noch nicht vorhanden, kann dieser unter Ausweis Typen als kundenspezifischer Typ angelegt werden (siehe weiter unten).

- Kunden Code: Der Kunden Code gibt Auskunft über die Codierung von Ausweisen und lautet für Standard Codierungen von GANTNER Datenträgern "220021“. Sollten Sie speziell codierte Ausweise verwenden, nennt Ihnen Ihr Errichter den passenden Kunden Code.

- Reader Synchro Mode: Hier können Sie den Mode (d.h. Art der Schnittstelle) wählen, wenn der Leser im synchronen Modus betrieben wird (Omron oder Wiegand).

► Auf der Registerkarte "Zusätzliche Anlagennummern" im oberen Bereich können Sie weitere Anlagennummern eintragen. Dies ist nur dann erforderlich, wenn Sie ganz bewusst auch Besitzer von Ausweisen anderer Firmen Zutritt zu Ihrer Anlage gewähren möchten. Voraussetzung ist, dass diese Ausweise die gleiche Codierung mit lediglich anderer Analgennummer aufweisen. Diese Funktion ist nicht bei allen Controllern möglich.

Hinweis! Um eine zusätzliche Anlagennummer aus einem Controller zu löschen reicht es nicht, nur diese Nummer im entsprechenden Feld zu löschen. Geben Sie deshalb zuerst in das zu löschende Feld "0000" ein. Danach initialisieren Sie den Controller neu. Dadurch wird diese zusätzliche Anlagennummer im Controller gelöscht. Erst jetzt können Sie das Feld "0" in diesem Fenster ganz löschen.

► Auf der Registerkarte "Technologien" im oberen Bereich könne Sie die RFID Technologien markieren, die der Leser unterstützen soll. Beachten Sie, dass diese Einstellungen nur für die Leser vom Typ GAT SR 73xx and GAT SLR 73xx und nicht für die GAT SR 3xx und GAT SLR 3xx Leser beachtet wird.

► Im Bereich "GAT Terminal 3000 / 3100 Einstellungen" und „GAT Terminal 2500 Einstellungen“ werden die Suchstrings eingegeben, die vom Controller zum Lesen der Datenträger benötigt werden. Es gibt hier vordefinierte Vorgaben, die Sie auswählen können. Die Einstellungen müssen nur die Controller eingetragen werden, die in Ihrer Anlage auch verwendet werden.

► Im Bereich "CardNET Einstellungen" werden die Einstellungen für die Funktion eines CardNET Systems definiert. Dadurch ist es möglich, dass Berechtigungen auf den Ausweisen zu den Offline-Schlössern transportiert werden.

- CardNET Segment ID: Definiert die Codierung des Datenbereich in dem die Berechtigungen auf dem Ausweis gespeichert werden. Für Standard Codierungen ist dieser Wert „0A“. Sollten Sie eine andere Codierung verwenden, erfahren Sie den passenden Wert von Ihrem Errichter.

- Batterie Segment ID: Definiert die Codierung des Datenbereichs in den Informationen wie z. B. Batteriewarnungen von den Offline-Schlössern an die Online Controller zurück transportiert werden. Für Standard Codierungen ist dieser Wert „0C“. Sollten Sie eine andere Codierung verwenden, erfahren Sie den passenden Wert von Ihrem Errichter.

- Sichere CardNET Daten Behandlung:
  Ist diese Option aktiviert, muss vor dem Schreiben von CardNET Berechtigungen an einem Online Leser die Person durch Eingabe des PIN-Codes oder durch eine Biometrische Verifikation sicher stellen, dass sie der rechtmäßige Besitzer des Ausweises ist. So kann sichergestellt werden, dass verlorene Ausweise vom Finder nicht mit CardNET Berechtigungen upgedatet werden können.
  Diese Funktion kann nur dann genutzt werden, wenn die alle Online Leser die zum Aktualisieren der CardNET Berechtigungen auch eine Eingabemöglichkeit für den PIN-Code oder einen Biometrieleser eingebaut haben!

- Gültigkeit (Tage): Dieser Wert legt fest, für wie lange die CardNET Berechtigungen nach dem Schreiben gültig sind. In diesem Zusammenhang ist auch die nächste Einstellung "Erneuerung vor Ablauf der Berechtigungen (Tage)" zu beachten.
  Über diesen Wert begrenzen Sie das Risiko, das beim Verlust eines Ausweises entsteht. Es wird darum empfohlen diesen Wert klein zu halten (typisch 3 bis 7 Tage) und auf Ihre Sicherheitsanforderungen anzupassen!

- Erneuerung vor Ablauf der Berechtigungen (Tage):'

  Dieser Wert legt fest, wieviele Tage vor Ablauf der CardNET Berechtigungen (siehe vorige Einstellung) diese erneuert werden. Es ist damit möglich
  Dieser Wert soll möglichst kurz eingestellt werden um die Bedienung an den Online Lesern möglichst flüssig zu gestalten. Der Wert wird typisch auf 3 Tage eingestellt. So werden Berechtigungen die am Sonntag ablaufen würden am Freitag schon erneuert. Dadurch ist am Montag ein Zutritt an den Offline Schlössern möglich, ohne dass zuvor an einem Online Leser die Berechtigungen erneuert werden müssen. Passen Sie diesen Wert an Ihre Sicherheitsanforderungen an.
  HINWEIS! Die Gültigkeitsdauer läuft jeweils einen vollen Tag. Das bedeutet, wird die Berechtigung an einem Terminal um 8:00 Uhr auf einen Datenträger geschrieben, ist dieser bis zum nächsten Tag um 7:59 Uhr gültig. Wenn Sie aber die Einstellung "Erneuerung vor Ablauf der Berechtigung" höher als die Einstellung "Gültigkeit (Tage)" setzen (z. B. Erneuerung auf 2 und Gültigkeit auf 1) wird die Gültigkeit jedes Datenträgers bereits zu Mitternacht gelöscht. Dadurch können Sie sicherstellen, dass sich alle Benutzer an jedem Tag als Erstes an einem bestimmten Terminal identifizieren müssen (z. B. zur Zeiterfassung). An diesem Terminal werden dann die Berechtigungen auf den Datenträgern erneuert und erst dann ist ein Zutritt möglich.

► Sichern Sie die gemachten Einstellungen mit der Schaltfläche "Speichern".
  ○ Sie gelangen zurück in das Einstellungsfenster "Ausweis Einstellungen" und die bearbeitete Leserkonfiguration wird in der Liste angezeigt.

Ausweis Typen

In Feld "Ausweis Typen" werden alle bereits definierten Typen und Codierungen aufgelistet. Diese können für die Leserkonfiguration verwendet werden. Die Daten beinhaltet Informationen, die festlegen, wie und wo die Daten auf einem Datenträger gefunden und interpretiert werden können. Deshalb ist es wichtig, je nach verwendeten Datenträgern die richtigen Suchstrings bzw. Kartenstrukturen anzulegen und diese bei der Leserkonfiguration entsprechend auszuwählen.

► Um einen neuen Ausweis Typ anzulegen klicken Sie auf das Symbol "Ausweis Typ hinzufügen".
  ○ Das Fenster "Ausweis Typ" wird geöffnet (siehe nächster Punkt).
► Um eine bestehende Ausweis Typ zu ändern doppelklicken Sie auf den Eintrag in der Ausweis Typen Liste.
  ○ Das Fenster "Ausweis Typ" wird geöffnet.

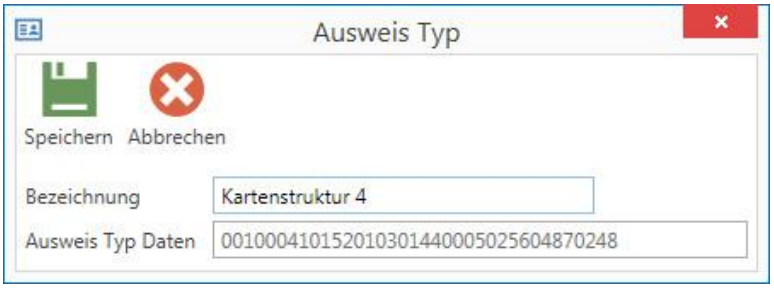


Bild 4.10 *- Ausweis Typen definieren*

► Geben Sie im Feld "Bezeichnung" die Bezeichnung des Ausweistyps ein. Unter diesem Namen kann der Ausweistyp bei der Leserkonfiguration ausgewählt werden.

► Tragen Sie im Feld "Ausweis Typ Daten" den Suchstring ein, mit dem die Daten auf den Datenträgern gefunden und ausgewertet werden. Bei kundenspezifischen Ausweisen erhalten Sie die erforderlichen Angaben von Ihrem Errichter.
Beispiele für den Suchstring für das Access Segment eines LEGIC Prime oder LEGIC Advant Datenträgers:

► Bestätigen Sie mit "Speichern".

○ Der bearbeitete Ausweis Typ wird in der Liste aktualisiert.

4.6 Einstellungsseite "Datenbankeinstellungen"

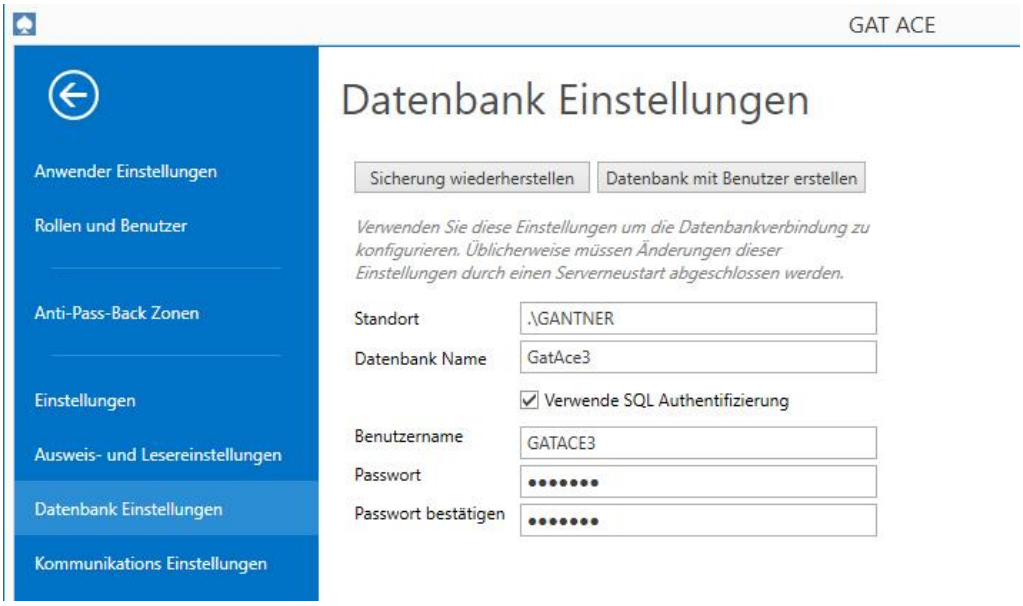


Bild 4.11 *- Programmeinstellungen - Datenbankeinstellungen*

In dieser Einstellungsseite legen Sie die Verbindungseinstellungen zur GAT ACE 3000 Datenbank fest.

- Sicherung wiederherstellen: Mit dieser Schaltfläche können Sie eine zuvor gespeicherte Sicherung der Datenbank laden und so die Datenbank auf den Stand der Sicherung wiederherstellen. Suchen Sie die Backup-Datei in dem "Öffnen"-Fenster und klicken

Sie auf "Öffnen". Im Kapitel "5.3.1. SQL Datenbanksicherung" ist beschrieben, wie Sie automatische Backups der Datenbank erstellen können.

- Datenbank mit Benutzer erstellen: Mit dieser Schaltfläche können Sie eine neue Datenbank erstellen. Wenn Sie auf die Schaltfläche klicken, werden folgende Einstellungen angezeigt:

***Bild 4.12** - Programmeinstellungen - Datenbankeinstellungen*

Um eine neue Datenbank anzulegen, geben Sie die benötigten Informationen ein (Datenbankname, Benutzername und Passwort). Alternativ können Sie auch die Standardeinstellungen, die bereits in den Feldern vorausgefüllt sind, verwenden. Wenn Sie auf "Zufällig generieren" klicken, werden diese Informationen aus Zufallswerten neu generiert. Wenn Sie auf "Erstellen" klicken, wird die neue Datenbank erstellt.

- Standort: Ort (Rechner und Datenbankinstanz) an dem sich die Datenbank von GAT ACE befindet. Bei lokalen Installationen (GAT ACE Client und GAT ACE 3000 Dienst auf dem selben PC) kann für den Standort ein "." gefolgt von dem Datenbanknamen eingegeben werden (Beispiel: "`.\Gantner`").
- Datenbank Name: Die beim Erstellen der Datenbank festgelegte Bezeichnung der Datenbank.
- Verwende SQL-Authentifizierung: Auswahl, ob zur Verbindung mit der Datenbank die Windows Authentifizierung des Benutzers oder die SQL Authentifizierung (mit Benutzername und Passwort) verwendet werden soll.

HINWEIS! Eine genaue Beschreibung der Datenbankeinstellungen finden Sie im Abschnitt "3.1.2 Datenbankeinstellungen".

4.7 Einstellungsseite "Kommunikations Einstellungen"

Bild 4.13 *- Programmeinstellungen - Kommunikationseinstellungen (Allgemeine Eigenschaften)*

Die Kommunikationseinstellungen legen die Parameter für die Kommunikation des GAT ACE Clients (grafischer Benutzeroberfläche) mit dem GAT ACE 3000 Dienst fest.

HINWEIS! Bei Installation von GAT ACE Client und dem GAT ACE 3000 Dienst auf demselben PC sind für eine funktionierende Kommunikation zwischen diesen beiden Komponenten keine Änderungen an den Standardeinstellungen notwendig. Ansonsten können Sie hier die entsprechenden Kommunikationsparameter ändern.

Bei notwendigen Änderungen:

► Wählen Sie in der linken Spalte den Eintrag das entsprechende Interface (z. B. "GatAceServerInterface").
  ○ Die möglichen Kommunikationseinstellungen werden auf der rechten Seite angezeigt.

► Legen Sie in der Registerkarte "Allgemeine Eigenschaften" die entsprechenden Werte und Optionsfeld-markierungen fest. Wichtige Einstellungen sind:

- RemoteLocation: Netzwerkname oder IP-Adresse des Rechners, auf dem der GAT ACE 3000 Dienst installiert ist. Befindet sich der GAT ACE Client und der GAT ACE 3000 Dienst auf demselben PC geben Sie "localhost" ein.
- PortNumber: Portnummer für die Kommunikation (Standard 8300)
- ResponseTimeout: Zeit (in Millisekunden), die zwischen Anfrage und Antwort gewartet wird. Wenn in dieser Zeit keine Antwort empfangen wird, wird eine Fehlermeldung angezeigt.
- MustLogin: Standardmäßig gesetzt. Wenn aktiv dann ist für die Kommunikation zwischen GAT ACE Client und GAT ACE 3000 Dienst ein Passwort notwendig
- Password: Das benötigte Passwort für die Kommunikation zwischen GAT ACE Client und GAT ACE 3000 Dienst, falls die Option "MustLogin" markiert ist. Dieses sollte auf dem Standard-Passwort belassen werden. Ansonsten müssen Sie dieses auch in dem GAT ACE 3000 Dienst ändern.

HINWEIS! Es können nur die Felder mit schwarzer Bezeichnung geändert werden. Die grau dargestellten Felder sind nicht änderbar und dienen nur der Informationsanzeige.

► Auf der Registerkarte "Verfügbare Kommandos" können die Kommandos markiert werden, die GAT ACE verarbeiten soll. Standardmäßig sind alle Kommandos markiert.

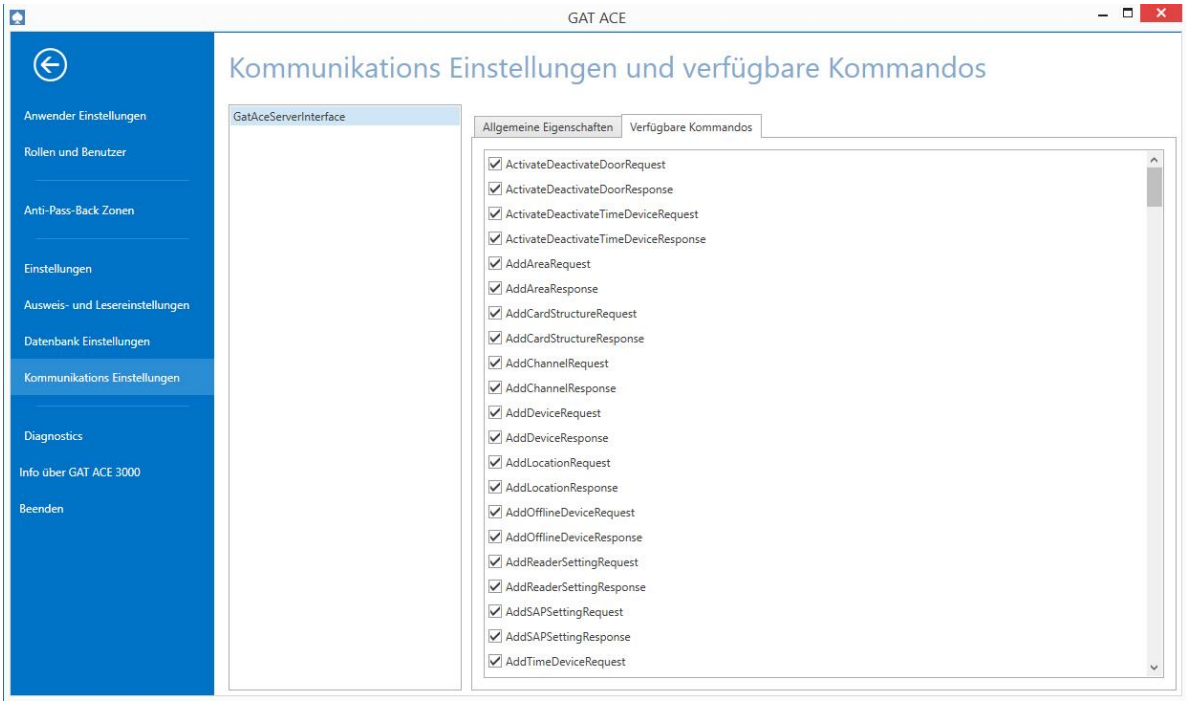


***Bild 4.14** - Programmeinstellungen - Kommunikationseinstellungen (Verfügbare Kommandos)*

4.8 Einstellungsseite "Exporteinstellungen der Zeitbuchungen"

Figure 4.15 *- Programmeinstellungen - Exporteinstellungen für Zeitbuchungen*

Wenn Zeiterfassungsterminals in Ihrem System vorhanden sind (z. B. GAT Terminal 1015 oder GAT Terminal 1032), kann GAT ACE die Zeitbuchungen dieser Terminals lesen und verarbeiten, sofern das entsprechende Lizenzmodul aktiviert ist (siehe "4.4. Einstellungsseite "Einstellungen""). Die Einstellungen für die Zeitbuchungen können hier eingestellt werden.

► Legen Sie folgende Einstellungen fest:

- Pfad für Zeitbuchungsexport: Klicken Sie auf die Schaltfläche "…" und wählen Sie den Pfad, wo die Zeitbuchungen exportiert werden sollen. Die Textdateien mit den Buchungen werden in diesem Verzeichnis generiert.
- Format für Zeitbuchungsexport: Wählen Sie das Format für die Zeitbuchungen.
  "Flex" nutzt das selbe Format wie die GAT Manager Software, was diese Buchungen rückwärtskompatibel zu älteren Installationen macht.
  "SAP" sichert die Buchungen in SAP kompatiblem Format.
- Leere Buchungsdatei erstellen: Wenn diese Option gewählt ist, wird für den Fall, dass keine Buchungen vorhanden sind, eine leere Datei erstellt. Ist die Option nicht gewählt, wird in diesem Fall keine Datei erstellt.
- Letzte fortlaufende Buchungsnummer: Die Buchungen erhalten eine fortlaufende ID. Werden nun Buchungen exportiert, wird die ID der zuletzt exportierten Buchung gespeichert. Beim nächsten Export werden nur neuer Buchungen exportiert. Sollen auch ältere Buchungen noch einmal exportiert werden, kann dieser Wert auf die gewünschte ID gesetzt werden und alle folgenden ID's bis zur neuesten Buchung werden exportiert.
- Zeitintervall für Zeitbuchungsexport: Hier können Sie ein Zeitintervall in Minuten eingeben, wenn die Buchungen automatisch exportiert werden sollen. Mit "0" wird die automatische Funktion deaktiviert.
- Datenträger im SAP Format: SAP kann nur max. 8-stellige Ausweisnummern verwalten. Ausweise mit längeren Ausweisnummern (z. B. Proxy Ausweise oder UID's) müssen somit umgewandelte werden. Hier kann eine Datei ausgewählt

werden, in dem die SAP Ausweisnummer und die Gantner Ausweisnummer für jeden Ausweis eingetragen werden. Dadurch werden die Nummern automatisch ausgetauscht. Hinweis: es kann die selbe Datei (selbes Format) wie bei dem SAP Interface CC1 für GAT Manager verwendet werden.
Die Konvertierungen können auch direkt in dieser Seite in der unteren Tabelle angegeben werden (kein Konvertierungsfile notwendig).

- Sekunden in den SAP Buchungen anzeigen:
  Da SAP keine Sekunden in den Buchungen verwalten kann, kann hier diese Option deaktivert werden, um die Sekunden automatisch auf 00 zu setzen. Wird eine andere Zeiterfassungslösung vewendet, die ebenfalls SAP Format verwendet aber Sekunden verwalten kann, können Sie diese Option markieren, um die Sekunden zu verwenden.

► Falls Sie die SAP Buchungstyp wählen fügen Sie die SAP Konvertierungseinsetllungen im Listenfeld unten ein. Dazu klicken Sie auf "SAP Konvertierungstabelle hinzufügen" und wählen Sie den SAP Einstellungstyp ("Buchungscode" or "Ausweis") und geben Sie die zusammengehörigen Flex und SAP Werte ein. Mit "Ausweis" können Sie die Konvertierung zwischen SAP und Gantner Kartennummer eingeben, und brauchen kein Konvertierungsfile.

► Klicken Sie "Sichern" und die Änderugen zu speichern.

4.9 Einstellungsseite "Diagnostics"

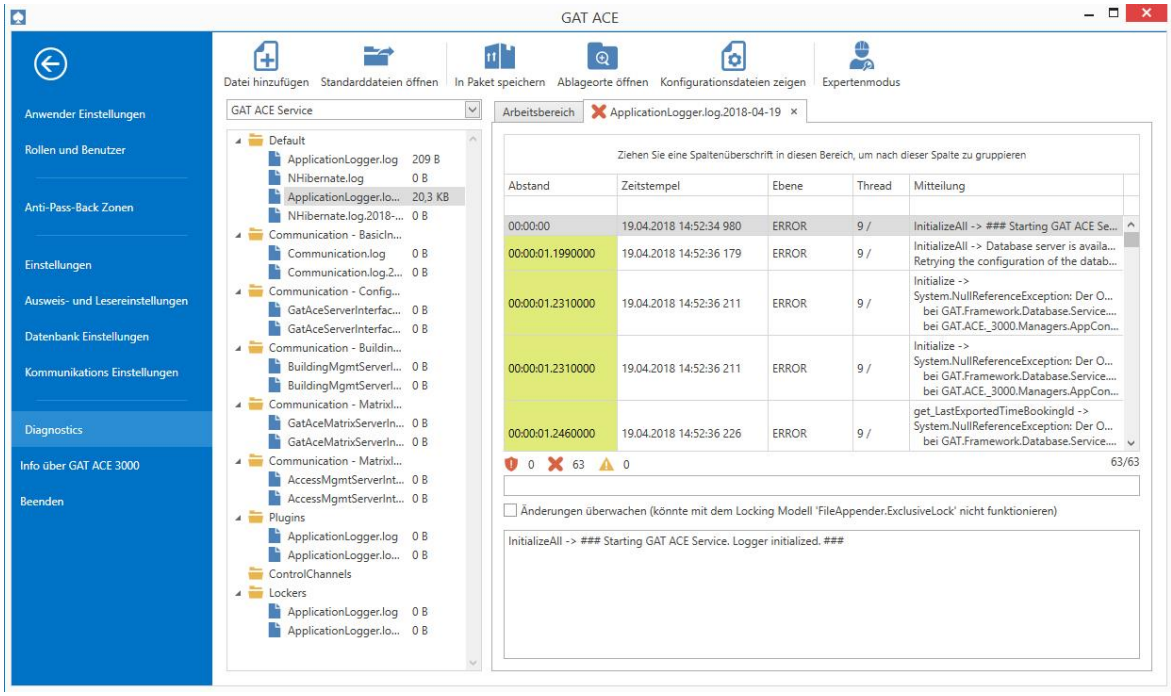


Bild 4.16 *- Programmeinstellungen - Diagnose*

GAT ACE zeichnet alle wichtigen Ereignisse und Aktionen in Log-Dateien auf. In der Einstellungsseite "Diagnostics" haben Sie die Möglichkeit, diese Log-Dateien auszuwerten oder diese auch, falls notwendig, in ein Packet zu speichern und an GANTNER Electronic oder Ihren Partner für weitere Auswertungen zu senden.

- ► Wählen Sie in dem linken oberen Feld eine "Sammlung" aus ("GAT ACE 3000" für die Log-Dateien des Dienstes und "GAT ACE" für die Log-Dateien der Benutzeroberfläche).
  - ○ In der Liste darunter werden alle Log-Dateien, die in dieser Sammlung enthalten sind, aufgelistet
- ► Doppelklicken Sie auf eine Log-Datei in der linken Liste.
  - ○ Die Einträge der Log-Datei werden im rechten Feld angezeigt. Wenn mehrere Log-Dateien geöffnet werden, sind diese über Reiter auswählbar.
- ► Klicken Sie mit der rechten Maustaste auf einen Log-Datei-Eintrag.
  - ○ Es öffnet sich ein Pop-Up Fenster mit verschiedenen Einstellmöglichkeiten.

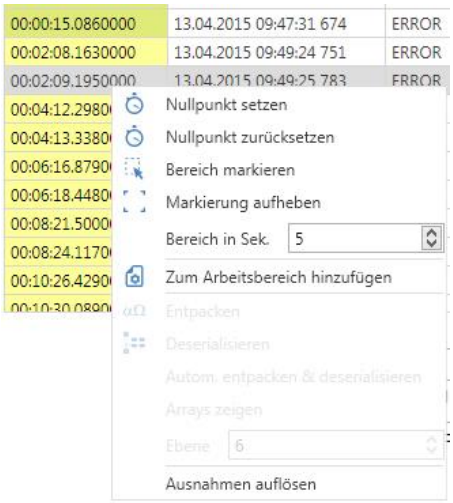


Bild 4.17 *- Programmeinstellungen - Diagnoseeinstellungen*

- ► Mit den Aktionen in diesem Menü können Sie die Anzeige der Log-Datei zeitlich filtern und den Zeit-Bezugspunkt (=grüne Markierung in den Log-Einträgen), von dem aus die Zeiten der Log-Einträge gerechnet werden, neu setzen.
- ► Um alle häufig benutzten Log-Dateien auf einmal zu öffnen klicken Sie auf das Symbol "Standarddateien öffnen" in der Multifunktionsleiste.
- ► Möchten Sie Log-Dateien zur Auswertung an eine bestimmte Stelle senden, können Sie diese mit dem Symbol "In Paket speichern" in eine ZIP-Datei komprimieren und direkt via Mail versenden. Nach Auswahl dieses Menüpunktes können Sie wählen, ob nur die in der Log-Liste angezeigten Dateien oder alle Dateien versendet werden sollen.
- ► Das Symbol "Ablageorte öffnen" öffnet den Windows Dateimanager und die Ordner, in denen sich die Log-Dateien befinden.
- ► Bei einigen Log-Dateien (z. B. "Communication - ConfiguratorInerface" und "Communication - MatrixInterface" werden die Logeinträge in gepackter Form gesendet. Um diese lesen zu können, können Sie den Expertmodus verwenden. Hierfür ist aus Sicherheitsgründen ein Passwort erforderlich.

5 BEDIENUNG

In diesem Kapitel finden Sie einen Funktionsüberblick sowie die detailliere Beschreibung der einzelnen Funktionen von GAT ACE.

5.1 Funktionsübersicht von GAT ACE

Dieser Abschnitt gibt einen Überblick über die wichtigsten Funktionen von GAT ACE.

Nach dem Start von GAT ACE muss sich der Benutzer mit Benutzername und Passwort einloggen (siehe "3.1.3. Anmeldebildschirm"). In GAT ACE sind Standardbenutzer mit bestimmten Passwörtern und Nutzerrollen (siehe "6.3.1. Standard-Benutzer") angelegt. Die einem Benutzer zugewiesene Rolle bestimmt, welche Funktionen der Benutzer in GAT ACE ausführen darf. In diesem Kapitel wird die Bedienung für den SYSTEM Benutzer beschrieben, der alle Funktionen ausführen darf.

Nach der erfolgreichen Anmeldung mittels Benutzername und Passwort wird der Hauptbildschirm von GAT ACE angezeigt. Dieser ist in verschiedene Bereiche eingeteilt.

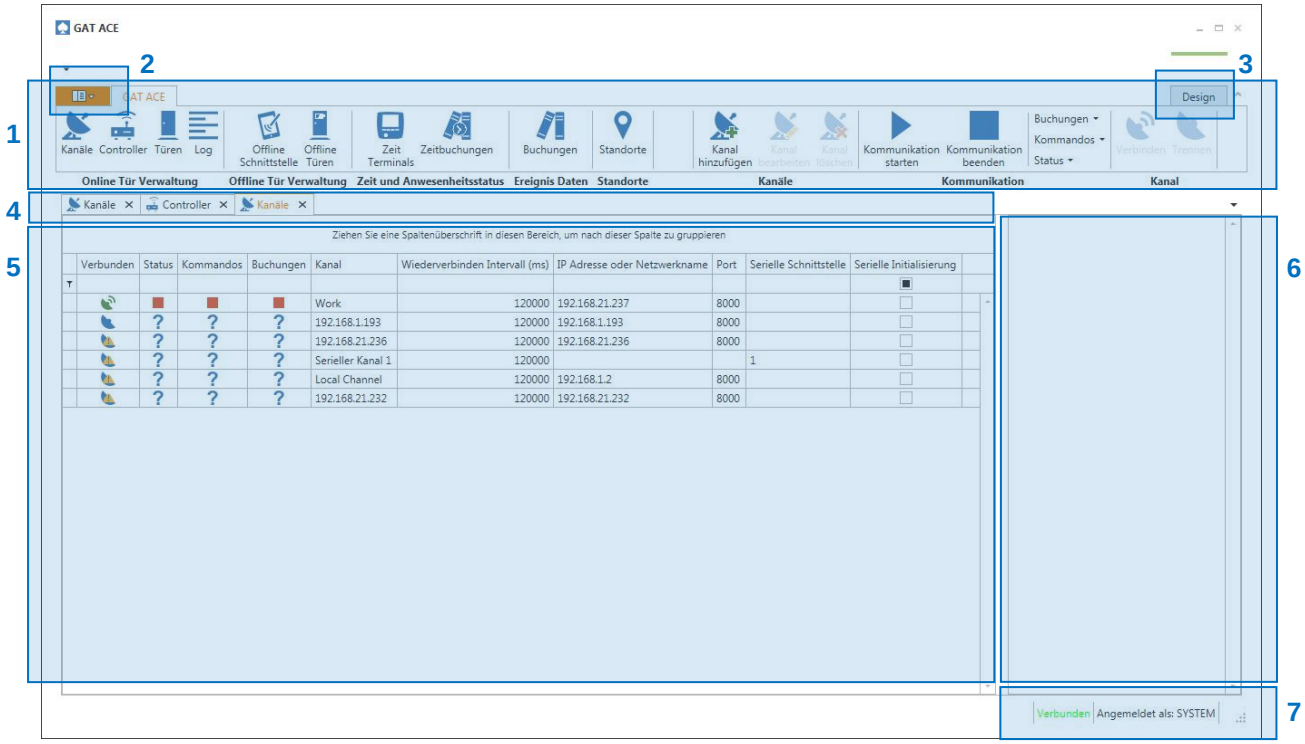


Bild 5.1 *- GAT ACE - Hauptbildschirm*

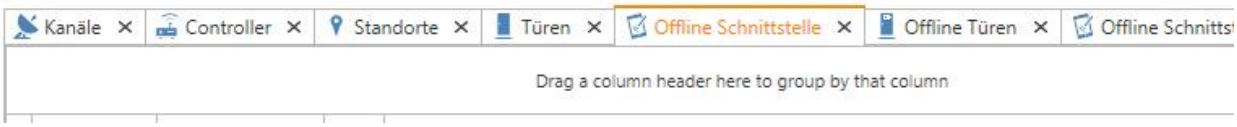
1 Multifunktionsleiste: In der linken Hälfte dieser Leiste finden Sie die Symbole, mit denen Sie auf die verschiedenen Ansichten in GAT ACE (siehe Punkt 4 weiter unten) Zugriff haben. Ein Klick auf eins dieser Symbole öffnet die entsprechende Ansicht. Die Symbole in der rechten Hälfte der Multifunktionsleiste zeigen alle Funktionen, die in der aktuell gewählten Ansicht verfügbar sind.

2	Programmeinstellungen:	Mit diesem Symbol gelangen Sie zur Liste der Programmeinstellungen, wo verschiedene allgemeine Einstellungen für GAT ACE definiert werden. Siehe dazu auch Kapitel "4. K".
3	Design:	Mit diesem Auswahlmenü kann das Aussehen der grafischen Oberfläche von GAT ACE geändert werden.
4	Liste der geöffneten Ansichten:	Zur Auflistung und Bearbeitung von Kanälen, Controllern, Türen, Offline-schnittstellen und -türen, Logeinträgen, Buchungen und Standorte werden in GAT ACE Ansichten verwendet. Die Ansichten werden in diesem Bereich (4) angezeigt.
5	Ansicht:	In diesem Bereich werden je nach gewählter Ansicht unterschiedliche Funk-tionen angezeigt. Dies ist der Haupt-Arbeitsbereich in GAT ACE, in dem Sie alle Konfigurationen durchführen.
6	Informationsanzeige:	Hier werden nähere Informationen zu dem Element angezeigt, das gerade in der Ansicht ausgewählt ist.
7	Statusanzeige:	Hier wird angezeigt, ob der GAT ACE Client mit dem GAT ACE 3000 Dienst verbunden ist. Nur bei Verbindung ("Connected") ist eine Kommunikation mit den Gräten/Controller möglich.

Über die Symbole, die sich in der Multifunktionsleiste in den Gruppen "Online Tür Verwaltung" und "Offline Tür Verwaltung" befinden, haben Sie Zugriff auf alle Konfigurationseinstellungen für die Controller, Türen und Leser der Anlage. Mit Klick auf diese Symbole öffnen Sie die entsprechende Ansicht unter halb der Multifunktionsleiste.

Diese Symbole in der Multifunktionsleiste öffnen die "Scheduler"-Ansicht, wo Sie wiederkehrende Aufgaben planen können, die "Buchungs"-Ansicht, wo alle Aktivitäten die von GAT ACE aufgezeichnet werden, aufgelistet sind, und die "Standorte"-Ansicht, in der Sie die Standorte für die Mandanten-fähigkeit von GAT ACE und GAT Matrix definieren können.

In GAT ACE können mehrere Ansichten gleichzeitig geöffnet sein. Sie können die gewünschte Auswahl dann über den zugehörigen Tab auswählen.



Wenn Sie einen Tab mit der Maus von der Tableiste wegziehen erscheinen Markierungen, über die sich die zugehörige Ansicht an einer anderen Stelle des GAT ACE Fensters platzieren lässt. Ziehen Sie einen Tab z. B. wie im nächsten Bild gezeigt auf den Rand der mittleren Markierung, können Sie Ansichten nebeneinander anordnen.

