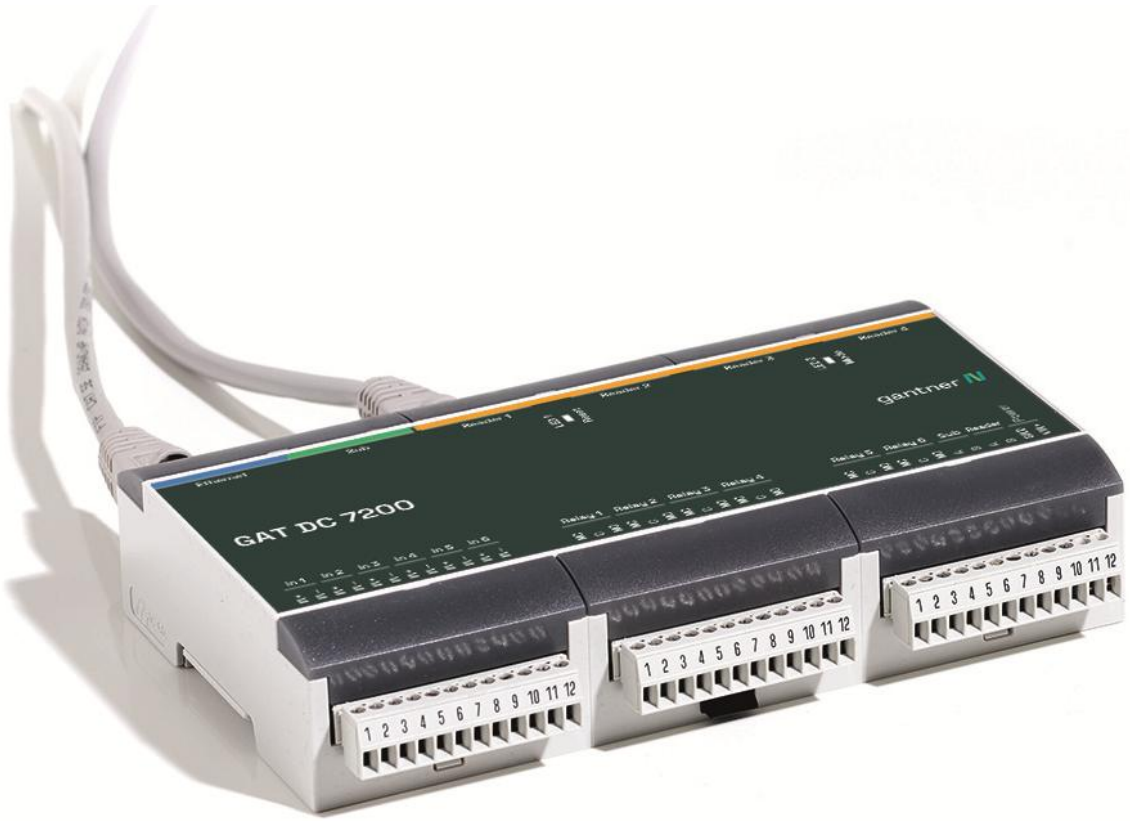
Gantner

GAT DC 7200

Türcontroller für die elektronische Zutrittskontrolle



Installation, Konfiguration, Bedienung
Dokumentversion 3.7
Firmwareversion 3.7

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 werden, dienen lediglich Identifizierungs- und Erklärungszwecken und je nach Bezeichnung kann es sich dabei um Warenzeichen oder eingetragene Warenzeichen der entsprechenden Firmen handeln.

Kontakt
Kontaktinformationen für Rückfragen bezüglich GAT DC 7200 oder generelle Anfragen finden Sie unten:

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

Wichtige Informationen

Verehrte Kundin, verehrter Kunde,
Damit unser Produkt in Ihrer Anlage zu Ihrer Zufriedenheit sicher und ohne Fehler arbeitet, weisen wir Sie auf folgende Grundregeln hin.

- Beachten Sie die Sicherheitshinweise in diesem Handbuch. Diese werden durch die Signalwörter "GEFAHR", "WARNUNG", "ACHTUNG" gekennzeichnet und informieren Sie über mögliche gefährliche Situationen und wie Sie diese vermeiden können.
- Beachten Sie auch Informationen, die mit dem Signalwort "HINWEIS" gekennzeichnet sind. Diese enthalten wichtige Informationen zur Vermeidung von Sachschaden.
- Achten Sie auch auf die Symbole und Warnhinweise auf dem Produkt.
- Lesen Sie alle Informationen in diesem Handbuch genau durch, bevor Sie das Gerät installieren und in Betrieb nehmen.
- Sofern dies nicht an anderer Stelle speziell dokumentiert ist, liegt die Installation, Inbetriebnahme und Wartung des Produkts in der Verantwortung des Kunden.
- Bewahren Sie dieses Handbuch an einem sicheren, für Nachschlagezwecke schnell zugänglichen Ort auf.

Schreibweise von Sicherheitsinformationen und Sicherheitssymbole

Dieses Handbuch enthält wichtige Sicherheitshinweise und Symbole zur Vermeidung von Personen- und Sachschäden. Diese Informationen und Symbole informieren den Anwender über gefährlichen Situationen und beschreiben den sicheren, sachgemäßen Umgang des Produkts. Die Sicherheitshinweise enthalten auch Informationen zur Vermeidung der gefährlichen Situationen. Lesen Sie diese Sicherheitshinweise unbedingt genau und handeln Sie danach.
Die folgenden Zeilen beschreiben die Struktur der in diesem Handbuch verwendeten Sicherheitshinweise und die Bedeutung der verwendeten Symbole.

1. Sicherheitshinweisen zu Personenschaden

Sicherheitshinweise enthalten ein Signalwort, und beschreiben die Art der Gefahr und wie Sie diese Gefahr vermeiden können.

Wird das Sicherheitsalarmzeichen ohne Signalwort verwendet, folgen immer wichtige sicherheitsrelevante Informationen, die genau gelesen und befolgt werden müssen. Nichtbeachtung kann zu Personenschaden führen.

Format von Sicherheitshinweisen, die sich auf einen ganzen Abschnitt beziehen:

Die Verwendung dieses Sicherheitshinweises ist mit oder ohne Symbol möglich.

⚠ VORSICHT

Elektrischer Schlag.

➔ *Das Berühren von spannungsführenden Teilen kann zu Verletzungen durch elektrischen Schlag führen.*

- Schutzeinrichtungen und Abdeckungen nicht entfernen.
- Anschlussklemmen nicht berühren, wenn das Produkt mit Strom versorgt wird.

Format von Sicherheitshinweisen, die im Text eingebettet sind und sich auf diese konkrete Stelle beziehen:

⚠ **ACHTUNG! Elektrischer Schlag.** Schutzeinrichtungen und Abdeckungen nicht entfernen. Anschlussklemmen nicht berühren, wenn das Produkt mit Strom versorgt wird.

2. Sicherheitshinweise zu Sachschaden

Sicherheitshinweise, die mögliche Gefahrensituationen für Sachschaden beschreiben, haben dasselbe Layout wie Sicherheitshinweise für Personenschaden, nur dass als Signalwort "HINWEIS" verwendet wird.

Format von Sicherheitshinweisen, die sich auf einen ganzen Abschnitt beziehen:

HINWEIS

Gefahr von Sachschaden für das Gerät und angeschlossener Geräte.

Gefahr von Fehlfunktion.

- Folgende Anweisungen genau lesen und befolgen, bevor Sie das Gerät installieren.

- Immer die Anweisungen befolgen.

Format von Sicherheitshinweisen, die im Text eingebettet sind und sich auf diese konkrete Stelle beziehen:

HINWEIS! Gefahr von Sachschaden für das Gerät und angeschlossener Geräte. Lesen Sie die folgenden Anweisungen genau, bevor Sie das Gerät installieren.

3. Bedeutung der verwendeten Signalwörter

⚠ VORSICHT	Kennzeichnet eine gefährliche Situation die, wenn sie nicht vermieden wird, zu leichten und mittelschweren Verletzungen führen kann.
HINWEIS	Kennzeichnet wichtige Informationen, die jedoch nicht verletzungsrelevant sind (z. B. Hinweise bezüglich möglichen Sachschaden).

4. Bedeutung der verwendeten Sicherheitssymbole

	**Vorsicht: Allgemeine Information** Dieses Symbol kennzeichnet allgemeine Warnungen, die sich nicht auf eine bestimmten Typ von Gefahren beziehen.
	**Vorsicht: Elektrischer Schlag** Dieses Symbol kennzeichnet Warnungen in Bezug auf elektrische Gefahren (gefährliche Spannungen und Ströme).
	**Verbot: Nicht auseinander nehmen, nicht demontieren** Dieses Symbol kennzeichnet Warnungen bezüglich nicht erlaubten auseinander nehmen und Demontage von bestimmten Teilen oder Geräten. Nichtbefolgung kann zu Beschädigungen oder Fehlfunktionen des Geräts führen kann.
	**Verpflichtende Tätigkeit: Allgemeine Information** Dieses Symbol kennzeichnet allgemeine Informationen die gelesen und befolgt werden müssen, bevor weitere Schritte durchgeführt werden.
	**Verpflichtende Tätigkeit: Instruktionen lesen** Dieses Symbol kennzeichnet Informationen die sich auf wichtige Instruktionen beziehen, die in diesem Handbuch oder an einem anderen Ort zu finden sind. Diese Texte müssen gelesen und befolgt werden.

⚠ Wichtige Sicherheitshinweise ⚠

- 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.
  - ➔ Arbeiten durch unqualifiziertes Personal kann zu Verletzungen führen (z. B. elektrischer Schlag).

- 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.
  - ➔ Wenn das Gerät nicht von der Versorgungsspannung getrennt ist, kann es durch Berührung von Klemmen oder internen Teilen zu leichten Verletzungen kommen (elektrischer Schlag).

- Es ist untersagt, Veränderungen am Produkt vorzunehmen (Gerät, Anschlusskabel):
  - ➔ Veränderungen am Produkt können zu Verletzungen oder Sachschaden führen und das Gerät beschädigen.
- Es ist untersagt, Schutz- und Abdeckhauben von Geräten zu entfernen.
  - ➔ Das Entfernen von Schutz- und Abdeckhauben vom Produkt können zu Verletzungen oder Sachschaden führen.
- 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.

- Installation, Inbetriebnahme, Betrieb und Wartung des erworbenen Produkts haben bestimmungsgemäß, d.h. innerhalb der in der zugehörenden Produktdokumentation aufgeführten technischen Einsatzbedingungen, zu erfolgen. Lesen Sie daher unbedingt die entsprechenden Kapitel in diesem Handbuch durch und handeln Sie danach.
- 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.
- 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.).

- 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.
- Wenn nicht anders festgelegt, trägt der Kunde die Verantwortung für bestimmungsgemäße Installation, Inbetriebnahme, Betrieb und Wartung des Produkts.
- Die GANTNER Electronic GmbH übernimmt keine Verantwortung für Verletzungen oder Schäden, die Folge eines unsachgemäßen Gebrauches sind.

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.

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.

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

Der GAT DC 7200 wurde unter dem Qualitätsmanagement-Standard ISO 9001 entwickelt und produziert. GANTNER Electronic GmbH ist nach ISO 14001 zertifiziert.

Hiermit bestätigt GANTNER Electronic GmbH, dass dieses Gerät in Übereinstimmung mit den folgenden EG-Richtlinien, einschließlich aller zutreffenden Ergänzungen, ist:
- 2014/53/EU (EMV-Richtlinie)
Der vollständige Text der CE-Konformitätserklärung ist über folgende Internet-Adresse online abrufbar:
http://www.gantner.com/de/produkte/downloads-GAT-DC-7200_o84nFQzc7D

Dieses GANTNER Produkt erfüllt oder übertrifft die Anforderungen aus der RoHS-Richtlinie (2011/65/EU). Die RoHS-Richtlinie verlangt für Geräte, die nach dem 1. Juli 2006 in der EU verkauft werden, dass Hersteller die Verwendung von Blei, Quecksilber, Cadmium, sechswertiges Chrom, polybromierte Biphenyle und polybromierte Diphenylether eliminiert oder unter bestimmte Grenzwerte reduziert.

Das WEEE-Symbol auf GANTNER Produkten oder deren Verpackungen weist darauf hin, dass das entsprechende Produkt und verwendete Batterien/Akkus nicht mit dem Hausmüll entsorgt werden dürfen. Sie müssen das so gekennzeichnete Altgerät und/oder Batterien/Akkus an entsprechende Sammelstellen zum Recycling elektrischer und elektronischer Geräte und/oder Batterien/Akkus übergeben. Das Recycling von Materialien hilft bei der Schonung natürlicher Ressourcen und gewährleistet eine für die menschliche Gesundheit und Umwelt sichere Art der Wiederverwertung. Weitere Informationen zum Recycling dieses Gerätes und/oder der Batterien/Akkus erhalten Sie bei Ihrer Stadtverwaltung oder Ihrem Entsorgungsbetrieb.

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Zu diesem Handbuch

Dieses Handbuch enthält alle Informationen zur Installation, Inbetriebnahme und Betrieb des Türcontrollers GAT DC 7200. Außerdem finden Sie hier die Serviceanleitung und Entsorgungshinweise sowie die technischen Daten des GAT DC 7200.
Die Konfiguration des GAT DC 7200 wird ebenfalls beschrieben. Diese erfolgt in einem Internetbrowser anhand der Web-Oberfläche des GAT DC 7200. Die für die Konfiguration notwendigen Informationen finden Sie in diesem Handbuch.

1.2 Kapitelübersicht

In Kapitel "2 ALLGEMEINE INFORMATIONEN" finden Sie die Funktionsbeschreibung und eine Geräteübersicht des GAT DC 7200, die vom Gerät unterstützten Leser und Peripheriegeräte sowie RFID-Technologien und eine Beschreibung der wichtigsten in diesem Handbuch verwendeten Begriffe.

In Kapitel "3 MONTAGE" ist die Hutschienen-Montage und Wandmontage des GAT DC 7200 beschrieben. Hier finden Sie auch die notwendigen Abmessungen für die Montage.

In Kapitel "4 ELEKTRISCHER ANSCHLUSS" wird der Anschluss der externen Leser und Peripheriegeräte sowie der digitalen Ein- und Ausgänge beschrieben. Der Anschluss des Netzwerks zur Kommunikation sowie der Spannungsversorgung finden Sie ebenfalls in diesem Kapitel.

In Kapitel "5 BEDIENELEMENTE UND SIGNALISIERUNG" finden Sie die die Bedienungsschritte am GAT DC 7200 und die Erklärung der Statusanzeigen.