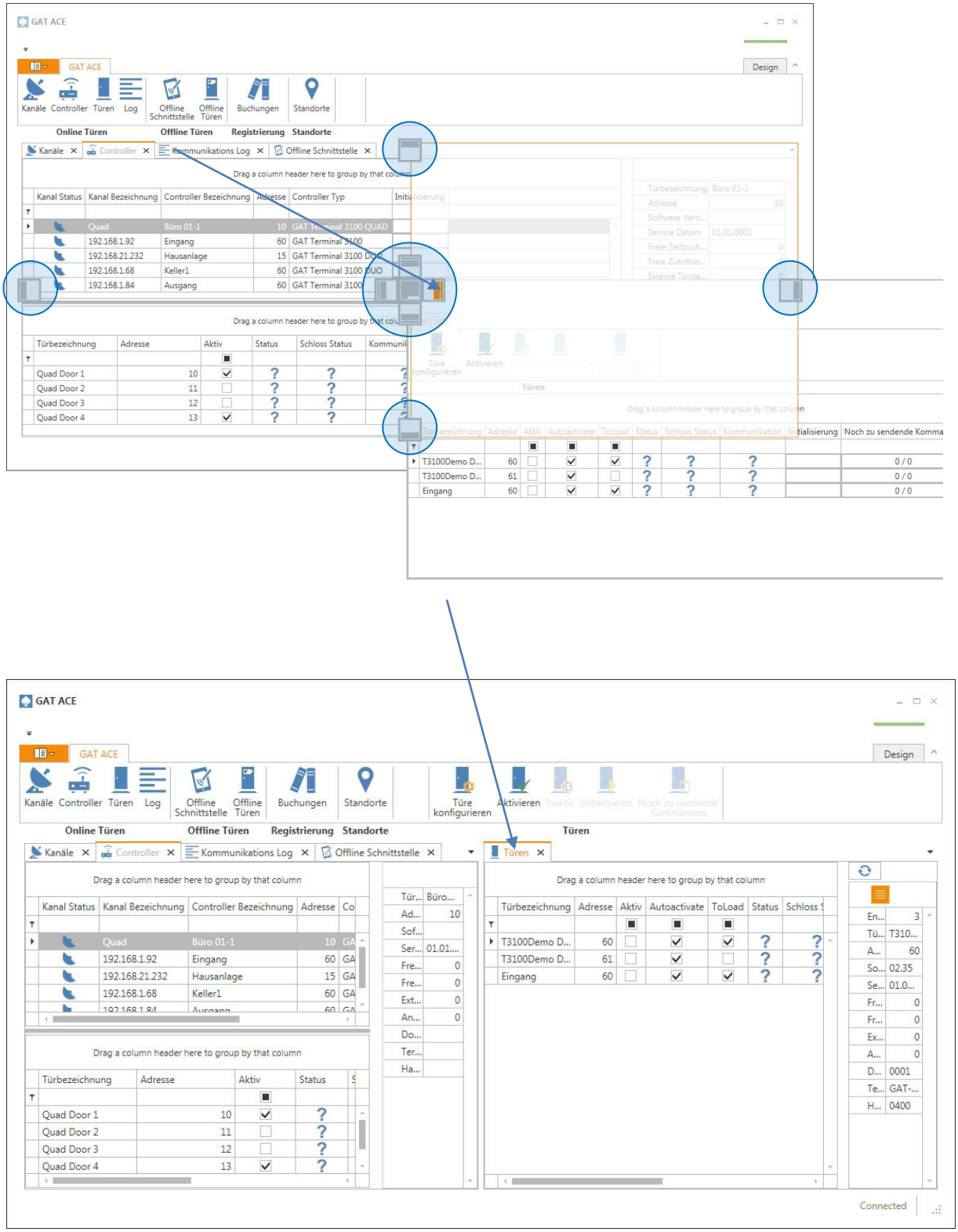


Bild 5.2 *- Anordnen von Ansichten*

5.1.1 Kommunikationskanäle

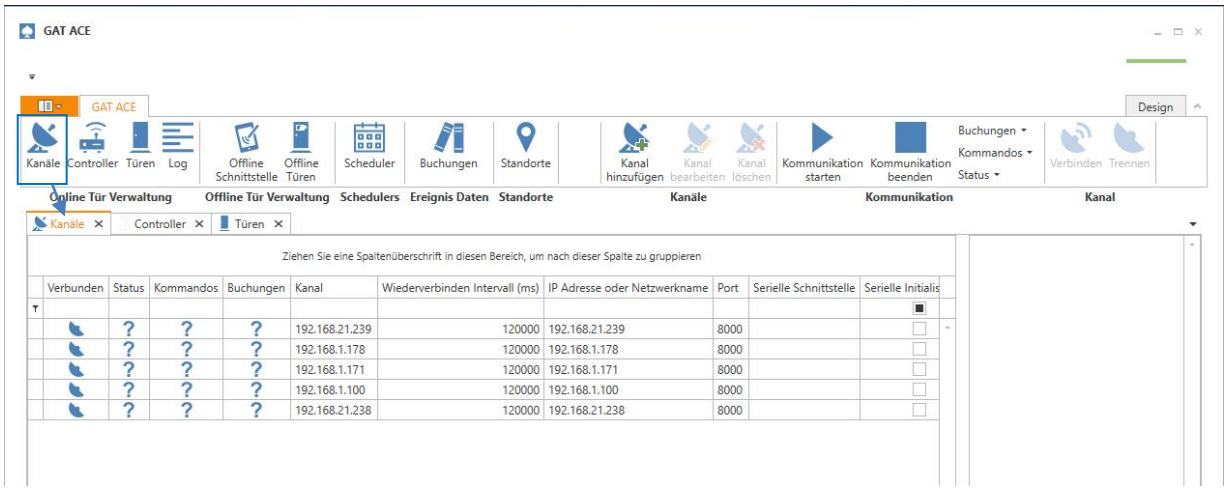


Bild 5.3 *- Kanalansicht*

GAT ACE kommuniziert mit den GANTNER Controllern über TCP/IP- oder serielle COM-Verbindungen. Diese Verbindungen werden in GAT ACE mittels Kanälen definiert, wobei für jede TCP/IP Adresse und jede serielle Schnittstelle COM-Port ein eigener Kanal angelegt wird.

Die Kanäle können in der Kanalliste von GAT ACE übersichtlich verwaltet werden. Sie erhalten in dieser Liste auch eine Anzeige, welche Kanäle online, d.h. verbunden, sind und bei welchen Kanälen es eventuell Probleme gibt.

Für jeden Kanal sind bestimmte Aktionen möglich, wie z. B. das Lesen von Buchungen, das Senden von Kommandos oder die Abfrage des aktuellen Status.

5.1.2 Tür-Controller

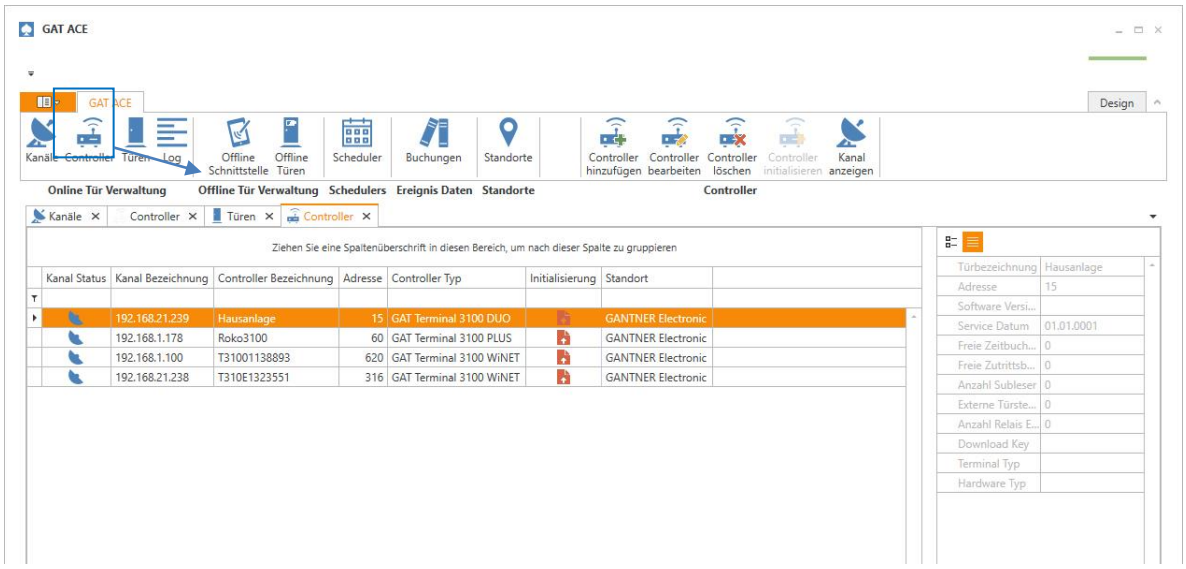


Bild 5.4 *- Controlleransicht*

Mit Controller werden die Geräte bezeichnet, die für die Zutrittskontrolle an den Türen einer Anlage verwendet werden. Ein Controller kann für die Zutrittskontroller von einer oder mehreren Türen verwendet werden. Außerdem sind je nach Controllertyp ein oder mehrere Leser anschließbar. Durch Konfiguration der Controller und der/des an jedem Controller angeschlossenen Leser/n kann die Funktion der Zutrittsanlage den Anforderungen angepasst werden.

GAT ACE 3000 zeigt alle im System definierten Controller übersichtlich in Listenform in der Controlleransicht an. Die wichtigsten Einstellungen zu jedem Controller sind hier direkt ersichtlich. Unterhalb der Controlleransicht sehen Sie die vom ausgewählten Controller ansteuerbaren Türen. Je nach Controllertyp kann dieser bis zu 16 Türen ansteuern. Die nicht verwendeten Türen können in der Liste deaktiviert werden (im Beispiel z.B. die "Quad Door 2" und "Quad Door 3") und die Liste lässt sich filtern so dass Zwecks Übersichtlichkeit nur die aktiven Türen angezeigt werden.

In der Controlleransicht können die Einstellungen der einzelnen Controller bearbeitet werden. Dazu zählen neben den Kommunikationseigenschaften auch die Auswahl der Leserkonfigurationen der am Controller angeschlossenen Leser sowie die Adressierung der Controller. Weiters lassen sich hier auch neue Controller hinzufügen, bestehende Controller löschen oder auch Controller neu initialisieren.

5.1.3 Türen

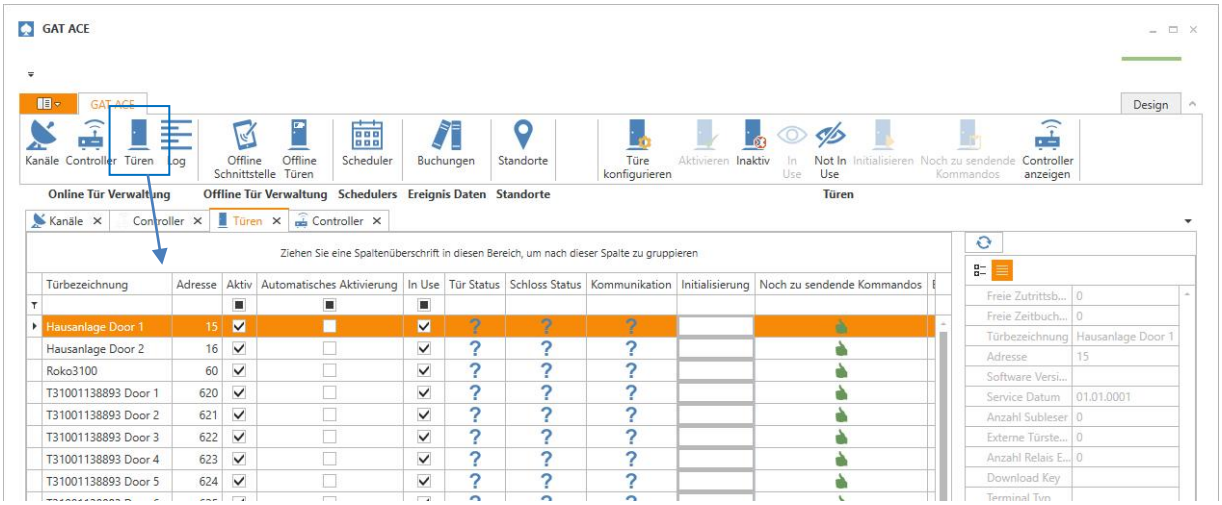


Bild 5.5 *- Türansicht*

Jeder Controller in einer Anlage kontrolliert den Zutritt an einer oder mehrerer Türen. Die maximal mögliche Anzahl kontrollierbarer Türen hängt vom Controllertyp ab (z. B. bis zu 4 Leser am GAT Terminal 3100 Quad) und auch davon, wie viele Leser pro Türe verwendet werden sollen.

Alle Türen in der Anlage werden in der Türansicht aufgelistet. Sie sehen hier für jede Tür unter anderem den aktuellen Status der Tür (geöffnet oder geschlossen, wenn eine Türrückmeldung angeschlossen und konfiguriert ist), der Verriegelung (ver- oder entriegelt) und ob die Kommunikation zur Tür besteht oder unterbrochen ist. Außerdem wird hier auch angezeigt, ob die Tür bereits initialisiert ist und ob noch Kommandos an die Tür gesendet werden müssen.

In der Türansicht können die Türen durch Doppelklick direkt konfiguriert werden. Weiters ist es auch möglich, einzelne Türen zu deaktivieren, zu initialisieren oder Kommandos an einzelne Türen zu senden.

5.1.4 Leserkonfiguration

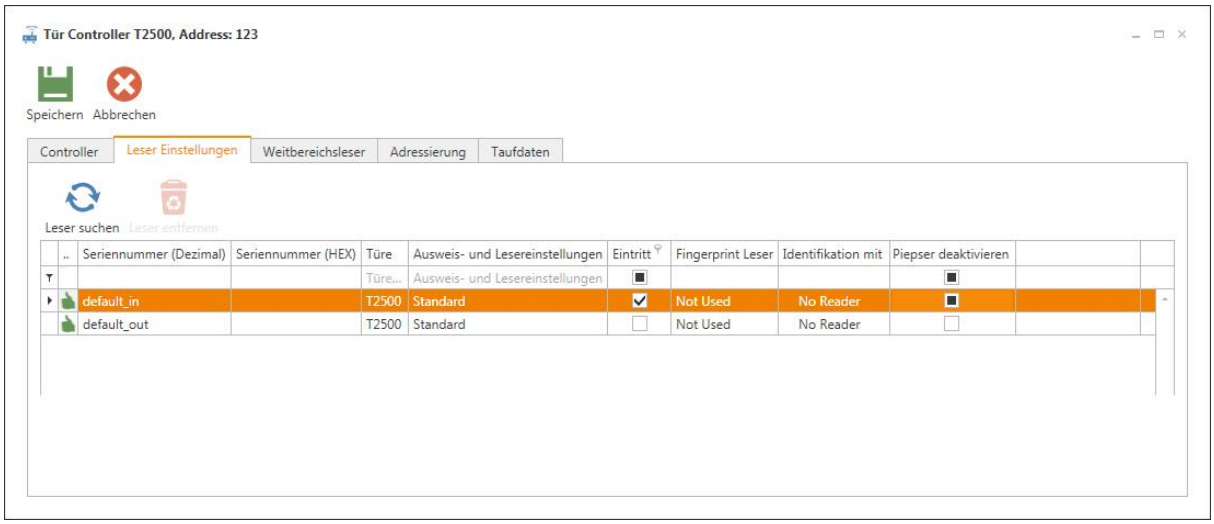


Bild 5.6 *- Leserkonfiguration*

Je nach Controllertyp können an einem Controller ein oder mehrere Leser angeschlossen werden. Für jeden Leser sind umfangreiche Einstellungen möglich. Das Bearbeiten dieser Einstellungen erfolgt auf eigenen Registerkarten in der Controllerkonfiguration.

Auf den Registerkarten "Leser Einstellungen", "WiNET Einstellungen" (nur bei GAT Terminal 3100 WiNET) und "Weitbereichsleser" können jedem Leser eine Funktion (Ein- oder Austritt) zugewiesen, der Typ des Lesers ausgewählt und die Konfigurationseinstellungen festgelegt werden. Außerdem werden dort auch die Leser den Türen zugeordnet. Es ist z. B. bei einem GAT Terminal 3100 Quad möglich, jeden Leser einer Tür zuzuordnen, um mit dem Controller den Eintritt an vier Türen zu kontrollieren oder alle 4 Leser nur einer Tür oder Schranke zuzuordnen, um verschiedene Identifikationsmöglichkeiten an der Tür zu bieten und sowohl Ein- als auch Austritt zu steuern.

5.1.5 Offline-Türen

Offline-Türen bzw. -Terminals sind nicht über eine Schnittstelle permanent mit GAT ACE bzw. einem Server verbunden. Sie werden einmal konfiguriert und führen dann die Zutrittskontrolle autonom durch. Die Konfiguration dieser Offline-Terminals erfolgt z. B. mit dem GAT MT 010 (GAT ST 22x Terminals) oder mit dem GAT DL 090 oder GAT DL 092 (GAT DL 3xx Terminals).

Pro Konfigurationskanal (Transportgerät) wird in GAT ACE in der Ansicht "Offline Schnittstellen" eine Schnittstelle angelegt. Durch die Zuordnung der Offline Türen zu unterschiedlichen Offline Schnittstellen ist es möglich, dass nur Konfigurations- und Änderungsdaten für jene Offline Türen an das Transportgerät übergeben, die auch mit diesem übertragen werden können. Weiter ist es dadurch möglich, dass Änderungsdaten unterteilt werden und so mehrere Mitarbeiter die Offline Türen beladen können (z. B. wenn diese an unterschiedlichen Standorten installiert sind).

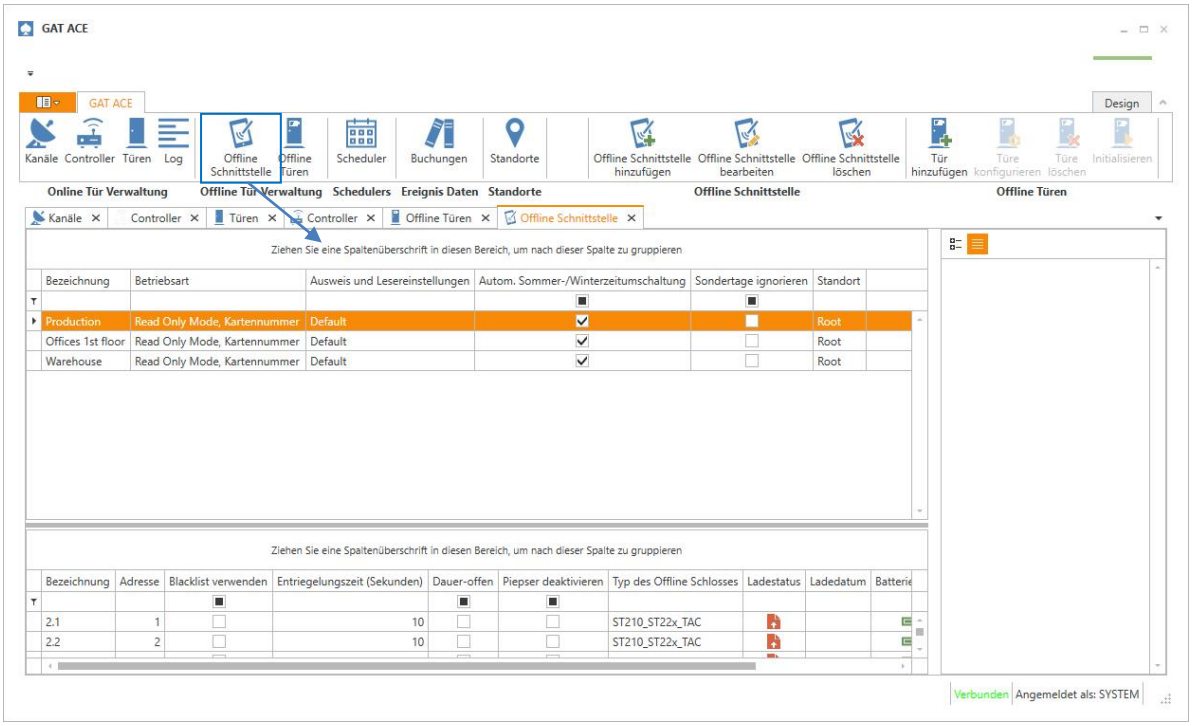


Bild 5.7 *- Offline Schnittstellen*

Die Offline-Terminals werden dann "virtuell" mit diesen Schnittstellen verbunden. Eine Übersicht der Offline Türen sehen Sie in der Ansicht "Offline Türen".

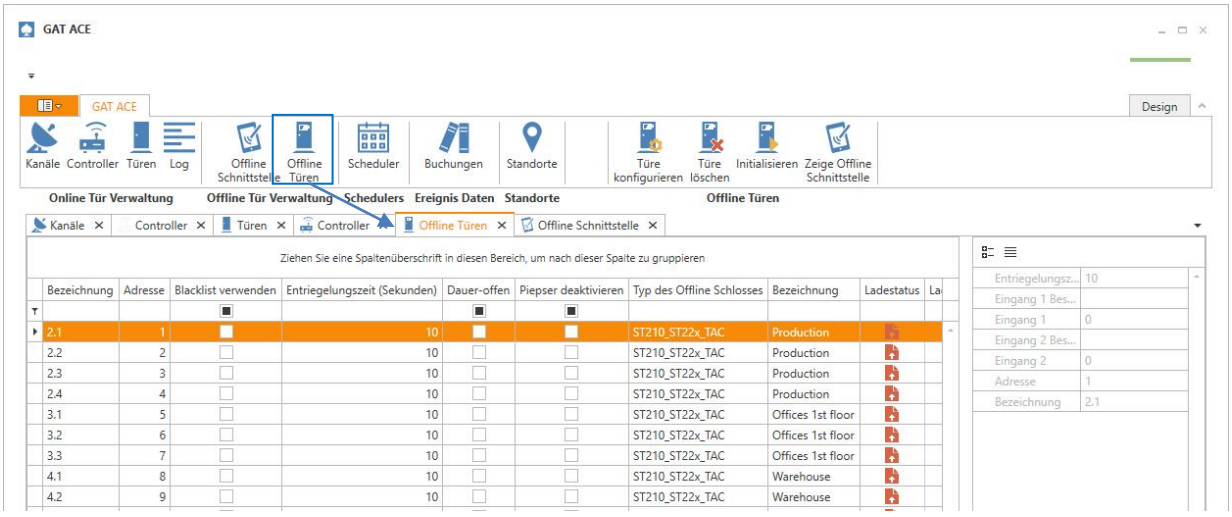


Bild 5.8 *- Offline Türen*

Hier wird für jede Tür die wichtigsten Informationen wie die Adresse, Betriebsart, Entriegelungszeit und Funktions-einstellungen angezeigt. Über die Symbole in der Multifunktionsleiste können die Türkonfigurationen bearbeitet und weitere Türen eingefügt werden.

5.1.6 Scheduler

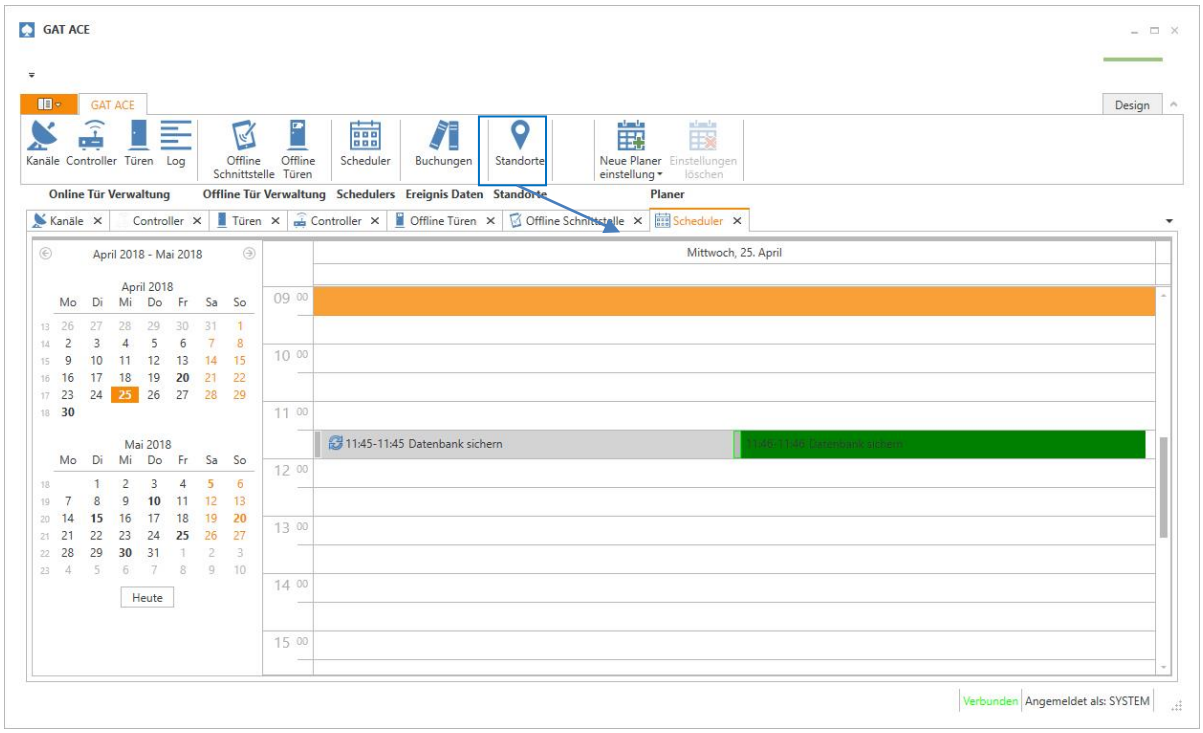


Bild 5.9 *- Scheduler*

Der Scheduler wird verwendet, um sich wiederholende Aufgaben autmoatisch durch GAT ACE 3000 ausführen zu lassen. Sie können den Scheduler verwenden um automatische Sicherungen der SQL Datenbank anzulegen oder alte Einträge aus den Buchungen zu löschen.

Wenn Sie den Scheduler aufrufen, wird der aktuelle Tag mit den geplanten Aufgaben angezeigt. Mit der Kalenderansicht links können Sie zu einem bestimmten anderen Tag springen.

5.1.7 Buchungen

Alle Controller in einer Zutrittskontrollanlage speichern die Bewegungen an Controllern (Identifikation bzw. Identifikationsversuch mittels Datenträgern) sowie wichtige Systemereignisse. Je nach Ereignis werden Informationen über den verwendeten Datenträger, Datum und Uhrzeit und Buchungsart und weitere Details gespeichert. Diese Buchungen ermöglichen somit eine Nachverfolgung aller Vorgänge an den Controllern.
Mit GAT ACE laden Sie Buchungen aus den Controllern und können diese am Bildschirm übersichtlich darstellen, durchsuchen, auswerten und exportieren.

Zeitbuchungen von Zeiterfassungsterminals können in GAT ACE ebenfalls geladen, angezeigt und exportiert werden. Diese Funktion ist jedoch nur verfügbar, wenn die entsprechende Lizenz für das Modul aktiviert siehe (siehe "4.4. Einstellungsseite "Einstellungen"").

5.1.8 Standorte

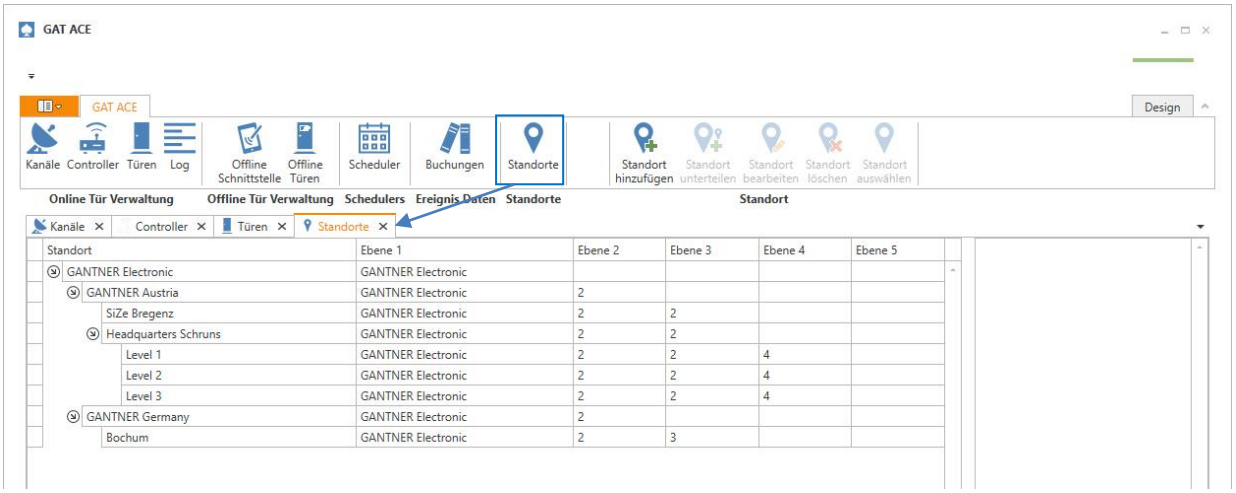


Bild 5.10 *- Standorte*

Um größere Systeme oder z. B. die Zutrittskontrolle einer Firmen mit mehreren Geschäftsstellen zu strukturieren kann die Standort-Verwaltung in GAT ACE verwendet werden. Über einen Strukturbaum werden die Standorte definiert. Diese können bei der Controllerkonfiguration den einzelnen Controllern zugewiesen werden.

Diese Funktion hilft beim Sortieren der Controllerliste. So ist es z. B. möglich, bei großen Anlagen nur die Controller und Türen für einen gewünschten Standort anzuzeigen.

Beim Beladen von Offline Türen kann durch Berücksichtigung der Standorte das Beladen vereinfacht werden, indem nur die am aktuellen Standort befindlichen Türen angezeigt werden.

5.1.9 Ausweis-Einstellungen

Für die Identifikation an den Zutrittscontrollern werden RFID Datenträger verwendet. Damit die Systemsicherheit gewährleistet werden kann und nur passende Datenträger in der Anlage verwendet werden, prüfen die Controller bestimmte Merkmale auf den Datenträger.
Sie können in den Programmeinstellungen genau festlegen, welche Datenträger verwendet werden dürfen. Siehe dazu "4.5. Einstellungsseite "Ausweis- und Lesereinstellungen"".

5.1.10 Anti-Pass-Back Zonen

Mit der Anti-Pass-Back-Funktion kann verhindert werden, dass mehrere Personen durch Weitergabe des Datenträgers von Person zu Person mit demselben Datenträger Zutritt erlangen. Die Einstellung von Anti-Pass-Back Zonen erfolgt in den Programmeinstellungen .
Nähere Informationen zu Anti-Pass-Back Funktion siehe "4.3. Einstellungsseite "Anti-Pass-Back Zonen"".

5.1.11 Log-Dateien auswerten

GAT ACE kann für Analysen die Kommunikation mit den Controllern anzeigen. In dieser Anzeige haben Sie die Möglichkeit nach bestimmten Informationen zu suchen oder Anzeige Filter zu aktivieren.

HINWEIS! Diese Funktion benötigt sehr viel Performance und Systemressourcen. Aktivieren Sie diese Funktion nur für einen einzelnen Kommunikationskanal und lassen Sie die Funktion nur so lange eingeschaltet wie Sie für die Analyse benötigen. Bleibt die Funktion zu lange aktiv, kann dies dazu führen, dass die Oberfläche auf Grund der vielen Meldungen nicht mehr bedienbar ist und neu gestartet werden muss!

Für die Langzeit Aufzeichnung der Kommunikation sind noch weitere Möglichkeiten vorhanden. Wenden Sie sich für Informationen dazu an unseren Support.

5.2 Eine Zutrittsanlage konfigurieren

Dieser Abschnitt beschreibt die grundlegende Vorgehensweise zur Konfiguration einer Zutrittskontrollanlage mit GAT ACE. Es werden die wichtigsten Punkte beschrieben, die normalerweise bei jeder Anlage einmal eingestellt werden müssen. Die Beschreibung von weitergehenden Einstellungen und Funktionen finden Sie in den folgenden Kapiteln.

5.2.1 Kommunikationskanal definieren

Jeder Controller muss einem Kommunikationskanal zugeordnet sein. Durch die Konfiguration der Kanäle wird eine Kommunikation mit dem Controller ermöglicht. Kanäle lassen sich starten und stoppen, um die Kommunikation mit den daran angeschlossenen Controllern zu unterbrechen oder starten.

► Klicken Sie auf das Symbol "Kanäle".

- Die Kanalliste wird angezeigt.

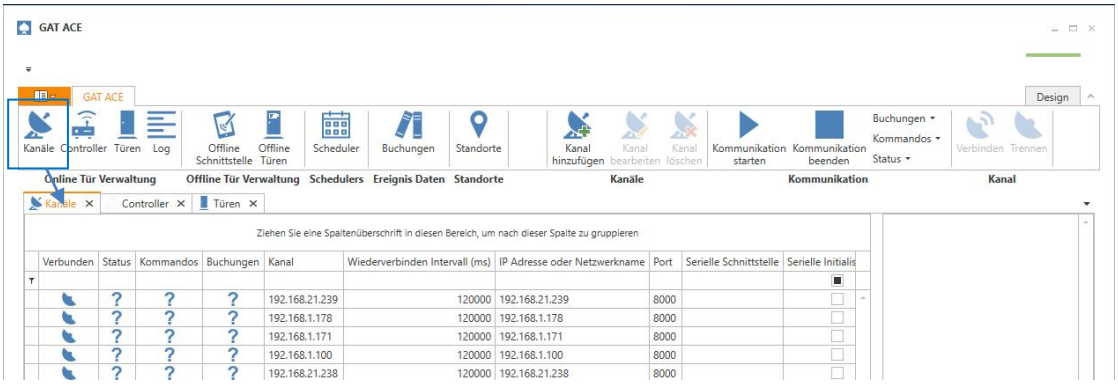


Bild 5.11 *- Kanalansicht*

Der Status jedes Kanals wird mit dem Symbol in der Spalte "Verbunden" angezeigt:

- ....Der Kanal ist nicht verbunden, d.h. es findet keine Kommunikation mit den Controllern an diesem Kanal statt. GAT ACE führt keine automatischen Verbindungsversuche durch.
- ....Die Verbindung mit diesem Kanal ist momentan unterbrochen, d.h. es findet keine Kommunikation mit den Controllern an diesem Kanal statt. GAT ACE führt automatische Verbindungsversuche durch. Wenn die Verbindung wieder hergestellt werden konnte, wechselt das Symbol auf das Folgende.
- ....Der Kanal ist verbunden und eine Kommunikation findet statt.

In den Spalten "Status", "Kommandos" und "Buchungen" werden folgende Symbole angezeigt.

- ....Die Funktion (Statusabfrage, Senden von Kommandos an den Controller, Buchungsabfrage) ist aktiviert.
- ....Die Funktion (Statusabfrage, Senden von Kommandos an den Controller, Buchungsabfrage) ist deaktiviert. **Hinweis:** Die Funktionen können durch Klick mit der rechten Maustaste und Wahl des entsprechenden Menüeintrags im Pop-Up Menü aktiviert oder deaktiviert werden.
- ....Der Status der entsprechenden Funktion konnte nicht ermittelt werden, da der Kanal nicht verbunden ist.

In der Kanalliste sind folgende Funktionen in der Multifunktionsleiste verfügbar:

- ► Fügen Sie einen neuen Kanal hinzu, indem Sie die Funktion "Kanal hinzufügen" wählen
- ► Oder editieren Sie einen bestehenden Kanal, indem Sie den Kanal auswählen und die Funktion "Kanal bearbeiten" wählen.
  - ○ In beiden Fällen öffnet sich das Fenster "Kanal Eigenschaften".

Bild 5.12 *- Allgemeine Kanaleinstellungen*

- ► Geben Sie hier folgende Daten ein:
  - Kanal: Mit dem hier eingegebenen Namen wird der Kanal in der Kanalliste angezeigt.
  - Kanal Typ: Auswahl der Art der Verbindung an diesem Kanal. Mögliche Verbindungsarten sind "TCP/IP" (Ethernet Verbindung) oder "COM" (serielle Verbindung über die RS 485 Schnittstelle).
  - IP Adresse oder Netzwerkname: Wird nur für TCP/IP Verbindungen angezeigt. Geben sie hier die IP-Adresse oder falls vorhanden den Netzwerknamen des Controllers ein, der an diesem Kanal verbunden wird.
  - Serielle Schnittstelle: Wird nur für serielle COM-Verbindungen angezeigt. Wählen Sie den zur Kommunikation zu verwendenden COM-Port des PC.
  - Baudrate: Wird nur für serielle COM-Verbindungen angezeigt. Wählen Sie die Übertragungs-geschwindigkeit an dem gewählten Kanal. Die Baudrate muss mit den Einstellungen der Controller an dem Kanal übereinstimmen.
- ► Wechseln Sie auf die Registerkarte "Advanced", um weitere Kanaleinstellungen zu definieren.
  - ○ Es werden folgende Einstellungen angezeigt.

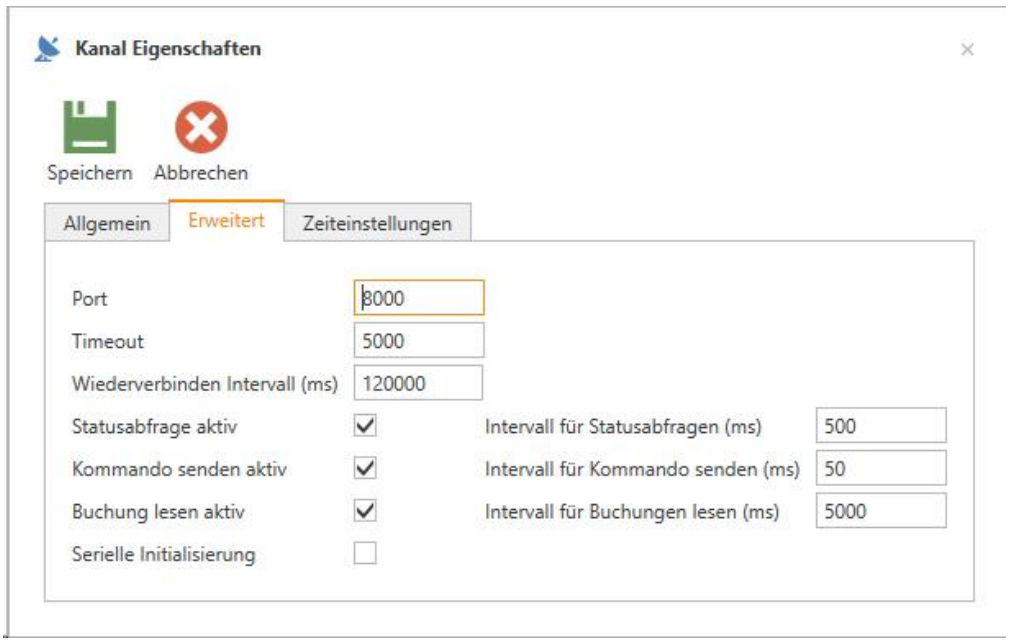


Bild 5.13 *- Erweiterte Kanaleinstellungen*

► Legen Sie hier die Verbindungseinstellungen des Kanals fest:

- Port: Diese Einstellung wird nur für TCP/IP Verbindungen angezeigt. Geben Sie hier den Port ein, der für die Kommunikation an diesem Kanal verwendet werden soll (Standard = 8000). Achten Sie darauf, dass der hier eingetragene Port in der Firewall-Konfiguration des PC freigegeben ist.
- Timeout: Zeit, die bei einer Kommunikation auf eine Antwort gewartet wird (in Millisekunden). Wenn diese Zeit verstreicht, ohne eine Antwort erhalten zu haben, wird die Kommunikation auf diesem Kanal unterbrochen.
- Wiederverbinden Intervall (ms): Wenn die Kommunikation auf diesem Kanal unterbrochen ist versucht GAT ACE jeweils in dem hier festgelegten Zeitintervall wieder eine Kommunikation aufzubauen. Dies wird in der Kanalliste durch das Symbol angezeigt.
- Statusabfrage aktiv: Wenn dieses Feld markiert ist, wird an dem Kanal periodisch in dem rechts angegebenen Zeitintervall (in Millisekunden) der Status der Türen abgefragt. Ist der Türstatus für die Türen an diesem Kanal nicht interessant, kann die Statusabfrage auf inaktiv gestellt werden um die Performance für andere Funktionen zu gewinnen.
- Kommando senden aktiv: Wenn dieses Feld markiert ist, werden an dem Kanal periodisch in dem rechts angegebenen Zeitintervall (in Millisekunden) Kommandos zu den angeschlossenen Türen gesendet um die Türen zu initialisieren. Sind alle Initialisierungskommandos gesendet, ist die Türe betriebsbereit. Um die Initialisierung schnell durchführen zu können, wird ein kurzes Intervall (z. B. 50 ms) empfohlen. Ist es jedoch wichtiger die Buchungen oder Änderungen des Türstatus schnell zu erkennen, soll das Intervall für Kommandos senden verlängert und die anderen Intervalle verkleinert werden. Wird Kommando senden auf inaktiv gestellt, werden Initialisierungsdaten nicht mehr an die Türen dieses Kanals gesendet.

- Buchungen lesen aktiv: Wenn dieses Feld markiert ist, werden an dem Kanal periodisch in dem rechts angegebenen Zeitintervall (in Millisekunden) die Buchungen aus den Türen dieses Kommunikationskanals gelesen. Sind die Buchungen für die Türen an diesem Kanal nicht interessant, kann Buchung lesen auf inaktiv gestellt werden um die Performance für andere Funktionen zu gewinnen. Sollen die Buchungen für die Weiterverarbeitung schnell verfügbar sein, so kann das Intervall für Buchungen lesen verkleinert werden.
- Serielle Initialisierung: Bei seriellen Kanälen mit vielen Türcontrollern sollte diese Option markiert werden. Dadurch wird bei der Initialisierung der Controller an diesem Kanal verhindert, dass diese zu lange außer Betrieb sind.
  NOTICE! Wenn diese Option nicht markiert ist, wird bei der Initialisierung zuerst der Speicher von jedem Controller gelöscht und die Controller danach reihenweise initialisiert. Dadurch können die letzten Controller für lange Zeit außer Betrieb sein. Mit Aktivierung dieser Funktion wird dies verhindert, indem die Speicher einzeln gelöscht und die Controller jeweils gleich initialisiert werden.

► Wechseln Sie auf die Registerkarte "Zeiteinstellungen", um die Zeitzone und Sommer-/Winterzeitumschaltung für den Kanal zu definieren.

○ Es werden folgende Einstellungen angezeigt.

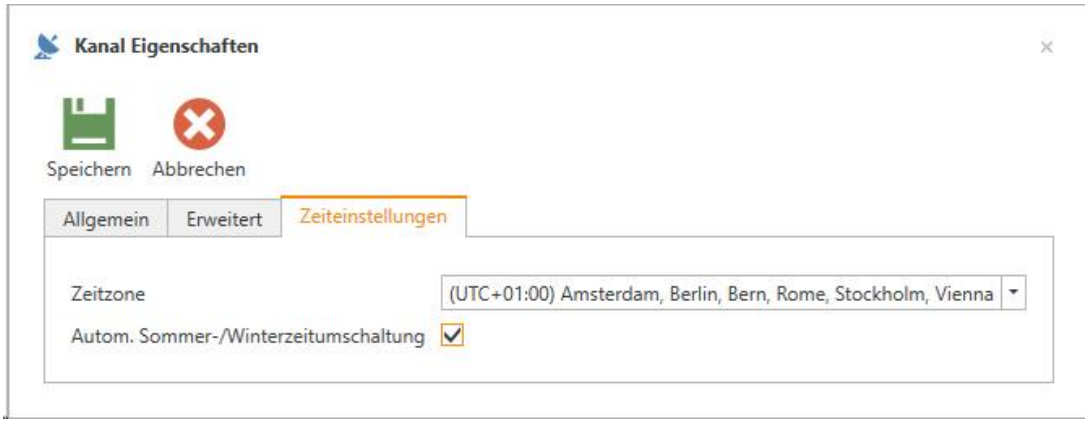


Bild 5.14 *- Zeiteinstellungen für den Kanal*

► Wählen Sie hier folgende Einstellungen:

- Zeitzone: Wählen Sie hier die Zeitzone aus, in der sich der Kanal bzw. die angeschlossenen Geräte befinden.
- Autom. Sommer-/Winterzeitumschaltung: Wenn dieses Optionsfeld markiert ist, wird GAT ACE 3000 die Umschaltung zwischen Sommer- und Winterzeit automatisch vornehmen.

► Speichern Sie die Einstellungen mit "Save" ab.

5.2.2 Standorte strukturieren

Die Eingabe von Standorten ist nicht unbedingt notwendig, um in GAT ACE eine Zutrittskontrollanlage zu konfigurieren. Allerdings kann die Standorteinteilung vor allem bei größeren Anlagen oder verschiedenen Firmenstandorten sehr hilfreich sein.

► Wählen Sie das Symbol "Standorte".

○ Es wird die Ansicht "Standorte" wird geöffnet.

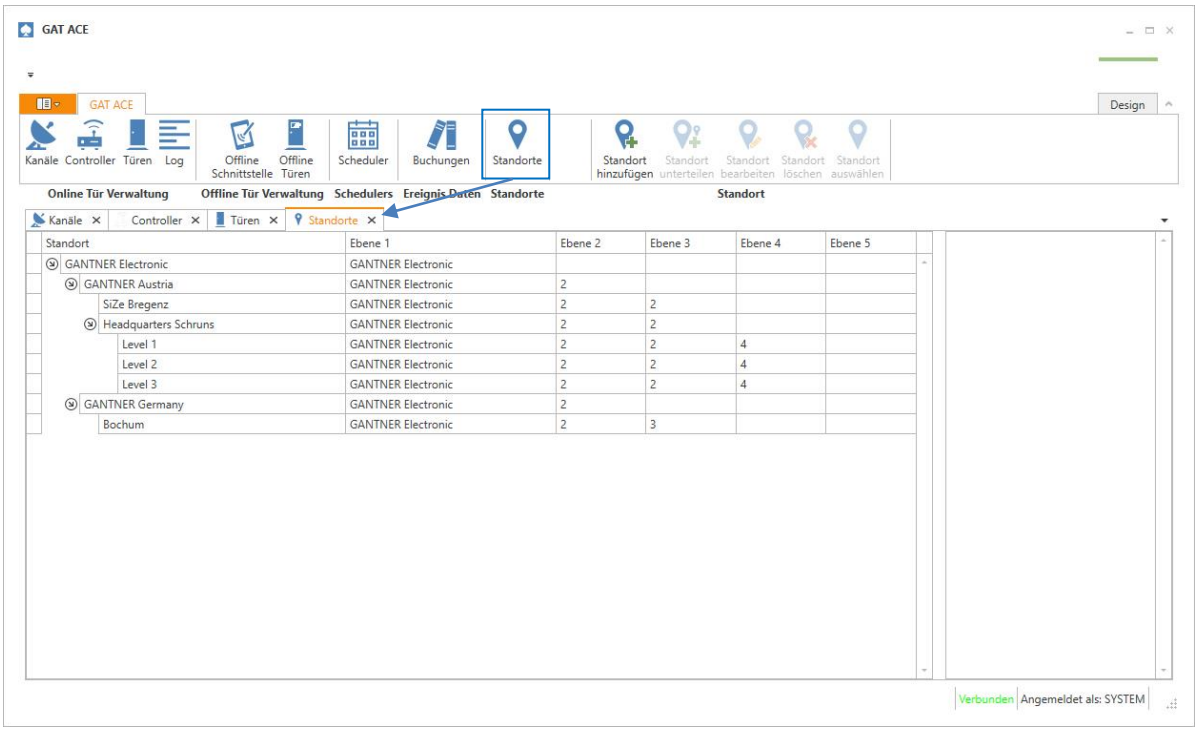


Bild 5.15 *- Standorte*

○ In der Standortansicht sind folgende Funktionen in der Multifunktionsleiste verfügbar.

► Wählen Sie die Funktion "Standort hinzufügen", um einen neuen Standort hinzuzufügen.

○ Folgendes Fenster wird angezeigt.

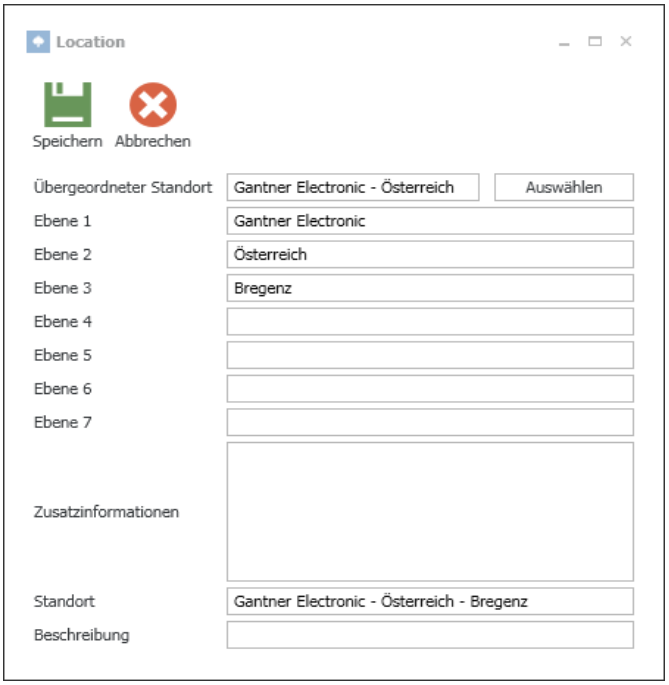


Bild 5.16 *- Neuen Standort eingeben*

► Tragen Sie hier folgende Informationen ein:

- Übergeordneter Standort: Mit Klick auf "Auswählen" erhalten Sie eine Liste, aus der Sie einen bereits definierten Standort auswählen können. Der neue Standort wird dann eine Ebene unterhalb des gewählten Standorts im Strukturbaum eingefügt. Wenn hier nichts ausgewählt wird, wird der neue Standort in der obersten Ebene des Strukturbaums eingefügt.
- Ebene x: Ist ein übergeordneter Standort ausgewählt, so werden in den Ebenen 1 bis 6 die für diesen Standort zutreffenden Bezeichnungen dargestellt. Es kann nun ein Wert für die neue Ebene eingegeben werden um neue Standorte zu erstellen. Die übergeordneten Werte können mit dieser Funktion nicht geändert werden. Wählen Sie dazu das Bearbeiten des Übergeordneten Standortes.
- Zusatzinformationen: Falls gewünscht können Sie hier zusätzliche Informationen oder eine nähere Beschreibung des einzufügenden Standorts eintragen. Diese wird bei Auswahl des Standorts in der Standortsanzeige im der rechten Info-Bereich angezeigt.
- Standort: Name des Standort, mit dem dieser im Strukturbaum angezeigt wird. Der Standort setzt sich automatisch aus den Ebenen zusammen. Dieser Wert kann aber auch überschrieben und durch eine andere Benennung ersetzt werden.
- Beschreibung: Eine kurze Zusätzliche Beschreibung des Standorts. Diese wird bei Auswahl des Standorts in der Standortsanzeige im der rechten Info-Bereich angezeigt.

► Bestätigen Sie mit "Speichern".

  ○ Der neue Standort wird an entsprechender Stelle im Strukturbaum eingefügt.

► Mit dem Symbol "Standort unterteilen" kann am markierten Standort ein weiterer Unterstandort eingefügt werden.

► Mit dem Symbol "Standort bearbeiten" können Sie die Einstellungen eines bestehenden Standorts ändern.

► Mit dem Symbol "Standort löschen" kann ein ausgewählter Standort gelöscht werden.

► Das Symbol "Standort auswählen" wird beim Hinzufügen eines Standorts benutzt, um einen übergeordneten Standort auszuwählen.

5.2.3 Controller hinzufügen

Um einen Controller zu konfigurieren müssen Sie diesen erst in der Controllerliste einfügen.

► Wählen Sie das Symbol "Controller".

- Es wird die Ansicht "Controller" wird geöffnet.

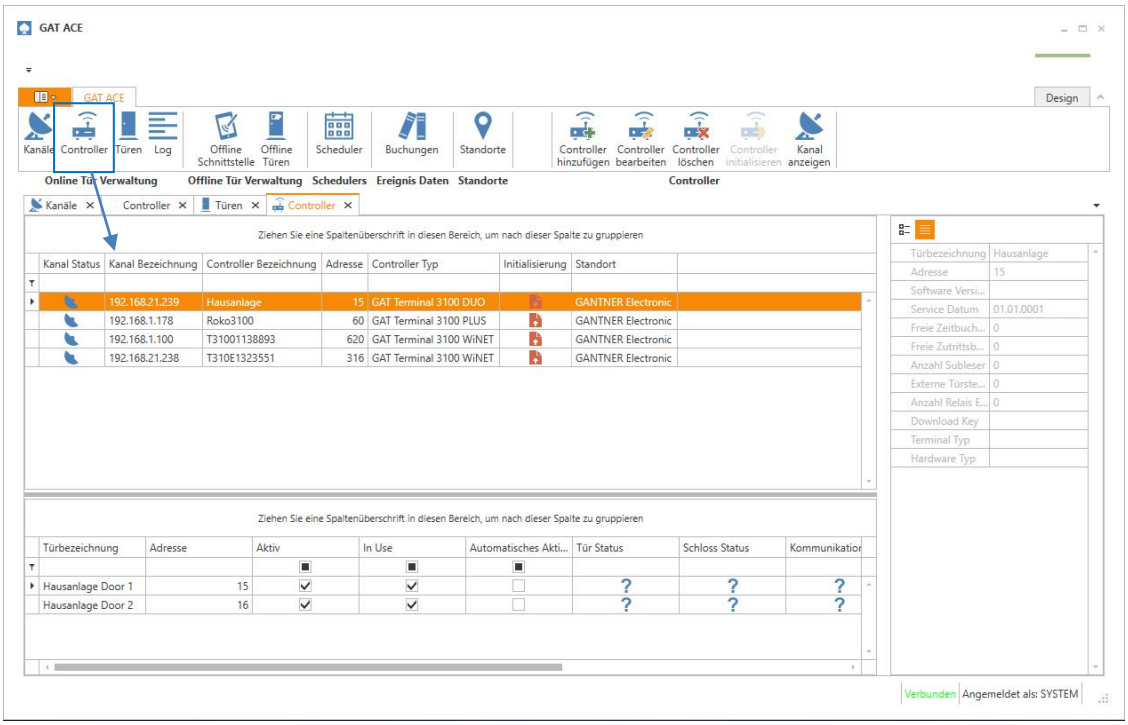


***Bild 5.17** - Controlleransicht*

- GAT ACE zeigt alle im System definierten Controller übersichtlich in Listenform in der Controlleransicht an. Die wichtigsten Einstellungen zu jedem Controller sind hier direkt ersichtlich. In der Spalte "Kanal Status" sehen sie den aktuellen Status jedes Controllers.
  .... Der Controller ist nicht verbunden, d.h. es findet keine Kommunikation mit dem Controller statt.
  .... Der Controller ist verbunden und eine Kommunikation mit diesem Controller findet statt.
- Unterhalb der Controlleransicht sehen Sie die vom ausgewählten Controller ansteuerbaren Türen.
- In der Controlleransicht sind folgende Funktionen in der Multifunktionsleiste verfügbar.

► Mit dem Symbol "Kanal anzeigen" zeigt GAT ACE direkt den Kanal an, an dem der ausgewählte Controller verbunden ist.

► Wählen Sie das Symbol "Controller hinzufügen", um einen neuen Controller der Liste hinzuzufügen.

- Es wird eine Abfrage angezeigt, ob das Netzwerk nach Controllern durchsucht werden soll.

► Wählen Sie "Ja ", wenn der gewünschte Controller im TCP/IP Netzwerk angeschlossen ist und Sie diesen im Netzwerk suchen möchten.

- Das Netzwerk wird durchsucht und alle gefundenen Controller werden in einem neuen Fenster angezeigt.

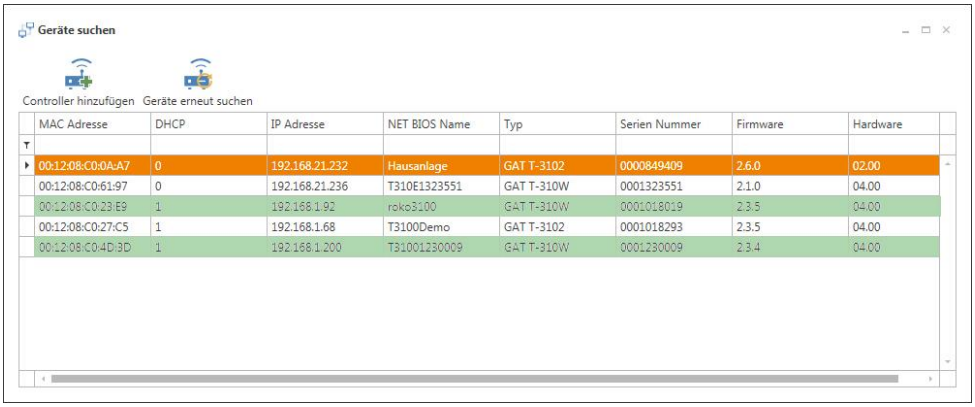


Bild 5.18 *- Controller am Netzwerk suchen*

► Wählen Sie den gewünschten Controller aus.

HINWEIS! Die in dieser Liste grün markierten Controller befinden sich bereits in der Controllerliste von GAT ACE.

► Fügen Sie den Controller mit "Controller hinzufügen" in die Controllerliste ein.

- Sie gelangen zurück in die Controllerliste, wo der neue Controller eingefügt wurde.

► Wählen Sie "Nein", wenn Sie einen neuen Controller manuell einfügen möchten.

- Es wird das Fenster "Neuer Controller" geöffnet.

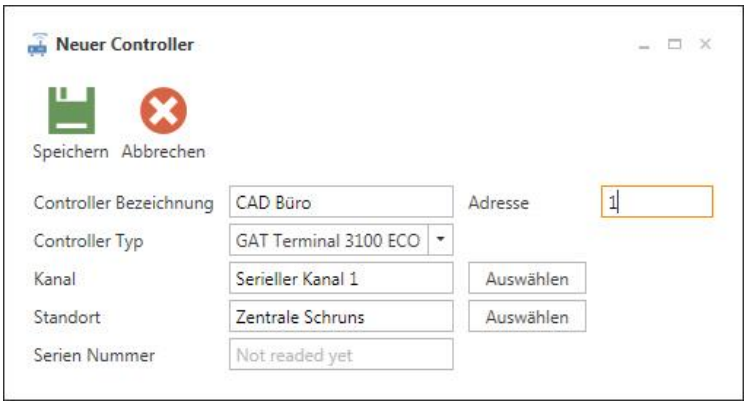


Bild 5.19 *- Neuer Controller*

► Geben Sie hier folgende Daten für den neuen Controller ein.

- Controller Bezeichnung: Name des Controllers, mit dem er in GAT ACE angezeigt wird.
- Adresse: Jeder Controller in einer Anlage besitzt eine eindeutige Adresse, über die er angesprochen werden kann.
- Controller Typ: Hier werden alle von GAT ACE 3000 unterstützten Typen von Controllern aufgelistet. Wählen Sie hier den richtigen Typ aus.
- Kanal: Auswahl des Kanals, an dem der Controller eingefügt werden soll. Wenn noch kein Kanal für den Controller angelegt wurde können Sie mit Klick auf "Auswählen" einen neuen Kanal anlegen. Informationen zur Kanaldefinition siehe "5.2.1. Kommunikationskanal definieren".
- Standort: Hier kann ein Standort für den Controller gewählt werden. Es ist nicht unbedingt notwendig, hier einen Standort zu wählen. Aber vor allem bei größeren Anlagen kann

durch die Standortzuordnung die Übersichtlichkeit in GAT ACE erhöht werden, weil die Controllerliste dann nach Standorten gefiltert werden kann.

- Seriennummer: Wenn der Controller initialisiert wird, wird die Seriennummer aus dem Controller ausgelesen und in diesem Feld dargestellt. Nicht alle Controller bieten die Funktion die Seriennummer auszulesen.

► Bestätigen Sie mit Klick auf "Sichern", um den neuen Controller in die Controllerliste einzufügen.
  ○ Sie gelangen zurück in die Controllerliste, wo der neue Controller eingefügt wurde.

► Um einen Controller aus GAT ACE zu entfernen, markieren Sie den Controller und wählen Sie "Controller löschen".

5.2.4 Controller konfigurieren

Um die Konfiguration eines Controllers einzustellen, gehen Sie wie folgt vor.

► Markieren Sie einen Controller in der Controllerliste und wählen Sie das Symbol "Controller bearbeiten", um die Einstellungen des markierten Controllers zu konfigurieren.
  ○ Es wird das Fenster zur Controllerkonfiguration geöffnet.

Bild 5.20 *- Controllerkonfiguration*

Die Einstellungen des Controllers sind in verschiedene Registerkarten unterteilt. Bei jedem Controller werden nur die für den Controllertyp notwendigen Registerkarten angezeigt.

Ergänzen oder ändern Sie die Einstellungen auf der Controller Seite, wenn diese nicht vollständig oder korrekt sind. Die Daten sind gleich, wie beim manuellen anlegen des Controllers beschrieben.

5.2.5 Leser eines Controllers zuordnen und konfigurieren

Die Leser, die an einem Controller angeschlossen oder eingebaut sind, müssen richtig konfiguriert sein, um verwendet werden zu können. Die Konfiguration ist in der Controllerkonfiguration auf einer eigenen Registerkarte möglich. Für Controller die mehr als eine Türe steuern können, werden hier die Leser auch den Türen zugeordnet.

Führen Sie dazu folgende Schritte aus:

► Rufen Sie die Controllerkonfiguration durch Doppelklick auf den Controller in der Controllerliste auf.
  ○ Das Fenster zur Controllerkonfiguration wird angezeigt.

► Wechseln Sie auf die Registerkarte "Leser Einstellungen".
  ○ Die Registerkarte "Leser Einstellungen" wird angezeigt.

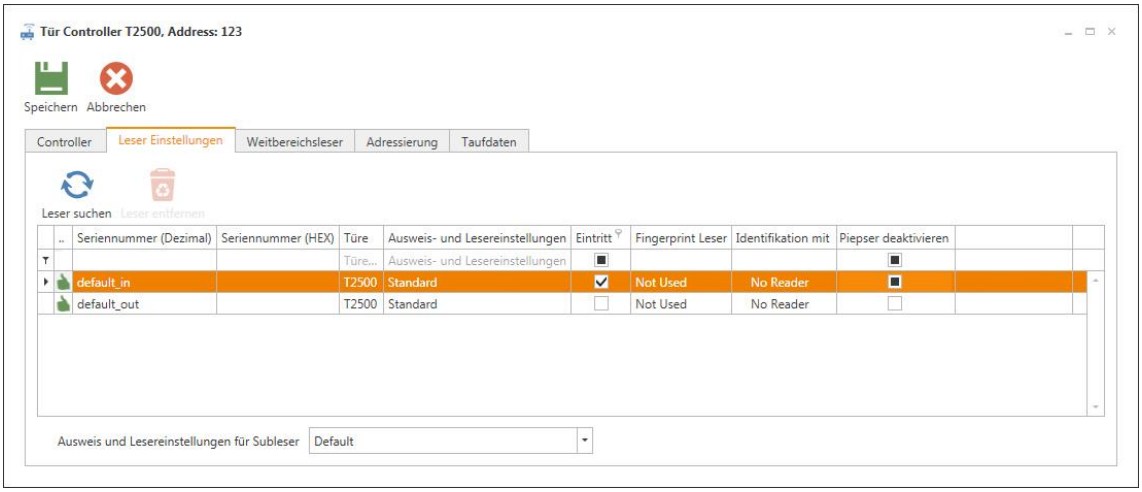


Bild 5.21 *- Konfiguration und Zuordnung der Leser, die am Controller angeschlossen sind*

► Mit dem Symbol "Leser suchen" können Sie Leser die über eine RS_485 Schnittstelle an den Controller angeschlossen sind suchen. Eingebaute Leser werden ohne Suche angezeigt.
  ○ Die gefundenen Leser werden in der Liste aufgelistet.

► Folgende Informationen werden für die Leser dargestellt:

- Seriennummer (Dezimal): Seriennummer des Lesers in dezimaler Form.
- Seriennummer (HEX): Seriennummer des Lesers in hexadezimaler Form.
- Türe: Auswahl der Türe, zu der der Leser zugeordnet werden soll. Werden mehrere Leser der gleichen Türe zugeordnet, ist damit eine Steuerung von Ein- und Austritt möglich oder es stehen mehrere Identifikationspunkte (z. B. PKW und LKW) zur Verfügung.
- Ausweis- und Lesereinst.: Diese Auswahl bestimmt, welche Datenträger am Leser verwendet werden können (Codierung, RFID-Typ, etc.). Die hier auswählbaren Ausweiseinstellungen werden in den Programmeinstellungen definiert (siehe "4.5. Einstellungsseite "Ausweis- und Lesereinstellungen" ").
- Eintritt: Diese Einstellung bestimmt, ob der Leser als Ein- oder Austrittsleser verwendet werden soll. Bei 2 Lesern an einer Tür kann somit eingestellt werden, welcher Leser für Eintritt und welcher für Austritt verwendet werden soll. Diese Einstellung ist für die Angabe der Richtung in den Buchungen und auch für die Anti-Pass-Back Funktion wichtig.

- Fingerprint Leser: Dieser Wert bestimmt, die Funktion des Fingerabdrucklesers. Ist kein Fingerabdruckleser angeschlossen, so ist die Einstellung „Nicht verwendet“ auszuwählen. Soll der Fingerprint zur Verifikation des Ausweisinhabers verwendet werden, ist die Einstellung „Verifikation“ zu wählen. Für eine Identifikation der Person mittels Fingerprint ist die Einstellung „Identifikation“ zu wählen.
- Identifikation mit: Bei der Einstellung "Ausweis" kann die Identifikation nur mit Ausweisen oder für den Fall der biometrischen Identifikation auch mit Fingerprint erfolgen. Bei der Einstellung „Ausweis oder Tastatur“ können sich Personen mit Sonderberechtigung auch durch Eingabe der Personalnummer identifizieren. Für diese Personen wird empfohlen eine Verifikation mittels PIN-Code oder Fingerprint zu aktivieren.
- Piepser deaktivieren: Diese Einstellung kann mit den Lesern der neuen Generation 73xx verwendet werden. Wenn die Option aktiviert ist (Haken) ist der Piepser des Lesers deaktiviert, was bedeutet, dass keine akustischen Signale am Leser ausgegeben werden.

► Im Feld "Ausweis und Lesereinstellungen für Subleser" können Sie eine der konfigurierten Ausweis- und Lesereinstellung auswählen, um festzulegen, welche Datenträger an einem Subleser am aktuellen Controller verwendet werden können.
  ○ Die Ausweis- und Lesereinstellungen werden im Konfigurationsmenü von GAT ACE 3000 bearbeitet (siehe "4.5. Einstellungsseite "Ausweis- und Lesereinstellungen" ").

► Bestätigen Sie die Konfiguration mit "Sichern".
  ○ Sie gelangen zurück in die Controlleransicht.

Beachten Sie, dass der Kontroller neu beladen werden muss, bevor die Einstellungen wirksam werden. Das Beladen kann automatisch oder manuell erfolgen (siehe "5.2.12. Türe").

5.2.6 WiNET Einstellungen eines Offline-Controllers konfigurieren

Bei einem Controller vom Typ "GAT Terminal 3100 WiNET" können auch die WiNET Einstellungen bearbeitet werden. Diese Registerkarte ist bei den anderen Controllern ausgeblendet. Sie sehen hier die erreichbaren WiNET Türschlösser und die verbundenen WiNET Access Points.

► Rufen Sie die Controllerkonfiguration durch Doppelklick auf den Controller in der Controllerliste auf.
  ○ Das Fenster zur Controllerkonfiguration wird angezeigt.

► Wechseln Sie auf die Registerkarte "WiNET Einstellungen".
  ○ Die Registerkarte "WiNET Einstellungen" wird angezeigt.

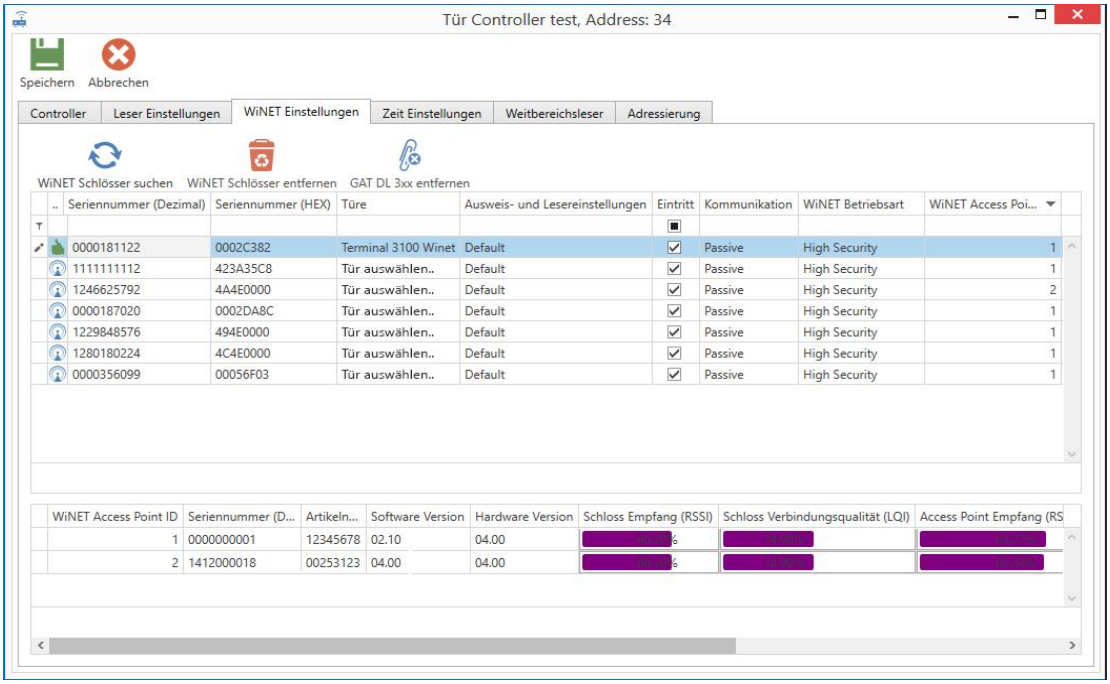


Bild 5.22 *- Einstellungen der WiNET Schlösser und Access Points*

► Drücken Sie die Schaltfläche "WiNET Schlösser suchen".

- Der Controller sucht nach WiNET Schlössern und zeigt alle gefundenen Schlösser in der obersten Liste an.
- In der unteren Liste sehen Sie alle WiNET Access Points, die am Controller verbunden sind.

HINWEIS! Wenn zwei oder mehrere Access Points verbunden sind und nur einer dieser Access Points nicht mehr erreichbar ist, werden auch die anderen Access Points nicht mehr angezeigt, d.h. die Liste ist leer.

- "WiNET Schlösser entfernen": Wird in der Liste ein WiNET Schloss angezeigt, das nicht mehr im Empfangsbereich der WiNET Access Points ist, wird für dieses Schloss ein Fehler angezeigt. Dieses Schloss kann gelöscht werden (z. B. weil es defekt ist), indem es in der Liste markiert und dann die Schaltfläche "WiNET Schlösser entfernen" gedrückt wird.

- "GAT DL 3xx entfernen": Soll ein WiNET Schloss ausgetauscht werden (z. B. im Falle einer Reparatur oder wenn das Schloss an einer anderen Türe, die von einem anderen Controller bedient wird, eingebaut werden soll) muss zuerst das bisher verwendete Schloss mit der Schaltfläche "GAT DL 3xx entfernen" vom Controller getrennt und aus der Datenbank gelöscht werden. Nur so kann sicher gestellt werden, dass das Schloss nach der Reparatur wieder an einer Türe verwendet werden kann. Wird dies nicht gemacht, ist die Zuweisung dieses WiNET Schlosses nicht möglich, da die Seriennummer des Schlosses nur einmal im System vorhanden sein kann.
  Die Funktion "GAT DL 3xx entfernen" ist auch dann erforderlich, wenn das WiNET Schloss nur in der Liste des Controllers gespeichert, aber keiner Türe zugewiesen ist. Um das WiNET Schlosses an einem anderen Controller verwenden zu können, muss das WiNET Schloss zuerst auf Werkseinstellungen zurückgesetzt und der WiNET Mode wieder aktiviert werden.

HINWEIS! Bitte beachten Sie beim Entfernen eines WiNET Schlosses, dass der gesamte WiNET Controller inklusive Speicherinitialisierung neu initialisiert werden muss.

5.2.7 Zeiteinstellungen für Leser konfigurieren

Für die Controller und Leser lassen sich Zeiten konfigurieren, die bestimmte Funktionen wie die Anzeige- oder Eingabezeit betreffen.

► Rufen Sie die Controllerkonfiguration durch Doppelklick auf den Controller in der Controllerliste auf.
  ○ Das Fenster zur Controllerkonfiguration wird angezeigt.
► Wechseln Sie auf die Registerkarte "Zeit Einstellungen".
  ○ Die Registerkarte "Zeit Einstellungen" wird angezeigt.