In Kapitel "6 INBETRIEBNAHME UND KONFIGURATION" finden Sie die Beschreibung, wie der GAT DC 7200 für den Einsatz konfiguriert und in Betrieb genommen wird. Die Konfiguration erfolgt mittels Web-Oberfläche in einem Internetbrowser. Hier werden die wichtigen Punkte der Oberfläche beschrieben und sie erhalten einen Überblick über die möglichen Konfigurationseinstellungen.

Im Kapitel "7 BERECHTIGUNGSVERGABE“ finden Sie Hinweise zur Berechtigungsverwaltung mit einer Zutrittskontrollsoftware.

Im Kapitel "8 STANDALONE MODUS“ finden Sie Hinweise zur Berechtigungsverwaltung ohne Zutrittskontrollsoftware.

Im Kapitel "9 FRAGEN UND ANTWORTEN“ finden Sie häufig gestellte Fragen und die Antworten dazu.

Kapitel "10 TECHNISCHE DATEN" enthält die technischen Daten des GAT DC 7200 und die Abmessungen des Geräts.

1.3 Zielgruppen

Dieses Handbuch enthält die notwendigen Informationen für die verschiedenen Lebenszyklen des GAT DC 7200 wie Installation, elektrischer Anschluss, Inbetriebnahme, Service und Wartung, unterteilt in entsprechende Kapitel. Ist ein Kapitel nur für eine bestimmte Zielgruppe bestimmt, wird diese zu Beginn des Kapitels angegeben. Die folgenden Zielgruppen finden Informationen in diesem Handbuch:

- Installationspersonal (Montage, Inbetriebnahme, Konfiguration)
- Servicetechniker der Zutrittsanlage (Service)
- Benutzer der GAT DC 7200 (Bedienungsanleitung)

Wenn die Zielgruppe nicht speziell angegeben wird, sind die Informationen für alle Zielgruppen bestimmt.

⚠ **ACHTUNG! Verletzung und Sach-/Geräteschaden.** Die Tätigkeiten, die laut diesem Handbuch für eine bestimmte Zielgruppe bestimmt sind, dürfen nur von dieser Zielgruppe ausgeführt werden. Ausführen der Tätigkeiten durch unqualifiziertes Personal kann zu Verletzungen oder Sach-/Geräteschaden führen.

1.1 Formatierung

Zur Identifikation von besonders interessanten, aber nicht sicherheitsrelevanten, Informationen wird folgende Formatierung in diesem Handbuch verwendet:

Informationstext Informationstext Informationstext Informationstext Informationstext Informationstext Informationstext Informationstext Informationstext

Tätigkeiten, die ein Anwender ausführen muss, und aus den Tätigkeiten resultierenden Ergebnisse sind wie folgt formatiert:

► Tätigkeitsbeschreibung Tätigkeitsbeschreibung Tätigkeitsbeschreibung Tätigkeitsbeschreibung Tätigkeitsbeschreibung Tätigkeitsbeschreibung Tätigkeitsbeschreibung.

  ○ Resultat nach Ausführung der Tätigkeit, Resultat nach Ausführung der Tätigkeit, Resultat nach Ausführung der Tätigkeit.

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

1.4 Ansprechpartner bei Rückfragen

Bei Fragen in Zusammenhang mit dem GAT DC 7200 wenden Sie sich bitte an die für Sie zuständige Vertretung oder direkt an eine der GANTNER Electronic GmbH Niederlassungen. Die Kontaktadressen finden Sie unter folgendem Link:
www.gantner.com/locations

2 ALLGEMEINE INFORMATIONEN

2.1 Bestimmungsgemäße Verwendung

Der Türcontroller GAT DC 7200 ist für die elektronische Zutrittskontrolle von Innen- und Außentüren in öffentlichen Gebäuden wie Firmen, Verkaufs- oder Fabrikgebäuden vorgesehen. Zusätzlich zum GAT DC 7200 wird dazu noch ein oder mehrere externe Leser (von GANTNER Electronic GmbH erhältlich) sowie ein elektronisches Türschloss benötigt. Die Identifikation der Benutzer an den angeschlossenen Lesern erfolgt berührungslos mittels RFID (Radio Frequency Identification) Datenträgern, Biometrie, Codeeingabe oder Mobilgeräten mit Mobile Credentials.

Die Typen der zu kontrollierenden Türen ist unabhängig von dem GAT DC 7200, es muss das passende elektronische Türschloss verwendet werden.

2.2 Funktionsbeschreibung

Um Zutritt zu einem, vom Türcontroller GAT DC 7200 gesicherten Bereich eines Gebäudes zu erhalten, identifiziert sich eine Person mit ihrem persönlichen RFID Datenträger oder Mobile Credential an der abgesetzten Leseeinheit, die am Türcontroller angeschlossen ist. Es können dabei auch mehrere Leser verwendet werden. Der Türcontroller überprüft nun die gelesenen Ausweisdaten mit den im Türcontroller gespeicherten Berechtigungsdaten und Zeitplänen. Ist der Zutritt erlaubt, steuert der Türcontroller über das konfigurierte Relais den elektronischen Türöffner bzw. entriegelt das elektronische Türschloss.

Der Türcontroller ist im gesicherten Bereich installiert und die Kommunikation zwischen Türcontroller und Leser erfolgt zum Schutz vor Manipulationsversuchen verschlüsselt. Auch die Kommunikation zur Konfiguration des Türcontrollers über die Webschnittstelle wird für optimale Sicherheit verschlüsselt durchgeführt (TLS/SSL Verbindung).

Die Türsteuerung kann sehr flexibel angepasst werden. Je nach Anwendung können auch mehrere Türen von einem Türcontroller überwacht und gesteuert werden und es sind auch bis zu 4 Leser (mit Zusatzlizenz bis zu 16) an einem GAT DC 7200 anschließbar. Dadurch lassen sich Funktionen wie Richtungserkennung (z. B. ein Leser für die Identifikation bei Eintritten und ein Leser für die Identifikation bei Austritten) realisieren. Zur Erweiterung der digitalen Ein- und Ausgänge des Türcontrollers können die GAT IO 7xxx Module angeschlossen werden.

Der Türcontroller GAT DC 7200 arbeitet autonom. Über die Ethernet-Schnittstelle wird er an eine Zutrittskontroll-software angeschlossen. GANTNER Electronic GmbH bietet dazu die Kommunikations- und Konfigurationssoftware GAT ACE 7000 und die Zutrittsberechtigungssoftware Matrix an. GAT ACE 7000 ist die zentrale Schnittstelle zwischen Matrix und Türcontroller und dient zur Konfiguration der Türcontroller, Leser und Anlage. In Matrix werden die Zeitpläne, Zutrittsberechtigungen der Personen, Datenträger usw. festgelegt und an den Türcontroller übertragen.

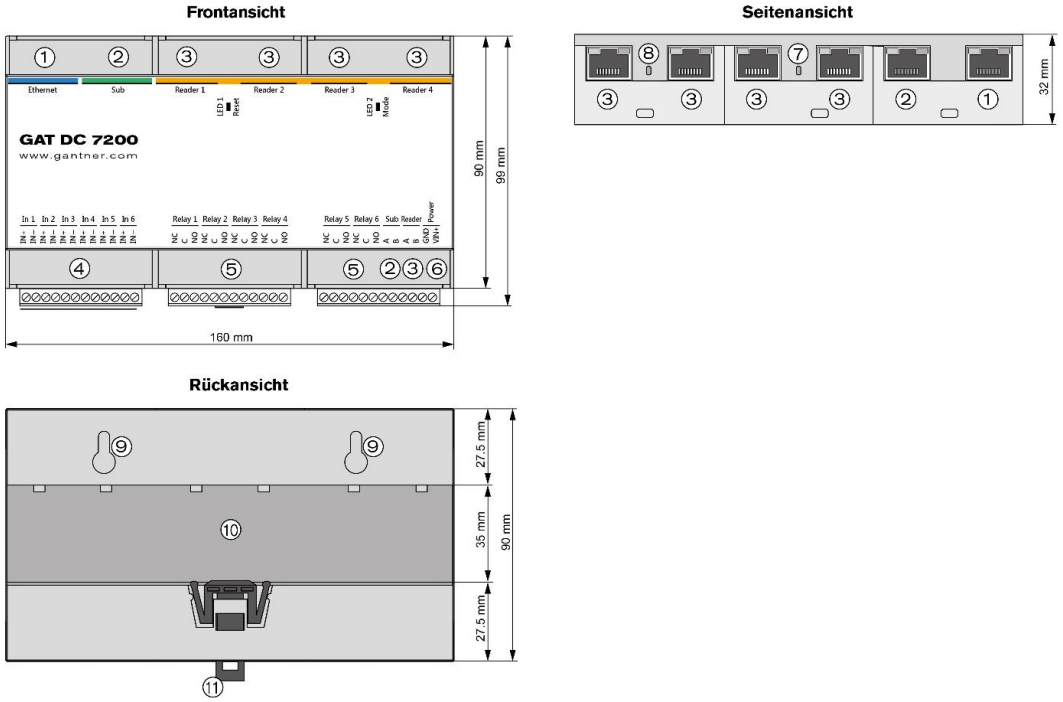
Über die GAT DIRECT.Connect Software mit passendem Adapter kann der GAT DC 7200 auch mit einer Fremdsoftware kommunizieren. Nähere Informationen siehe "9.53. GAT DIRECT.Connect Schnittstelle".

Alle Zutritte und Zutrittsversuche werden vom GAT DC 7200 intern aufgezeichnet und können über das Netzwerk ausgelesen und dargestellt werden.

2.3 Highlights

- Zutrittskontroller für bis zu 4 Türen (mit Lizenz erweiterbar auf 16 Türen)
- Bis zu 16 Multitechnologie-Leser für LEGIC®, MIFARE®, ISO 15693 und HID iClass anschließbar
- Identifikation mit Smartphones oder Smartwatches
- Automatische Lesererkennung
- Plug & Play Installation
- Ethernet-Anschluss über RJ45 Stecker
- 6 Relaisausgänge und digitale Eingänge
- Erweiterung der Relaisausgänge und digitalen Eingänge mittels anschließbarer GAT IO 7xxx Modulen.
- Sub-Schnittstelle für Peripheriegeräte
- Konfiguration mittels übersichtlicher, geschützter Weboberfläche (TLS/SSL Verbindung)
- Einbindung in die Zutrittskontrollsoftware GAT ACE 7000 und Matrix
- Anbindung an Drittsoftware mittels GAT DIRECT.Connect möglich
- Unterstützung der SVN Funktion von SALTO
- Uhr mit automatischer Sommer-/Winterzeitumschaltung, gegen Stromausfall geschützt
- Einfache Hutschienenmontage

2.4 Gerätemerkmale



1 … Netzwerkanschluss (Ethernet)
2 … Sub-Schnittstelle für Peripheriegeräte
3 … Anschluss externer Leser
4 … Optokopplereingänge
5 … Relaisausgänge
6 … Spannungsversorgungseingang
7 … Status-LED 1, Taste RESET
8 … Status-LED 2, Taste MODE
9 … Befestigungslöcher für Wandmontage
10 … Hutschienenhalterung
11 … Hutschienen-Sicherungshebel

***Bild 2.1** – Gerätemerkmale*

Bestellhinweise	Art.Nr.
GAT DC 7200 Türcontroller, 4 externe Leser pro Tür, 6 digitale Eingänge, 6 Relaisausgänge, Ethernet-Schnittstelle, Sub-Schnittstelle	**532220**

Erweiterungen Hinweis: Der Begriff „email“ in der Bezeichnung ermöglicht die Aktivierung der betreffenden Lizenz per E-Mail	Art.Nr.
GAT DC 7200 PLUS license **GAT DC 7200 PLUS license email** Lizenzerweiterung des GAT DC 7200 von 4 auf 16 Türen	**753023** **732222**
GAT DC 7200 elevator license **GAT DC 7200 elevator license email** Lizenzerweiterung für Lift- und Schließfachsteuerungen	**794028** **793936**
GAT DC 7200 APB and online license **GAT DC 7200 APB and online license email** Lizenzerweiterung für die Anti-Pass-Back-Funktion und Online Management (z. B. für GAT DIRECT.Connect)	**1100191** **1100190**
GAT DC 7200 Mobile Credential license **GAT DC 7200 Mobile Credential license email** Erweiterungslizenz für GAT DC 7200 für die Verwendung von “Mobilgeräten als Datenträger"	**1117572** **1117571**

Zubehör	Art.Nr.
GAT SP 070 2.0A Hutschienen-Netzgerät. Ausgang: DC 12 V, I = 2 A	**759534**
GAT SP 070 7.1A Hutschienen-Netzgerät. Ausgang: DC 12 V, I = 7,1 A	**759433**
GAT SP 070 UPS Online 30W Hutschienen-Netzgerät mit integriertem Akku. Ausgang: DC 12 V, I = 2,5 A	**1104715**
GAT SP 070 UPS Online 55W Hutschienen-Netzgerät mit integriertem Akku. Ausgang: DC 12 V, I = 4,6 A	**1104716**
GAT SP 074 1.5A Hutschienen-Netzgerät. Ausgang: DC 24 V, I = 1,5 A	**759231**
GAT SP 074 3.8A Hutschienen-Netzgerät. Ausgang: DC 24 V, I = 3,8 A	**759332**
GAT SP 074 10A Hutschienen-Netzgerät. Ausgang: DC 24 V, I = 10 A	**1102259**
GAT SP 074 20A Hutschienen-Netzgerät. Ausgang: DC 24 V, I = 20 A	**1102258**
GAT SP 074 UPS Online 30W Hutschienen-Netzgerät mit integriertem Akku. Ausgang: DC 24 V, I = 1,25 A	**1104717**
GAT SP 074 UPS Online 55W Hutschienen-Netzgerät mit integriertem Akku. Ausgang: DC 24 V, I = 2,3 A	**1104718**
GAT SP 07x Fuse Block Sicherungen für GAT SP 07x für Hutschienenmontage	**803726**
Installation Box 9118 Kleinverteiler mit 1 Hutschiene, IP 65, B:40 x H:33 x T:13 cm	**803625**

Installation Box 9236 Kleinverteiler mit 2 Hutschienen, IP 65, B:40 x H:48 x T:13 cm	**803524**
Installation Box 9354 Kleinverteiler mit 2 Hutschienen, IP 65, B:40 x H:63 x T:13 cm	**1105526**
GAT IO 7054 IO Erweiterungseinheit mit 4 Aus- und 12 Eingängen, RS-485 Schnittstelle	**1105454**
GAT IO 7054 NW IO Erweiterungseinheit mit 4 Aus- und 12 Eingängen, RS-485 Schnittstelle, Funkschnittstelle	**1105455**
GAT IO 7055 IO Erweiterungseinheit mit 8 Aus- und 16 Eingängen, RS-485 Schnittstelle	**1105456**
GAT IO 7055 NW IO Erweiterungseinheit mit 8 Aus- und 16 Eingängen, RS-485 Schnittstelle, Funkschnittstelle	**1105457**

2.5 Begriffsdefinition

Einige Begriffe werden in diesem Handbuch öfters verwenden und sind wie folgt definiert.