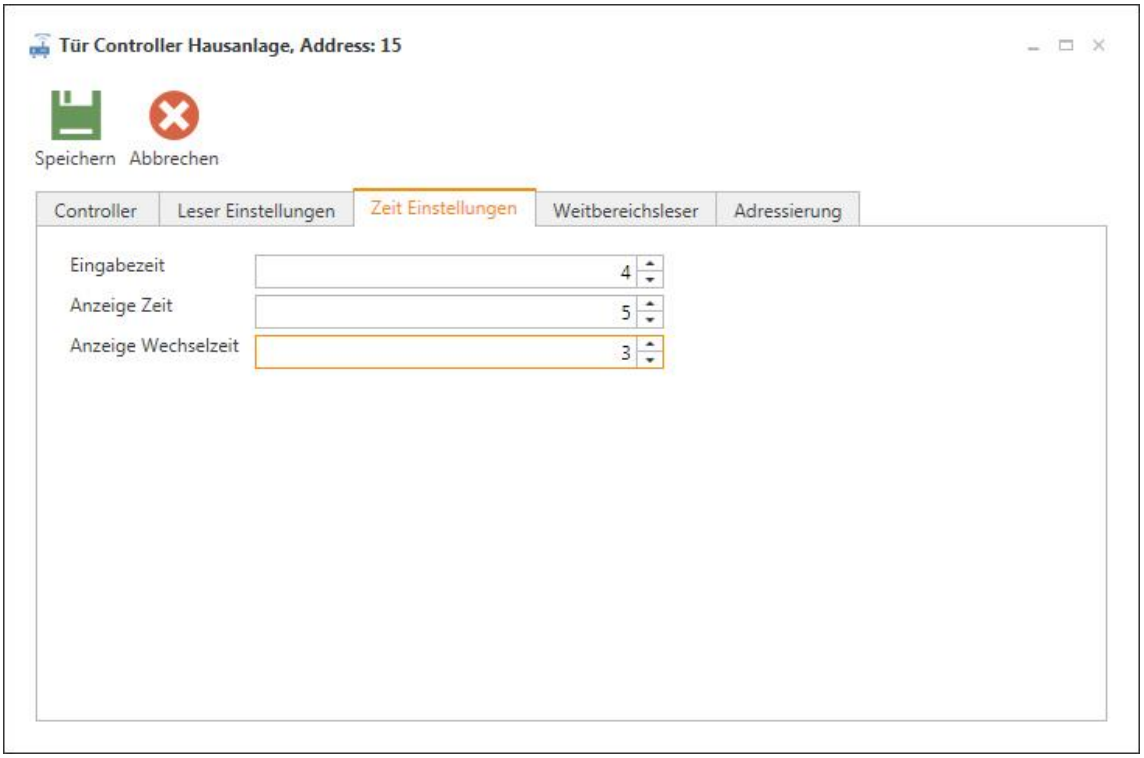


Bild 5.23 *- Zeiteinstellungen für die Leser der Controller definieren*

- Eingabezeit: Diese Eingabe (in Sekunden) bestimmt, wie lange auf die Eingabe eines PIN Codes oder der Erfassung eines Fingerprints gewartet wird.
- Anzeige Zeit: Diese Eingabe (in Sekunden) bestimmt, wie lange der Leser eine Benutzer-information wie z. B. "Zutritt erlaubt" oder "Zutritt verweigert" am Display und/oder mittels den LEDs am Leser angezeigt wird, bevor die Anzeige wieder in den Grundzustand wechselt.
- Anzeige Wechselzeit: Diese Eingabe (in Sekunden) bestimmt, wie lange die erfolgreiche Erstellung einer Zeitbuchung angezeigt wird, bevor auf die Anzeige des Zutritts gewechselt wird. Diese Einstellung hat nur bei der Konfiguration „Zeitbuchung mit automatischem Zutritt“, die nur an einigen Controllern zur Verfügung steht, eine Bedeutung.

5.2.8 Weitbereichsleser konfigurieren

Wenn am Controller ein Weitbereichsleser GAT Reader 868 verwendet wird, können Sie diese auf einer eigenen Registerkarte konfigurieren.

► Rufen Sie die Controllerkonfiguration durch Doppelklick auf den Controller in der Controllerliste auf.
  ○ Das Fenster zur Controllerkonfiguration wird angezeigt.
► Wechseln Sie auf die Registerkarte "Weitbereichsleser", um die Einstellungen dieses Lesers einzustellen.
  ○ Die Registerkarte "Weitbereichsleser" wird angezeigt.

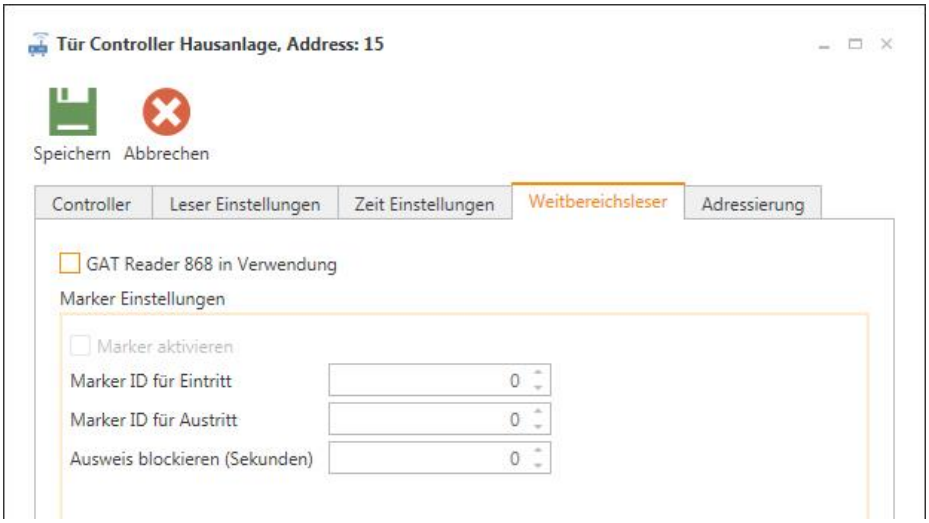


Bild 5.24 *- Weitbereichsleser konfigurieren*

► Falls ein Weitbereichsleser GAT Reader 868 am Controller verwendet wird, markieren Sie das Optionsfeld "GAT Reader 868 in Verwendung".
► Geben Sie dann darunter folgende Informationen ein:
  - Marker aktivieren: Marker können bei den Weitbereichslesern zur Erkennung der Bewegungsrichtung verwendet werden. Für einen Weitbereichsleser können 2 Marker verwendet werden. Bei Erkennung eines Datenträgers wird über die Marker festgestellt, an welcher Stelle (innen oder außen) sich der Datenträger befindet. Es ist auch möglich, Weitbereichsleser ohne Marker zu verwenden. Sollen Marker verwendet werden, markieren Sie das Optionsfeld "Marker aktivieren".
  - Marker ID für Eintritt: Geben Sie hier die ID-Nummer an, mit die der Marker für den Eintritt hat.
  - Marker ID für Austritt: Geben Sie hier die ID-Nummer an, mit die der Marker für den Austritt hat
► Um die Controllerkonfiguration abzuschließen drücken Sie "Sichern".
  ○ Sie gelangen zurück in die Controlleransicht.

Beachten Sie, dass der Kontroller neu beladen werden muss, bevor die Einstellungen wirksam werden. Das Beladen kann automatisch oder manuell erfolgen (siehe "5.2.12. Türe").

5.2.9 Türen konfigurieren

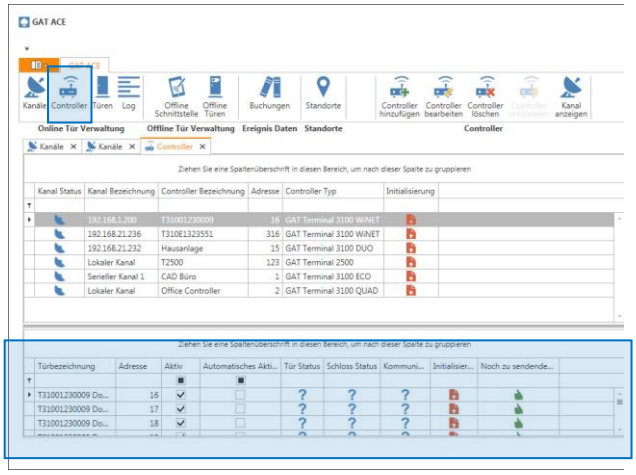
Jeder Controllertyp hat eine bestimmte Anzahl maximal ansteuerbarer Türen. Wenn ein Controller in GAT ACE neu angelegt wird, werden standardmäßig immer die max. mögliche Anzahl Türen angezeigt. Die davon verwendeten Türen müssen entsprechend konfiguriert werden, um die Zutrittsfunktion entsprechend festzulegen.

In der Konfiguration einer "Tür" werden alle Einstellungen zusammengefasst, die die Zutrittsfunktion der Tür bestimmen. Darunter fallen Einstellungen wie die Entriegelungszeiten, die Einstellung der Relaisausgänge und Optokopplereingänge und der weitern Funktionalitäten wie Anti-Pass-Back oder 4-Augen-Prinzip.

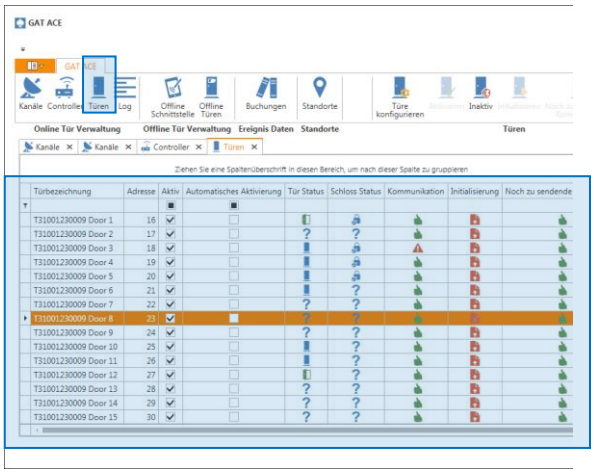
Hinweis: In GAT ACE ist zwischen den Begriffen "Leser" und "Tür" zu unterscheiden. Leser bezeichnet die wirklich physikalisch installierten Leseeinheiten und Tür bezeichnet das zu steuernde Objekt (Türe, Schranke, Tor, etc.). So können z. B. an ein GAT Terminal 3100 QUAD vier Leser angeschlossen werden. Je nach Installation der Leser kann der Controller dann eine Tür (alle vier Leser sind an dieser Tür installiert) oder bis zu vier Türen (ein Leser pro Türe) kontrollieren.

Grundsätzlich gibt es zwei verschiedene Möglichkeiten, die Türen in einer Anlage anzuzeigen.

- Bei der Konfiguration der Controller werden nach Auswahl eines Controllers dessen Türen in der unteren Liste angezeigt (linkes Bild).
- Mit dem Symbol "Türen" in der Multifunktionsleiste wechseln Sie auf die Türansicht und es werden alle Türen in der Zutrittsanlage angezeigt (rechtes Bild).



Türen des ausgewählten Controllers



Liste der gesamten Türen einer Anlage

***Bild 5.25** - Türen einer Anlage*

GAT ACE zeigt zu allen Türen verschiedene Hinweise an:

- Adresse: Zeigt die Adresse an, die bei der Kommunikation mit der Türe verwendet wird.
- Aktiv: Zeigt an, ob die Tür aktiv (Feld ist markiert) oder inaktiv ist. Werden nicht alle Türen eines Controllers verwendet, so sind die nicht verwendeten Türen auf inaktiv zu stellen. Mit inaktiven Türen findet keine Kommunikation mit GAT ACE statt.
  Um eine Türe zu aktivieren oder auf inaktiv zu stellen, verwenden Sie die Funktionen in der Multifunktionsleiste oder im Kontextmenü das angezeigt wird, wenn Sie mit der rechten Maustaste auf die Türe klicken.
  Sie können die Liste mit dem obersten Feld filtern, um nur aktive Türen anzuzeigen.

- Aut. Aktivierung: Dieses Feld ist gesetzt, wenn die Kommunikation mit der Türe unterbrochen wurde (siehe auch Spalte Kommunikation). GAT ACE wird in diesem Fall in einem einstellbaren Intervall versuchen die Türe wieder automatisch zu aktivieren. Die Zeit für die automatische Aktivierung wird in den Systemeinstellungen festgelegt (siehe "4.4. Einstellungsseite "Einstellungen"").
  Ist dieses Feld nicht gesetzt, so ist die Türe entweder nicht aktiv oder die Verbindung mit der Türe ist korrekt.
- Tür Status: Zeigt den aktuellen Öffnungsstatus der Türe. Die Anzeige kann nur mit angeschlossener und richtig konfigurierter Türrückmeldung korrekt dargestellt werden.
   .... Türe ist geschlossen
   .... Türe ist geöffnet
   ..... Türstatus ist nicht bekannt
- Schloss Status: Zeigt den aktuellen Status des Relais, das für die Ansteuerung des Türschlosses verwendet wird, an.
   .... Das Schloss der Türe ist verriegelt
   .... Das Schloss der Türe ist entriegelt
   ..... Schlossstatus ist nicht bekannt
- Kommunikation: Zeigt den aktuellen Status der Kommunikation mit dem Schloss an.
   .... Die Kommunikation mit der Türe ist OK
   .... Kommunikationsunterbrechung mit der Türe
   ..... Kommunikationsstatus ist nicht bekannt
- Initialisierung: Das Symbol zeigt den Initialisierungsstatus der Türe an.
   .... Die Türe ist vollständig initialisiert und betriebsbereit
   .... Die Tür wurde bereits initialisiert. Es wurde aber danach am zugehörigen Controller eine Änderung an der Konfiguration vorgenommen. Der Controller sollte darum neu beladen werden. Die Tür ist aber mit der bestehenden Konfiguration bereits betriebsbereit.
   …. Die Türe muss initialisiert werden, da Änderungsdaten vorhanden sind, die nur mit der Initialisierung an die Türe geladen werden.
   ..... Das Rufzeichensymbol zeigt an, dass die Tür gerade initialisiert wird. Eine Initialisierung sollte nicht länger als einige Minuten dauern.
- Noch zu sendende Kommandos:
  Wenn die Konfiguration einer Tür geändert wird, werden entsprechende Kommandos generiert, die an die Türe gesendet werden müssen. In dieser Spalten sehen Sie die noch zu sendenden Kommandos (erste Zahl) und die Gesamtanzahl der zu Kommandos um den Fortschritt der Initialisierung beurteilen zu können. Bei 0 / x ist die Türe vollständig initialisiert und in der Spate Initialisierung wird das Symbol  angezeigt.

► Um eine Funktion an einer Tür auszuführen, markieren Sie die Tür in der Liste.
  ○ Es sind dann folgende Funktionen in der Multifunktionsleiste verfügbar.

► Mit dem Symbol "Controller anzeigen" können Sie sich direkt den, zu der ausgewählten Tür gehörenden Controller anzeigen lassen.
► Wählen Sie das Symbol "Türe konfigurieren", um die Türkonfiguration zu öffnen.
  ○ Das Fenster den Konfigurationsdaten für die gewählte Tür wird angezeigt. Dieses ist in mehrere Registerkarten unterteilt.

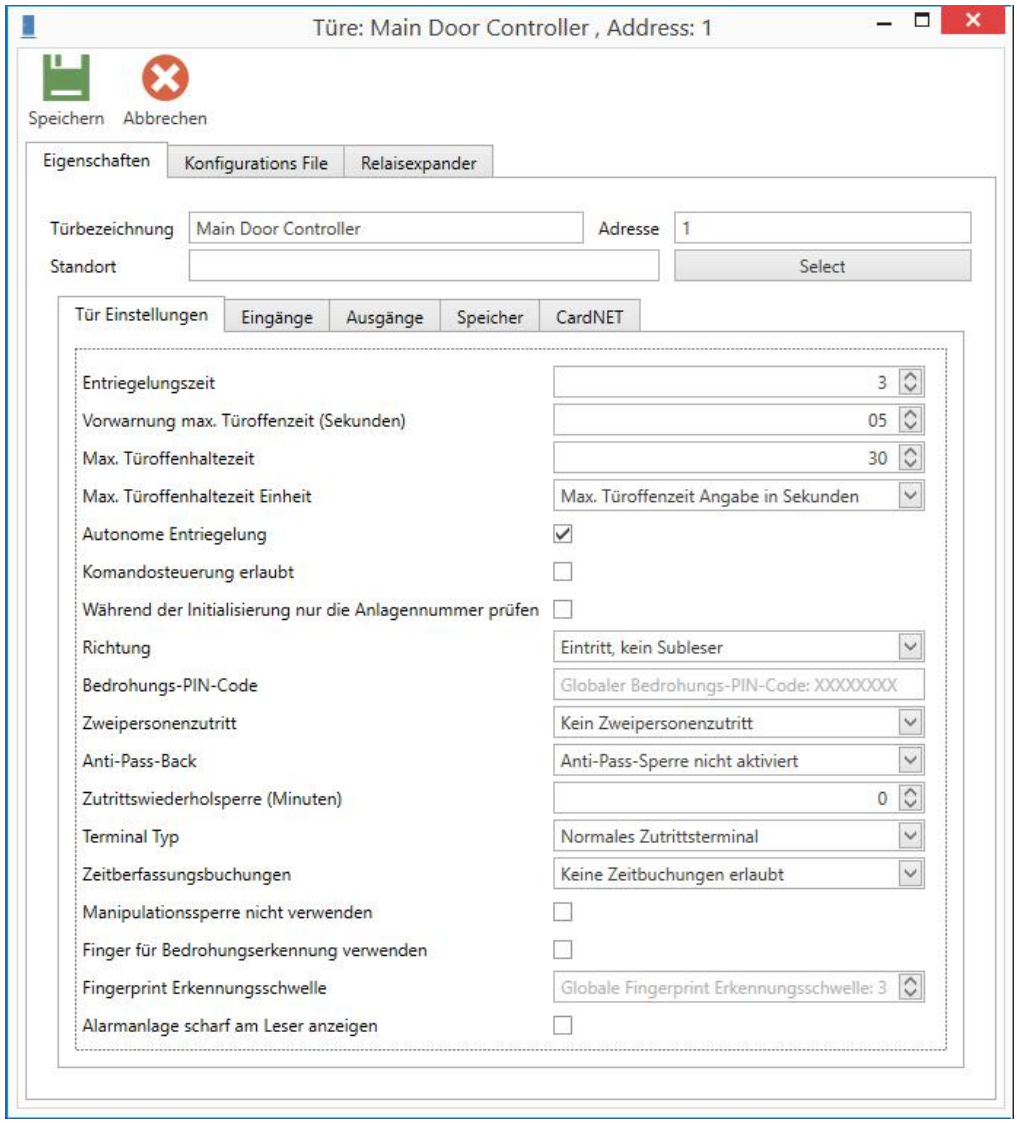


Bild 5.26 *- Tür konfigurieren, allgemeine Einstellungen*

► Definieren Sie auf der Registerkarte "Eigenschaften" die Einstellungen der Tür. Folgende Einstellungen sind möglich:

- Entriegelungszeit: Zeit (in Sekunden) für die die Tür bei gültiger Identifikation entriegelt wird.
- Vorwarnung max. Türoffenzeit: Diese Zeit (in Sekunden) bestimmt bei einer geöffneten Tür, wieviele Sekunden vor Erreichen der "Max. Türoffenhaltezeit" (siehe nächster Punkt) eine Vorwarnung ausgelöst wird.
- - Max. Türoffenhaltezeit: Diese Zeit bestimmt, wie lange die Tür nach gültiger Identifikation geöffnet sein darf, bevor ein Alarm ausgelöst wird. Wenn ein Relais des Controllers als "Tür-Offen-Alarm" definiert ist, wird dieses Relais aktiviert.
- - Max. Türoffenhaltezeit Einheit: Hier wird eingestellt, in welcher Einheit (Sekunden oder Minuten) die Türoffenhaltezeit eingegeben wird.
- - Autonome Entriegelung: Ist diese Option aktiviert, entscheidet der Controller, ob eine Identifizierung/ Zutrittsversuch gültig ist oder nicht. Falls dieses Feld nicht angekreuzt ist, muss die Autorisierungsentscheidung von einem höherrangigen System (Server) getroffen werden.
- - Kommandosteuerung erlaubt: Mit dieser Option kann eingestellt werden, ob der Controller mit Kommandos ferngesteuert werden kann. Diese Markierung muss gesetzt werden, wenn das Feld "Autonome Entriegelung" nicht markiert ist, oder falls ein Gebäudemanagementsystem die Tür durch das Senden eines Kommandos an den Controller öffnen können soll.
- - Während der Initialisierung nur die Anlagennummer prüfen:
  Während der Initialisierung einer Türe kann diese für einige Zeit keine vollständige Zutrittsprüfung durchführen. Soll während dieser Zeit trotzdem ein Zutritt möglich sein, so kann dieses Optionsfeld markiert werden. In dem Fall prüft der Controller während der Initialisierung nur, ob die Anlagennummer auf dem Datenträger mit den Ausweiseinstellungen übereinstimmt. D.h. es haben in der Zeit alle Datenträger, die in dieser Anlage gültig sind, Zutritt. Diese Funktion ist nur für codierte Datenträger möglich.
- - Richtung: Die Richtung wird für Türen und Controller älterer Bauform verwendet um zu spezifizieren welcher Leser für Eintritt und welcher für Austritt verwendet wird.
  - Eintritt, kein Subleser
  - Austritt, kein Subleser
  - Eintritt, Subleser Austritt
  - Austritt, Subleser Eintritt

  Für Türen und Controller neuer Bauform (an denen die Richtung in der Leserkonfiguration festgelegt wird) erfolgt mit dieser Einstellung die Definition der Richtung für Tasterentriegelungen.
- - Bedrohungs-PIN-Code: Es ist möglich einen Bedrohungs-PIN-Code zu definieren. Dieser kann mit dem persönlichen PIN-Code kombiniert werden, um im Falle einer erzwungenen Türöffnung einen stillen Bedrohungsalarm auszulösen.

  HINWEIS! Bei den Programmeinstellungen kann ein globaler Bedrohungs-PIN-Code definiert werden. Wenn bei der Türkonfiguration ein Wert für den Bedrohungs-PIN-Code eingetragen wird, wird die

globale Einstellung für diese Türe übersteuert. Wird nichts eingetragen, wird der globale Wert verwendet.
Im Bedrohungs-PIN-Code werden nur für einige Stellen des Codes die an diesen Stellen einzugebenden Zahlen definiert. Die restlichen Stellen werden mit "X" angegeben. An diesen Stellen muss die jeweilige Stelle des persönlichen PIN-Codes eingegeben werden.

Beispiel:

X	X	1	X	3	4	X	0	← Bedrohungs PIN-Code
-	-	-	2	4	8	8	2	← persönlicher PIN-Code
-	**-**	**1**	**2**	**3**	**4**	**8**	**0**	← PIN-Code, der eingegeben werden muss, um den Bedrohungs-Alarm auszulösen.

- Zweipersonenzutritt:

Diese Option wird auch "Vier-Augen-Zutritt" genannt. Um Zutritt zu erhalten sind hier zwei gültige Identifikationen hintereinander erforderlich.
Folgende Auswahlen sind möglich:
- Kein Zweipersonenzutritt
- Zweipersonenzutritt ohne Masterzwang
- Zweipersonenzutritt mit Masterzwang

- Anti-Pass-Back:

Ist die Option "Anti-Pass-Back" aktiviert, so ist es immer notwendig, Ein- und Austritt-Buchungen abwechselnd durchzuführen. Es ist dann nicht möglich, zwei Eintritt-Buchungen ohne dazwischenliegender Austritt-Buchung durchzuführen.

Ein lokales Anti-Pass-Back kann mit der Grundlizenz von GAT ACE realisiert werden. Dazu muss für eine Türe ein Ein- und ein Austrittsleser verwendet werden. Ein Anti-Pass-Back für eine Zone mit mehreren Türen ist nur mit einer entsprechenden Zusatzlizenz möglich.

Folgende Einstellungen sind möglich:

- nicht aktiviert:
  Die Anti-Pass-Back Funktion ist deaktiviert. Die Türe kann auch keine Anti-Pass-Back Zone zugewiesen werden.
- aktiviert:
  Die Anti-Pass-Back Funktion ist aktiviert. Beim Anti-Pass-Back in einer Zone wird die Anti-Pass-Back Prüfung auch dann durchgeführt, wenn nicht alle Türen der Zone online sind. Dies kann dazu führen, dass die Zone an der gleichen Türe verlassen werden muss wie sie betreten wurde.Nähere Informationen dazu siehe "4.3. Einstellungsseite "Anti-Pass-Back Zonen"".
- aktiviert, wenn das Terminal online ist:
  Die Anti-Pass-Back Funktion ist nur aktiv, wenn der Controller online ist, d.h. wenn Kommunikation zu GAT ACE besteht. In diesem Fall wird bei einer Kommunikationsunterbrechung die Anti-Pass-Back Funktion spätestens nach einer Minute deaktiviert und bei Wiederherstellung der Kommunikation automatisch wieder aktiviert.
  Diese Einstellung eignet sich für ein Zonen Anti-Pass-Back wenn der Komfort Mode für die Zone aktiviert wird.
  Nähre Informationen dazu siehe "4.3. Einstellungsseite "Anti-Pass-Back Zonen"".

- Zutrittswiederholsperre: Dadurch wird verhindert, dass nach einem gültigen Zutritt während einer gewissen Zeitspanne ein erneuter Zutritt mit derselben Karte (z. B. durch Weitergabe der Karte an eine andere Person) durchgeführt werden kann. Nach Ablauf der Zeitspanne ist ein Zutritt mit dem Datenträger wieder möglich.
- Terminal Typ: Hier wird die Art der Berechtigungsprüfung des Controllers definiert.
  - Normales Zutrittsterminal:
    Alle gelesenen Datenträger werden vollständig überprüft. Dies ist die Standardeinstellung.
  - Foyer Term. mit Branchenkennungspr.:
    Nur die ersten beiden Stellen der Datenträgernummern werden überprüft. Stimmen diese mit den definierten Branchencodes überein, ist ein Zutritt möglich.
  - Foyer Term. mit Bankleitzahlprüfung:
    Die auf den Datenträgern gespeicherten Bankleitzahlen werden auf Übereinstimmung mit der gespeicherten Liste von Bankleitzahlen überprüft.
- Zeiterfassungsbuchungen: In diesem Feld kann festgelegt werden, ob am Controller Zeitbuchungen möglich sein sollen und wenn ja, welche Zutrittsfunktion dabei ausgeführt werden soll.
  - Keine Zeitbuchungen erlaubt:
    Es sind keine Zeitbuchungen am Controller möglich.
  - Zeitbuchung erlaubt, kein automatischer Zutrittsversuch bei 'Kommen-Buchung':
    Es sind Zeitbuchungen am Controller möglich. Für einen Zutritt ist eine weitere, Identifikation notwendig.
  - Zeitbuchung erlaubt, automatischer Zutrittsversuch bei 'Kommen-Buchung':
    Es sind Zeitbuchungen am Terminal möglich. Wird eine gültige "Kommen"-Buchung erstellt, so wird die Tür automatisch entriegelt, sofern die Person anhand der gespeicherten Berechtigungsdaten zu diesem Zeitpunkt zutrittsberechtigt ist.
  - Zeitbuchung mit zusätzlicher Fingerprint-Verifikation erlaubt, kein automatischer Zutrittsversuch bei 'Kommen-Buchung':
    Es sind Zeitbuchungen am Controller möglich, wobei eine zusätzliche Verifikation mittels Fingerabdrucksensor möglich ist. Der Leser muss dafür über einen Fingerabdrucksensor verfügen (z. B. GAT FR 055). Für einen Zutritt ist eine weitere, gültige Identifikation notwendig.
  - Zeitbuchung mit zusätzlicher Fingerprint-Verifikation erlaubt, automatischer Zutrittsversuch bei 'Kommen-Buchung':
    Es sind Zeitbuchungen am Controller möglich, wobei eine zusätzliche Verifikation mittels Fingerabdrucksensor möglich ist. Der Leser muss dafür über einen Fingerabdrucksensor verfügen (z. B. GAT FR 055). Wird eine gültige "Kommen"-Buchung erstellt, so wird die Tür automatisch entriegelt, sofern die Person anhand der gespeicherten Berechtigungsdaten zu diesem Zeitpunkt zutrittsberechtigt ist.

- Manipulationssperre nicht verw.: Als Standard wird bei fünfmaliger Falscheingabe des PIN-Codes oder bei fünfmal ungültiger Verifikation mit einem Fingerabdruck die Person auf Grund eines Manipulationsversuchs gesperrt.
  Die Manipulationssperre kann durch Aktivierung dieses Punktes deaktiviert werden, so dass beliebig viele Versuche durchgeführt werden können. Dies kann ein Sicherheitsrisiko bedeuten!
  Die Deaktivierung ist nur bei Controllern des Type GAT Terminal 3100 und aktueller Firmware möglich. In älteren Versionen oder bei anderen Controllern bleibt die Manipulationssperre immer aktiv.
- Finger für Bedrohungserkennung verwenden:
  Wenn der Leser an der zu konfigurierenden Tür einen Fingerabdruckleser enthält, muss dieses Feld markiert werden, um den Fingerabdruckleser nutzen zu können.
- Fingerprint Erkennungsschwelle: Die Erkennungsschwelle definiert für einen Fingerabdruckleser wie genau die gelesenen Fingerabdrücke mit den gespeicherten Daten übereinstimmen müssen. Niedrigere Werte bedeuten hier, dass die Überprüfung der Fingerabdrücke anhand von weniger Merkmalen und mit höherer Toleranz erfolgt, wodurch die Fingerabdrücke häufiger akzeptiert werden.
  Höherer Werte bedeuten, dass die gelesenen Fingerabdrücke exakter mit den gespeicherten Fingerabdrücken übereinstimmen müssen was die Sicherheit erhöht, aber öfters zu Abweisungen und dadurch in mehrfachem Auflegen der Finger resultieren kann. Die Erkennungsschwelle sollte passend den Sicherheitsbedürfnissen gewählt werden. Der Standartwert ist 3
  HINWEIS! Bei den Programmeinstellungen kann eine globale Fingerprint Erkennungsschwelle definiert werden. Wenn bei der Türkonfiguration ein Wert für die Erkennungsschwelle eingetragen wird, wird dieser Wert verwendet und übersteuert den globalen Wert. Wird nichts eingetragen, wird der globale Wert verwendet.
- Alarmanlage scharf am Leser anzeigen:
  Wenn diese Funktion aktiviert ist, wird eine aktive Alarmanlage am Leser signalisiert.

► Wechseln Sie auf die Registerkarte "Eingänge", um die Funktion der Optokopplereingänge für die Tür zu definieren.
  ○ Die folgende Registerkarte wird angezeigt.

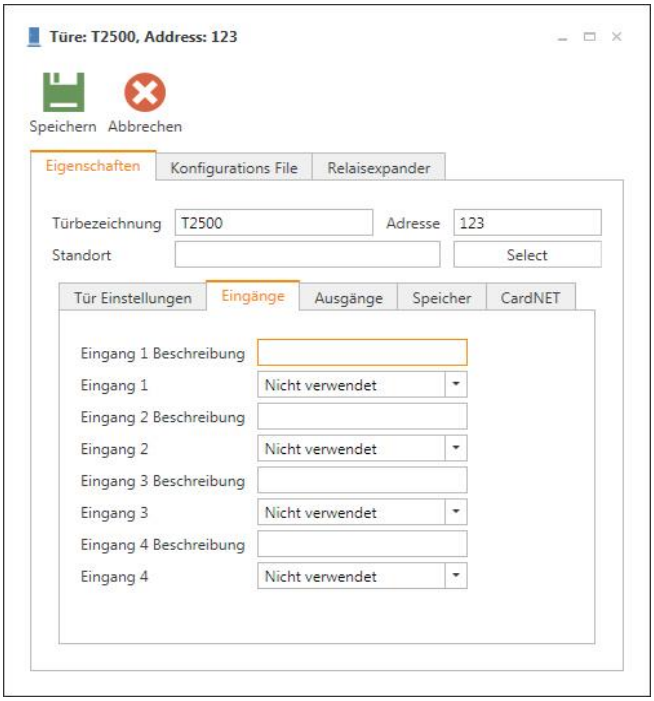


Bild 5.27 *- Tür konfigurieren, Eingänge*

► Definieren Sie hier die Funktion der Optokopplereingänge an der Tür. Folgende Einstellungen:

- Eingang x Beschreibung: Geben Sie für die verwendeten Eingänge einen Namen ein.
- Eingang x: Wählen Sie hier die Funktion der Eingänge. Um die korrekte Funktion sicherzustellen muss die gewählte Funktion mit der realen Verdrahtung der Eingänge übereinstimmen. Die meisten Funktionen sind in der Variante "Bestromung" oder "Unbestromt" verfügbar. Dieser Zusatz bestimmt, wann die jeweilige Funktion aktiv ist (d.h. aktiv wenn der Eingang bestromt oder unbestromt ist). Die prinzipielle Funktion ist aber bei den 2 Varianten dieselbe und wird darum für beide Varianten gemeinsam beschrieben.

Einstellung in GAT ACE	Einstellung in GAT Manager	Bedeutung	Wert
Nicht verwendet	Nicht verwendet	Wählen Sie diese Funktion für jene Eingänge, die nicht verwendet werden.	
Türrückmeldung, bestromt wenn Türe offen Türrückmeldung, nicht bestromt wenn Türe offen	Türe offen bei Bestromung Türe offen bei Stromunterbrechung	Über diesen Eingang wird dem Controller signalisiert, ob die Türe offen ist. Je nachdem, welche der beiden Funktionen gewählt wurde, ist die Türe bei bestromten oder unbestromten Eingang offen. Die Funktion wird üblicherweise über einen Türkontakt realisiert, der an diesem Eingang angeschlossen ist. Das Entriegelungsrelais fällt ab, sobald der Türstatus als offen gemeldet wird.	

		Erfolgt keine Identifikation, Tasteröffnung oder Fernsteuerung per Kommando und wird über den Eingang dennoch eine Türöffnung gemeldet, so führt dies zu einem Tür-Offen-Alarm (sofern nicht im Türzeitplan unterdrückt). Bei einer normalen Türöffnung wird über diesen Eingang auch die max. Türoffenhaltezeit überwacht (sofern nicht im Türzeitplan unterdrückt).	
Tasterentriegelung, bestromt für Türöffnung Tasterentriegelung, nicht bestromt für Türöffnung	Taster Entriegelung bei Bestromung Taster Entriegelung bei Stromunterbrechung	Ist diese Funktion aktiv (z.B. durch Drücken eines Tasters, Drückerbetätigung oder Sprechanlage), so wird eine Türöffnung ausgelöst und dieser Vorgang als Buchung protokolliert. Die Ein-/Austrittsrichtung dieser Buchung ist entgegengesetzt der Richtung die für die Türe definiert ist, d.h. ist. Die Entriegelungsdauersetzt sich aus der Zeit der Tasterbestromung/ -unterbrechung plus der eingestellten Entriegelungszeit zusammen.	
Sperre Ein- u . Austritt, bestromt für Sperre Sperre Ein- u . Austritt, nicht bestromt für Sperre	Verriegelung Ein- und Austritt bei Bestromung Verriegelung Ein- und Austritt bei Stromunterbrechung	Ist diese Funktion aktiv, so ist weder ein Eintritt noch ein Austritt möglich. Auch die Tasterentriegelung hat keine Funktion mehr. Dies wird z.B. bei Schleusen verwendet um eine Türe zu sperren solange die gegenüberliegende Türe geöffnet ist.	
Sperre Eintritt, bestromt für Sperre Sperre Eintritt, nicht bestromt für Sperre	Verriegelung Eintritt bei Bestromung Verriegelung Eintritt bei Stromunterbrechung	Ist diese Funktion aktiv, so ist kein Eintritt möglich. Dies wird z.B. bei Schleusen verwendet wenn eine Person im Schleusenraum ist um zu verhindern, dass die Schleuse von außen geöffnet werden kann. Diese Funktion kann aber genauso verwendet werden, um einen Zutritt zu verhindern wenn die Einbruchmeldeanlage scharf geschaltet ist.	
Allgemeiner Alarm, bestromt für Alarm Allgemeiner Alarm, nicht bestromt für Alarm	Allgemeiner Alarm bei Bestromung Allgemeiner Alarm bei Stromunterbrechung	Ist diese Funktion aktiv, so wird ein Alarm erzeugt und gespeichert. Dies ist sowohl als Buchung als auch als online Statusmeldung (z. B. für einen Gebäudeleitstand) zu erkennen. Dieser Alarm bleibt solange gespeichert bis er über ein Kommando quittiert wird.	
Überwachung 0 (Online Anzeige, keine Buchungen bei Statuswechsel)	Statusmeldung 0, Online Anzeigemöglichkeit ohne Buchung bei Statuswechsel	Der aktuelle Status des Eingangs wird erfasst und kann als online Statusmeldung abgefragt werden. Es erfolgt keine Speicherung des Status und es werden bei Statusänderungen keine Buchungen erstellt.	

Überwachung 1 (Buchung bei Statuswechsel)	Statusmeldung 1, Buchung bei Statuswechsel	Bei jedem Statuswechsel wird eine Buchung erzeugt, in den Zusatz-informationen der Buchung ist erkennbar, in welche Richtung der Status gewechselt ist. Eine Abfrage dieses Signals als online Statusmeldung ist NICHT möglich.	
Überwachung 2 (Onlineanzeige, Buchung bei Statuswechsel, Relais)	Statusmeldung 2, Buchung bei Statuswechsel und Onlineanzeigemöglic hkeit	Bei jedem Statuswechsel wird eine Buchung erzeugt. In den Zusatz-informationen der Buchung ist erkennbar, in welche Richtung der Status gewechselt ist. Eine Abfrage des Status als online Statusmeldung st möglich und somit kann der Status auch am PC angezeigt wer-den. Außerdem kann ein Relais definiert werden, das bei einem Statuswechsel angesteuert wird (siehe "Konfiguration der Ausgänge").	
Riegelrückmeldung, bestromt wenn Riegel zurückgezogen Riegelrückmeldung, nicht bestromt wenn Riegel zurückgezogen	Türe offen bei Bestromung mit voller Entriegelungszeit Türe offen bei Stromunterbrechung mit voller Entriegelungszeit	Wenn dieser Eingang aktiv ist, ist der Riegel der Türe zurückgezogen, d.h. die Türe ist entriegelt und kann geöffnet werden. Im Gegensatz zur Türrückmeldung wird jedoch das Entriegelungsrelais durch diesen Eingang nicht zurückgesetzt. Die weiteren Funktionen sind wie bei der Türrückmeldung.	
Alarmanlage bereit, bestromt wenn EMA scharfschaltebereit Alarmanlage bereit, nicht bestromt wenn EMA scharfschaltebereit	Schaltrelais Freigabe bei Bestromung Schaltrelais Freigabe bei Stromunterbrechung	Der Ausgang „EMA ein/aus“ (siehe Ausgangskonfiguration) kann über die Taste "ON" am Controller nur dann betätigt werden, wenn dieser Eingang aktiviert ist. Damit kann z.B. die Scharfschalt-bereitschaft einer Einbruchmeldeanlage an den Controller gemeldet werden.	
Türzeitplan unter-drücken, bestromt wenn GO unterdrückt werden soll Türzeitplan unter-drücken, nicht bestromt wenn GO unterdrückt werden soll	Generell-Offen-Unterdrückung bei Bestromung Generell-Offen-Unterdrückung bei Stromunterbrechung	Ist diese Funktion aktiv während ein Türzeitplan aktiv ist, so wird die Entriegelung, die im Türzeitplan definiert ist, unterdrückt. Zutritte von Personen sind möglich, wenn diese im Zeitplan der Personen zugelassen sind. Wird diese Funk-tion deaktiviert, so ist der Türzeitplan wieder aktiv.	
Tasterentriegelung, Türöffnung bei Wechsel von nicht bestromt auf bestromt	Tasterentriegelung bei Bestromung (flankengesteuert)	Wechselt der Eingang von unbe-stromt auf bestromt, so wird eine Türöffnung ausgelöst und dieser Vorgang als Buchung protokolliert. Die Entriegelungszeit wird bei dieser Optokoppler Einstellung nur durch die eingestellte Entriegelungszeit nicht aber durch die Dauer der	

		Optokoppler Bestromung bestimmt. Die weiteren Funktionen sind wie bei der normalen Tasterentriegelung.	
Tasterentriegelung, Türöffnung bei Wechsel von bestromt auf nicht bestromt	Tasterentriegelung bei Stromunterbrechung (flankengesteuert)	Wechselt der Eingang von bestromt auf unbestromt, so wird eine Tür-öffnung ausgelöst und dieser Vor-gang als Buchung protokolliert. Die Entriegelungszeit wird bei dieser Optokoppler Einstellung nur durch die eingestellte Entriegelungszeit nicht aber durch die Dauer der Optokoppler Bestromung bestimmt. Die weiteren Funktionen sind wie bei der normalen Tasterentriegelung.	
EMA scharf, bestromt wenn Alarmanlage scharf EMA scharf, nicht bestromt wenn Alarmanlage scharf	Alarmanlage scharf bei Bestromung Alarmanlage scharf bei Strom Unterbrechung	Über diesen Eingang kann der Status einer Alarmanlage an den Controller gemeldet werden. Damit kann die Sperre der Zutritts, die Verwendung der Taste OFF und die Signalisierung des Zustands der Einbruchmeldeanlage am Leser gesteuert werden.	

► Wechseln Sie auf die Registerkarte "Ausgänge", um die Funktionen der Relaisausgänge an der Tür festzulegen.
  ○ Die folgende Registerkarte wird angezeigt.

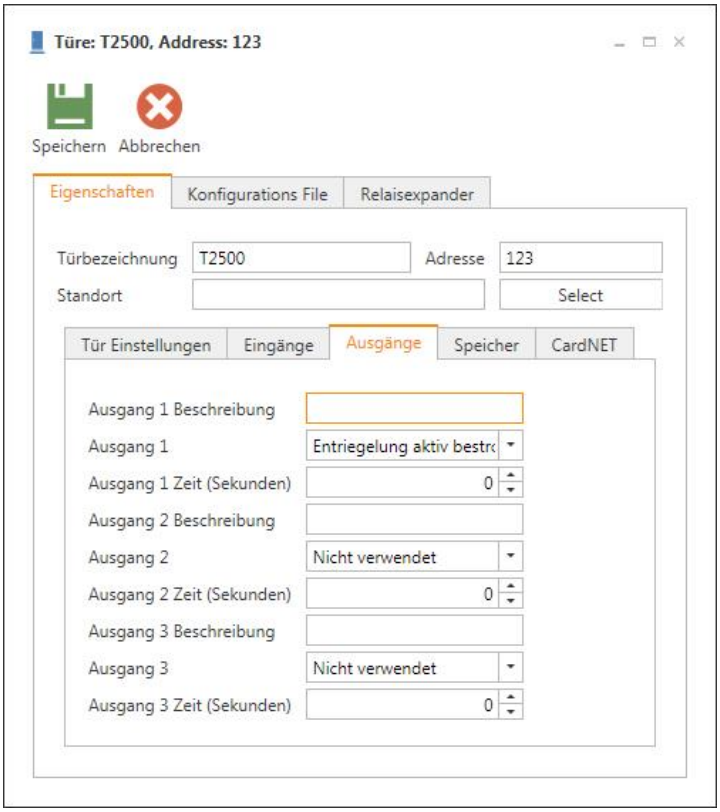


Bild 5.28 *- Tür konfigurieren, Ausgänge*

► Definieren Sie hier die Funktion der Relaisausgänge an der Tür. Folgende Einstellungen sind möglich:

- Ausgang x Beschreibung: Geben Sie für die verwendeten Ausgänge einen Namen ein.
- Ausgang x: Wählen Sie hier die Funktion der Relaisausgänge für die Tür. Um die korrekte Funktion sicherzustellen muss die gewählte Funktion mit der realen Verdrahtung der Ausgänge übereinstimmen. Die meisten Funktionen sind in der Variante "Relais aktiv" oder "Relais passiv" möglich. Dieser Zusatz bestimmt, wie das Relais geschaltet wird. Relais aktiv = Relais wird bestromt, wenn die betreffende Funktion aktiv ist. Relais passiv = Relais wird bestromt, wenn die betreffende Funktion nicht aktiv ist. Die prinzipielle Funktion ist bei den zwei Varianten dieselbe und wird deshalb für beide Varianten gemeinsam beschrieben.

Einstellung in GAT ACE	**Einstellung in GAT Manager**	**Bedeutung**	**Wert**
Nicht verwendet	Nicht verwendet	Wählen Sie diese Funktion für jene Ausgänge, die nicht verwendet werden.	
Entriegelung Ein- und Austritt, Relais aktiv Entriegelung Ein- und Austritt, Relais passiv	Entriegelung Ein- und Austritt, Arbeitskontakt Entriegelung Ein- und Austritt, Ruhekontakt	Das Relais wird für die Türentriegelung verwendet. Wenn eine Person eine Identifikation vornimmt und die Berechtigung zum Öffnen der Türe vorliegt ist die Funktion aktiv, d.h. das Relais wird je nach gewählter Variante bestromt bzw. nicht bestromt. Der Zeitraum, das Ablaufdatum usw. wird bei der Berechtigungsprüfung mit herangezogen. Genauso ist diese Funktion aktiviert, wenn ein Türzeitplan aktiv ist oder eine Öffnung über eine Tasterentriegelung vorgenommen wird oder vom PC ein Öffnungsbefehl kommt. Die Einstellung der Zeit hat bei dieser Funktion keine Bedeutung.	
Alarmunterdrückung, Relais aktiv Alarmunterdrückung, Relais passiv	Alarmunterdrückung, Arbeitskontakt Alarmunterdrückung, Ruhekontakt	Diese Funktion wird verwendet um z.B. einen Magnetkontakt einer Alarmschleife zu überbrücken, wenn die Einbruchmeldeanlage scharf geschaltet ist aber bei einem gültigen Zutritt kein Alarm ausgelöst werden soll. Der Ausgang wird zusammen mit dem Entriegelungsrelais angesteuert. Die Zeit bei dieser Funktion bestimmt, wie lange das Alarmunterdrückungsrelais angesteuert wird. Es bleibt so lange aktiviert, wie die Türe offen ist plus die im Feld angegebenen Zeit (um durch ein Prellen des Magnetkontakts keinen Alarm auszulösen).	

Türe-offen-Alarm, Relais aktiv Türe-offen-Alarm, Relais passiv	Tür-offen-Alarm, Arbeitskontakt Tür-offen-Alarm, Ruhekontakt	Bei Überschreitung der "Tür zu lange offen" Zeit oder bei einer Türöffnung ohne Identifikation (z. B. Aufbruch) wird diese Funktion aktiviert. Der genaue Grund der Alarmauslösung kann im online Status oder in den Buchungen ausgewertet werden. Die einzelnen Gründe können im Türzeitplan deaktiviert werden (z. B. Öffnen ohne Berechtigung deaktivieren). Die Zeit bei dieser Funktion bestimmt, wie lange das Relais aktiviert bleibt (Sekunden). Bei der Eingabe von 0 Sekunden wird es so lange aktiviert wie die Türe offen bleibt.	
Bedrohungs-Alarm, Relais aktiv Bedrohungs-Alarm, Relais passiv	Bedrohungsarlarm, Arbeitskontakt Bedrohungsalarm, Ruhekontakt	Diese Funktion wird dann aktiviert, wenn abweichend vom PIN-Code der Person ein Bedrohungs-PIN-Code eingegeben wird oder die Identifikation mit dem definierten Bedrohungsfingerabdruck erfolgt. Der Bedrohungs-PIN-Code wird aus einer Kombination des persönlichen PIN-Codes und des Bedrohungs-Codes gebildet. Die Zeit bei dieser Funktion bestimmt, wie lange das Relais aktiviert bleibt (Sekunden).	
Entriegelung Eintritt, Relais aktiv Entriegelung Eintritt, Relais passiv	Entriegelung Eintritt, Arbeitskontakt Entriegelung Eintritt, Ruhekontakt	Diese Funktion ist dann aktiv, wenn eine Person eine Identifikation am Eintrittsleser vornimmt und die Berechtigung zum Öffnen der Türe vorliegt. Der Zeitraum, das Ablaufdatum usw. wird bei der Berechtigungsprüfung mit berücksichtigt. Die Einstellung der Zeit hat bei dieser Funktion keine Bedeutung.	
Entriegelung Austritt, Relais aktiv Entriegelung Austritt, Relais passiv	Entriegelung Austritt, Arbeitskontakt Entriegelung Austritt, Ruhekontakt	Diese Funktion ist dann aktiv, wenn eine Person eine Identifikation am Austrittsleser vornimmt und die Berechtigung zum Öffnen der Türe vorliegt. Der Zeitraum, das Ablaufdatum usw. wird bei der Berechtigungsprüfung mit berücksichtigt. Die Einstellung der Zeit hat bei dieser Funktion keine Bedeutung.	
Video Überwachung, Relais aktiv	Video Funktion, Arbeitskontakt	Diese Funktion wird aktiviert sobald am Terminal ein Datenträger eingelesen wird (unabhängig ob berechtigt oder nicht) oder eine Taste betätigt wird. Somit kann diese Relaisfunktion z. B. benutzt	

		werden, um zum Beilspiel eine Überwachungskamera zu aktivieren, sobald an der Türe eine Aktion erfolgt. Die Zeit bei dieser Funktion bestimmt, wie lange das Relais aktiviert bleibt (Sekunden).	
Sonderberechtigung, Relais aktiv Sonderberechtigung, Relais passiv	Sonderberechtigung, Arbeitskontakt Sonderberechtigung, Ruhekontakt	Wenn für eine Person an der Türe die Sonderberechtigung definiert ist, so wird diese Funktion bei einer gültigen Identifikation mit genau dem gleichen Zeitverhalten wie das Entriegelungsrelais angesteuert.	
EMA ein/aus (0 .. 24 Uhr, mit Sonder-berechtigung), Relais aktiv EMA ein/aus (0 .. 24 Uhr, mit Sonder-berechtigung), Relais passiv	Schaltrelais, Arbeitskontakt Schaltrelais, Ruhekontakt	Mit dieser Funktion kann von Personen, die an der Türe eine Sonderberechtigung besitzen, über die Taste "ON" (früher Taste "8") die Einbruchmeldeanlage aktiviert werden. Ist die Zeit auf 0 gestellt oder ein Eingang mit der Funktion „EMA scharf“ definiert kann das Relais über die Taste "OFF" (früher Taste "2") zurück gestellt werden. Ist die Zeit ungleich 0 eingestellt und kein Eingang „EMA scharf“ definiert wird nur auf die Taste "ON" reagiert und ein Impuls mit entsprechender Länge abgesetzt. Die Betätigung der Tasten "ON" und "OFF" ist nur für Personen mit Sonderberechtigung möglich. Für die Taste "OFF" ist zwingend die Eingabe eines PIN-Codes er-forderlich. Die Verwendung der Taste "ON" kann über den Eingang "Alarm-anlage bereit" verhindert werden wenn die Einbruchmeldeanlage nicht bereit ist, scharf geschaltet zu werden.	
EMA ein/aus (Zeitplan gesteuert), Relais aktiv EMA ein/aus (Zeitplan gesteuert), Relais passiv	Schaltrelais zeitplangesteuert, Arbeitskontakt Schaltrelais zeitplangesteuert, Ruhekontakt	Diese Funktion erlaubt die scharf/ unscharf Schaltung der Einbruch-meldeanlage mit den gleichen Prüfungen wie der Zutritt gestattet wird. Wird zum jeweiligen Zeitpunkt für den Zutritt ein PIN Code benötigt, muss auch für die EMA Steuerung ein PIN Code eingegeben werden. Die Sonderberechtigung und die Scharfschaltebereitschaft der EMA wird nicht geprüft.	

Überwachungseingang, Relais aktiv bei steigender Flanke von Überwachung 2 Überwachungseingang, Relais aktiv bei fallender Flanke von Überwachung 2	Impuls bei steigender Flanke der Statusmeldung 2 Impuls bei fallender Flanke der Statusmeldung 2	Wird ein Optokopplereingang als "Überwachung 2" definiert, so wird beim Wechsel vom unbestromten in den bestromten Zustand ("positive Flanke") bzw. vom bestromten in den unbestromten Zustand ("negative Flanke") des Opto-kopplers dieser Ausgang aktiviert. Die Zeit bei dieser Funktion be-stimmt, wie lange die Funktion aktiviert wird (Sekunden).	
Türe offen Ausgang, Relais aktiv wenn Türe offen	Türoffen Ausgang	Wird ein Optokopplereingang als Türrückmeldung ("Türrückmeldung bestromt wenn Türe offen/geschlossen") definiert, so wird der Türstatus auf diesem Aus-gang als potentialfreier Kontakt zur Verfügung gestellt. Das Relais wird angesteuert wenn die Türe über den Optokoppler als offen gemeldet wird.	
EMA aus Impuls (0 .. 24 Uhr, mit Sonderberechtigung), Relais aktiv EMA aus Impuls (0 .. 24 Uhr, mit Sonderberechtigung), Relais passiv	Schaltrelais Impuls unscharf aktiv bestromt Schaltrelais Impuls unscharf passiv bestromt	Diese Funktion erlaubt es Personen mit Sonderberechtigung über die Taste "OFF" (früher Taste "2") einen Impuls zu erzeugen, der die Einbruch-meldeanlage auf unscharf stellt. Die Funktion ist nur zusammen mit dem Eingang „EMA scharf“ einsetzbar. Die Eingabe eines PIN Codes ist zwingend erforderlich. Ist die Zeit für den Impuls kann zwi-schen 1 und 5 Sek. gewählt werden.	

► Wechseln Sie auf die Registerkarte "Speicher".

○ Die folgende Registerkarte wird angezeigt.

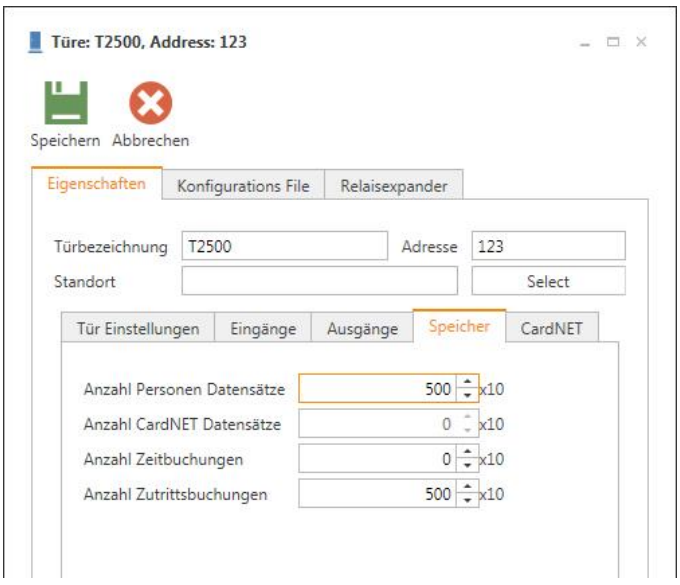


Bild 5.29 *- Tür konfigurieren, Speicher*

► Definieren Sie hier den Speicher, der für die Tür zur Verfügung stehen soll, um Daten zu speichern.

HINWEIS! Beachten Sie, dass für einige Controllertypen die Eingaben mit 10 multipliziert werden, d.h. im Beispiel oben ist die Anzahl Personen Datensätze mit 500 angegeben -> 5000 Personendatensätze können gespeichert werden.

Folgende Einstellungen sind möglich:

- Anzahl Personen Datensätze: Anzahl der personenbezogenen Datensätze, die im Controller für diese Tür reserviert sind.
- Anzahl CardNET Datensätze: Anzahl der personenbezogenen Datensätze für den Einsatz im CardNET Modus, bei dem die Personaldaten für den CardNET Modus im Controller gespeichert und dort auf die Datenträger übertragen werden können. Wenn der CardNET Modus nicht verwendet wird (siehe nächste Registerkarte), kann dieses Feld mit 0 belassen werden.
- Anzahl Zeitbuchungen: Das ist die Anzahl der Zeitbuchungen, die im Terminal gespeichert werden können. Wenn der Speicher voll ist, sind keine weiteren Zeitbuchungen möglich.
- Anzahl Zutrittsbuchungen: Das ist die Anzahl der Zutrittsbuchungen, die im Terminal gespeichert werden können. Der Speicher für die Zutrittsbuchungen wird als Ringbuffer verwaltet, was bedeutet, dass die älteste Buchung überschrieben wird, wenn der Speicher voll ist und eine neue Buchung gespeichert werden soll.

► Um den CardNET Modus zu konfigurieren wechseln Sie auf die Registerkarte "CardNET".

HINWEIS! Im CardNET Modus werden die Berechtigungen für Offline Türen auf die Datenträger der Personen gespeichert. Das Schreiben dieser Daten kann an Online Türen erfolgen, bei denen der CardNET Modus aktiviert ist. Das Schreiben erfolgt dann automatisch sobald ein Datenträger am Leser des Controllers gelesen wird.

○ Die folgende Registerkarte wird angezeigt.

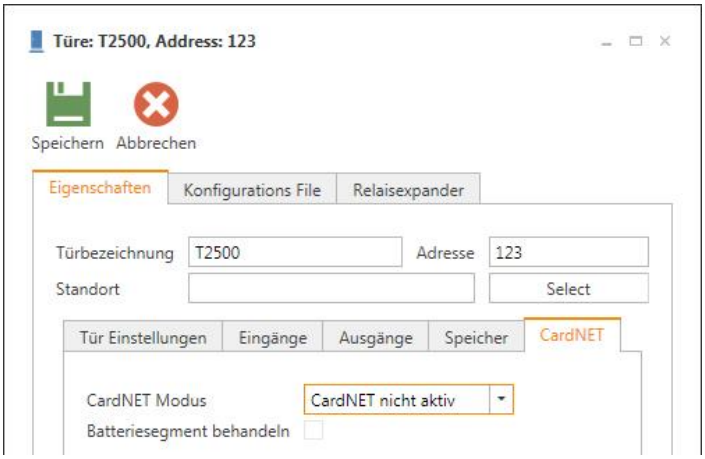


***Bild 5.30** - Tür konfigurieren, CardNET*

► Definieren Sie hier die Funktion des CardNET Modus. Folgende Einstellungen sind möglich:

- CardNET Modus: Wählen Sie den gwünschten CardNET Modus aus:
  - CardNET nicht aktiv:
    Es werden an dieser Türe keine CardNET Berechtigungen auf Datenträger geschrieben

- CardNET aktiv:
  Berechtigungen für Offline Türen werden an dieser Türe auf Datenträger geschrieben. Auch wenn der Schreibvorgang nicht erfolgreich war, wird der Zutritt gestattet, sofern dieser für die Person zum entsprechenden Zeitpunkt auch gestattet ist.
- Zutritt nach erfolgreichem CardNET Schreibvorgang:
  Der Zutritt wird nur dann gestattet, wenn der Schreibvorgang erfolgreich abgeschlossen werden konnte.
  HINWEIS! Diese Funktion darf nur dann aktiviert werden, wenn alle Datenträger mit entsprechenden Datenbereichen für CardNET Berechtigungen codiert sind. Anderenfalls wäre für Personen ohne diese Datenbereiche der Zutritt nicht möglich.

- Batteriesegment behandeln: Wird diese Option aktiviert, werden Batteriewarnungen und sonstige Rückmeldungen vom Offline Schloss ausgewertet und behandelt und so Informationen über einen erforderlichen Batterietausch zurückgemeldet.
  HINWEIS! Diese Funktion soll nur dann deaktiviert werden, wenn kein Datenbereich für Batteriemeldungen auf den Ausweisen codiert wurde.

► Die verfügbaren Parameter für Tür werden aus Konfigurations Files gelesen und die Einstellungen in eine Kommandodatei eingetragen. Diese kann in der Registerkarte "Konfigurations File" angezeigt werden.
HINWEIS! Ändern Sie diese Files nur in Rücksprache mit unserem Support, da anderen Falls die Funktion des Systems gestört werden kann.

► Wird an der Tür ein oder mehrere Relaisexpander verwendet, können sie diesen unter der Registerkarte "Relaisexpander" konfigurieren.

Folgende Registerkarte wird angezeigt.

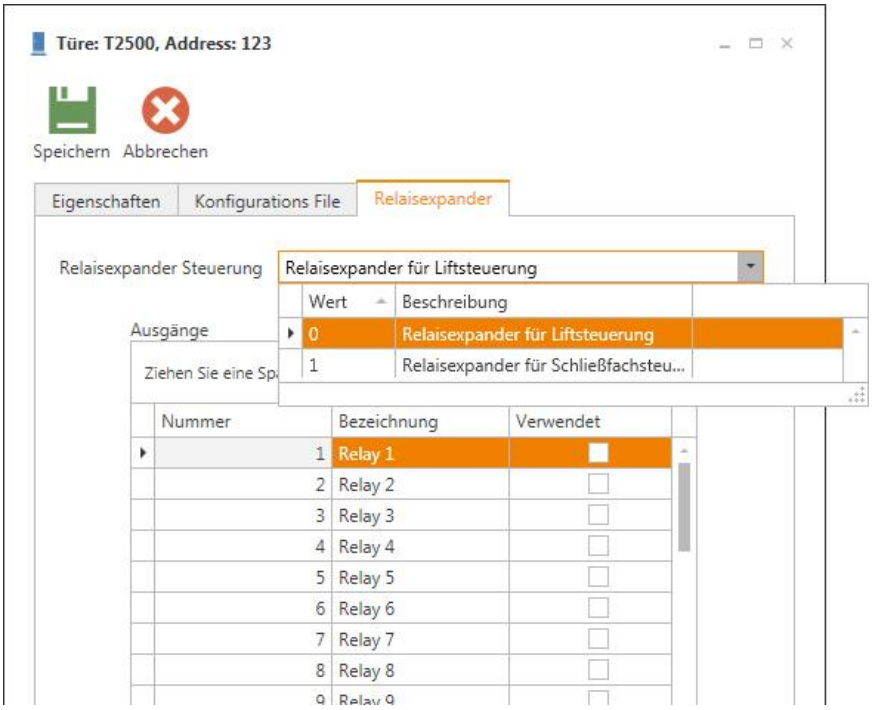


Bild 5.31 *- Tür konfigurieren, Weitere Ausgänge mittels Relaisexpander*

► Wählen Sie im Feld "Relaisexpander Steuerung" den Modus für die erweiterten Relaisausgänge. Folgende Auswahl steht zur Verfügung:

- .. für Liftsteuerung: Bis zu 32 Relaisausgängen werden entsprechend den Berechtigungen der Person aktiviert. Die Relais werden gleichzeitig mit dem Entriegelungsrelais angesteuert. Diese Funktion wird für die Auswahl eines Stockwerks am Tableau des Aufzugs verwendet.
- .. für Schließfachsteuerung: Die gewünschte Fachnummer (1 - 32) muss nach der Identifikation eigegeben werden. Bei vorliegender Berechtigung wird nur das Relais des gewählten Fachs angesteuert. In der Buchung wir d die Fachnummer protokolliert. Hinweis: Diese Funktion ist nur möglich, wenn der verwendete Leser eine Tastatur zur Eingabe der Nummer hat!

► Markieren Sie die Relais des Relaisexpanders, die verwendet werden sollen und geben Sie den Relais eine passende Bezeichnung. Dadurch ist die Verwaltung der Berechtigungen in GAT Matrix wesentlich einfacher.

► Wählen Sie das Symbol "Speichern", um die Konfiguration der Tür zu speichern und in die Türansicht zurückzugelangen.

5.2.10 Türe aktivieren und deaktivieren

Damit Berechtigungen an eine Türe geladen werden, muss diese in GAT ACE aktiviert sein. Alle nicht verwendeten Türen können deaktiviert werden. Dies hilft für mehr Übersicht in der Türliste und der Controlleransicht, indem die dort dargestellten Listen so gefiltert werden, dass nur aktive Türen angezeigt werden.
Ob eine Türe aktiviert ist sehen Sie in der Türansicht an der Markierung in der Spalte "Aktiv". Ein Haken bedeutet, dass die Türe aktiviert ist.

► Um eine Tür zu aktivieren oder deaktivieren markieren Sie die Tür in der Türliste.

► Wählen Sie das Symbol "Aktivieren", um eine Tür zu aktivieren. Jede Tür, die in der Anlage verwendet werden soll, muss aktiviert sein.

► Wählen Sie das Symbol "Inaktiv", um die markierte Tür zu deaktivieren.

► Eine weitere Möglichkeit ist die Auswahl dieser beiden Punkte aus dem Pop-Up Menü das erscheint, wenn die Tür mit der rechten Maustaste geklickt wird.

Automatisches aktivieren:

Wenn für eine Tür die Option "Automatische Aktivierung" aktiv ist, wurde die Kommunikation mit der Türe unterbrochen. GAT ACE wird in periodischen Abständen wieder versuchen, eine Verbindung aufzubauen und die Tür zu aktivieren. Die Zeitspanne, nach denen GAT ACE jeweils diese Versuche durchführt, kann bei den Programmeinstellungen definiert werden (siehe "4.4. Einstellungsseite "Einstellungen"").

5.2.11 Controller initialisieren

Beim Initialisieren eines Controllers werden der entsprechende Konfigurationsparameter für den Controller und alle an diesen Controller angeschlossenen Türen gesendet. Dieser Vorgang ist für die erste Inbetriebnahme des Controllers aber auch bei Änderungen der Hardware (z. B. angeschlossenen Leser) notwendig.

Sobald Änderungen an den Controllereinstellungen vorgenommen wurden, wird dies in der Liste der Controller in der Spalte "Initialisierung" durch das Symbol angezeigt. Über diese Spalte können Sie eine Filterung vornehmen, so dass nur jene Controller angezeigt werden, die initialisiert werden müssen. Sie können in diesem Fall alle angezeigten Controller auswählen und diese gemeinsam initialisieren.

Durch die Initialisierung des Controllers mit Formatierung des Speichers wird der Controller am Beginn der Initialisierung bis auf die Kommuniaktionsparameter auf Werkseinstellungen zurückgesetzt. Bei einigen Controllern kann es dadurch auch zu einem Verlust von Buchungen kommen. Achten Sie aus diesem Grund darauf, dass alle Buchungen aus dem Controller ausgelesen wurden, bevor Sie die Speicherformatierung durchführen.

HINWEIS: Wenn ein WiNET Schloss von einem WiNET Controller entfernt wird, muss der gesamte Controller inklusive Speicherformatierung neu initialisiert werden.

- ► Markieren Sie den zu initialisierenden Controller in der Controlleransicht.
- ► Um diesen zu initialisieren wählen Sie das Symbol "Initialisieren".
- ► Wählen Sie aus, ob Sie die Speicher Formatierung durchführen möchten oder nicht
- ► In der Spalte Initialisierung wird für die Dauer der Initialisierung ein Fortschrittsbalken gezeigt, aus dem ersichtlich ist wie viele Kommandos noch zu senden sind.
- ► Ist die Initialisierung korrekt abgeschlossen, so wird in der Spalte "Initialisierung" ein grüner Daumen angezeigt.
- ► Im Fehler Fall erscheint in der Spalte Initialisierung ein rotes Rufzeichen . Dieses zeigt an, dass es bei der Initialisierung ein Problem gab und die Türe unter Umständen nicht korrekt funktionieren wird. Weitere Informationen dazu erhalten Sie bei unserem Support.
- ► Wurde der Speicher formatiert, so wird im Anschluss der Controller Initialisierung auch eine automatische Initialisierung der Türen des Controllers gestartet um die Türen wieder betriebsbereit zu machen. Mehr dazu finden Sie im folgenden Kapitel.

5.2.12 Türe initialisieren

Wenn in GAT ACE Konfigurationsänderungen an Türen durchgeführt wurden, müssen die betreffenden Türen initialisiert werden, d.h. die Änderungen müssen an die Türen gesendet werden. Dies erfolgt mit der Funktion Türe initialisieren.

Sobald Änderungen an einer Türkonfiguration vorgenommen werden, wird dies in der Liste der Türen in der Spalte "zu laden" angezeigt. Über diese Spalte können Sie eine Filterung vornehmen, so dass nur jene Türen angezeigt werden, die initialisiert werden müssen. Sie können in diesem Fall alle angezeigten Türen auswählen und diese gemeinsam initialisieren.

Berechtigungen, die von GAT Matrix an GAT ACE gesendet werden, werden automatisch an die Türen gesendet, so dass in diesem Fall keine Initialisierung in GAT ACE erforderlich ist.

HINWEIS! Erst wenn eine Türe korrekt initialisiert ist, sind Konfigurations- und Berechtigungsänderungen wirksam. Achten Sie darauf, dass der GAT ACE 3000 Dienst läuft, da sonst kein Beladen stattfindet und Konfigurationsänderungen nicht wirksam werden können.

► Markieren Die die zu initialisierende Tür in der Türansicht.

► Um die Tür zu initialisieren wählen Sie das Symbol "Initialisieren".

In der Spalte „Noch zu sendende Kommandos“ erscheinen ein Fortschrittsbalken und eine Anzahl wie viele Kommandos noch zu senden sind.

- Ist die Initialisierung korrekt abgeschlossen, so wird in der Spalte "Initialisierung" ein grüner Daumen angezeigt.
- Im Fehler Fall erscheint in der Spalte Initialisierung ein rotes Rufzeichen . Dieses zeigt an, dass es bei der Initialisierung ein Problem gab und die Türe unter Umständen nicht korrekt funktionieren wird. In diesem Fall können Sie die Kommandos die nicht korrekt gesendet werden konnten Kontextmenu unter „Kommandos zeigen“ anzeigen.

5.2.13 Zu sendende Kommandos anzeigen

Nach der Änderung einer Türkonfiguration oder wenn die Tür initialisiert werden muss erstellt GAT ACE entsprechende Kommandos, die an den Controller der Tür gesendet werden müssen. Die Anzahl der gesendeten und noch zu übertragenden Kommandos wird in der Spalte "Noch zu sendende Kommandos" angezeigt. Sie können diese Kommandos anzeigen und falls gewünscht einzeln übertragen oder löschen.

Das Löschen von Kommandos ist üblicherweise nicht erforderlich, da alle Kommandos von den Controllern verarbeitet werden müssen. Aus Gründen der Rückwärtskompatibilität kann es aber erforderlich sein, gezielt einzelne Kommandos zu entfernen, um die Anlage in Betrieb nehmen zu können.

► Markieren Sie die gewünschte Tür in der Türliste.

► Wählen Sie das Symbol "Noch zu sendende Kommandos".

○ Das Fenster "Noch zu sendende Kommandos" wird geöffnet, in dem alle Kommandos aufgelistet sind.

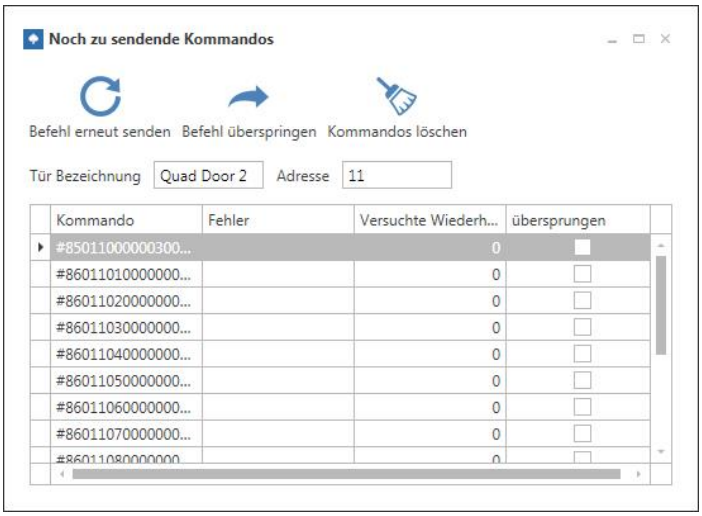


Bild 5.32 *- Tür konfigurieren, Zu sendende Kommandos*

- Wenn beim Senden eines Kommandos ein Fehler auftritt, wird eine entsprechende Meldung angezeigt. GAT ACE versucht dann, das Kommando erneut zu senden. Die versuchten Wiederholungen werden ebenfalls angezeigt.

► Um ein Kommando in der Liste zu deaktivieren, so dass es nicht gesendet wird (z. B. weil bei diesem Kommando Fehlermeldungen angezeigt werden), markieren Sie das Kommando und klicken auf das Symbol "Befehl überspringen".

- Das zu überspringende Kommando wird in der letzten Spalte "übersprungen" mit einem Haken markiert.

► Um ein Kommando erneut zu senden markieren Sie das Kommando und wählen das Symbol "Befehl erneut senden".

► Um alle Kommandos zu löschen klicken Sie auf das Symbol "Kommandos löschen".

- Alle Kommandos werden aus der Liste gelöscht und somit nicht mehr an die Tür bzw. den Controller gesendet.

HINWEIS! Das Überspringen oder Löschen von Kommandos kann einen Zustand bewirken, in dem die Türe nicht mehr korrekt funktioniert! Führen Sie diese Schritte bitte ausschließlich nach Rücksprache mit unserem Support durch.