Benutzer / Anwender
Die Begriffe "Benutzer" und "Anwender" bezeichnen in diesem Handbuch die Personen, die an einer Tür mit GAT DC 7200 Zutritt erlangen möchten und sich dazu am Leser mit ihrem Datenträger oder ihrem Finger identifizieren.

Anlage
Bezeichnet das Gebäude, in dem Zutritte zu bestimmten Bereichen mit den GAT DC 7200 kontrolliert werden.

Computer / PC
Diese Begriffe bezeichnen alle Desktop- und Laptop-Computer, die als Betriebssystem Microsoft® Windows® verwenden, um z. B. den GAT DC 7200 zu konfigurieren.

Controller / Türcontroller
Allgemeiner Begriff für die Zutrittskontrollgeräte zur Türsteuerung.

Schloss
Diese Bezeichnung allgemein das elektronische Türschloss, das von einem GAT DC 7200 angesteuert wird.

Tür
Mit diesem Begriff ist in diesem Handbuch die vom GAT DC 7200 angesteuerte Schließvorrichtung gemeint. Dabei handelt es sich üblicherweise um eine Tür, die den Zutritt zu einem Raum oder Bereich darstellt. Es können aber auch Tore, Drehkreuze oder ähnliche Vorrichtungen gesteuert und überwacht werden. Ein GAT DC 7200 kann bis zu 4 Türen (mit Zusatzlizenz bis zu 16 Türen) überwachen.

Leser
Leser sind die an einem GAT DC 7200 über serielle RS-485 Schnittstelle angeschlossene Geräte, welche die Datenträger der Benutzer lesen und die Informationen an den Controller übertragen. Es können verschiedene Arten von Lesern verwendet werden.

Datenträger
Ein Ausweismedium (z. B. in Form eines Schlüsselanhängers oder einer Chipkarte) mit elektronischem Speicher und ID-Nummer, mit dem sich die Benutzer einer Anlage an den Lesern, die an den Türcontrollern angeschlossen sind, identifizieren können. Die Datenträger sind für unterschiedliche Identifikationssysteme (LEGIC, MIFARE™, ISO 15693) verfügbar.

RFID (Radio-Frequency Identification = Identifizierung mit Hilfe elektromagnetischer Felder)
Bezeichnet in diesem Handbuch die Identifizierung einer Person über Funk im Nahbereich. Als Ausweismedium dient ein RFID Datenträger, z. B. die Form eines Schlüsselanhängers oder einer Chipkarte.

FID (Firmen-ID) und Site Key
LEGIC Systeme verwenden die FID Nummer, in MIFARE® Systemen wird der Site Key verwendet, welcher eine Kombination von FID und den Lese- und Schreibschlüsseln ist. Die FIDs und die Site Keys sind Unikate für jede Anlage. Diese Nummern sind in allen Datenträgern und allen Geräten codiert und dadurch wird sichergestellt, dass ein Datenträger nicht in verschiedenen Anlagen verwendet wird.

Webschnittstelle
Zur Konfiguration des GAT DC 7200 kann mittels eines Webbrowsers über die IP-Adresse oder den Gerätenamen direkt auf den GAT DC 7200 zugegriffen werden. Die Konfigurationsoberfläche wird nach gültiger Anmeldung direkt im Browser dargestellt. Mit dem Begriff Webschnittstelle wird in diesem Handbuch diese Konfigurationsverbindung und -darstellung bezeichnet.

TLS / SSL
Verschlüsselungsprotokoll für die sichere Datenübertragung z. B. bei der Konfiguration des GAT DC 7200 über die Webschnittstelle. In diesem Handbuch wird die neue Bezeichnung TLS (Transport Layer Security) verwendet. Die ältere Bezeichnung dieser Technologie ist SSL (Secure Sockets Layer), was gleichbedeutend mit TLS ist.

GAT DIRECT.Connect
Software für die Einbindung von Geräten wie GAT DC 7200 in diverse Softwarepakete mit passendem Software Adapter.

Mobile Credential
Identifikation von Benutzern mittels ihren Mobilgeräten (z. B .Smartphone oder Smartwatch). Im Mobilgerät wird ein Berechtigungsausweis gespeichert (z. B. in der Google Wallet oder Apple Wallet). Es sind bestimmte Voraussetzungen für diese Anwendung zu erfüllen (siehe "2.7. Mobile Credential").

2.6 RFID Technologie und Datenträger

Um sich berührungslos mittels Funkdatenträger an einem GAT DC 7200 identifizieren zu können sind bei GANTNER Electronic GmbH verschiedene RFID Leser (= Radio-Frequency Identification) und Technologien erhältlich.
Da der GAT DC 7200 keinen integrierten Leser besitzt und die Kommunikation mit den angeschlossenen externen Lesern über RS-485 im entsprechenden Protokoll erfolgt, spielt es für den GAT DC 7200 keine Rolle, welche RFID-Technologie verwendet wird.
Die Informationen in diesem Handbuch gelten damit allgemein für RFID-Technologien, welche von dem GAT DC 7200 mit angeschlossenen RFID Lesern unterstützt werden. Dies sind im Wesentlichen folgende Technologien:

- LEGIC prime
- LEGIC advant
- MIFARE DESFire EV1®, EV2® und EV3®
- ISO 14443A
- ISO 14443B
- ISO 15693
- Sony Felica
- Inside Contactless (HID iClass)

Zusätzlich zu den angeführten RFID-Technologien können mit dem GAT SR 7000 Wiegand Interface zahlreiche andere Technologien (z. B. 125 kHz, UHF Longrange etc.) verwendet werden.

2.7 Mobile Credential

Der GAT DC 7200 bietet ab Version 3.7 die Möglichkeit, mittels passender Lizenz und Konfiguration auch die auf Mobilgeräten wie Smartphones und Smartwatches gespeicherten Mobile Credentials (Ausweis in Google oder Apple Wallet) für die Identifikation der Benutzer zu verwenden. Dazu sind bestimmte Voraussetzungen notwendig.

Voraussetzungen für die Verwendung von Mobile Credential:
- GAT DC 7200 Firmware: V3.7 oder neuer
- Leser Firmware: V03.06 oder neuer
- LEGIC Chip OS in den Lesern: V5.3.1 oder neuer
- Unterstütze Leser: GR7.13xx, GR7.23xx, GR7.73xx, GAT SR 73xx, GAT SLR 73xx
- GAT DC 7200 Mobile Credential Lizenz muss installiert sein
- Im Leser muss eine gültige Konfiguration (VCP) geladen sein.
- Der passende ECP-Frame muss im GAT DC 7200 eingetragen werden
- Die Einstellungen für die Google Wallet oder Apple Wallet muss in den Datenträgereinstellungen konfiguriert werden
- Das Mobilgerät muss Mobile Credentials und NFC unterstützen.
- Der Betrieb der Anlage muss in Ländern erfolgen, für die die Funktion von Apple und Google auch unterstützt wird. Die aktuellen Informationen für Apple Wallet sind im Apple Support zu finden. Für Google Wallet sind diese Informationen im Google Support verfügbar.

Link zu Apple Wallet Information:

https://support.apple.com/en-mk/102775

Link zu Google Wallet Information:

https://support.google.com/wallet/answer/12060037?hl=en#zippy=%2Cuse-google-wallet-for-payments-and-storing-passes

Im Kapitel "6.5. Mobile Credential konfigurieren" finden Sie die genaue Anleitung für die Aktivierung und Konfiguration von Mobile Credential.

3 MONTAGE

Dieses Kapitel beschreibt die mechanische Befestigung des GAT DC 7200, die möglichen Einsatzorte und was bei der Montage beachtet werden muss.

HINWEIS

Beschädigung oder Fehlfunktion des GAT DC 7200

- *Lesen Sie die Informationen in diesem Kapitel genau, bevor Sie den GAT DC 7200 montieren.*
- *Den GAT DC 7200 nur an einem trockenen Ort, geschützt vor Regen oder Tropfwasser, installieren.*
- *Maßzeichnungen genau beachten.*
- *Richtiges Werkzeug für die Montage des GAT DC 7200 verwenden.*

3.1 Zielgruppe

Dieses Kapitel enthält Informationen für die Techniker, die den Türcontroller GAT DC 7200 montieren. Eine Erfahrung in mechanischer Arbeit und elektrotechnisches Grundwissen wird vorausgesetzt. Vorkenntnisse zum GAT DC 7200 oder dem Zutrittssystem von GANTNER sind nicht erforderlich.

3.2 Systemübersicht

Der GAT DC 7200 kann ein oder mehrere Türen kontrollieren und es können ein oder mehrere Lesern angeschlossen werden. Außerdem muss der GAT DC 7200 an einem Ethernet-Netzwerk angeschlossen sein und benötigt eine Spannungsversorgung. Weitere Anschlüsse wie elektronische Türöffner oder Türrückmeldungen sind ebenfalls anschließbar. Diese Anschlüsse und die daraus ergebenden Verkabelungen müssen bei der Wahl des Montageortes berücksichtig werden.

Das folgende Bild zeigt eine beispielhafte Installation.

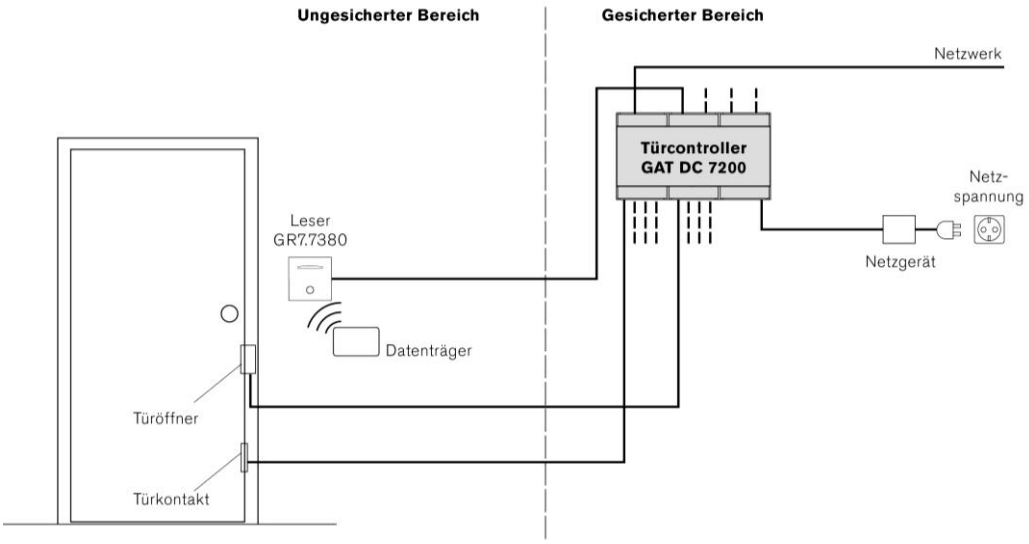


***Bild 3.1** - Systemübersicht*

3.3 Montage

Der GAT DC 7200 ist für die Hutschienen-Montage in einem 19" Rack (z. B. in Serverschränken) vorgesehen. Der GAT DC 7200 kann wie im folgenden Bild zu sehen, auf eine Hutschiene aufgesteckt werden.

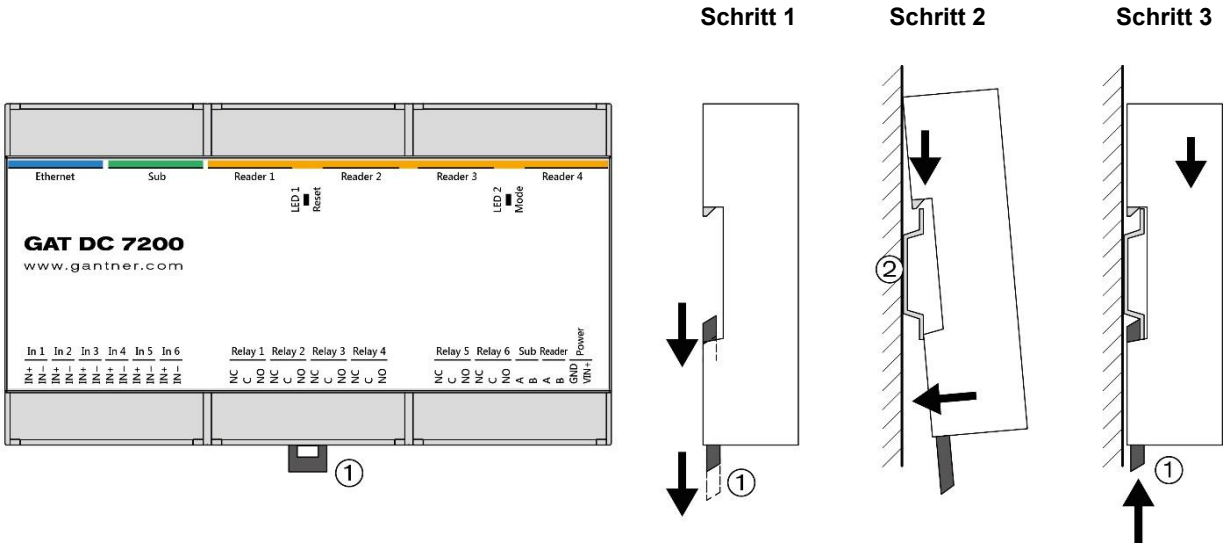


***Bild 3.2** – Hutschienenmontage*

- ► Ziehen Sie den Hutschienen-Sicherungshebel (1) nach unten und halten Sie ihn in dieser Position.
- ► Stecken Sie den GAT DC 7200 von oben auf die Hutschiene (2), und klappen Sie das Gerät auf der unteren Seite nach hinten.
- ► Drücken Sie den Hutschienen-Sicherungshebel (1) wieder nach oben.
  - o Die Lasche des Sicherungshebels rastet in der Hutschiene ein.
- ► Stellen Sie sicher, dass der GAT DC 7200 festen Halt hat.

Alternativ ist auch die Montage mit zwei Schrauben an einer Wand möglich.