5.2.14 Offline-Schnittstellen und Offline-Türen

Offline-Türen sind nicht permanent über eine Schnittstelle mit GAT ACE bzw. dem Server verbunden, sondern werden über ein Programmiergerät mit Daten versorgt. Für die Konfiguration dieser Offline-Türen und die Transportgeräte sind die Offline-Schnittstellen und die Offline Türen erforderlich.

Folgende Typen von Offline-Türen können mit GAT ACE konfiguriert werden:

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

Die Übertragung der Konfigurationsdaten an diese Offline-Türen erfolgt bei den GAT ST 21x und GAT ST 22x und dem TAC mit dem Handheld-Gerät GAT MT 010 (Übertragung der Konfigurationsdaten vor Ort via Kabelverbindung) und bei den GAT DL 32x, GAT DL 34x, GAT DL 350, GAT DL 360 GAT DL 370 mit dem GAT DL 090 oder GAT DL 092 (Übertragung der Konfigurationsdaten über Funkverbindung). Werden diese Offline-Türen im WiNET Mode betrieben, erfolgt die Kommunikation über eine permanente Funkverbindung und somit gelten dies Türen als Online-Türen und werden auch als Online-Türe konfiguriert.

5.2.15 Offline-Schnittstellen konfigurieren

Über die Offline-Schnittstelle werden mehrere Offline-Türen zusammen gefasst, die die gleiche Betriebsart verwenden, die über das gleiche Handheld-Gerät beladen werden und die im gleichen Gebäude oder Zutrittsbereich angeordnet sind.

Durch die Unterteilung einer Anlage in mehrere Offline-Schnittstellen, kann die Beladung der Türen optimiert werden, dass nur jene Geräte die im näheren Umkreis sind und über das gleiche Handheld-Gerät beladen werden auf dieses übertragen werden, um die Beladung zu erleichtern.

► Wählen Sie das Symbol "Offline Schnittstelle".

- Die Ansicht "Offline Schnittstelle" wird angezeigt.

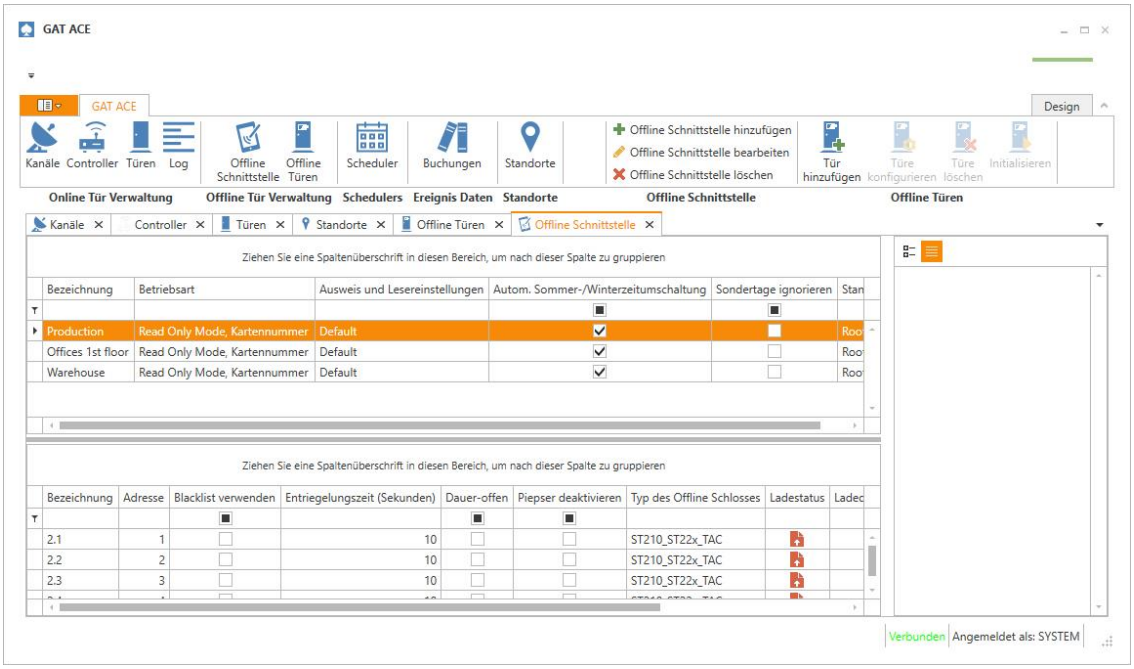


Bild 5.33 *- Offline Schnittstellen definieren*

- Hier werden alle definierten Offline Schnittstellen aufgelistet. Bei jeder Schnittstelle sehen Sie die wichtigsten Daten dieser Schnittstelle
- Unterhalb der Schnittstellenliste werden die Offlinetüren, die der ausgewählten Schnittstelle zugeordnet sind, angezeigt.
- In der Offlineschnittstellenansicht sind folgende Funktionen in der Multifunktionsleiste verfügbar (die letzten drei Symbole werden bei der Offlinetürkonfiguration beschrieben).

► Wählen Sie das Symbol "Offline Schnittstelle hinzufügen", um eine neue Schnittstelle zu definieren.

► Wählen Sie das Symbol "Offline Schnittstelle bearbeiten", um die Einstellungen der ausgewählten Schnittstelle zu bearbeiten.
  ○ In beiden Fällen wird das Fenster "Offline Schnittstelle" geöffnet.

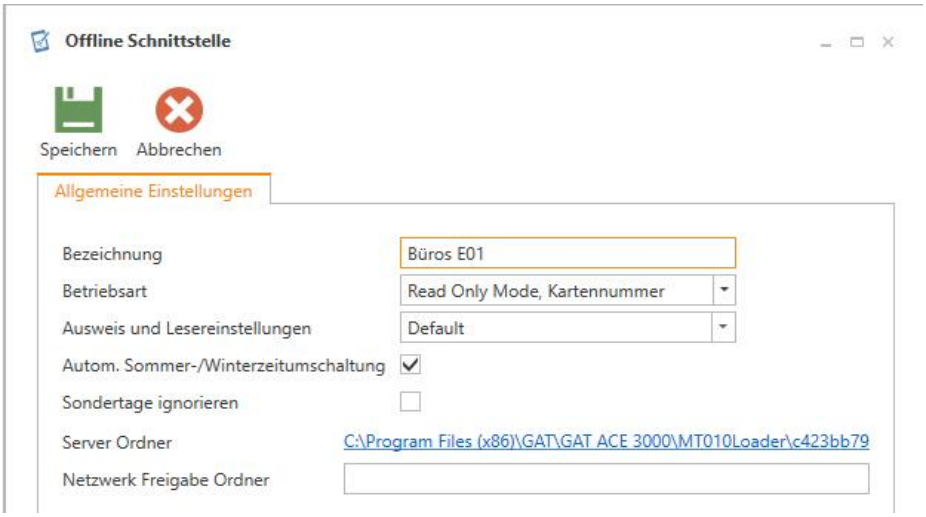


Bild 5.34 *- Eine Offline Schnittstelle konfigurieren - Allgemeine Einstellungen*

► Geben Sie im Feld "Bezeichnung" einen Namen für die Schnittstelle ein.

► Wählen Sie im Feld "Betriebsart" die Betriebsart für die Schnittstelle aus. Folgende Betriebsarten stehen zur Verfügung:
  - Read Only Mode, Unikatsnummer: Berechtigte Personen werden im Schloss gespeichert. Als Kartennummer wird die Unikatsnummer des Datenträgers verwendet.
  - CardNET Mode: Die Berechtigungen der Personen werden auf den Mitarbeiterausweisen gespeichert und so zum Schloss übertragen.
  - Anlagennummer Mode: Es wird nur geprüft, ob der Datenträger zum System gehört.
  - Hotel Mode: Berechtigungen für Gäste und Personal werden auf Ausweisen gespeichert.
  - Read Only Mode, Kartennummer: Berechtigte Personen werden im Schloss gespeichert. Als Kartennummer wird die codierte Kartennummer des Datenträgers verwendet.

► Wählen Sie im Feld "Ausweis und Lesereinstellungen" die voreingestellte Konfiguration für Leser bzw. Datenträger aus.

► Markieren Sie "Autom. Sommer-/Winterzeitumschaltung", wenn diese Funktion bei den Terminals an der Schnittstelle verwendet werden soll.

► Wenn das Feld "Sondertage ignorieren" aktivert ist, werden Sondertage, die im Betriebskalender definiert sind und an denen vom Standard abweichende Berechtigungen aktiviert sein können, von den Offline Schlössern an der Offline-Schnittstelle ignoriert. Es wird dann auch an den Sondertagen der normale Tagesplan verwendet.

► Im Feld "Server Ordner" sehen Sie den Ordner, in dem die Konfigurationsdateien für die Offline-Türen durch den GAT ACE 3000 Service gespeichert werden. Dieser Speicherort wird automatisch vergeben. Ein Klick auf den Link öffnet den Ordner (wenn Sie am Server arbeiten). Mit "Strg"+"Klick" auf diesen Link können Sie den Pfad bearbeiten.

► Der Server Ordner muss im Netzwerk freigegeben werden, damit auch an den Arbeitsplätzen und von den Transfergeräten auf die Daten zugegriffen werden kann. Den Netzwerk Freigabenamen können Sie im Feld "Netzwerk Freigabe Ordner" eingeben. Ein Klick auf den Link öffnet den Ordner. Mit "Strg"+"Klick" auf diesen Link können Sie die Daten bearbeiten.

► Speichern Sie mit Klick auf "Speichern".
  ○ Sie gelangen zurück in die Liste der Offline-Schnittstellen.

5.2.16 Offline-Türe konfigurieren

Alle Offline-Türen werden den entsprechenden Offline-Schnittstellen zugeordnet. Wenn eine Offline-Schnittstelle in der Offline Schnittstellen Ansicht ausgewählt wird, sehen Sie darunter die Offline-Türen, die dieser Schnittstelle zugeordnet sind. Nachfolgend erhalten Sie eine Beschreibung, wie die Offline-Türen konfiguriert werden.

► Markieren Sie eine Offline-Schnittstelle und klicken Sie auf das Symbol "Tür hinzufügen" in der Multifunktionsleiste, um eine neue Offline-Türe zu hinzuzufügen.

○ Das Fenster "Offline Türe" wird angezeigt. Dieses Fenster ist in 2 Registerkarten unterteilt.

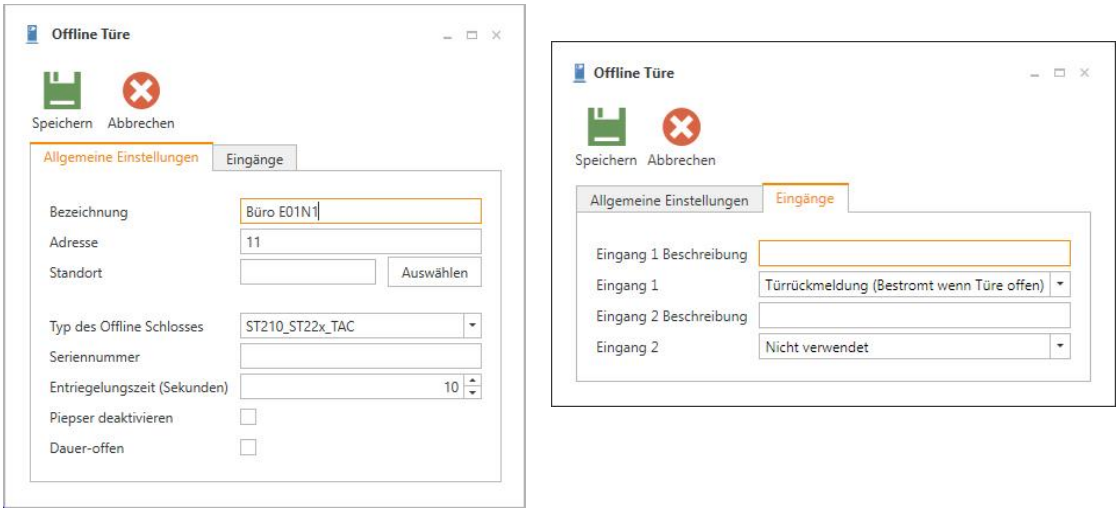


Bild 5.35 *- Eine Offlinetüre konfigurieren - Basic Info (Basic Info -> Türeinstellungen , Inputs -> Eingänge)*

► Tragen Sie hier für die neue Türe folgende Informationen ein.

- Bezeichnung: Geben Sie der Offlinetür hier einen Namen.
- Adresse: Mit der Adresse wird das Offline-Terminal an der Offlinetür identifiziert. Deshalb muss jedes Offline-Terminal eine eindeutige Adresse besitzen, die nicht schon für ein anderes Offline-Terminal verwendet wird. Wird eine bereits verwendete Adresse eingegeben, erhalten Sie beim Speichern der Türdaten eine Fehlermeldung.
- Standort: Mit dem Feld "Auswählen" können Sie einen Standort auswählen, um die Offlinetüre dem Standort zuzuweisen.
- Typ des Offline Schlosses: Wählen Sie hier den Typ des Offline-Terminals aus.
- Seriennummer: Geben Sie die Seriennummer des Offline-Terminals ein, das an der Offline-Türe installiert ist. Dies ermöglicht bei einigen Gerätetypen die automatische Adressierung und erleichtert somit die Inbetriebnahme.
- Entriegelungszeit (Sekunden): Diese Zeit bestimmt, wie lange die Tür bei einer gültigen Identifikation entriegelt wird.
- Blacklist verwenden: Dieses Einstellung ist für den CardNET und Hotel Mode relevant. Wenn dieses Feld markiert ist, werden Datenträger, die gelöscht werden, in eine Sperrliste eingetragen. Wird diese dann mit dem Handheld-Gerät an das Schloss übertragen, ist der Ausweis nicht mehr berechtigt, auch wenn die Daten auf dem Mitarbeiter Ausweis noch eine gültige Berechtigung ergeben würden. So können verlorene Ausweise sofort gesperrt werden.

- Piepser deaktivieren: Wenn dieses Feld markiert ist, werden an der Offlinetüre keine Signaltöne ausgegeben. Standard ist, dass Töne ausgegeben werden, das Feld also nicht markiert ist.
  Diese Funktion kann nur bei Lesern vom Typ GAT SR 73xx und GAT SLR 73xx verwendet werden und hat auf Leser vom Typ GAT SR 3xx und GAT SLR 3xx keine Auswirkung.
- Dauer-offen: Diese Funktion wird nur von den Offline-Schlössern der älteren Generation TAC oder GAT ST 2xx unterstützt. Bei aktivierter Dauer-offen-Funktion wird die Tür dauerhaft entriegelt, wenn ein Benutzer nach einem gültigen Zutritt innerhalb von 2 Sekunden erneut einen gültigen Zutritt durchführt (Datenträger erneut lesen). Die Tür wird erst wieder versperrt, wenn ein berechtigter Benutzer erneut einen gültigen Zutritt durchführt.

► Wechseln Sie nun auf die Registerkarte "Inputs", um die Eingänge der Offlinetür zu konfigurieren. Offlinetüren können, abhängig vom Typ, bis zu zwei Optokopplereingänge besitzen, mit denen Statussignale erfasst werden können. Geben Sie in den unteren Feldern eine Beschreibung ein und wählen Sie eine Funktion aus. Folgende Funktionen sind möglich:

- Türrückmeldung (nicht bestromt/bestromt, wenn Türe offen):
  An diesem Eingang ist ein Türkontakt angeschlossen, der meldet, ob die Türe geschlossen oder offen ist. Je nachdem, welche der beiden Funktionen gewählt wurde, signalisiert eine Bestromung oder eine Stromunterbrechung die geöffnete Tür.
- Tasterentriegelung (Bestromen/Stromunterbrechung für Türöffnung):
  An diesem Eingang ist ein Taster angeschlossen, mit dem die Tür entriegelt werden kann. Je nachdem, welche der beiden Funktionen gewählt wurde, wird für eine gewünschte Türöffung der Eingang durch Tasterbetätigung bestromt oder die Bestromung unterbrochen.

► Speichern Sie die Türkonfiguration mit "Sichern".

○ Die neue Offlinetüre wird in der Offlinetürliste eingefügt und der zuvor gewählten Offline-Schnittstelle zugeordnet.

HINWEIS! Sollten Sie eine Adresse eingegeben, die bereits von einem anderen Offline Terminal verwendet wird, so kann die Konfiguration nicht gespeichert werden.

► Es ist auch möglich, eine Übersicht aller Offlinetüren anzuzeigen. Klicken Sie dazu das Symbol "Offline Türen".

○ Es wird sehen Sie in der Ansicht "Offline Türen".

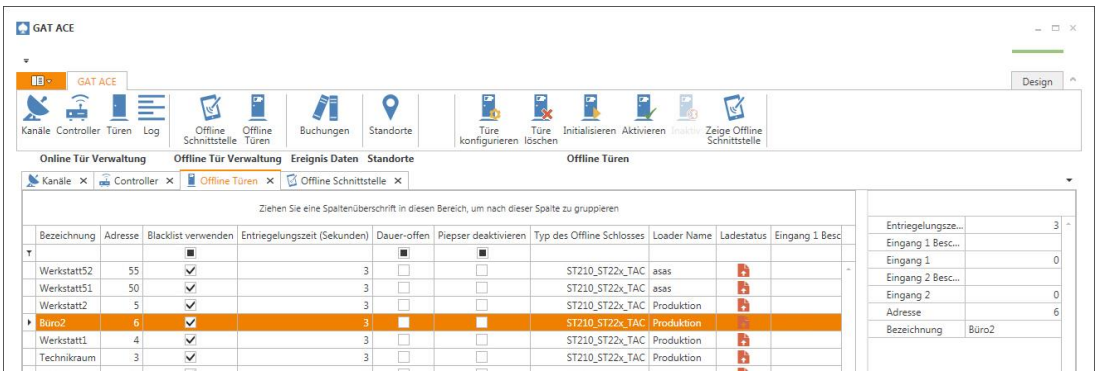


Bild 5.36 *- Offline Türen*

- Hier wird für jede Tür die wichtigsten Informationen wie die Adresse, Betriebsart, Entriegelungszeit und Funktionseinstellungen angezeigt.
- Über die Symbole in der Multifunktionsleiste können die Türkonfigurationen bearbeitet und weitere Türen eingefügt werden.

► Konfigurieren Sie die Offlinetüren wie auf der vorigen Seite bei den Offline-Schnittstellen beschrieben.

► Um eine Offlinetüre zu aktivieren oder deaktivieren verwenden Sie das entsprechende Symbol "Aktivieren" oder "Inaktiv" in der Symbolleiste von GAT ACE. Eine deaktivierte Tür wird von GAT ACE nicht bearbeitet.

► Mit dem Symbol "Show Loader" können Sie direkt die Offlineschnittstelle, an dem die aktuell markierte Tür verbunden ist, anzeigen lassen.

5.2.17 Offlinetüre initialisieren

Beim Initialisieren einer Offlinetüre werden die Daten für die Offline-Türe erstellt und für das Handheld Gerät im passenden Ordner zur Verfügung gestellt. Dass eine Initialisierung erforderlich ist, ist durch das Symbol ersichtlich.

► Damit eine Offlinetüre initialisiert wird, markieren Sie die diese in der Liste der Offlinetüren.

► Klicken Sie nun auf das Symbol "Initialisieren" in der Multifunktionsleiste.

- Sind Änderungen vorhanden, werden die Daten erstellt und es ist in GAT ACE und in GAT Matrix durch das Symbol ersichtlich, dass die Daten nun mit dem Handheld Gerät an die Offline-Türe übertragen werden müssen.

► Verwenden Sie das Handheld-Gerät entsprechend der jeweiligen Beschreibung.

- Wird die korrekte Übertragung mittels Handheld-Gerät zurück gemeldet, wird die Türe durch das Symbol als korrekt initialisiert angezeigt. Die Möglichkeit der Rückmeldung ist abhängig vom Typ des Handheld Gerätes und dem Softwarestand.

5.2.18 Batteriewarnung bei Offlinetüre

Die Offline-Schlösser generieren Batteriewarnungen für unterschiedliche Batterienzustände.

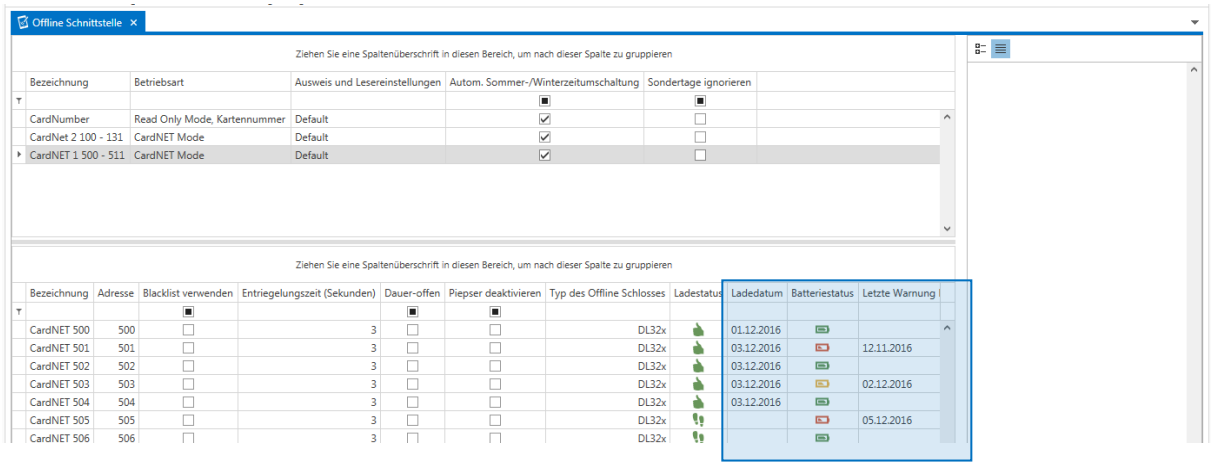


Bild 5.37 *- Offline Türen - Batteriewarnungen*

- Ladedatum: Hier wird angezeigt, wann die Offline-Tür zum letzten Mal beladen wurden. Wird kein Datum angezeigt (Fußsymbole in der Spalte "Ladestatus") sind seit dem letzten Beladen Änderungen gemacht worden und die Offline-Türe muss neu beladen werden.
- Batteriestatus: Der Batteriestatus für jede Offline-Tür wird in der Spalte "Batteriestatus" angezeigt.
  .... Der Batteriestatus ist gut.
  .... Die Batterie ist teilweise entladen und muss in Kürze getauscht werden.
  .... Batteriewarnung. Die Batterie ist leer und muss ausgetauscht werden.
  Am Offline-Schloss wird optisch und akustisch zusätzlich die Batteriewarnung signalisiert.
- Letzte Warnung: Dieses Datum zeigt an, wann die letzte Batteriewarnungsinformation erzeugt wurde.

Möglichkeiten zur Quittierung von Batteriewarnung sind:

► Eine Person macht einen Zutritt an einer Offline-Türe, bei der die Batterie gewechselt wurde. Bucht die Person danach an einer Online-Türe mit CardNET Funktion, wird die Batteriewarnung automatisch zurück gesetzt. Diese Funktion ist für die GAT DL 3xx Schlösser verfügbar.

► Eine Person macht einen Zutritt an einer Offline-Türe, bei der die Batterie gewechselt wurde. Bucht die Person danach an einem Zeiterfassungsgerät mit CardNET Funktion, wird die Batteriewarnung automatisch zurück gesetzt. Diese Funktion ist für die GAT DL 3xx Schlösser verfügbar.

► Werden mit dem Transportgerät die Buchungen einer Offline-Türe nach einem Batteriewechsel ausgelesen und mit der GAT ACE 3000 synchronisiert, werden die Batteriewarnungen ebenfalls zurückgesetzt. Diese Möglichkeit ist bei allen Offline-Schlössern verfügbar.

► Es besteht auch die Möglichkeit die Batteriewarnungen in der GAT ACE 3000 zurückzusetzen. Dazu muss in der Offline-Schlossliste mit der rechten Maustaste auf ein Batteriewarnsymbol (rot) geklickt und im angezeigten Menü der Menüpunkt "Batteriewarnung quittieren" gewählt werden. Dieser Fall soll aber nur in Ausnahmefällen verwendet werden, da der Datenkreislauf dadurch nicht geschlossen ist und weitere Batteriewarnungen für einen Zeitraum von 1 Monat ignoriert werden.
HINWEIS! Es wird protokolliert, welcher Benutzer diese Funktion angewendet hat.

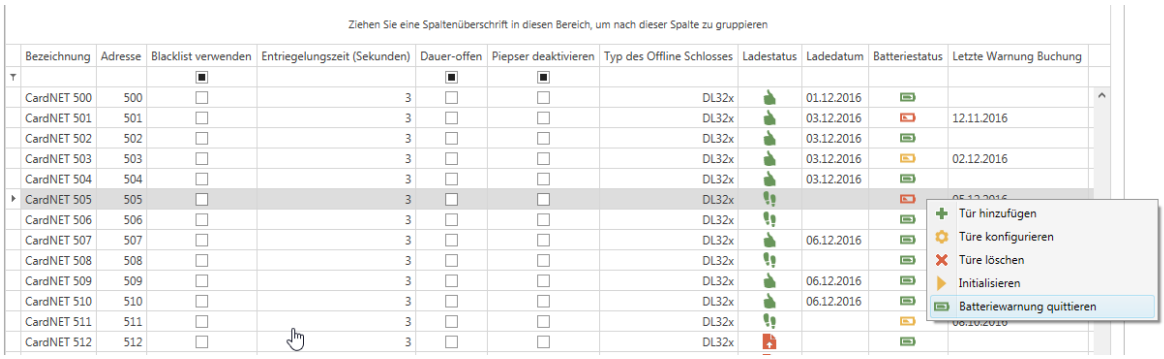


Bild 5.38 *- Offline Türen - Batteriewarnungen*

HINWEIS! Für den Batterietausch ist es erforderlich, dass die Batteriekarte nach dem Tausch der Batterie an den Leser der Offline-Türe gehalten wird, um den Tausch zu dokumentieren! Um die Uhrzeit nach dem Batterietausch auf den korrekten Wert zu stellen und einen aktuellen Betriebskalender zu laden, ist eine Beladung der Offline-Türe mit aktuellen Daten dringend zu empfehlen! Nach dem Synchronisieren des Transportgerätes mit der GAT ACE 3000 sind auf diesem Weg auch die Batteriewarnungen zurückgesetzt

Empfehlung: Bei Batteriewechsel oder Verwendung des Transportgerät sollten die Produkte auf korrekte Funktion sowie auch Montage geprüft werden.

5.3 Scheduler

In dem Fenster "Scheduler" können wiederkehrende Aufgaben geplant werden. Diese werden dann automatisch ausgeführt, sofern der GAT ACE 3000 Dienst läuft. Die folgenden Aufgaben können geplant werden:

- Sicherung der SQL Datenbank erstellen
- Alte Einträge aus der Buchungs-Datenbank löschen

► Klicken Sie auf das Symbol "Scheduler".

  ○ Es wird der aktuelle Tag mit allen geplanten Aufgaben angezeigt. Mit der Kalenderansicht auf der linken Seite können Sie zu einem anderen Tag navigieren.

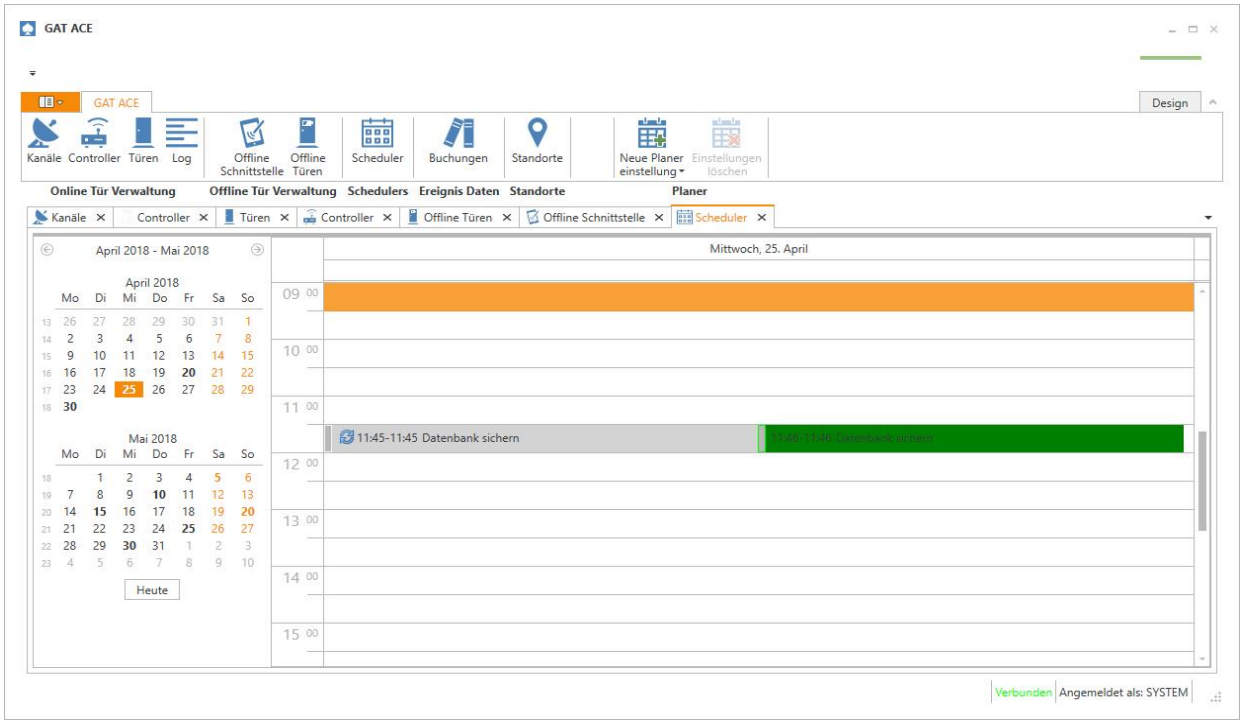


Bild 5.39 *- Offline Türen - Batteriewarnungen*

► Um eine neue Aufgaben zu planen, klicken Sie auf das Symbol "Neue Planereinstellung" und wählen Sie die gewünschte Aufgabe aus dem angezeigten Menü.

  ○ Es öffnet sich das Fenster "Planereinstellung" mit den Einstellmöglichkeiten für die gewählte Aufgabe. Die Planereinstellungen werden in den folgenden Abschnitten beschrieben.

► Um eine bestehende Aufgabe zu löschen, klicken Sie auf die Aufgabe und wählen Sie "Einstellungen löschen".

5.3.1 SQL Sicherung

Die SQL Datenbank enthält alle Daten des Zutrittssystems, z. B. die Controller/Tür-Konfigurationen und die Buchungsdaten. Die Planeraufgabe "SQL Sicherung" erlaubt die automatische Sicherung der SQL-Datenbank in regelmäßigen Abständen. Bei jeder Sicherung wird eine neue Datei erstellt. Datum und Zeit der Sicherung sind im Dateinamen enthalten. Wenn Fehler in der Software oder der Bedienung auftreten kann eine Sicherung in GAT ACE importiert werden, um die Daten auf den Stand der Sicherung zurückzusetzen.

HINWEIS! Daten, die nach dem Ausführen dieser Aufgabe gelöscht werden, können nicht wiederhergestellt werden.

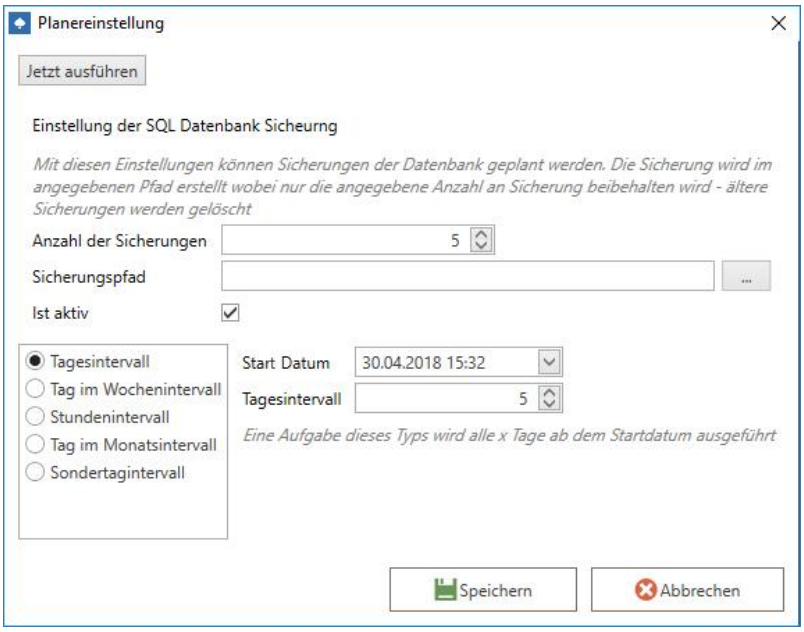


***Bild 5.40** - Aufgabe für die automatische Sicherung der SQL-Datenbank erstellen*

- ► Geben Sie im Feld "Anzahl der Sicherungen" die Anzahl der Sicherungsdateien ein, die jeweils gespeichert bleiben sollen. Um Platz zu sparen löscht GAT ACE 3000 automatisch die älteste Sicherung, wenn eine neue erstellt wird. Wird hier z. B. "5" eingegeben und es sind bereits 5 Sicherungen gespeichert, so wird die älteste Sicherung gelöscht wenn eine neue erstellt wird. Werden Sicherungen sehr häufig gemacht, z. B. jede Stunde, so sollte dieser Wert nicht zu klein eingestellt werden, damit in einem Fehlerfall genügend Sicherungen zur Verfügung stehen.
- ► Im Feld "Sicherungspfad" geben Sie den Pfad ein, in dem die Sicherung gespeichert werden soll. Es wird empfohlen, einen Netzwerkpfad einzugeben, damit die Sicherungen bei einem PC/Serverdefekt nicht verloren gehen.
- ► Markieren Sie die Option "Ist aktiv", um diese Aufgabe zu aktivieren.

  HINWEIS! Wenn das Feld nicht markiert ist, wird die Sicherung nicht durchgeführt, die Aufgabe bleibt aber im Planer gespeichert.
- ► Wählen Sie im linken Feld den Interval-Typ, in dem die Aufgabe periodisch ausgeführt werden soll.
- ► Geben Sie im Feld "Start Datum" das Begin-Datum ein, an dem die Aufgabe das erste Mal ausgeführt werden soll.
- ► Je nach Intervall-Typ wird noch ein zweites Feld angezeigt (im Beispiel oben "Tagesintervall"). Tragen Sie hier das gewünschte Intervall ein.
- ► Bestätigen Sie die Eingaben mit "Speichern". Die neue Aufgabe wird im Planer eingefügt.
- ► Mit der Schaltfläche "Jetzt ausführen" können Sie die Aufgaben mit den eingegebenen Daten manuell ausführen.

5.3.2 Bereinigung der Datenbanktabelle

Mit dieser Aufgabe im Planer können Sie eine Bereinigung, d.h. Löschung, von alten Datenbankeinträgen in der Datenbank vornehmen, um Platz frei zu machen. Aktuell können nur Einträge in der Buchungsdatenbank für die Bereinigung gewählt werden. Die Buchungsdatenbank zeichnet alle Aktivitäten im System, wie z. B. Zutritte oder Zutrittsversuche, auf (siehe Kapitel "5.5. Buchungen").

HINWEIS! Daten, die bereits an die Zutrittskontrollsoftware (z. B. GAT Matrix) übertragen wurden, bleiben in dieser Zutrittskontrollsoftware bestehen, auch wenn die Buchungen mit dieser Aufgabe in GAT ACE bereinigt werden.

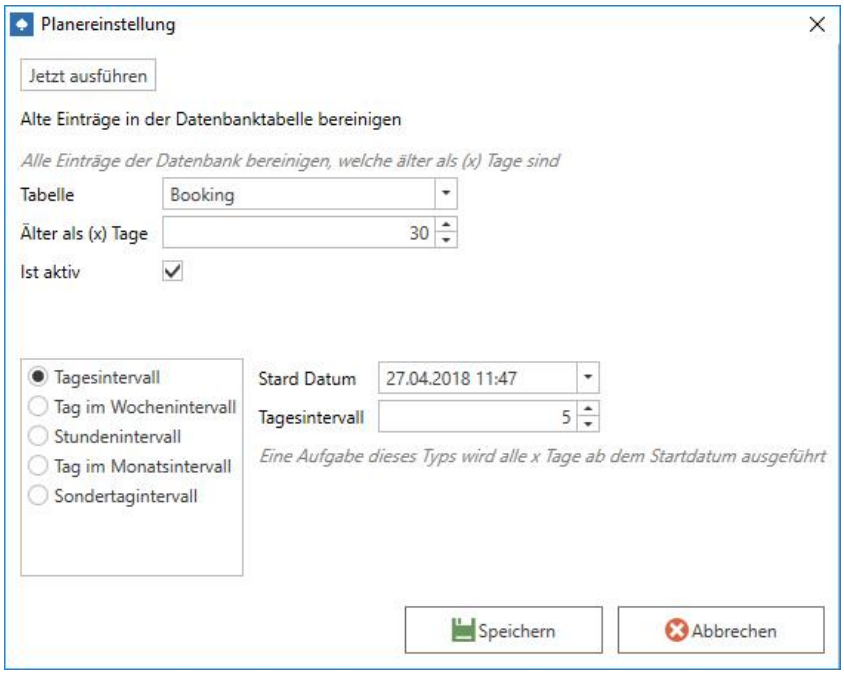


***Bild 5.41** - Aufgabe für die automatische Sicherung der SQL-Datenbank erstellen*

- ► Im Feld "Tabelle" wählen Sie "Booking" aus. Dies ist aktuell die einzige Option für diese Aufgabe.
- ► Geben Sie im Feld "Älter als (x) Tag" die Anzahl der Tage ein, nach denen die Einträge in der Buchungsdatenbank gelöscht werden sollen. Mit den Einstellungen im Bild 5.41 werden alle Einträge gelöscht, die älter als 30 Tage sind.
- ► Markieren Sie die Option "Ist aktiv", um diese Aufgabe zu aktivieren.

  HINWEIS! Wenn das Feld nicht markiert ist, wird die Sicherung nicht durchgeführt, die Aufgabe bleibt aber im Planer gespeichert.
- ► Wählen Sie im linken Feld den Interval-Typ, in dem die Aufgabe periodisch ausgeführt werden soll.
- ► Geben Sie im Feld "Startdatum" das Beginn-Datum ein, an dem die Aufgabe das erste Mal ausgeführt werden soll und tragen Sie dann im Feld darunter das gewünschte Intervall ein. Welches Feld hier angezeigt wird hängt davon ab, welchen Intervall-Typ sie gewählt haben.
- ► Bestätigen Sie die Eingaben mit "Speichern". Die neue Aufgabe wird im Planer eingefügt.
- ► Mit der Schaltfläche "Jetzt ausführen" können Sie die Aufgaben mit den eingegebenen Daten manuell ausführen.

5.4 Logdateien auswerten

Die Kommunikation zwischen GAT ACE und den Controllern wird mitprotokolliert und dieses Protokoll kann in GAT ACE angezeigt werden. Dies wird nur für den Fall von Fehleranalysen benötigt und diese Funktion muss deshalb bewusst aktiviert werden.

► Wählen Sie das Symbol "Log" in der Multifunktionsleiste aus.
  ○ Die Logansicht wird geöffnet.

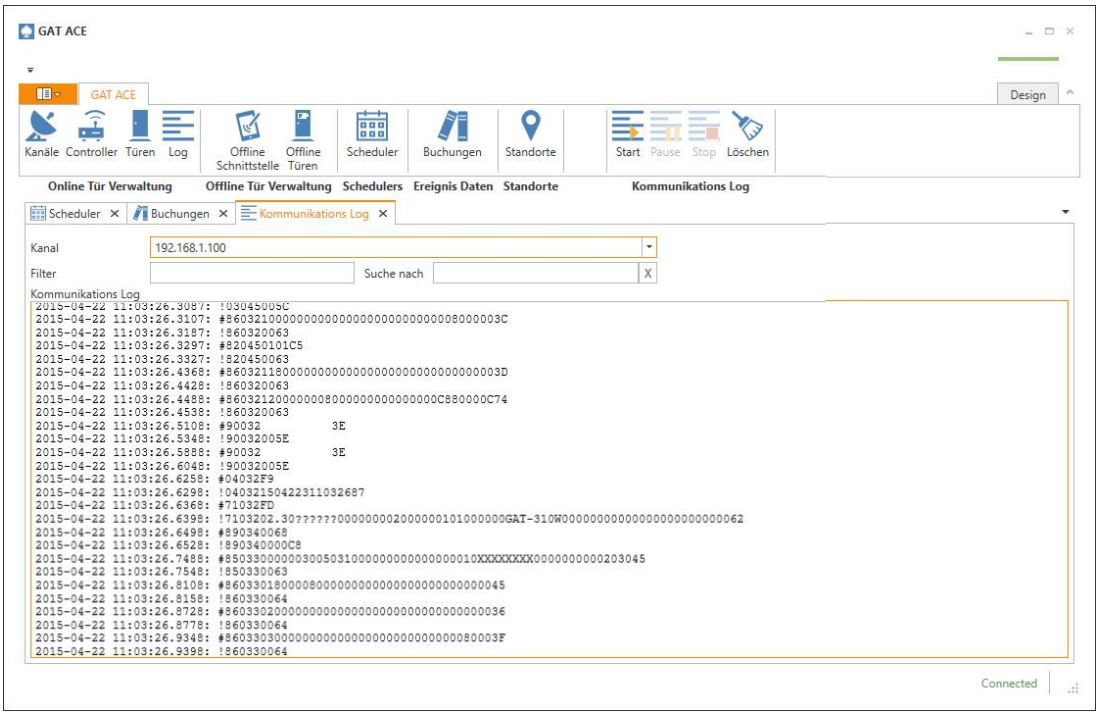


Bild 5.42 *- Logdateien auswerten*

► Wählen Sie im Feld "Kanal" den Kanal aus, dessen Logeinträge sie sehen möchten.
  ○ Die gespeicherten Logeinträge werden angezeigt.
► Im Feld "Filter" können Sie einen Begriff oder Zeichen eingeben, nach denen in den Logeinträgen gesucht werden soll (z. B. eine Controlleradresse).
  ○ Die Logeinträge werden anhand des eingegebenen Filters durchsucht und nur die passenden Einträge angezeigt.
► Im Feld "Suche nach" können Sie einen Begriff eingeben, den sie in den Logeinträgen suchen möchten.
  ○ Die zu dem Suchbegriff passenden Stellen in der Logdatei werden angezeigt/markiert.

Für weitere Informationen wenden Sie Sich an unseren Support.

5.5 Buchungen

Die Controller speichern alle Identifikationsversuche und Zutritte/Austritte als Buchungen ab. Jede Buchung enthält Angaben über die verwendete Ausweisnummer, Uhrzeit und Datum, Typ der Buchung usw.. Somit lassen sich alle Vorgänge an den Controllern für eventuell spätere Überprüfungen nachvollziehen.

GAT ACE kann die Buchungen der Controller auslesen und listet diese in der Ansicht "Buchungen" gesammelt auf. In dieser Ansicht können die Buchungen nach verschiedenen Kriterien gefiltert werden.

► Wählen Sie das Symbol "Buchungen" in der Multifunktionsleiste aus.
  ○ Es wird die Buchungsansicht geöffnet und die vorhandenen Buchungen angezeigt.

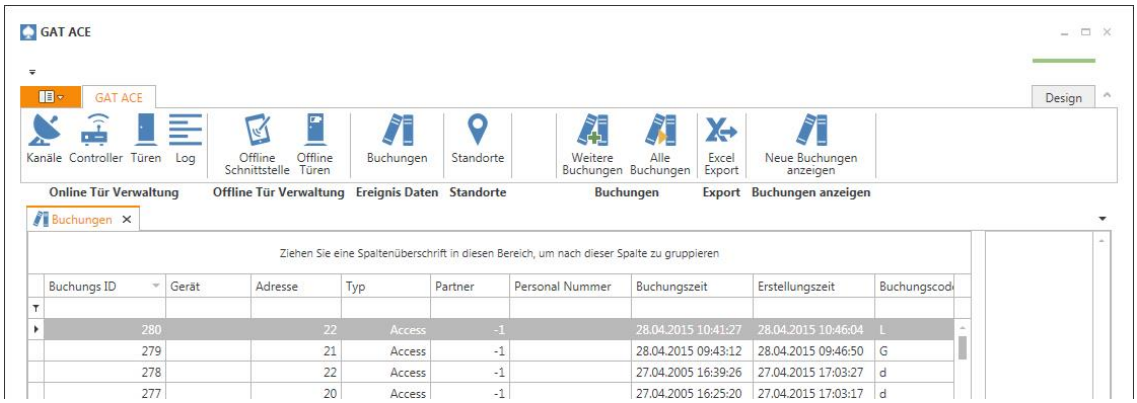


Bild 5.43 *- Buchungsanzeige*

Die aktuellsten Buchungen werden automatisch angezeigt. Möchten Sie ältere Buchungen sehen verwenden Sie die folgenden Funktionen aus der Multifunktionsleiste:

► Mit dem Symbol "Weitere Buchungen" werden die nächst älteren Buchungen vom Server abgerufen. Die Anzahl ist begrenzt, um bei einer großen Anzahl von gespeicherten Buchungen die Wartezeit nicht unnötig groß werden zu lassen. Sie können diese Funktion mehrfach aufrufen um immer weiter in die Vergangenheit blättern zu können.

► Mit dem Symbol "Alle Buchungen“ werden alle am Server gespeicherten Buchungen auf einmal abgerufen. Dies kann bei einer großen Anzahl von Buchungen sehr lange dauern.

► Mit dem Symbol "Buchungen holen anhalten" kann das Holen von allen Buchungen beendet werden, wenn die Buchungen des benötigten Zeitraums angezeigt werden. Dieses Symbol ist nur angezeigt, wenn Buchungen geholt werden.

► Mit dem Symbol "Excel Export" werden die angezeigten Buchungen in eine Excel-Datei exportiert.

► Ist die Funktion „Neue Buchungen anzeigen“ aktiv, werden Buchungen die neu erstellt werden automatisch in der Buchungsliste angezeigt. Ist die Funktion nicht aktiv, so wird die Buchungsliste nicht aktualisiert, bis über die Funktionen „Buchungen“, „Weitere Buchungen“ oder „Alle Buchungen“ eine Aktualisierung durchgeführt wird.
Achtung: Wird die Funktion „Neue Buchungen anzeigen“ wieder aktiviert, werden in der Zwischenzeit erstellte Buchungen nicht automatisch in der Anzeige nachgetragen. Diese sind aber natürlich in der Datenbank gespeichert.

5.6 Zeiterfassungs-Terminals and Zeitbuchungen

GAT ACE ermöglicht das Laden und Exportieren von Zeitbuchungen von Zeiterfassungsterminals (z. B. das GAT Terminal 1015 und 1032 oder die GAT p.time Terminals von GANTNER Electronic GmbH). Zuerst müssen Sie die Zeiterfassungsgeräte in GAT ACE hinzufügen und dann können Sie die Buchungen aus den Geräten laden (manuell oder automatisch).

Hinweis: Um die Zeitbuchungsfunktion zu aktivieren, müssen Sie die Lizenz für dieses Modul eintragen (siehe "4.4. Einstellungsseite "Einstellungen"").

► Wählen Sie das Symbol "Zeit Terminals" aus der Multifunktionsleiste.
  ○ Die Zeit Terminals Ansicht wird geöffnet und zeigt die bereits hinzugefügten Geräte an.

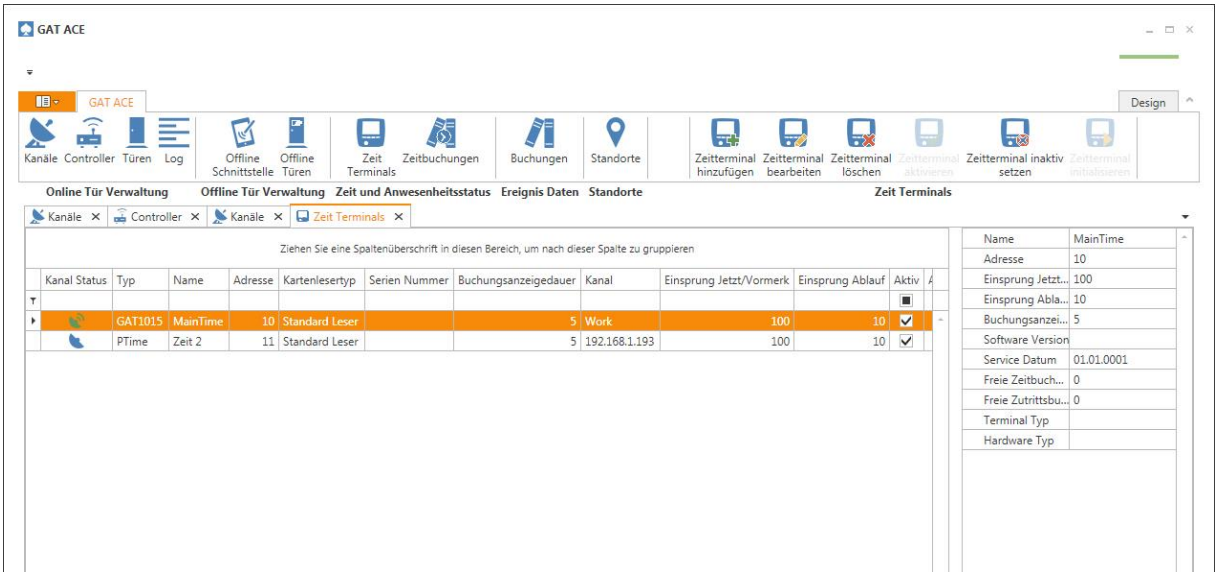


Bild 5.44 *- Zeiterfassungsgeräte*

Mit den folgenden Symbolen in der Multifunktionsleiste können Sie die weiteren Funktionen auswählen:

► Mit dem Symbol "Zeitterminal hinzufügen" wird ein neues Gerät in der Liste hinzugefügt. Bei Klick auf dieses Symbol wird das Fenster "Zeit Terminal" geöffnet, in dem die Einstellungen des Terminals definiert werden (siehe unten).

► Mit dem Symbol "Zeitterminal bearbeiten" können Sie die Einstellungen des ausgewählten Terminals ändern. Das Fenster "Zeit Terminal" wird geöffnet (siehe unten).

► Das Symbol "Zeitterminal löschen" löscht das in der Liste ausgewählte Terminal. Das Löschen muss in einem zusätzlich angezeigten Pop-Up Fenster bestätigt werden.

► Die Symbole "Zeitterminal aktivieren" und "Zeitterminal inaktiv setzen" setzen das Terminal in den deaktivierten oder aktivierten Zustand. Wenn ein Terminal deaktiviert ist, wird keine Zeitbuchung gelesen.

► Mit dem Symbol "Zeitterminal initialisieren" kann das gewählte Zeitterminal initialisiert werden.

5.6.1 Zeitterminaleinstellungen

Wenn ein neues Zeitterminal zu GAT ACE hinzugefügt wird oder Sie auf "Zeitterminal editieren" klicken, öffnet sich das Fenster "Zeit Terminal", wo Sie dessen Einstellungen festlegen können.

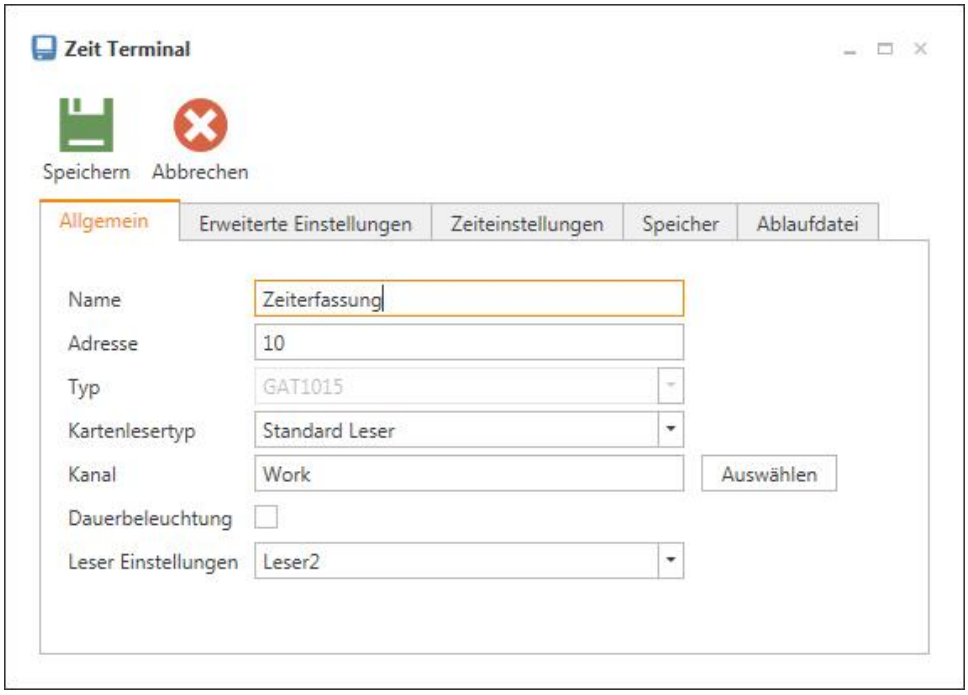


***Bild 5.45** – Zeiterfassungsterminal - Allgemeine Einstellungen*

Die Konfigurationseinstellungen sind in verschiedene Registerkarten unterteilt.

Registerkarte "Allgemein"

- Name: Geben Sie einen Namen für das Terminal ein mit dem es in der Liste angezeigt wird.
- Addresse: Geben Sie die Terminaladresse ein. Jedes Terminal muss eine eindeutige Adresse haben.
- Typ: Wählen Sie den Terminaltyp.
- Kartenlesertyp: Wählen Sie den Typ des Lesers am Terminal aus, der zur Personalerfassung dient. "Standard Leser" bedeutet ein kontaktloser Leser für RFID oder Infrarot Datenträger. "Magnetkartenleser" wird für Karten mit Magnetstreifen benutzt und "Magnetkartenleser (Var. Kartenstruktur)" muss für Magnetstreifenkarten gewählt werden, die nicht die Gantner Standard Segment Kodierung verwenden.
- Dauerbeleuchtung: Ist diese Option gewählt, so wird die Beleuchtung des Terminaldisplays permanent eingeschaltet. Ist es nicht markiert, wird die Displaybeleuchtung nur kurz eingeschaltet, wenn ein Datenträger gelesen oder eine Taste gedrückt wird. Durch Deaktivierung der Dauerbeleuchtung des Terminals kann die Lebensdauer des Displays erhöht werden.
- Leser Einstellungen: Wählen Sie eine definierte Lesereinstellung aus der Liste aus. Die Lesereinstellungen werden in den allgemeinen Einstellungen von GAT ACE festgelegt (siehe "4.5. Einstellungsseite "Ausweis- und Lesereinstellungen"").

Registerkarte "Erweiterte Einstellungen"

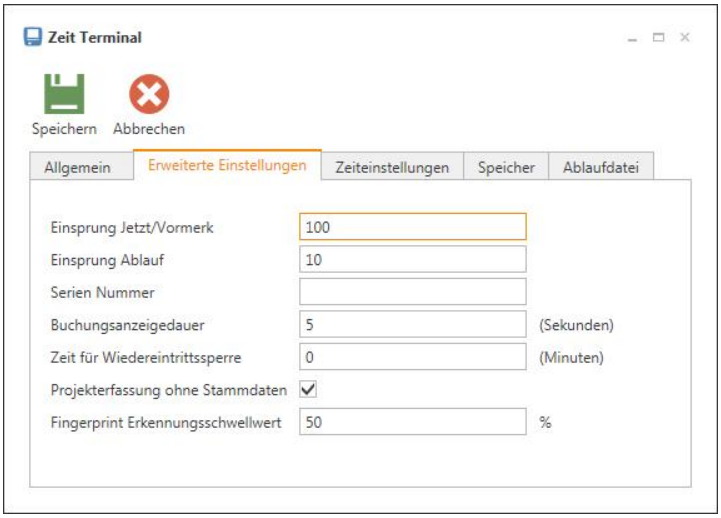


Bild 5.46 *- Zeiterfassungsterminal - Erweiterte Einstellungen*

- Einsprung Jetzt/Vormerk: Einsprungadresse für Jetzt/Vormerk Buchungen. Hängt von der Ablaufdatei ab.
- Einsprung Ablauf: Einsprungandresse für den Ablauf. Dieser Wert ist üblicherweise auf 10 gesetzt. Andere Werte hängen von der Ablaufdatei ab.
- Serien Nummer: Seriennummer des Terminals.
- Buchungsanzeigedauer: Diese Zeit gibt an, wie lange die Erstellung einer Buchung am Terminal angezeigt wird.
- Zeit für Wiedereintrittssperre: Hinweis: Diese Einstellung wird für die Kompatibilität zu GAT Manager verwendet und von GAT ACE nicht unterstützt.
- Projekterfassung ohne Stammdaten:
  Ist die Option markiert können alle Projekte erfasst werden (solange das durch die Ablaufdatei erlaubt ist). Ansonsten können nur Projekte erfasst werden, für die Daten in das Terminal geladen wurden.
- Fingerprint Erkennuntsschwellwert:
  Hinweis: Diese Einstellung wird für die Kompatibilität zu GAT Manager verwendet und von GAT ACE nicht unterstützt.

Register Card "Time Settings"

Bild 5.47 *- Zeiterfassungsterminal - Zeiteinstellungen*

Hier können Sie das Zeitverhalten des Terminals einstellen.

- Eingabezeit: Timeout-Zeit für die Eingabe von Werten in das Terminal.
- Anzeige Zeit: Legt die Zeit fest, die eine Information (z.B. Buchung) am Display des Terminals angezeigt wird, bevor in die Standardanzeige zurückgeschaltet wird.
- Anzeige Wechselzeit: Diese Einstellung wird für die Kompatibilität zu GAT Manager verwendet und von GAT ACE nicht unterstützt.

Registerkarte "Speicher"

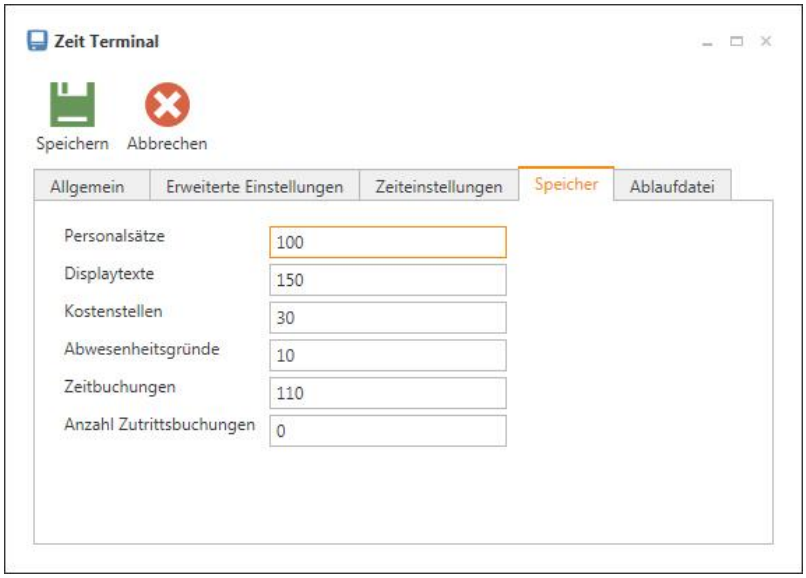


Bild 5.48 *- Zeiterfassungsterminal - Speichereinstellung*

Hier können Sie festlegen, wie der Speicher des Terminals aufgeteilt werden soll. Dies hilft bei der Anpassung an verschiedene Anforderungs-Situationen.

- Personalsätze: Anzahl der Personalsätze, die im Terminal gespeichert werden können. Größe jedes Personalsatzes kann variieren.
- Displaytexte: Wieviele Displaytexte im Terminal gespeichert werden können.
- Kostenstellen: Anzahl Kostenstellen bzw. Projekte, die im Terminal gespeichert werden können.
- Abwesenheitsgründe: Anzahl der Abwesenheitsgründe, die im Terminal gespeichert werden können.
- Zeitbuchungen: Anzahl der Zeitbuchungen, die im Terminal gespeichert werden können. Ist der Speicherplatz voll, können keine weiteren Zeitbuchungen erstellt werden, bis die Buchungen aus dem Speicher ausgelesen wurden.
- Anzahl Zutrittsbuchungen: Anzahl Zutrittsbuchungen, die im Terminal gespeichert werden können. Dieser Speicher ist ein Ringspeicher, d.h. wenn der Speicher voll ist warden die jeweils ältesten Buchungen durch neu auftretende überschrieben.

Registerkarte "Ablaufdatei"

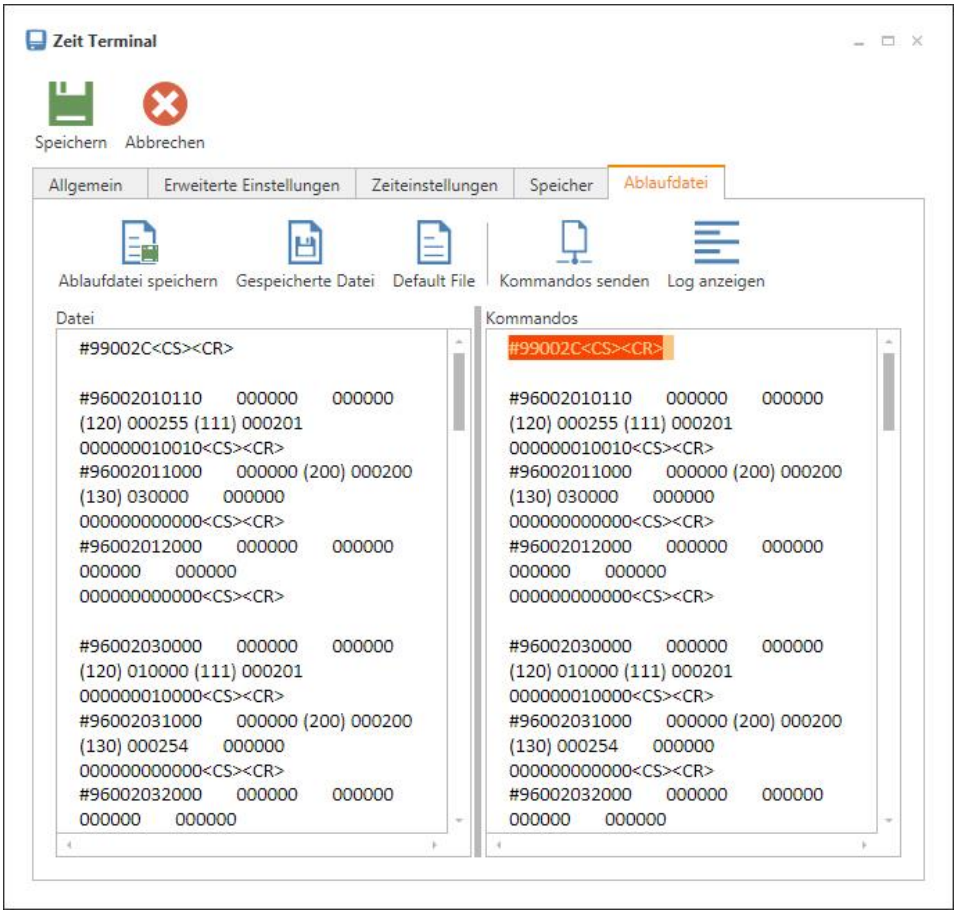


Bild 5.49 *- Zeiterfassungsterminal - Ablaufdatei*

Hier sehen Sie die Ablaufdatei des Terminals. Die Ablaufdatei bestimmt das Verhalten des Terminals. Wenn andere Funktionen als in der Standard Ablaufdatei vorgegeben, benötigt werden, kann die Ablaufdatei hier editiert und an das Terminal gesendet werden.

- ► Sie können die angezeigte Ablaufdatei in der linken Spalte "Datei" ändern und mit "Ablaufdatei speichern" sichern.
- ► Um eine vorher gespeicherte Ablaufdatei zu laden, klicken Sie auf "Gespeicherte Datei".
- ► Um die Standard-Ablaufdatei zu laden, klicken Sie auf "Default File".
- ► Um die Ablaufdatei an das Terminal zu senden, klicken Sie auf "Kommandos senden".
  - ○ Die Kommandos in der Ablaufdatei werden übertragen und Sie sehen den Vortschritt im Bereich "Kommandos".
- ► Sie können das Senden der Kommandos abbrechen, indem Sie auf "Kommandos senden beenden" klicken, was nur angezeigt wird, wenn Kommandos gesendet werden.

5.6.2 Zeitbuchungen

► Um Zeitbuchungen anzuzeigen, klicken Sie auf "Zeitbuchungen" in der Multifunktionsliste.
  ○ Die Zeitbuchungs-Ansicht wird geöffnet und die geladenen Zeitbuchungen angezeigt.

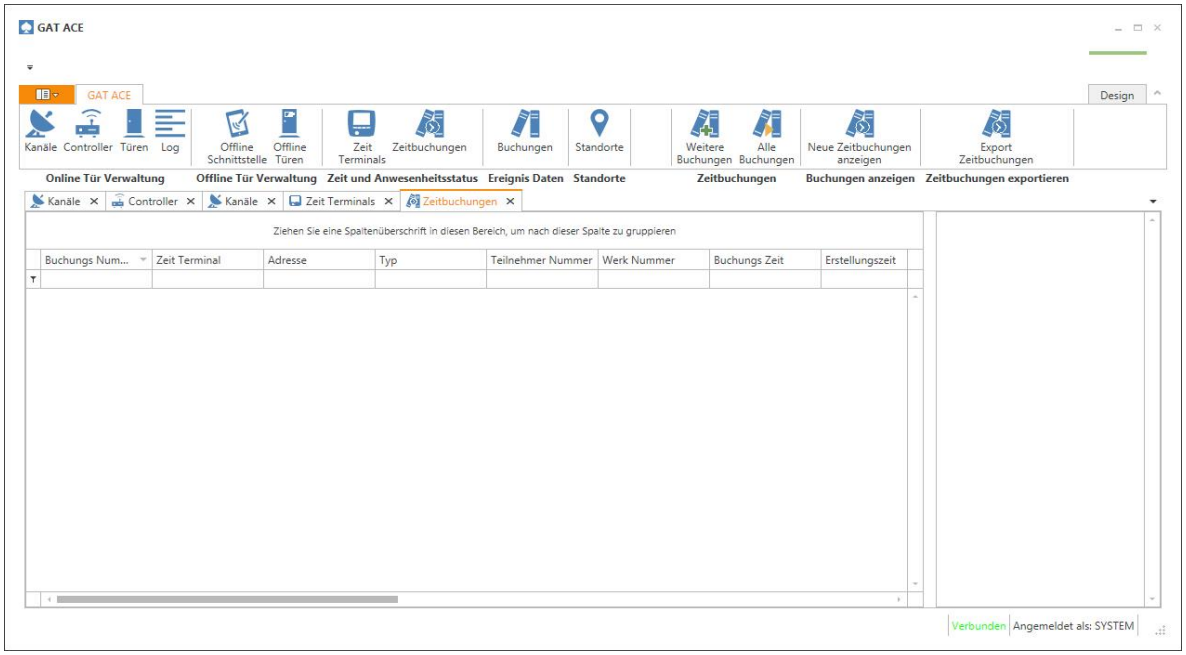


Bild 5.50 *- Zeitbuchungsanzeige*

Die aktuellsten Buchungen werden automatisch angezeigt. Möchten Sie ältere Buchungen sehen verwenden Sie die folgenden Funktionen aus der Multifunktionsleiste:

► Mit dem Symbol "Weitere Buchungen" werden die nächst älteren Buchungen abgerufen. Die Anzahl ist begrenzt, um bei einer großen Anzahl von gespeicherten Buchungen die Wartezeit nicht unnötig groß werden zu lassen. Sie können diese Funktion mehrfach aufrufen um immer weiter in die Vergangenheit blättern zu können.

► Mit dem Symbol "Alle Buchungen“ werden alle gespeicherten Buchungen auf einmal abgerufen. Dies kann bei einer großen Anzahl von Buchungen sehr lange dauern.

► Mit dem Symbol "Buchungen holen anhalten" kann das Holen von allen Buchungen beendet werden, wenn die Buchungen des benötigten Zeitraums angezeigt werden. Dieses Symbol ist nur angezeigt, wenn Buchungen geholt werden.

► Mit dem Symbol "Neue Zeitbuchungen anzeigen" werden die letzten Zeitbuchungen von den Zeiterfassungsterminals geladen.

► Mit dem Symbol "Export Zeitbuchungen" werden die gerade angezeigten Zeitbuchungen in eine externe Datei gespeichert. Der Export erfolgt anhand der Einstellungen auf der Seite "Exporteinstellungen der Zeitbuchungen" (siehe "4.8. Einstellungsseite "Exporteinstellungen der Zeitbuchungen"").

6 BERECHTIGUNGS-MANAGEMENT

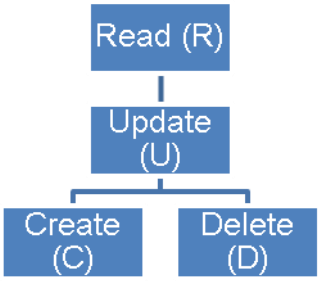
GAT ACE bietet die Möglichkeit, mehrere Benutzer mit unterschiedlichen Zugriffsrechten in GAT ACE anzulegen. Dies wurde anhand eines einfachen, rollenbasierten Berechtigungssystems realisiert. Jeder Benutzer kann genau einer Rolle zugeordnet werden, der Benutzer erbt entsprechend die Berechtigungen von dieser Rolle. Eine Rolle ist in diesem Kontext eine Sammlung von Berechtigungen für mehrere Funktionsblöcke der Software. Weiters können die Berechtigungen speziell für einzelne Benutzer überschrieben werden.

6.1 Funktionsblöcke

Ein Funktionsblock ist eine Gruppe von einfachen Aktionen (z.B. Geräteeinstellungen verwalten, Datenbankeinstellungen verwalten, Anti-Pass-Back Zonen verwalten) für welche gleichzeitig Berechtigungen vergeben werden können. Abhängig vom Funktionsblock können Rechte zum Lesen, Ändern, Erstellen und Löschen (CRUD; engl. Create, Read, Update, Delete) oder Ausführen (E; engl. Execute) erteilt werden.

Ein Beispiel ist der Funktionsblock „Geräteeinstellungen verwalten“. Hier können CRUD Berechtigungen vergeben werden. Dadurch ist es möglich, dass manche Benutzer die Geräteeinstellungen nur ansehen aber nicht bearbeiten können, andere Benutzer hingegen dürfen diese auch ändern.

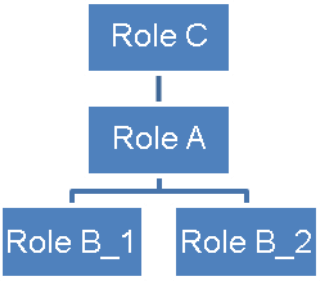
Die CRUD Berechtigungen sind hierarchisch organisiert. Dadurch ist es nicht möglich, Update Berechtigungen zu erteilen ohne dass dem Benutzer / der Rolle Read Berechtigungen erteilt wurden. Das Diagramm auf der rechten Seite zeigt die Hierarchie der Berechtigungsstufen.



Die "Benutzerverwaltung" und "Rollenverwaltung" Funktionsblöcke werden verwendet, um Benutzern das Bearbeiten von Benutzer- und Rollenrechte zu ermöglichen.

Zusätzlich zu den CRUD Berechtigungen und der Execute Berechtigung kann noch die Berechtigung zur Weitergabe von Berechtigungen (G; engl. Grant) vergeben werden. Diese befugt einen Benutzer, seine Berechtigungen für einen speziellen Funktionsblock an einen anderen Funktionsblock zu erteilen, sofern der Benutzer selbst die Grant Berechtigung für diesen Funktionsblock besitzt und die Rolle / der Benutzer, der / dem die Berechtigung erteilt werden soll, ein Nachfahre der Rolle des eingeloggten Benutzers ist.

Für die Abbildung auf der rechten Seite bedeutet das, dass ein Benutzer, welcher der Rolle A zugeordnet ist und die Grant Berechtigung besitzt, seine Berechtigungen auch an die Rollen B_1 und B_2 weitergeben kann. Der Benutzer kann jedoch maximal seine eigenen Berechtigungsstufen weitergeben. (Es ist nicht möglich, CRUD Berechtigungen zu erteilen, wenn der Benutzer selbst nur RU Berechtigungen besitzt).



6.2 Rollenverwaltung

Eine Rolle repräsentiert eine Sammlung von Berechtigungen für die Funktionsblöcke, welche in der Software definiert sind. Rollen sind hierarchisch geordnet. Jede Rolle ist genau einer übergeordneten Rolle zugeordnet und kann mehrere Kinder haben. Die hierarchische Struktur beinhaltet, wer welche Rollen und folglich auch die Benutzer dieser Rolle verwalten darf. Benutzer einer Rolle können nur Nachfahren der eigenen Rolle sowie deren Benutzer verwalten (sofern der Benutzer die Berechtigung für die „Benutzerverwaltung“ und „Rollenverwaltung“ besitzt).