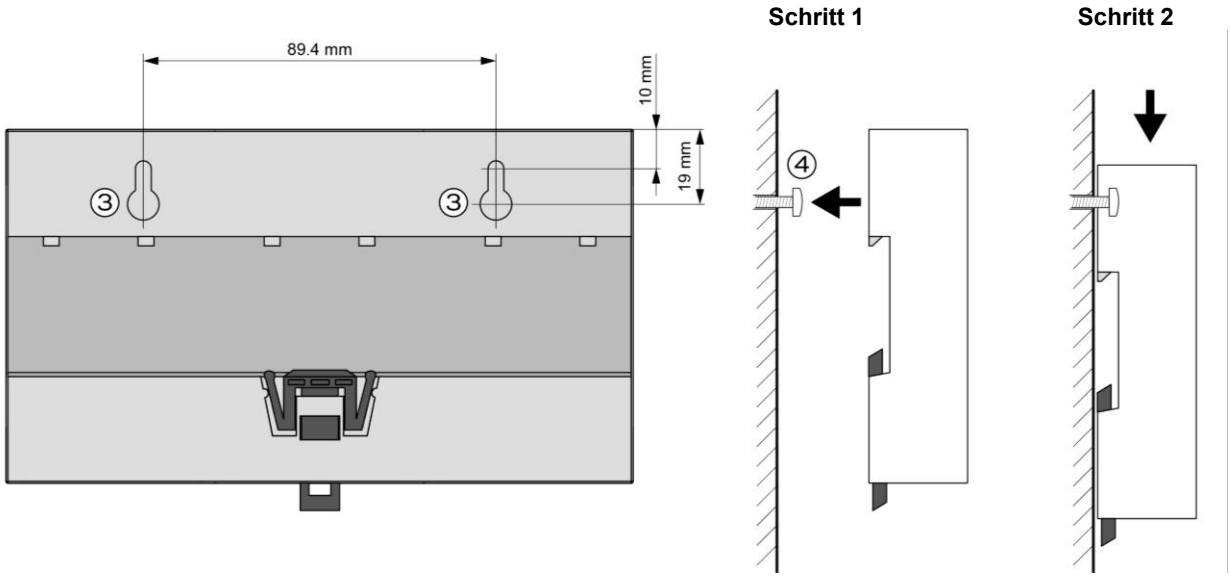


***Bild 3.3** – Wandmontage mit 2 Schrauben*

- ► Zeichnen Sie die 2 Montagelöcher (3) an der Wand an (horizontale Ausrichtung, 89,4 mm Abstand).
- ► Bohren Sie die 2 Befestigungslöcher.

  HINWEIS! Verwenden sie je nach Wandmaterial die entsprechenden Bohrer sowie Schrauben und Dübel (falls notwendig), so dass der GAT DC 7200 sicheren Halt hat. Der GAT DC 7200 wiegt ca. 210 g.
- ► Befestigen Sie die Schrauben in der Wand, so dass diese ca. 5 mm von der Wand vorstehen.
- ► Stecken Sie den GAT DC 7200 auf die Schrauben und drücken Sie in dann nach unten, so dass die Schrauben in den Montagelöcher einrasten.
- ► Stellen Sie sicher, dass GAT DC 7200 festsitzt.

4 ELEKTRISCHER ANSCHLUSS

Dieses Kapitel beschreibt den Anschluss der Leitungen zu Netzwerk, Spannungsversorgung, Lesern und Peripheriegeräten.

⚠ VORSICHT

Elektrischer Schlag

➔ *Berührung von spannungsführenden Leitungen kann zu Verletzungen durch elektrischen Schlag führen.*

- Elektrische Anschlüsse dürfen nur durch die angegebene Zielgruppe erfolgen.
- Beachten Sie die Angaben in diesem Kapitel genau.

HINWEIS

Beschädigung oder Fehlfunktion des GAT DC 7200

- Lesen Sie die Informationen in diesem Kapitel genau, bevor Sie den GAT DC 7200 anschließen.
- Kabelanschluss in der beschriebenen Reihenfolge und an den beschriebenen Klemmen durchführen.

4.1 Zielgruppe

Dieses Kapitel enthält Informationen für das Fachpersonal, das die elektrischen Anschlüsse am GAT DC 7200 herstellt. Beachten Sie die gesetzlichen Vorgaben für Elektroinstallationen für den Einsatzort des GAT DC 7200 (z.B. Elektrischer Anschluss nur durch entsprechend ausgebildete Elektriker, Vorgaben zu verwendeten Materialien und Werkzeugen). Beachten Sie die räumlichen und klimatischen Einsatzbedingungen des GAT DC 7200.

4.2 Netzwerkanschluss

Für die Kommunikation mit dem übergeordneten Zutrittskontrollsystem und zur Konfiguration ist eine Ethernet-Verbindung notwendig. Das GAT DC 7200 verfügt dazu über eine 10/100 Mbit Schnittstelle mit RJ45 Buchse.

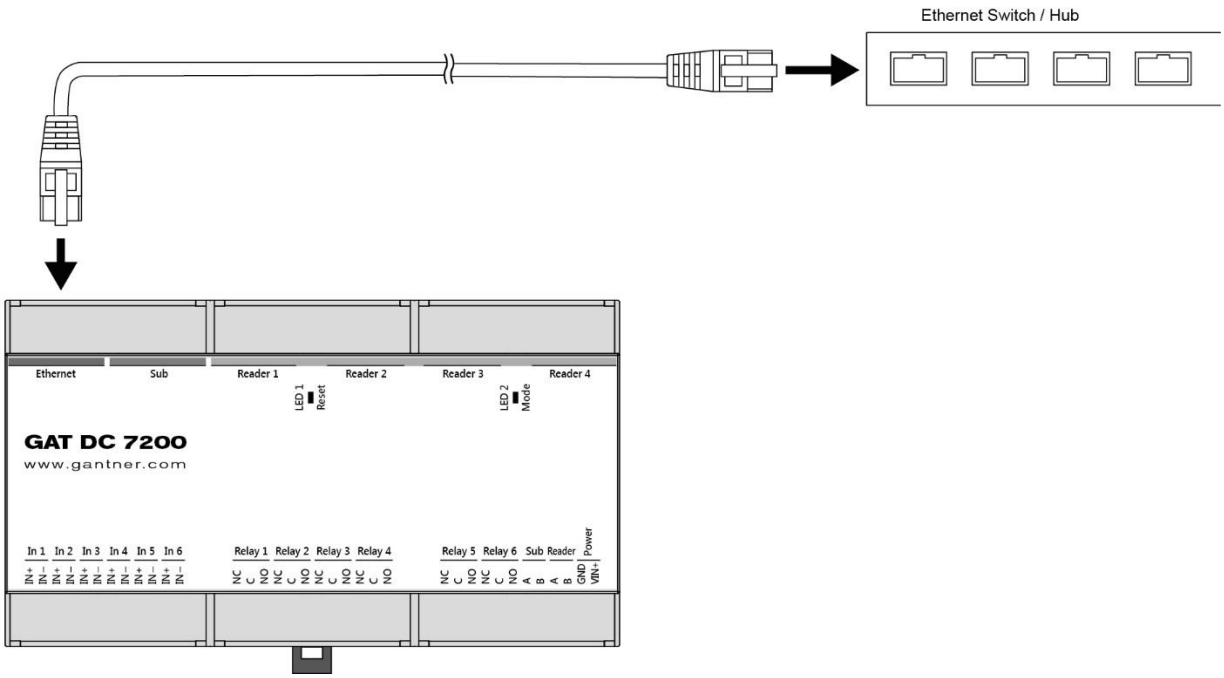


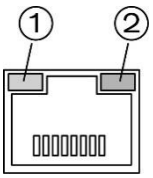
***Bild 4.1** – Netzwerkanschluss GAT DC 7200*

Beachten Sie für den Netzwerkanschluss folgende wichtigen Punkte.

- Kabel Typ: Min. CAT 5 (STP)
- Kabellänge: max. 100 m (according to Ethernet standard)
- Kabelverbinder: RJ45
- Anschluss an Netzwerk-Hub oder -Switch

4.2.1 Statusanzeige

An der RJ45 Buchse der Ethernet Schnittstelle befinden sich 2 LEDs, die folgenden Informationen anzeigen.



LED	Status	Bedeutung
orange (1)	ein	100 MBit
	aus	10 MBit
grün (2)	blinkt	Verbindung (Link) und Kommunikation aktiv
	aus	keine Verbindung und keine Kommunikation

***Tabelle 4.1** – LED-Anzeigen Ethernet*

4.3 Leseranschluss

Folgende GANTNER RFID-Leser und -Geräte der neuesten Generation können an den GAT DC 7200 angeschlossen werden:

- GR7.1300
- GR7.1310
- GR7.2300
- GR7.2310
- GR7b.2300
- GR7b.2310
- GR7.7380
- GAT DL 091 und WiNET Komponenten

Auch die bisherige Generation der RFID-Lesegeräte von GANTNER kann an den GAT DC 7200 angeschlossen werden:

- GAT SR 73xx
- GAT SLR 73xx
- GAT SR 3xx
- GAT SLR 3xx

HINWEIS! Die GAT S(L)R 3xx Leser unterstützen die CardNET-Funktion nicht (siehe Kapitel “9.17 CardNET”).

In diesem Handbuch sind nur die Anschlüsse für die neueste Gerätegeneration enthalten. Hinweise zum Anschluss der GAT S(L)R 73xx-Leser an den GAT DC 7200 entnehmen Sie bitte der jeweiligen Dokumentation.

Die Kommunikation mit den Lesern erfolgt über die serielle RS-485 Schnittstelle.

Die Leser werden an den mit "Reader" gekennzeichneten Steckplätzen angeschlossen. Je nach Kabel zum Leser ist der Anschluss an den 4 mit "Reader 1" … "Reader 4" gekennzeichneten RJ45 Steckern oder an der "Reader" Schraubklemme möglich.

HINWEIS! Der GAT DL 091 kann auch an der "Sub" Schnittstelle angeschlossen werden. Dies ist der empfohlene Anschluss für den GAT DL 091. Lesen Sie dazu den Abschnitt "4.4. Access Point GAT DL 091".

Der Anschluss an den RJ45 Steckern hat den Vorteil der Plug&Play PLUS Funktion. Dabei erkennt der Controller automatisch die angeschlossenen Leser und ordnet dem Leser an Anschluss "Reader 1" die Tür 1 zu, dem Leser an "Reader 2" die Tür 2, usw. Mit dieser Funktion kann ein Leser ausgetauscht werden, ohne dass die Konfiguration geändert werden muss.