GAT ACE bringt bereits eine übergeordnete Rolle mit, die SYSTEM Rolle. Die SYSTEM Rolle beinhaltet genau einen Benutzer, den SYSTEM Benutzer, wobei dieser immer alle Rechte hat. Jede Rolle ist auch ein Nachfahre der SYSTEM Rolle.

Die maximalen Rechte einer Rolle sind immer die Rechte der übergeordneten Rolle. Wenn eine Berechtigung aus der übergeordneten Rolle entfernt wird, wird dieses Recht folglich auch allen Nachfahren entzogen.

► Um eine neue Rolle zu definieren, öffnen sie die Rollenübersicht über den Menüpunkt "Rollen und Benutzer" aus dem System Menü.
  ○ Die Einstellungsseite "Rollen und Benutzer" wird geöffnet.

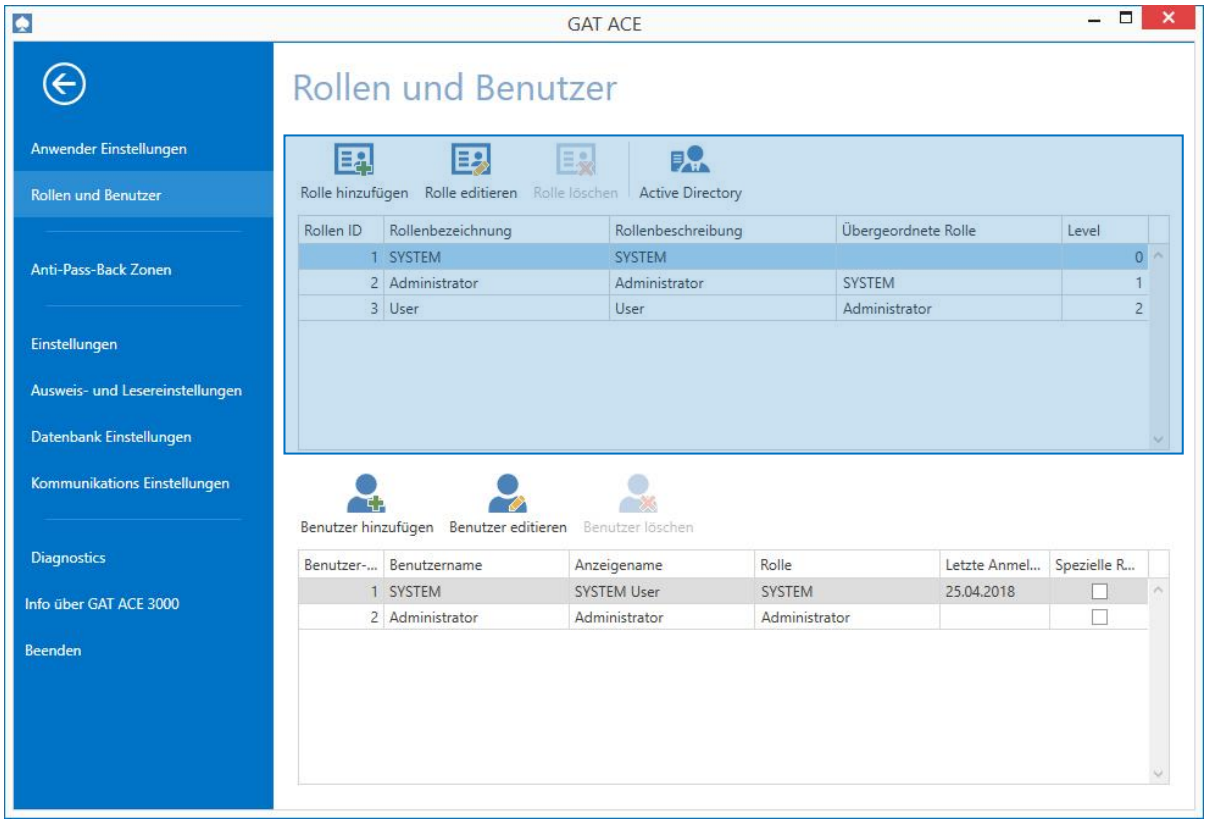


Bild 6.1 *- Rollenübersicht*

► Klicken Sie "Rolle hinzufügen", um eine neue Rolle hinzuzufügen.
  ○ Ein neues Fenster, in dem die Einstellungen der neuen Rolle festgelegt werden, wird geöffnet.

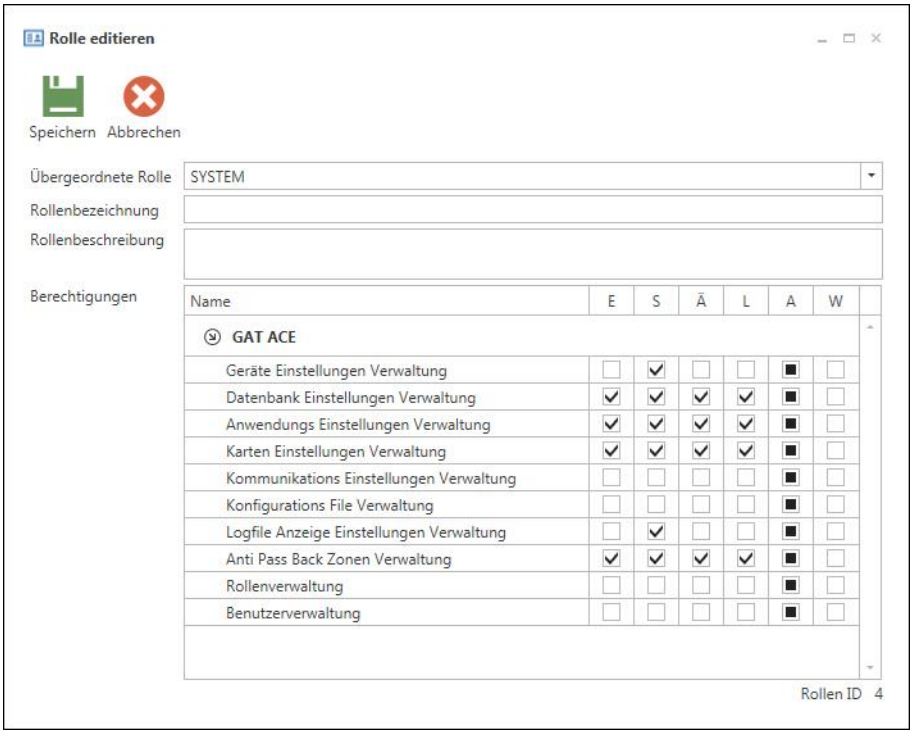


Bild 6.2 *- Rolleneinstellungen (Benutzer "SYSTEM")*

- ► Wählen Sie im Feld "Übergeordnete Rolle" die Rolle aus, von welcher die zu bearbeitende Rolle die Einstellungen erben soll.
- ► Geben Sie für die neue Rolle einen Namen im Feld "Rollenbezeichnung" ein. Jede Rolle muss eine eindeutige Bezeichnung erhalten.
- ► Im Feld "Rollenbeschreibung" geben Sie eine kurze Beschreibung zu der Rolle ein.
- ► Im Feld Berechtigungen legen Sie dann die einzelnen Berechtigungen für die Funktionsblöcke der Rolle fest.

Abhängig von der übergeordneten Rolle werden einzelne Berechtigungen veränderbar sein oder nicht. Im oberen Bild ist es z. B. möglich, für jeden Funktionsblock in GAT Relaxx die Berechtigungen zu vergeben, weil in diesem Fall der SYSTEM Benutzer eingeloggt ist, welcher die Grant Berechtigung für alle Funktionsblöcke besitzt. Mit den Optionsfeldern der einzelnen Funktionen haben Sie die Möglichkeit, die einzelnen Berechtigungen für die Funktionen einzustellen. Die Spalten bedeuten dabei:

- E: "Erstellen" (engl. "Create") Berechtigung - Erstellen von Datensätzen für die Funktion
- S: "Sehen" (engl. "Read") Berechtigung - Ansehen von Datensätzen der Funktion
- Ä: "Ändern" (engl. "Update") Berechtigung - Ändern von bestehenden Datensätzen der Funktion
- L: "Löschen" (engl. "Delete") Berechtigung - Löschen von bestehenden Datensätzen der Funktion
- A: "Ausführen" (engl "Executing") Berechtigung - Ausführen von Aktionen die Funktion betreffend
- W: "Weitergeben" (engl. "Grant") Berechtigung - Weitergeben der Berechtigung dieser Funktion an andere Benutzer

Die Rollen-ID wird automatisch berechnet und ist nur von Interesse wenn externe Anwendungen verwendet werden.

6.3 Benutzerverwaltung

Jeder Benutzer von GAT ACE hat einen eigenen Benutzer-Account mit einem eindeutigen Benutzernamen und Passwort. Durch das Passwort wird verhindert, dass Personen sich mit einem fremden Benutzernamen einloggen können. Jeder Benutzer in GAT ACE muss genau einer Rolle zugeordnet werden (siehe "6.2. Rollenverwaltung"). Es ist nicht möglich, dass ein Benutzer keiner Rolle zugeordnet wird. Die Benutzer erben die Berechtigungen von der Rolle.

Weiters ist es möglich, Berechtigungen von der Rolle explizit auf Benutzerebene für einzelne Funktionsblöcke zu überschreiben. Diese Benutzerberechtigungen bleiben auch erhalten, wenn die Berechtigung auf Rollenebene verändert wird.

► Um einen Benutzer-Account anzulegen, wählen Sie den Menüpunkt " Rollen und Benutzer" im System-Menü.
  ○ Die Einstellungsseite "Rollen und Benutzer" wird angezeigt.

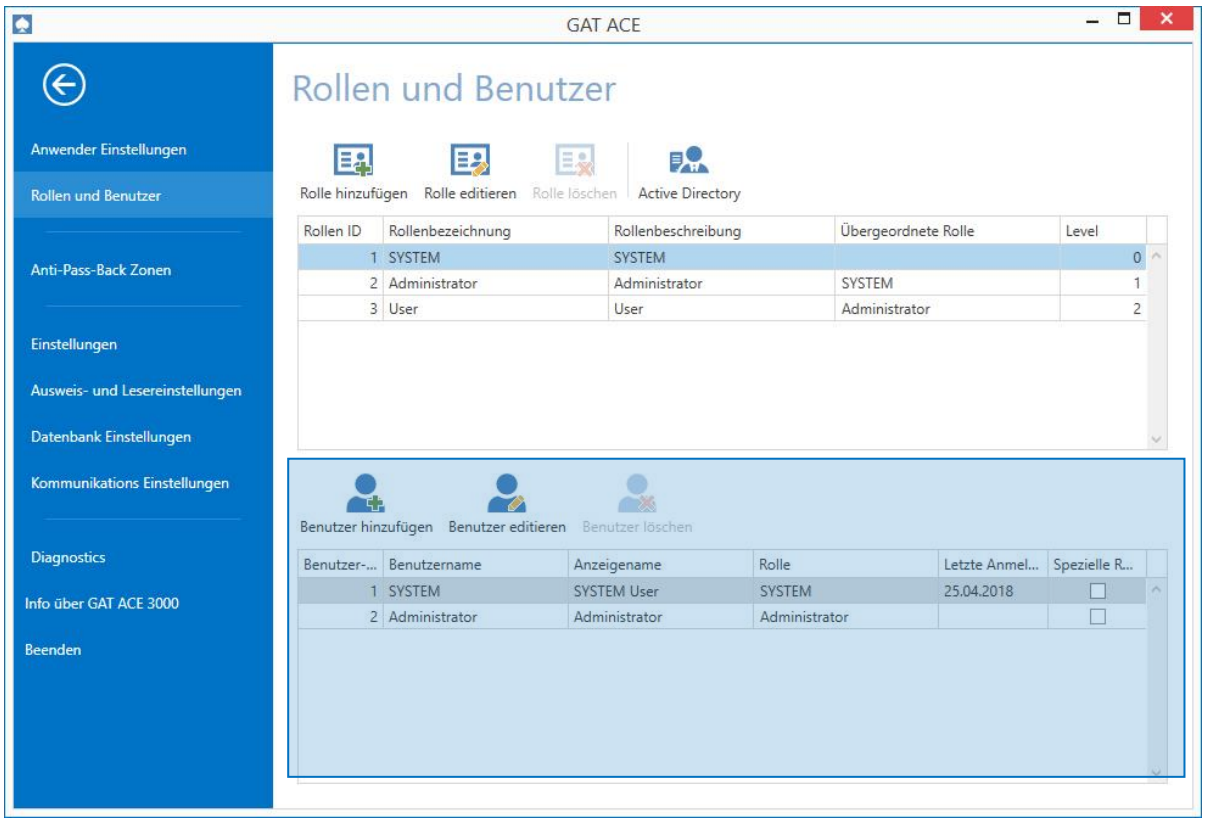


Bild 6.3 *- Benutzerübersicht*

Hier werden alle im Moment angelegten Benutzer-Accounts aufgelistet. Die Standard-Benutzer, welche nach Installation von GAT ACE automatisch angelegt sind, sind in Abschnitt "6.3.1. Standard-Benutzer" beschrieben. Sie können einen definierten Benutzer auswählen und seine Einstellungen mit "Benutzer editieren" bearbeiten.

► Um einen neuen Benutzer anzulegen, klicken Sie auf "Benutzer hinzufügen". Das Fenster "Benutzer editieren" wird geöffnet.

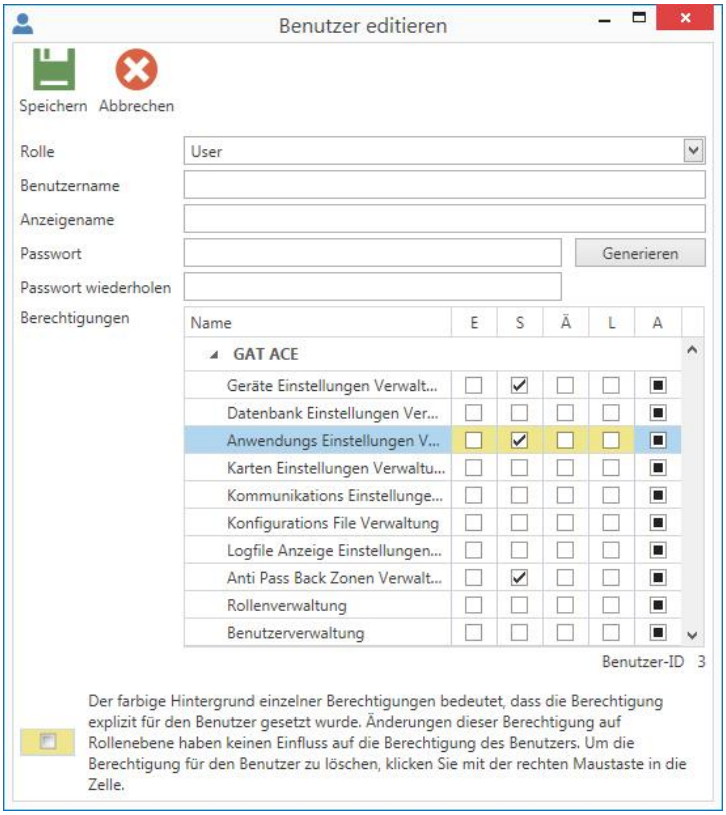


Bild 6.4 *- Benutzereinstellungen*

- ► Im Feld "Benutzername" muss ein eindeutiger Name für den Benutzer eingetragen werden. Mit diesem Namen kann sich der Benutzer später einloggen.
- ► Im Feld "Anzeigename" wird der Name eingetragen, den GAT ACE zur Anzeige des Benutzers im Programm verwendet. Dieser Name wird z. B. in den Log-Dateien verwendet.
- ► Geben Sie ein Passwort für den Benutzer ein. Dieses muss zur Überprüfung zweimal eingegeben werden.

Hinweis: Benutzen Sie ein starkes Passwort. Das Passwort soll mind. 7 Zeichen lang sein und mind. einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten. Mit der Schaltfläche "Generieren" können Sie sich ein möglichst sicheres Passwort von GAT Relaxx generieren lassen.

Die Benutzer-ID wird automatisch berechnet und ist nur für externe Anwendungen relevant.

- ► Im ersten Feld "Rolle" wählen sie die Rolle, die dem Benutzer für die Berechtigungsvergabe zugeordnet wird.
  - ○ Die Berechtigung der Funktionsblöcke wird entsprechend der gewählten Rolle gesetzt.
- ► Falls gewünscht können die von der Rolle definierten Berechtigungen überschrieben werden, indem in der Tabelle die jeweiligen Berechtigungen explizit gesetzt werden.
  - ○ Berechtigungen, die direkt bei einem Benutzer gesetzt werden, werden zur Kennzeichnung mit einem ockerfarbenen Hintergrund dargestellt. Im Beispiel in Bild 6.4 wurden die Leserechte ("S") des Funktionsblocks "Anwendungseinstellungen Verwaltung" gesetzt, welche die vererbten Rechte der Rolle an diesen Stellen überschreiben.
- ► Um explizit gesetzte Rechte zurückzunehmen, klicken Sie mit der rechten Maustaste auf die entsprechenden Felder.

6.3.1 Standard-Benutzer

Nach Installation von GAT ACE sind folgende Benutzer als Standard bereits angelegt.

Benutzer:	**SYSTEM**	**Administrator**
Rolle:	SYSTEM	Administrator
Passwort:	GAT	Mirone59

Ändern Sie nach der Installation von GAT ACE aus Sicherheitsgründen die Standard Passwörter auf sichere, geheime Passwörter ab.

Berechtigungen für Rolle "SYSTEM":

Name	Erstellen (Create)	Sehen (Read)	Ändern (Update)	Löschen (Delete)	Ausführen (Execute)	Weitergeben (Grant)
Geräte Einstellungen Verwaltung	X	X	X	X	-	X
Datenbank Einstellungen Verwaltung	X	X	X	X	-	X
Anwendungs Einstellungen Verwaltung	X	X	X	X	-	X
Karten Einstellungen Verwaltung	X	X	X	X	-	X
Kommunikations Einstellungen Verw.	X	X	X	X	-	X
Konfigurations File Verwaltung	X	X	X	X	-	X
Logfile Anzeige Einstellungen Verw.	X	X	X	X	-	X
Anti Pass Back Zone Verwaltung	X	X	X	X	-	X
Rollenverwaltung	X	X	X	X	-	X
Benutzerverwaltung	X	X	X	X	-	X

X … erlaubt
O … nicht erlaubt
- … nicht verfügbar

Berechtigungen für Rolle "Administrator":

Name	Erstellen (Create)	Sehen (Read)	Ändern (Update)	Löschen (Delete)	Ausführen (Execute)	Weitergeben (Grant)
Geräte Einstellungen Verwaltung	X	X	X	X	-	X
Datenbank Einstellungen Verwaltung	X	X	X	X	-	X
Anwendungs Einstellungen Verwaltung	X	X	X	X	-	X
Karten Einstellungen Verwaltung	X	X	X	X	-	X
Kommunikations Einstellungen Verw.	O	O	O	O	-	O
Konfigurations File Verwaltung	O	O	O	O	-	O
Logfile Anzeige Einstellungen Verw.	X	X	X	X	-	X
Anti Pass Back Zone Verwaltung	X	X	X	X	-	X
Rollenverwaltung	X	X	X	X	-	X
Benutzerverwaltung	X	X	X	X	-	X

X … erlaubt
O … nicht erlaubt
- … nicht verfügbar

7 UMSTIEG VON GAT MANAGER AUF GAT ACE

GAT ACE wurde als moderner Nachfolger für die GAT Manager Software von GANTNER Electronic GmbH entwickelt. Bestehende Anlagen, welche die GAT Manager Software verwenden und auf GAT ACE umgestellt werden sollen, können das Software-Tool "Gm2AceConverter" von GANTNER Electronic GmbH verwenden, mit dem die bestehende Datenbank mit den Controller-Konfigurationen in GAT ACE importiert werden kann. In diesem Abschnitt erhalten Sie einen Überblick über dieses Tool.

Das Tool Gm2AceConverter ist ohne Installation lauffähig.

- ► Kopiere Sie das Paket mit dem Gm2AceConverter in einen Ordner auf dem PC, auf dem GAT Manager installiert ist.
- ► Starten Sie in diesem Ordner die Daten "Gm2AceConverter.exe".
  - ○ Folgende Oberfläche wird angezeigt.

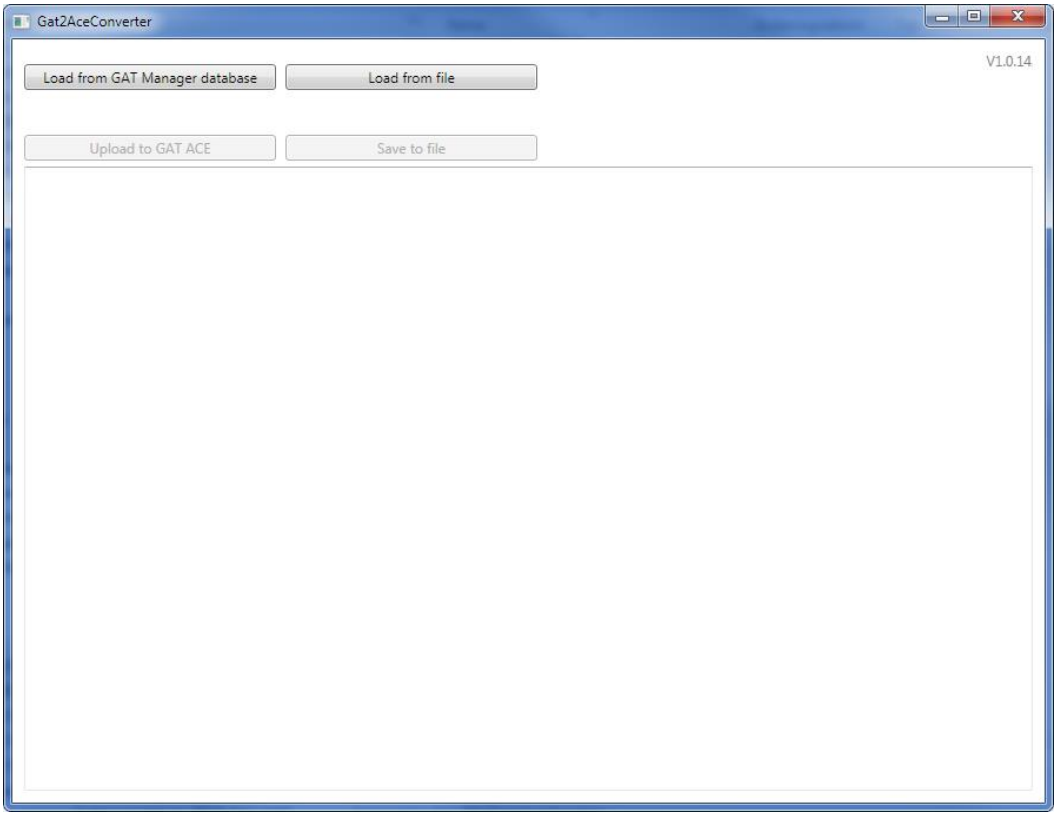


Bild 7.1 *- Programmfenster von Gat2AceConverter*

- ► Klicken Sie auf die Schaltfläche "Load from GAT Manager database".
- ► Wählen Sie den Ort, an dem die GAT Manager Datenbankfiles liegen.
  - ○ Die Daten werden aus der Datenbank gelesen.
- ► Sichern Sie die Datenbank in eine Datei, in dem Sie die Schaltfläche "Save to file" klicken.

- ► Kopieren Sie nun das Paket mit dem Gm2AceConverter in einen Ordner auf dem PC, auf dem GAT ACE installiert ist.
- ► Kopieren Sie die zuvor erstellte Datei auf den GAT ACE PC.
- ► Starten Sie das Tool "Gm2AceConverter.exe" auf dem PC wo der GAT ACE 3000 Dienst bereits gestartet ist.
- ► Klicken Sie auf "Load from file", und wählen Sie die Datei, die Sie auf dem GAT Manager PC erstellt haben aus, um diese zu laden.
- ► Klicken Sie auf die Taste "Upload to GAT ACE", um die Daten in GAT ACE zu übernehmen.
  - ○ Sie können GAT ACE nun starten und alle Einstellungen von GAT Manager wurden übernommen.
- ► Überprüfen Sie die Einstellungen der Controller auf eventuell fehlende Einstellungen, die in GAT ACE neu sind.

Achtung: Der Gm2Ace Converter benötigt auf dem GAT Manager Rechner ein .NET Framework 4.5.
Kann dieses auf Grund des Alters des Betriebssystems nicht installiert werden, können Sie die Datenbank des GAT Managers sowie die Datei FLEX.INI auf einen anderen PC übertragen, auf dem ein GAT Manager oder die Borland Database Engine installiert ist und auf dem das .NET Framework 4.5 vorhanden ist. Die Konvertierung kann dann auch auf diesem PC erfolgen.

8 DATENSCHUTZ

8.1 Datenschutz-Grundverordnung (DSGVO)

Ab 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO). Die neuen Regelungen betreffen alle Unternehmen, die personenbezogene Daten verarbeiten. Die DSGVO regelt den Umgang mit personenbezogenen Daten und legt die Bedingungen fest, unter denen Unternehmen diese Daten verarbeiten dürfen (z. B. Mitarbeiterdaten). Die DSGVO betrifft sowohl Einpersonenunternehmen als auch große Unternehmen.

Die DSGVO ist inhaltlich auf sieben Prinzipien aufgebaut, die als Orientierung für Ihre Datenschutzbemühungen herangezogen werden können. Diese sind:

- Prinzip der Speicherbegrenzung
- Prinzip der Datenminimierung
- Prinzip der Zweckbindung
- Prinzip der Richtigkeit
- Prinzip der Integrität und Vertraulichkeit
- Prinzip der Rechenschaftspflicht
- Prinzip der Rechtmäßigkeit und Transparenz

Definition von persönlichen Daten und Datenverarbeitung

Persönliche Daten sind alle jene Daten, die direkt oder indirekt einen Rückschluss auf eine konkrete Person ermöglichen, wie beispielsweise E-Mail, Name, Foto. Als sensible persönliche Daten gelten besonders schutzwürdige, personenbezogene Daten, wie zum Beispiel biometrische oder genetische Daten. Aber auch Informationen zur ethnischen Herkunft, politischen Meinung, Gewerkschaftszugehörigkeit, religiösen oder philosophischen Überzeugung, Gesundheit oder Sexualität gelten als sensibel.

Datenverarbeitung beschreibt das Sichten und Speichern von Daten sowie jede automatisierte oder manuelle Form der Verarbeitung. Eine Datenanwendung liegt dann vor, wenn personenbezogene Daten zur Gänze oder teilweise automationsunterstützt geordnet sind.

Damit ist klar, dass für Zutrittskontrolle die DSGVO relevant ist. In weiteren Schritten ist somit zu klären, was hinsichtlich Zutrittskontrolle unternommen werden muss und welche Möglichkeiten GAT ACE 3000 dazu bietet. Die Schritte werden in den folgenden Abschnitten zusammengefasst.

8.1.1 Führen Sie eine Bestandsanalyse durch

Prüfen Sie, welche Daten in Ihrer Zutrittskontrolle erfasst und gespeichert werden. Hinterfragen Sie, für welche Zwecke die Daten benötigt werden, wie lange sie gespeichert werden und wer darauf Zugriff hat. Prüfen Sie auch, ob die Daten an Externe weitergegeben werden.

Die Zutrittskontrolle kann oftmals mit einem Namen (der auch anonymisiert werden könnte) und einer Ausweisnummer arbeiten. Mitunter werden aber noch zusätzliche Felder wie z. B. ein PIN-Code erfasst, um höhere Sicherheit gewährleisten zu können. Weitere Informationen, die z. B. in optionalen Feldern gespeichert werden, sind nicht unmittelbar relevant für die Zutrittskontrollentscheidung. In diesen Fällen gilt es zu prüfen, ob diese Daten in der Zutrittskontrollsoftware gespeichert werden müssen.

Verarbeitungsverzeichnis erstellen

Nach dem Sie die Bestandsanalyse durchgeführt haben, muss ein Verarbeitungsverzeichnis erstellt werden. Das Verarbeitungsverzeichnis ist eine der zentralen Neuerungen der DSGVO und ersetzt die derzeitigen DVR Meldungen. Es muss u.a. Namen und Kontaktdaten des Verantwortlichen, den Zweck der Datenverarbeitung (Zutrittskontrolle), die Kategorien der betroffenen Personen und der personenbezogenen Daten, die Kategorien von Empfängern und die Beschreibung der Datensicherheitsmaßnahmen enthalten.

Bei der Kategorie der betroffenen Personen handelt es sich im Normalfall um Mitarbeiter. In Ausnahmefällen können auch Lieferanten oder Kunden von der Zutrittskontrolle behandelt werden.

In der Zutrittskontrolle hat GANTNER auf das **Prinzip der Datenminimierung** und das **Prinzip der Zweckbindung** der personenbezogenen Daten geachtet. Es werden nicht mehr Daten gespeichert, als für den Betrieb der Systeme notwendig sind. Im Wesentlichen wird eine Ausweisnummer als Identifikationsmerkmal und ein Name der Person gespeichert. Weitere Daten wie z. B. ein PIN-Code, eine Personalnummer oder Salden sind optional und dienen der Erhöhung der Sicherheit oder der Schaffung von Komfort. Es werden in den Systemen standardmäßig keine sensiblen Daten gespeichert. Ausnahme ist allerdings, wenn im System Fingerabdrücke verwendet werden. Hierbei handelt es sich um biometrische Daten.

Die Daten der Zutrittskontrolle werden im Normalfall nicht an andere Systeme weitergegeben.

Das **Prinzip der Richtigkeit** der Daten muss im Interesse des Systembetreibers liegen, denn schlussendlich hängen davon auch die Sicherheit des Unternehmens bzw. die Kosten für Personalaufwände ab. Das **Prinzip der Integrität und Vertraulichkeit** der Daten wird sichergestellt, indem nur berechtigte Personen Zugriff auf die Software erlangen und die Benutzer der Software nur Zugriff auf jene Daten erhalten, die für die Erfüllung ihrer Aufgaben benötigt werden (siehe Abschnitt "6.3. Benutzerverwaltung").

8.1.2 Datenschutz Folgeabschätzung

Eine Datenschutz Folgeabschätzung ist im Normalfall nicht erforderlich, da kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Es werden bekannte Technologien verwendet und es erfolgen keine systematischen Auswertungen und Bewertungen persönlicher Aspekte. Bei Verwendung von Fingerabdrücken ist eine individuelle Betrachtung für den jeweiligen Fall zu empfehlen.

8.1.3 Informationspflichten befolgen und Zustimmungserklärungen

Von einer Datenverarbeitung betroffene Personen müssen über diese informiert werden können (was, wer, zu welchem Zweck, wie lange, wohin?). Auch Betroffenenrechte (z.B. Auskunft, Löschung) müssen unverzüglich, spätestens innerhalb eines Monats, erfüllt werden.

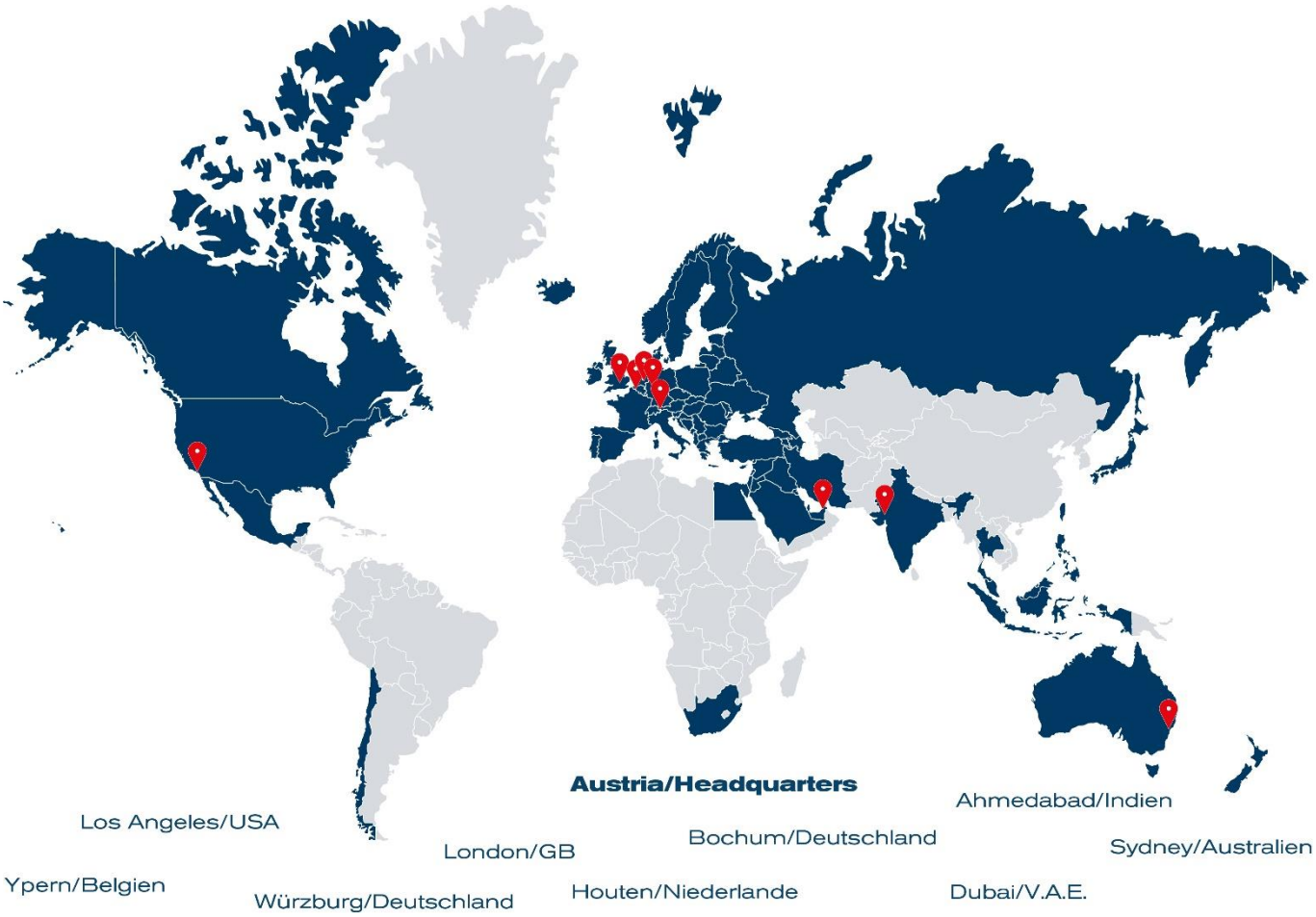
Die Zustimmung der Personen für die Verwendung der persönlichen Daten zum Zweck der Zutrittskontrolle und Zeiterfassung sollte in den Dienstverträgen oder in einer Betriebsvereinbarung definiert sein. Dadurch kann das **Prinzip der Rechtmäßigkeit und Transparenz** sichergestellt werden.

Die Speicherfrist der Daten ist abhängig von der Anforderung der Nachvollziehbarkeit von Zutritten, die Sie in Ihrem Unternehmen benötigen. Durch diese Löschung von Daten kann das **Prinzip der Speicherbegrenzung** erfüllt werden (siehe Abschnitt "5.3.2. Bereinigung der Datenbanktabelle").

Wenn Sie in Ihrem Unternehmen einen Verantwortlichen für die Datenschutzpolitik benannt haben, die rechtlichen Rahmenbedingungen erfüllt, die technischen und organisatorischen Maßnahmen ergriffen und die Dokumentation erstellt haben, können Sie auch dem **Prinzip der Rechenschaftspflicht** nachkommen und sind gut vorbereitet für das Inkrafttreten der Datenschutz-Grundverordnung.

Zusammenfassend möchten wir Sie darauf hinweisen, dass Sie mit einer GAT ACE 3000, Version 3.0 oder höher sehr einfach die Möglichkeit haben, der DSGVO entsprechend nachzukommen. Bitte scheuen Sie sich nicht, bei Fragen oder Unklarheiten sich mit Ihrem Vertriebsbeauftragten in Verbindung zu setzen.

Hinweis:
Dieses Handbuch ist gültig ab 29. July 2019. Änderungen und Ergänzungen dieses Handbuchs sind jederzeit ohne Vorankündigung möglich!
Informationen in diesem Handbuch beziehen sich auf die GAT ACE Version 3.0.0 oder neuer.



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

Schruns, 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.: 534929