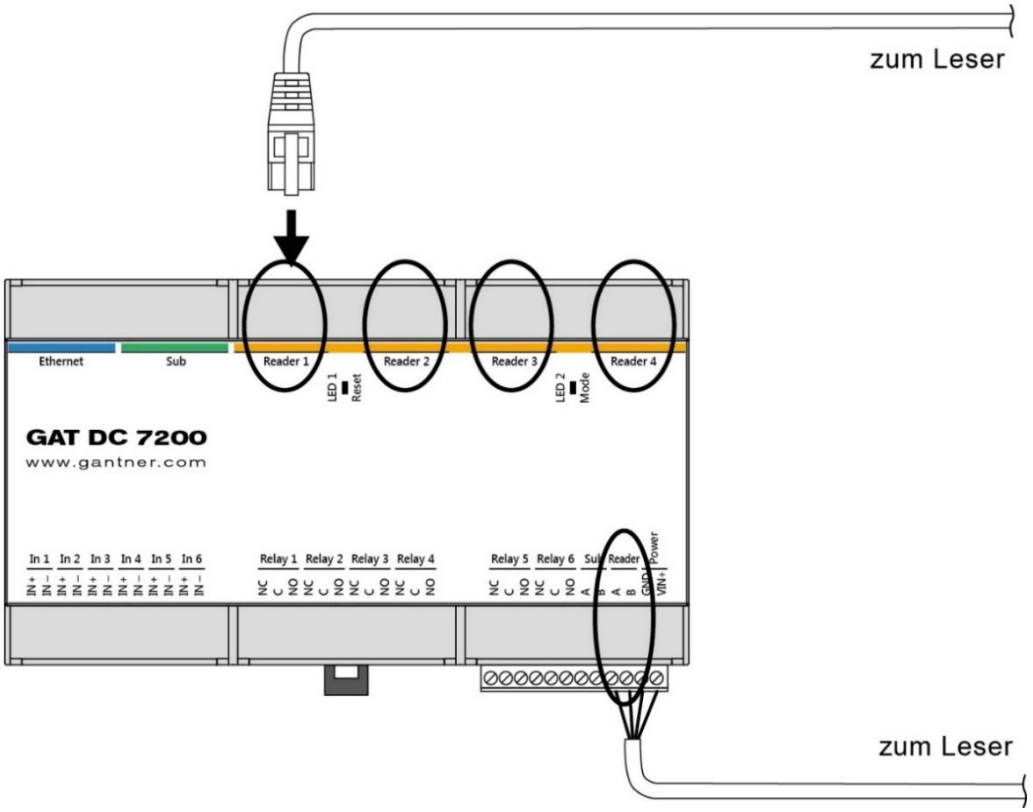


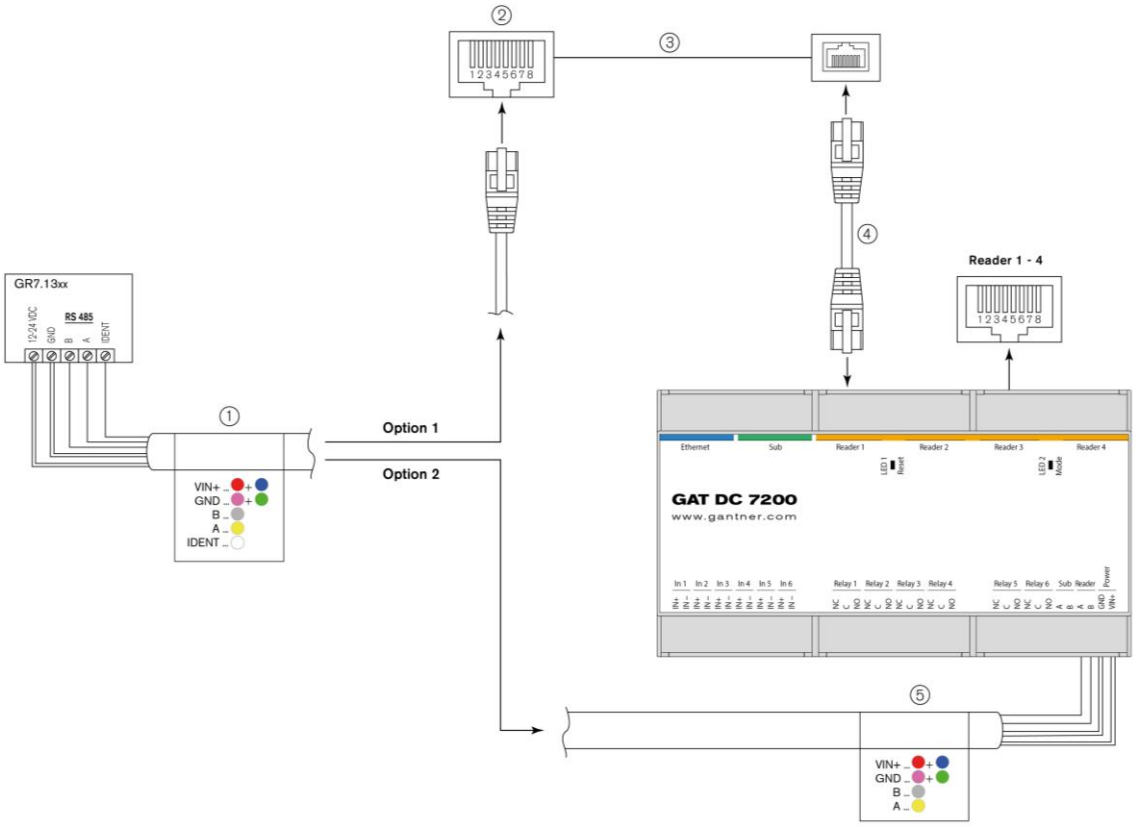
***Bild 4.2** – Leseranschluss*

Insgesamt können standardmäßig 4 Leser, mit Zusatzlizenz bis max. 16 Leser, an einem GAT DC 7200 angeschlossen werden. Verwenden Sie z. B. einen Y-Adapter um mehrere Leser an einem Steckplatz anzuschließen. Die Spannungsversorgung der Leser wird von GAT DC 7200 bereitgestellt oder kann wahlweise auch durch ein eigenes Netzgerät erfolgen. Bei den RJ45 Buchsen wird die Spannung an der Buchse ausgegeben. Die Spannung ist an jeder Buchse einzeln schaltbar und die Steckplätze sind gegen Überlast und Kurzschluss einzeln abgesichert. Beachten Sie, dass der Strom pro RJ45 Buchse 1 A nicht übersteigen darf. Außerdem darf die gesamte Leistung, die an allen RJ45 Buchsen des GAT DC 7200 zusammen entnommen wird, 40 VA nicht übersteigen.

Bei Anschluss an der "Reader" Klemme können Sie die Spannung von der Versorgung des GAT DC 7200 abnehmen oder den Leser mit einem eigenen Netzgerät versorgen. Die folgenden Kapitel zeigen den Anschluss an den RJ45 Buchsen und den Schraubklemmen bei Verwendung der GR7 Leser.

Beachten Sie, dass beim Anschluss eines Lesers an den Schraubklemmen die IDENT-Leitung des Lesers nicht verwendet werden kann und die Plug&Play Funktion somit nicht zur Verfügung steht.

4.3.1 Beispiel: Anschluss eines GR7.13xx am GAT DC 7200



1…Mitgeliefertes, angeschlossenes Kabel (Art.Nr.: 1104997). PIN-Belegung und Adernfarben:

PIN	Adernfarbe	Signal
1	weiß	IDENT
2	-	-
3	grün	GND
4	gelb	A
5	grau	B
6	rosa	GND
7	blau	+VIN (DC 12-24 V)
8	rot	+VIN (DC 12-24 V)

HINWEIS

- Den braunen Draht abschneiden.
- Optional ist das GR7.1xxx Cable Set 3 m (Art.Nr.: 1106193) erhältlich.

Anschlussoption 1

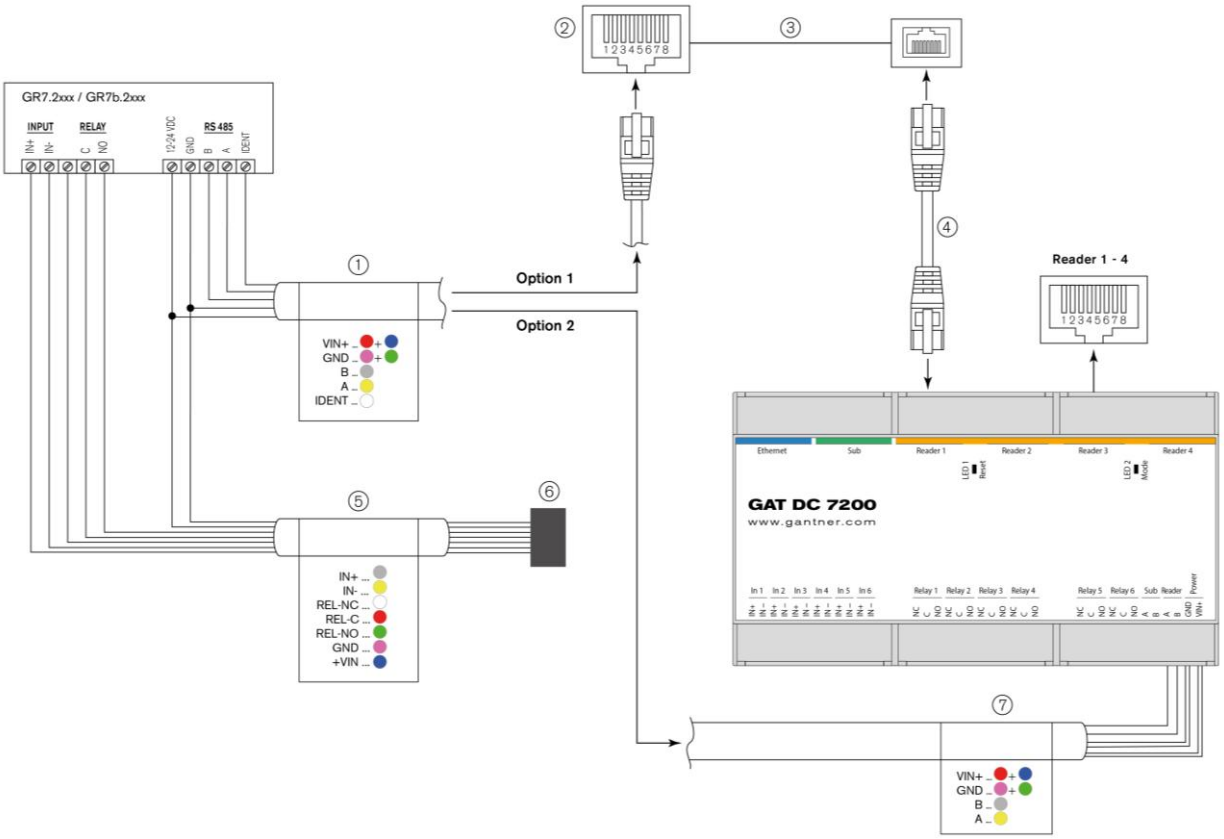
2…RJ45-Stecker
3…strukturierte Gebäudeverkabelung
4…Patchkabel

Anschlussoption 2

5… Anschluss über Klemmen. Für diese Option wird das IDENT-Kabel nicht verwendet.

***Bild 4.3** – Anschluss eines GR7.13xx an einen GAT DC 7200*

4.3.2 Beispiel: Anschluss eines GR7.23xx / GR7b.23xx am GAT DC 7200



1… Mitgeliefertes, angeschlossenes Kabel (Art.Nr.: 1104994). PIN-Belegung und Adernfarben:

PIN	Adernfarbe	Signal
1	weiß	IDENT
2	-	-
3	grün	GND
4	gelb	A
5	grau	B
6	rosa	GND
7	blau	+VIN (DC 12-24 V)
8	rot	+VIN (DC 12-24 V)

HINWEIS

- Den braunen Draht abschneiden.
- Optional ist das GR7.2xxx Cable Set 3 m (Art.Nr.: 1106194) erhältlich.

Anschlussoption 1

2…RJ45-Stecker
3…strukturierte Gebäudeverkabelung
4…Patchkabel
5… Mitgeliefertes, angeschlossenes Kabel (Art.Nr.: 1104995). PIN-Belegung und Adernfarben:

PIN	Adernfarbe	Signal
1	grau	IN +
2	gelb	IN -
3	weiß	REL NC
4	rot	REL C
5	grün	REL NO
6	rosa	GND
7	blau	+VIN (DC 12-24 V)
8	-	-

HINWEIS
Den braunen Draht abschneiden.

6… Stecker. **HINWEIS!** Ein zweiter Stecker (Typ F) und eine Verbindung zwischen den beiden Steckern sind im Montagematerial beigelegt, um eine einfache Verkabelung zu ermöglichen.

Anschlussoption 2

7… Anschluss über Klemmen. Für diese Option wird das IDENT-Kabel nicht verwendet.

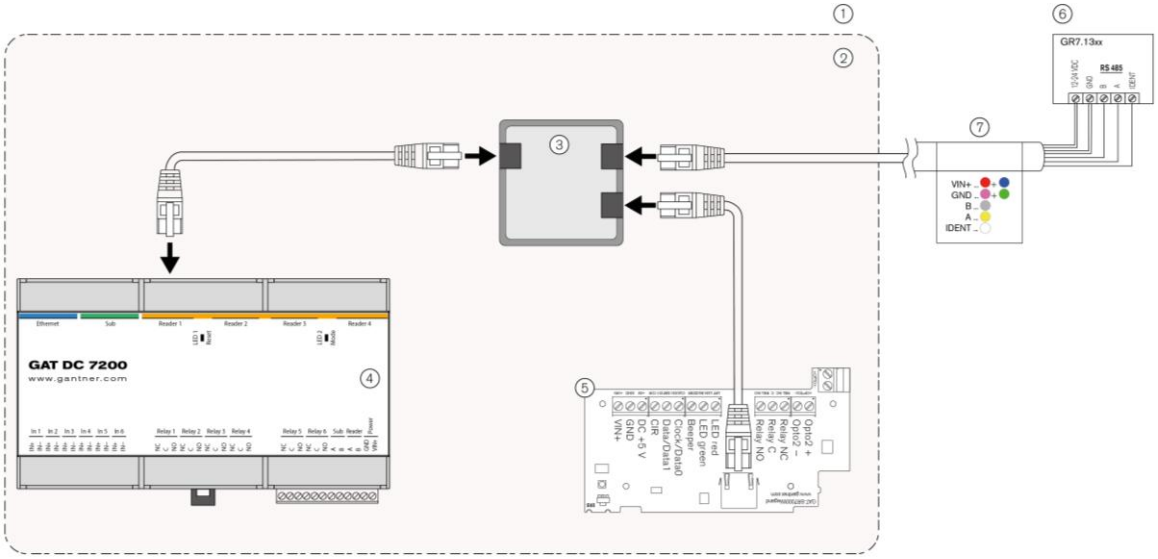
***Bild 4.4** – Anschluss eines GR7.23xx / GR7b.23xx an einen GAT DC 7200*

HINWEIS! Die GAT SR 73xx und SLR 73xx Leser dürfen nur, wie beschrieben, an den mit "Reader 1" bis "Reader 4" gekennzeichneten RJ45 Buchsen oder der "Reader" Klemme erfolgen. Verwenden Sie niemals die mit "SUB" oder "Ethernet" gekennzeichneten Anschlüsse.

4.3.3 Beispiel: Anschluss eines GR7.13xx und GAT SR 7000 Wiegand an Tür

Für den Fall, dass zwei RS-485 Leitungen an einem GAT DC 7200 angeschlossen werden soll (z. B. wenn ein bestehendes System auf den GAT DC 7200 erweitert wird) und kein zusätzliches Kabel verlegt werden soll, kann ein RJ45 Splitter verwendet werden.

In diesem Beispiel werden der RFID Leser (GR7.13xx) und das I/O Modul (GAT SR 7000 Wiegand), das im gesicherten Innenbereich montiert ist, an den RJ45 Splitter angeschlossen. Damit kann die Türsteuerung und -überwachung im gesicherten Innenbereich erfolgen und es wird nur der RFID Leser im ungesicherten Außenbereich montiert.



1.....gesicherter Bereich
2.....ungesicherter Bereich
3.....RJ45 Splitter
4.....GAT DC 7200
5.....GAT SR 7000 Wiegand
6.....GR7.13xx
7.....Mitgeliefertes, angeschlossenes Kabel (Art.Nr.: 1104997). PIN-Belegung und Adernfarben:

PIN	Adernfarbe	Signal
1	weiß	IDENT
2	-	-
3	grün	GND
4	gelb	A
5	grau	B
6	rosa	GND
7	blau	+VIN (DC 12-24 V)
8	rot	+VIN (DC 12-24 V)

HINWEIS!
- Den braunen Draht abschneiden.
- Optional ist das GR7.1xxx Cable Set 3 m (Art.Nr.: 1106193) erhältlich.

***Bild 4.5** – RJ45 Splitter für den Anschluss eines RFID-Leser und I/O Moduls*

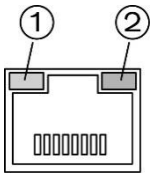
HINWEIS! Für diese Installationsart müssen folgende Anforderungen erfüllt werden.

- In der Web-Oberfläche des GAT DC 7200 muss die Funktion "Leser automatisch der Türe zuweisen" für die globale Konfiguration der Leser deaktiviert sein (zu finden unter "Konfiguration" -> "Leser" -> "Leser automatisch der Türe zuweisen….").
- In GAT Matrix werden für den GAT DC 7200 2 Türlizenzen benötigt (eine für den GR7.x3xx und eine für den GAT SR 7000 Wiegand). Außerdem werden in GAT DC 7200 2 Türen benötigt, eine pro Komponente.

Wenn keine strukturierte Verkabelung verwendet werden kann, kann die RS-485 Leitung auch an den Schraubklemmen "Reader A" und "Reader B" des GAT DC 7200 angeschlossen werden. Ein RJ45 Stecker muss am Kabelende, das mit dem GAT SR 7000 Wiegand verbunden wird, abgeschlossen werden. Die PIN-Belegung für den RJ45 Stecker ist im Abschnitt "4.3.1. Beispiel: Anschluss eines GR7.13xx am GAT DC 7200" beschrieben.

4.3.4 Statusanzeige

An der RJ45 Buchse der Leserschnittstelle befinden sich 2 LEDs, die folgenden Informationen anzeigen.



LED	Status	Bedeutung
orange (1)	ein	Versorgung für angeschlossenen Leser OK
	aus	Versorgung deaktiviert oder Störung
grün (2)	blinkt	Kommunikation zum angeschlossenen Leser OK (nur bei angeschlossener IDENT-Leitung und Geräten die Plug&Play PLUS unterstützen)
	aus	Keine Kommunikation (oder IDENT-Leitung nicht angeschlossen oder Plug&Play PLUS wird vom angeschlossenen Gerät nicht unterstützt)

***Tabelle 4.2** – LED-Anzeigen Leserschnittstelle*

4.3.5 Automatische Lesererkennung (IDENT)

Die Leser der GR7 Serie besitzen eine IDENT-Leitung zur Plug&Play PLUS Inbetriebnahme, die bei Anschluss der Leser an den RJ45 Steckern des GAT DC 7200 zur automatischen Leserzuordnung verwendet wird. Die angeschlossenen Leser werden dabei automatisch erkannt und den Türen mit derselben Nummer wie der Leseranschluss zugewiesen (Reader 1 an Tür 1, Reader 2 an Tür 2, usw.).

Alternativ kann für die GR7 Leser oder bei Verwendung von mehr als 4 Lesern in der Konfiguration des GAT DC 7200 eine automatische Lesersuche durchgeführt und die Leser manuell den Türe 1 bis 16 zugeordnet werden. Die gefundenen Leser werden mit richtigem Typ in der Konfiguration eingefügt. Die genaue Beschreibung der Leserkonfiguration an einem GAT DC 7200 ist im Handbuch der Konfigurationssoftware GAT ACE beschrieben.

HINWEIS! Leser der Baureihen GAT SR 3xx und GAT SLR 3xx unterstützen die Plug&Play PLUS Funktion nicht und müssen somit manuell konfiguriert werden.

4.3.6 Manipulationsalarm

Der GAT DC 7200 erkennt automatisch, wenn ein Leser im Betrieb getrennt wird und löst in diesem Fall einen auf die betreffende Tür (Leser) bezogenen Manipulationsalarm aus. Mögliche Ursachen können das Durchtrennen des Kabels oder eine Kommunikationsunterbrechung sein. Der Manipulationsalarm wird intern als Buchung gespeichert und, falls ein Relais des GAT DC 7200 für den Manipulationsalarm konfiguriert ist, wird das Relais aktiviert.

4.3.7 Relaisausgänge und Optokopplereingänge

Einige Leser (z. B. GR7.23xx) besitzen einen Relaisausgang und einen potentialfreien Optokopplereingang. Die Funktion und das Zeitverhalten dieser Ein- und Ausgänge kann bei Anschluss am GAT DC 7200 frei konfiguriert werden.

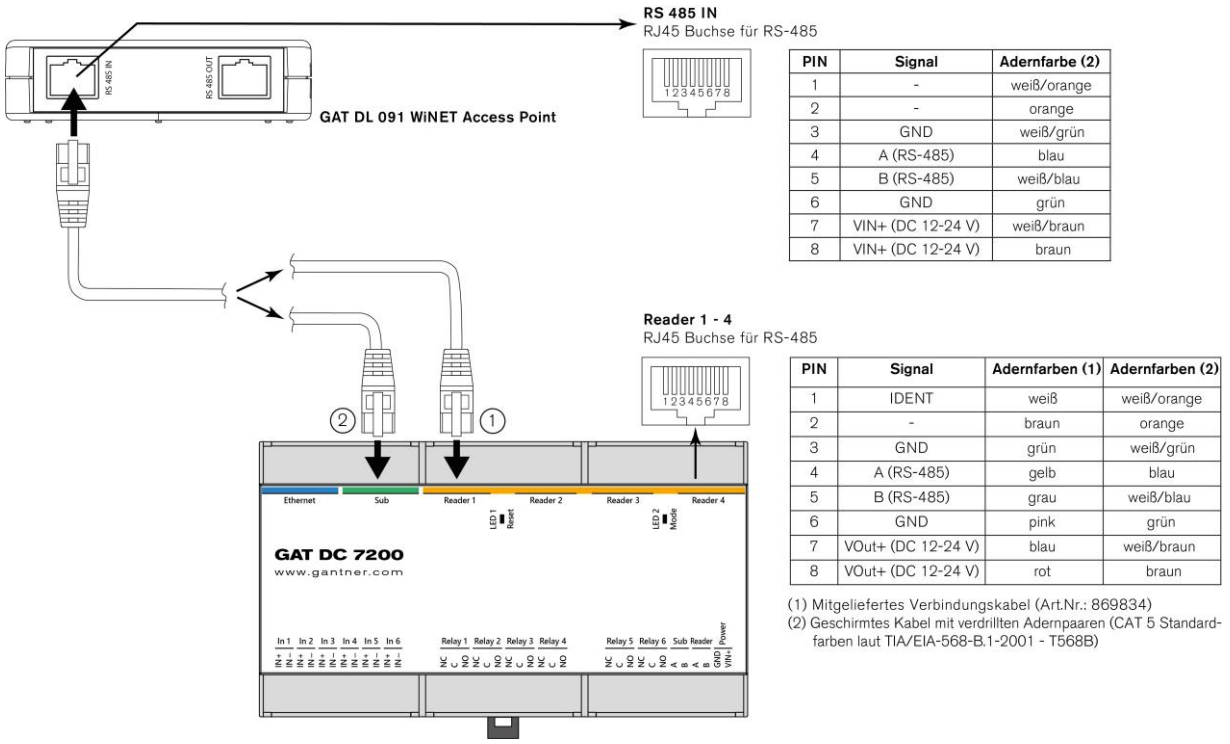
HINWEIS! Ungeschützte Ein-/Ausgänge. Beachten Sie, dass der Relaisausgang und der Optokopplereingang dieser Leser bei unbefugtem Öffnen des Gehäuses ungeschützt sind. Schließen Sie deshalb an diesen Klemmen keine sicherheitskritischen Elemente an. Sie können mit dem Relaisausgang z. B. ein Schließgitter oder eine Beleuchtung steuern, die bei Identifikation oder zeitgesteuert an-/ausgeschaltet werden.

Eine genaue Beschreibung aller möglichen Funktionen finden Sie im Bedienungshandbuch der Konfigurationssoftware GAT ACE von GANTNER Electronic GmbH. Beachten Sie auch die Hinweise im Datenblatt des GR7.x3xx

4.4 Access Point GAT DL 091

Beim empfohlenen Anschluss des GAT DL 091 WiNET Access Point am GAT DC 7200 werden die RJ45 Anschlüsse "Sub" **oder** "Reader x" verwendet. Das ermöglicht eine optimale Kabellänge und Kommunikation.

Es können bis zu 4 GAT DL 091 WiNET Access Point an einem GAT DC 7200 angeschlossen werden.



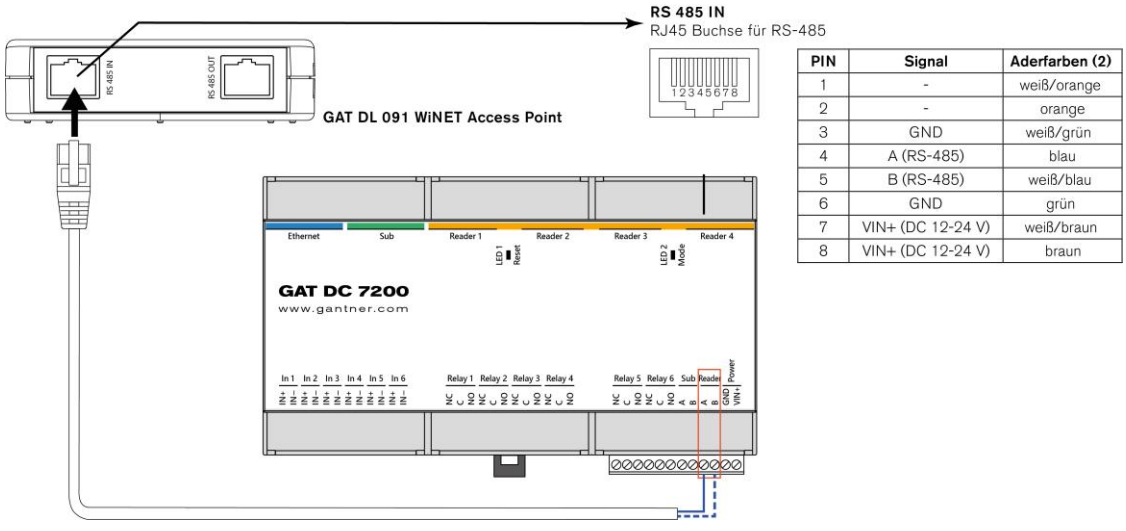
PIN	Signal	Adernfarbe (2)
1	-	weiß/orange
2	-	orange
3	GND	weiß/grün
4	A (RS-485)	blau
5	B (RS-485)	weiß/blau
6	GND	grün
7	VIN+ (DC 12-24 V)	weiß/braun
8	VIN+ (DC 12-24 V)	braun

PIN	Signal	Adernfarben (1)	Adernfarben (2)
1	IDENT	weiß	weiß/orange
2	-	braun	orange
3	GND	grün	weiß/grün
4	A (RS-485)	gelb	blau
5	B (RS-485)	grau	weiß/blau
6	GND	pink	grün
7	VOut+ (DC 12-24 V)	blau	weiß/braun
8	VOut+ (DC 12-24 V)	rot	braun

(1) Mitgeliefertes Verbindungskabel (Art.Nr.: 869834)
(2) Geschirmtes Kabel mit verdrillten Adernpaaren (CAT 5 Standard-farben laut TIA/EIA-568-B.1-2001 - T568B)

***Bild 4.6** – Empfohlener Anschluss des GAT DL 091 am GAT DC 7200*

Als Alternative kann der GAT DL 091 auch an den Schraubklemmen für "Sub" oder "Reader" (Klemmen "A" und "B") angeschlossen werden. Als Beispiel wir nachfolgend der Anschluss an der Schraubklemme "Reader" gezeigt.



PIN	Signal	Aderfarben (2)
1	-	weiß/orange
2	-	orange
3	GND	weiß/grün
4	A (RS-485)	blau
5	B (RS-485)	weiß/blau
6	GND	grün
7	VIN+ (DC 12-24 V)	weiß/braun
8	VIN+ (DC 12-24 V)	braun

***Bild 4.7** – Alternativer Anschluss des GAT DL 091 am GAT DC 7200*

Wenn der GAT DL 091 Access Point mit einer Leitungslänge >100 m angeschlossen ist, können Verbindungsstörungen und -unterbrechungen auftreten. Als Lösung kann der Abschlusswiederstand (220 Ohm), der mit dem Access Point mitgeliefert wird, am GAT DC 7200 angeschlossen werden (siehe unten).

► Zur Überprüfung, ob der Widerstand notwendig ist, wechseln Sie in der Web-Oberfläche des GAT DC 7200 in das Menü "Wartung" -> "Eingänge/Ausgänge".

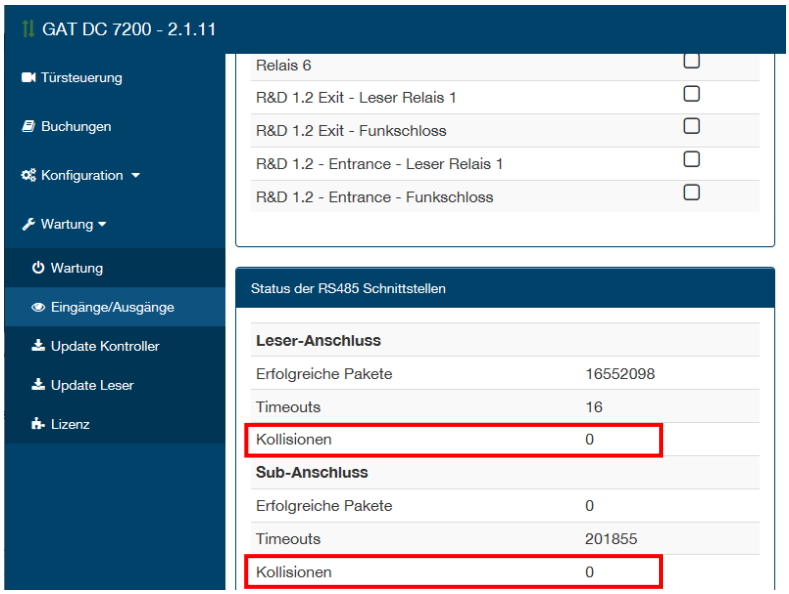


***Bild 4.8** – Anzeige des Status der RS-485 Schnittstelle*

► Der Wert in der Zeile "Kollision" sollte bei der Schnittstelle, an dem der/die GAT DL 091 verbunden ist/sind, "0" anzeigen. Falls der Wert nicht null ist, schließen Sie den Widerstand (1) an den Schraubklemmen "A" und "B" desselben Schnittstellentyps, an dem auch der GAT DL 091 angeschlossen ist, an. Das folgende Bild zeigt die Verwendung der "Sub" Schnittstelle.
HINWEIS! Werden mehrere GAT DL 091 verwendet (bis zu 4 werden unterstützt), darf trotzdem nur ein Widerstand verwendet werden.

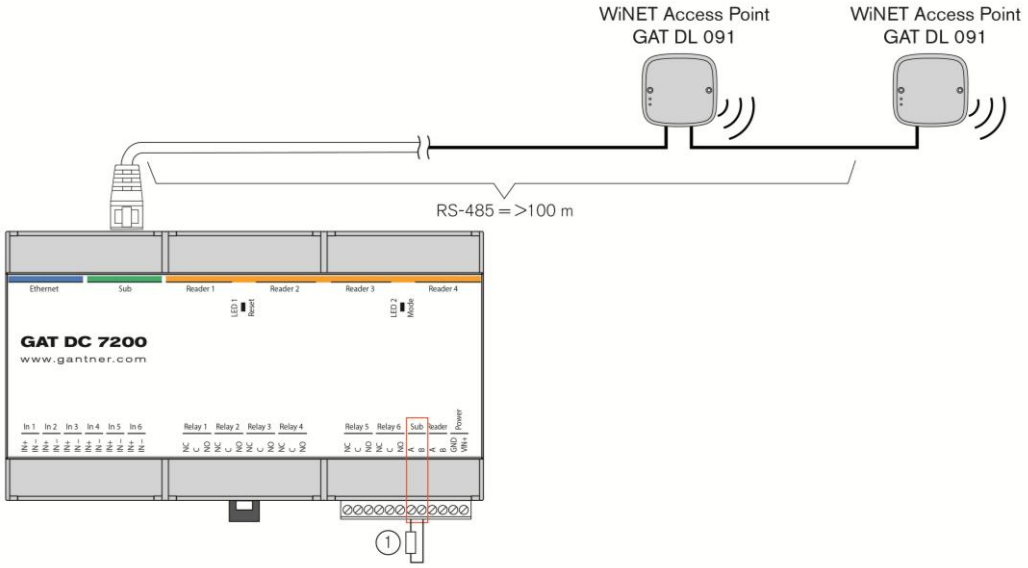


***Bild 4.9** – Widerstand für GAT DL 091 zur Signalverbesserung (Beispiel zeigt Verwendung der "Sub" Schnittstelle)*

4.5 Peripheriegeräte

Der Anschluss von Peripheriegeräten zur Erweiterung der Controller-Funktionen erfolgt an der mit "Sub" gekennzeichneten Schnittstelle. Sie können hier z. B. Relaisexpander anschließen, um die Anzahl der Signaleingänge und Relaisausgänge zu erhöhen und damit Liftsteuerungen zu realisieren.

Der Anschluss von Peripheriegeräten kann entweder über RJ45 Stecker oder Schraubklemmen erfolgen. Der Strom, der an der RJ45 Sub-Buchse entnommen wird, darf 1 A nicht übersteigen. Außerdem darf die gesamte Leistung, die an allen RJ45 Buchsen des GAT DC 7200 zusammen entnommen wird, 40 VA nicht übersteigen.

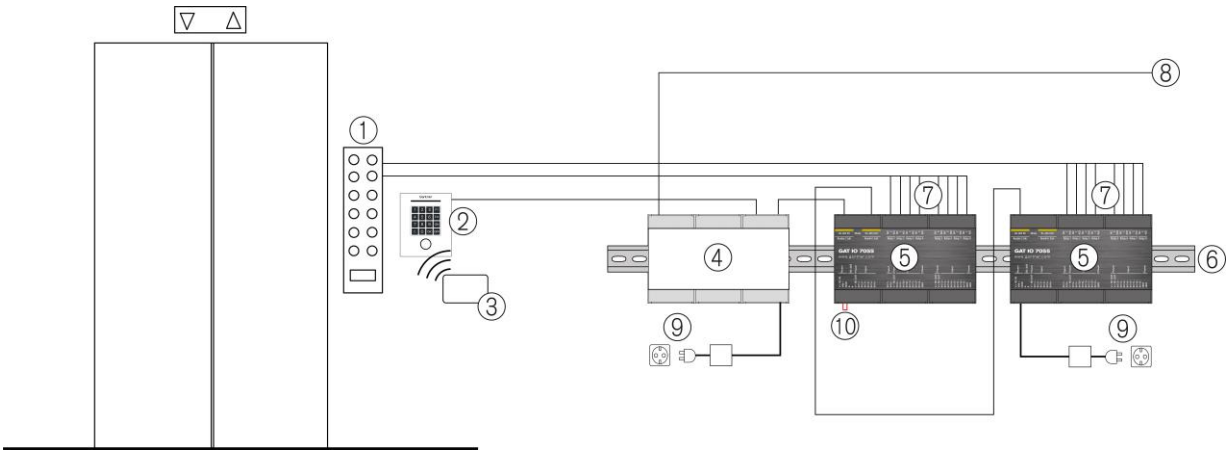
GAT DIRECT.Connect kann Peripheriegeräte nur dann nutzen, wenn sie als Ein- und Ausgänge von Standard-Türfunktionen verwendet werden. Die Verwendung als Lift- oder Schließfachsteuerung wird nicht unterstützt.

4.5.1 Anschluss eines Expanders GAT IO 7054 oder GAT IO 7055

Mit einem GAT IO 7054 und GAT IO 7055 kann die Anzahl der Statuseingänge und -ausgänge eines GAT DC 7200 erweitert werden. Damit ist es möglich, mit einem Türcontroller mehr als 6 Ausgänge zu schalten, z. B. um bei Liftsteuerungen die einzelnen Stockwerke gezielt freischalten zu können, und auch mehr als 6 Statussignalen zu erfassen und verarbeiten.

An einem GAT DC 7200 können 8 GAT IO 705x angeschlossen werden. Ein Mischbetrieb aus GAT IO 7054 und 7055 ist möglich.

Für den Anschluss der GAT IO 7054 und GAT IO 7055 werden hier nur die wichtigsten Punkte für den Anschluss am GAT DC 7200 erklärt. Bitte lesen Sie auch das Beilageblatt dieser Module.

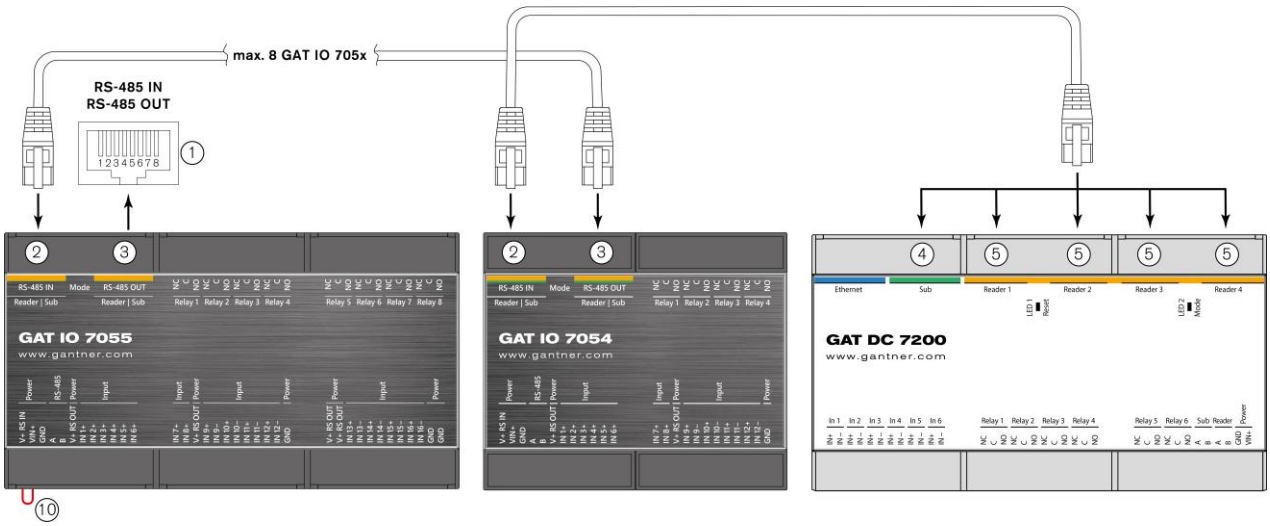


1 … Aktivierung der Stockwerke
2 … GR7 Leser
3 … Datenträger für Identifikation
4 … GAT DC 7200
5 … GAT IO 7055
6 … DIN-Hutschiene
7 … Relaisausgänge
8 … Netzwerk
9 … Lokales Netzteil
10 … Brücke für Versorgungsspannung über strukturierte Verkabelung

Bild 4.10 *– Anwendungsbeispiel*

Ein GAT IO 705x wird mittels RS 485 Schnittstelle an einem GAT DC 7200 angeschlossen. Die Spannungsversorgung kann über die strukturierte Verkabelung (RS 485 Schnittstelle) oder mittels separaten Netzteils erfolgen. Bei Versorgung über die strukturierte Verkabelung muss die Drahtbrücke (10) eingesetzt werden. Empfohlen wird mind. ein CAT 5 Kabel mit Versorgung über 2 Adernpaare.

Das folgende Bild zeigt den Anschluss der GAT IO 705x. Befolgen Sie auch die Anweisungen aus dem Beilageblatt.



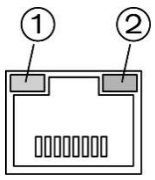
1 … RJ45-Buchse der RS-485 Schnittstelle
2 … GAT IO 705x: RS-485 IN
3 … GAT IO 705x: RS-485 OUT
4 … GAT DC 7200: "Sub" Buchse
5 … GAT DC 7200: "Reader x" Buchse
10 … Brücke für Versorgungsspannung über strukturierte Verkabelung

***Bild 4.11** – Anschluss eines GAT IO 7054 und 7055 am GAT DC 7200*

Der Anschluss der Relaisausgänge und Optokopplereingänge an den GAT IO 705x Modulen erfolgt analog zum Anschluss am GAT DC 7200 (siehe "4.6. Relaisausgänge und Optokopplereingänge").

4.5.2 Statusanzeige

An der RJ45 Buchse der Peripherieschnittstelle "Sub" befinden sich 2 LEDs, die folgenden Informationen anzeigen.



LED	Status	Bedeutung
orange (1)	ein	Versorgung für angeschlossenes Gerät OK
	aus	Versorgung deaktiviert oder Störung
grün (2)	blinkt	Kommunikation zum angeschlossenen Leser OK (nur bei angeschlossener IDENT-Leitung und Geräten die Plug&Play PLUS unterstützen)
	aus	Keine Kommunikation (oder IDENT-Leitung nicht angeschlossen oder Plug&Play PLUS wird vom angeschlossenen Gerät nicht unterstützt)

***Tabelle 4.3** – LED-Anzeigen an der Sub Schnittstelle*

4.6 Relaisausgänge und Optokopplereingänge

Der GAT DC 7200 ist mit 6 Relaisausgängen und 6 potentialfreien Optokopplereingängen ausgestattet. Die Funktion und das Zeitverhalten dieser Ein- und Ausgänge können frei konfiguriert werden.

Eine übliche Anwendung der Relaisausgänge ist die Ansteuerung des Entriegelungsrelais einer überwachten Tür. Bei gültiger Identifikation und Zutrittsberechtigung wird das betreffende Relais für die konfigurierte Zeit aktiviert und dadurch das elektronische Türschloss entriegeln.

Die Optokopplereingänge dienen als digitale Statuseingänge, um z. B. Türzustände zu erfassen oder eine Taster Entriegelungen zu ermöglichen. Auch die Funktion und das Zeitverhalten dieser digitalen Eingänge kann bei der Konfiguration individuell eingestellt werden.

Eine genaue Beschreibung aller möglichen Funktionen finden Sie im Bedienungshandbuch der Konfigurationssoftware GAT ACE 7000 von GANTNER Electronic GmbH.

Das folgende Bild zeigt den Anschluss eines elektronischen Türöffners und eines Türrückmeldeeingangs.

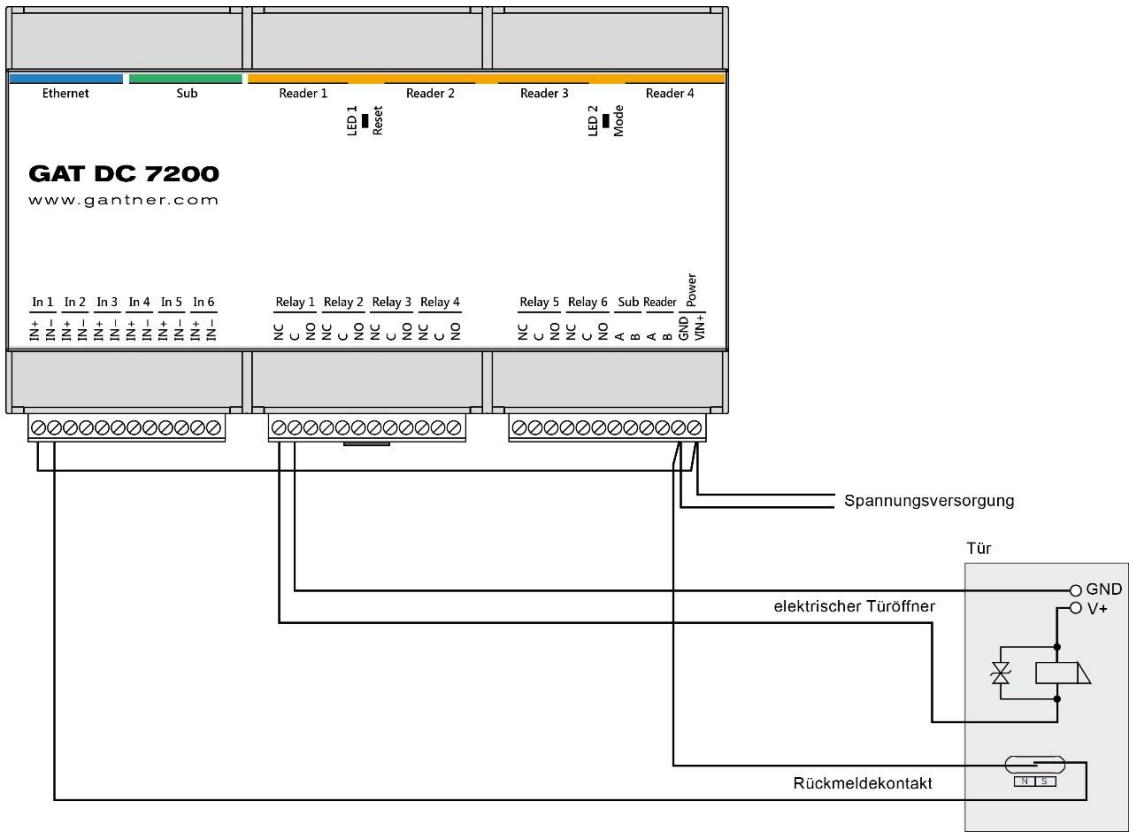


***Bild 4.12** – Verdrahtung der Relaisausgänge und Optokopplereingänge*

Die Spannung für die Optokopplereingänge kann z. B. von der Versorgung des Türcontroller GAT DC 7200 oder durch eine externe Quelle erfolgen. Beachten Sie die erlaubten Spannungs- und Stromwerte (siehe "10 TECHNISCHE DATEN"). Die Spannung für die Relaisausgänge muss von einer externen Quelle geliefert werden.

4.7 Spannungsversorgung

⚠ **ACHTUNG! Elektrischer Schlag.** Berühren Sie nie Netzspannung und verwenden Sie ein LPS (Limited Power Source) Netzgerät mit den entsprechenden technischen Daten (siehe "10 TECHNISCHE DATEN").

Der GAT DC 7200 benötigt eine Gleichspannungsversorgung. Der zulässige Spannungsbereich beträgt 10 - 28 V und die Nennspannung 12 und 24 V. Für die Spannungsversorgung des GAT DC 7200 darf nur ein LPS (Limited Power Source) Netzgerät verwendet werden.

Die Leistungsaufnahme des GAT DC 7200 ohne angeschlossene Geräte liegt unter 5 VA. Für die Dimensionierung der Spannungsversorgung sind alle angeschlossenen Geräte mitzubetrachten. Die Daten dieser Geräte sind in den jeweiligen Datenblättern zu finden.

► Schließen Sie die Versorgungsleitungen an den Klemmen +VIN und GND der "Power" Schraubklemmen des GAT DC 7200 an.

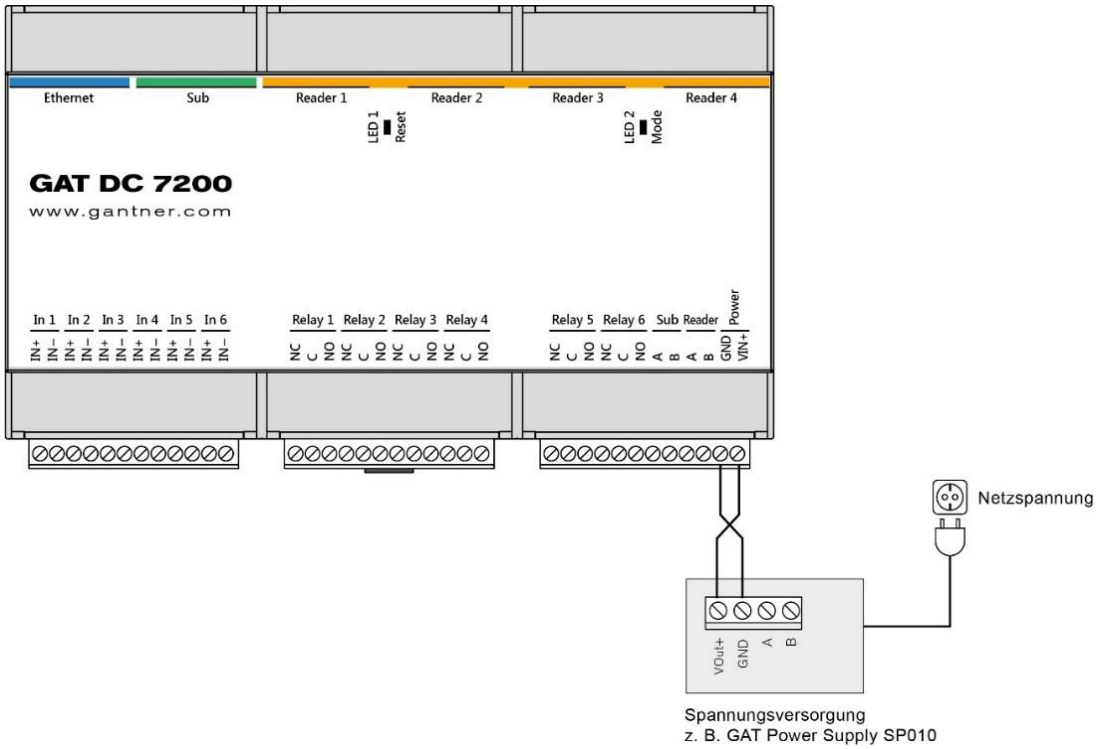


***Bild 4.13** – Anschluss der Versorgungsspannung*

► Stellen Sie sicher, dass alle Kabel (Netzwerk, Leser, Peripherie, etc.) am, GAT DC 7200 angeschlossen sind.

► Stecken Sie das Netzkabel der Spannungsversorgungseinheit in die Netzsteckdose ein.

- Wird die Netzspannung eingeschaltet, startet der GAT DC 7200 hoch. Es dauert, abhängig von der Konfiguration, ca. 10 bis 20 Sekunden, bis der Türcontroller und die Leser einsatzbereit sind.

5 BEDIENELEMENTE UND SIGNALISIERUNG

5.1 Allgemein

Der Türcontroller GAT DC 7200 arbeitet mit der eingestellten Konfiguration und den Berechtigungsdaten und wartet auf eine Identifikation an einem angeschlossenen Leser oder ein Signal an einem digitalen Eingang. Für die Auswahl von Funktionen oder Eingabe von PIN-Codes können Leser mit Tastatur angeschlossen werden.

Diverse Statusinformationen werden vom GAT DC 7200 mit akustischen Signalen und LEDs angezeigt. Über einen Taster kann der GAT DC 7200 neu gestartet, das Passwort und Netzwerkeinstellungen zurückgesetzt oder der GAT DC 7200 auf Werkseinstellungen zurückgesetzt werden.

5.2 Zielgruppe

Dieses Kapitel enthält Informationen für die Service-Techniker, falls Störungen am GAT DC 7200 auftreten. Diese Informationen sind nicht für die Benutzer der Zutrittsanlage bestimmt.

5.3 Neustart

Diese Funktion kann helfen, wenn der GAT DC 7200 nicht reagiert. Bei einem Neustart ist der GAT DC 7200 ca. 20 Sekunden außer Betrieb, bis er neu gestartet wurde. Es gehen dabei keine Daten und Einstellungen im GAT DC 7200 verloren.

Der Reset-Taster befindet sich an der Seite der RJ45 Buchsen.

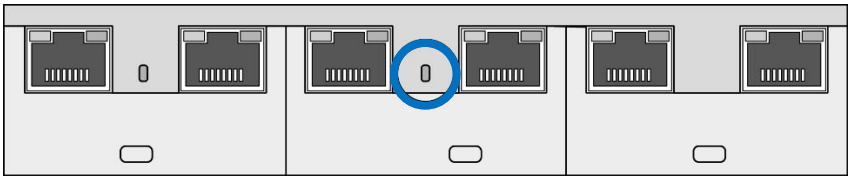


***Bild 5.1** – Taster zum Neustart des GAT DC 7200*

- ► Führen Sie einen dünnen (nicht spitzen!) Gegenstand in die im Bild gezeigte Öffnung ein.
- ► Drücken Sie den hinter der Öffnung befindlichen Taster kurz und lassen Sie los.
  - o Der GAT DC 7200 gibt einen kurzen Ton aus und startet neu. Dieser Vorgang dauert 10 bis 20 Sekunden. Danach ist der GAT DC 7200 wieder einsatzbereit.

5.4 Konfigurationspasswort und Netzwerkeinstellungen rücksetzen

Wenn das Passwort für die Konfiguration des GAT DC 7200 mittels Web-Oberfläche vergessen wurde oder die Netzwerkeinstellungen nicht korrekt sind, können diese Informationen auf die Standardeinstellungen zurückgesetzt werden. Dabei werden außer den Netzwerkeinstellungen und dem Passwort keine weiteren Daten im GAT DC 7200 gelöscht.

Der Reset-Taster befindet sich an der Seite der RJ45 Buchsen.

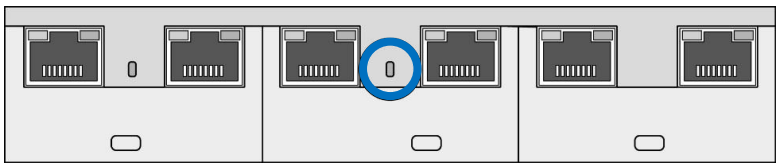


***Bild 5.2** – Taster zum Rücksetzen von Passwort und Netzwerkeinstellungen*

- ► Führen Sie einen dünnen (nicht spitzen!) Gegenstand in die im Bild gezeigte Öffnung ein.
- ► Drücken Sie den hinter der Öffnung befindlichen Taster 5 Sekunden lang, bis 2 Signaltöne zu hören sind.
- ► Lassen Sie den Taster los und drücken Sie ihn nochmals kurz zur Bestätigung.
  - Passwort und Netzwerkeinstellungen werden zurückgesetzt und der GAT DC 7200 startet neu.
  - Sollte dieser Vorgang nicht funktioniert haben, ist ein tiefer Signalton zu hören.

5.5 Neustart und Rücksetzen auf Werkseinstellungen

Diese Funktion kann helfen, wenn der GAT DC 7200 nicht reagiert oder falsch konfiguriert wurde. Beim Rücksetzen auf Werkseinstellungen werden alle Konfigurationsdaten, Buchungen, Zeitpläne etc. im GAT DC 7200 gelöscht und auf die bei der Auslieferung eingestellten Werte gesetzt. Die Konfiguration und Berechtigungsdaten müssen nach dem Rücksetzen neu erstellt bzw. geladen werden.

HINWEIS! Sichern Sie Buchungen und Daten, die Sie benötigen, bevor Sie den GAT DC 7200 auf Werkseinstellungen zurücksetzen.

Der Reset-Taster befindet sich an der Seite der RJ45 Buchsen.

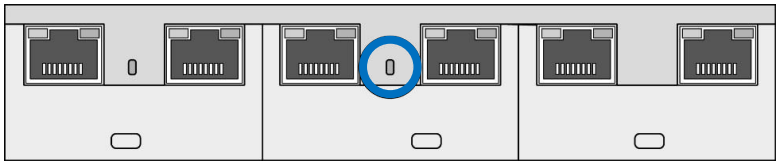


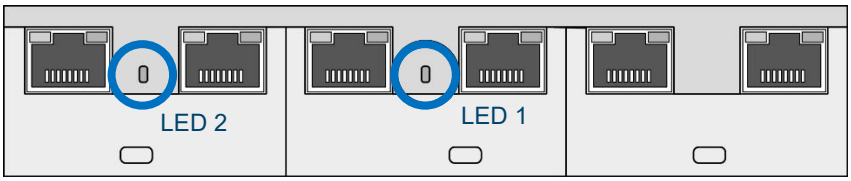
***Bild 5.3** – Taster zum Rücksetzen auf Werkseinstellungen*

- ► Führen Sie einen dünnen (nicht spitzen!) Gegenstand in die im Bild gezeigte Öffnung ein.
- ► Drücken Sie den hinter der Öffnung befindlichen Taster 10 Sekunden lang, bis 3 Signaltöne zu hören sind.
- ► Lassen Sie den Taster los und drücken Sie ihn nochmals kurz zur Bestätigung.
  - Die Daten im GAT DC 7200 gelöscht und der Controller startet neu mit den Werkseinstellungen.
  - Sollte dieser Vorgang nicht funktioniert haben, ist ein tiefer Signalton zu hören.

5.6 Signalisierungsübersicht

Der GAT DC 7200 besitzt verschiedene LEDs zur Anzeige von Statusinformationen und Betriebszustände. Die folgende Tabelle listet die möglichen Zustände auf.

Allgemein

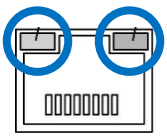


LED	Signal		Beschreibung
LED 1	grün		Verbindung zur Host-Software OK
	rot		keine Verbindung zur Host-Software
	blinkt rot/grün		Bootloader
LED 2	blau		für zukünftige Anwendungen reserviert

***Tabelle 5.1** - Übersicht der allgemeinen LED-Zustände*

RS-485 Schnittstellen (RJ45 Buchsen) für Leser und Peripherie

LED Orange LED Grün

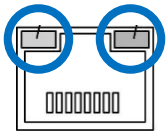


LED	Signal		Beschreibung
LED Orange	orange		Versorgung für die angeschlossenen Geräte ist OK
	aus		Versorgung für die angeschlossenen Geräte ist deaktiviert oder Störung
LED Grün	blinkt grün		Kommunikation zum angeschlossenen Gerät ist OK (nur Geräte die Plug&Play PLUS unterstützen)
	aus		Keine Kommunikation oder Gerät unterstützt die Plug&Play PLUS Funktion nicht

***Tabelle 5.2** - Übersicht der LED-Zustände an den RJ45 Buchsen der Leser- und Peripherieschnittstellen*

Ethernet-Schnittstellen (RJ45 Buchse)

LED Orange LED Grün



LED	Signal		Beschreibung
LED Orange	orange		100 MBit Verbindung
	aus		10 MBit Verbindung
LED Grün	blinkt grün		Link und Kommunikation

***Tabelle 5.3** - Übersicht der LED-Zustände an der RJ45 Buchse der Ethernet-Schnittstelle*

6 INBETRIEBNAHME UND KONFIGURATION

Um den GAT DC 7200 nach der Montage und Installation in Betrieb zu nehmen, müssen die Konfigurationsdaten bearbeitet werden. Dies erfolgt über das Netzwerk mittels Web-Oberfläche. Die notwendigen Informationen für die Bearbeitung der Konfiguration finden Sie in diesem Kapitel.

Die Konfiguration beinhaltet die Funktionseinstellungen des Türcontrollers. Dazu zählen z. B. das Zeitverhalten für Entriegelung, max. erlaubte Türöffnung usw., die Funktionseinstellungen der digitalen Ein- und Ausgänge, Einstellungen für die angeschlossenen Leser (Typ, RFID-Technologie, Datenformat, usw.), die Ansteuerung einer Alarmanlage und Einstellung des Bedrohungs-PIN-Codes.

Die Berechtigungsdaten der Personen für den Online-Modus sind nicht Teil der Konfiguration und diese werden über eine Zutrittskontrollsoftware (z. B. Matrix) definiert. Die Berechtigungskonfiguration für den Standalone-Modus finden Sie in Kapitel "8. STANDALONE MODUS".

6.1 Zielgruppe

Dieses Kapitel enthält Informationen für die Techniker, die den GAT DC 7200 in Betrieb nehmen und konfigurieren. Ein elektrotechnisches Grundverständnis wird vorausgesetzt. Außerdem wird empfohlen, an einer GANTNER Schulung über das Zutrittskontrollsystem teilzunehmen.

6.2 Versorgung einschalten

► Stellen Sie sicher, dass alle notwendigen Anschlüsse (Netzwerk, Leser, etc.) wie in Kapitel „4 ELEKTRISCHER ANSCHLUSS“ beschrieben korrekt sind.

► Stecken Sie das Netzkabel der Spannungsversorgungseinheit in die Netzsteckdose ein.

- Wird die Netzspannung eingeschaltet, startet der GAT DC 7200 hoch. Es dauert ca. 10 bis 20 Sekunden, bis der Türcontroller einsatzbereit ist.

6.3 Erster Start

Beim ersten Einschalten nach der Auslieferung ist der Türcontroller mit den Werkseinstellungen vorkonfiguriert. Dies bedeutet:

- Angeschlossenen Leser und GAT IO 705x werden automatisch erkannt und aktiviert. Mit der Plug&Play PLUS Funktion werden außerdem Leser, die an den RJ45 Anschlüssen angeschlossen werden, entsprechend der Anschlussnummer (Reader 1 bis Reader 4) automatisch den Türen 1 bis 4 zugeordnet.
- Die Leser sind auf das Lesen der Unikatsnummern der Datenträger eingestellt. Es müssen nur noch die Berechtigungen der Personen in der Zutrittskontrollsoftware definiert, den entsprechenden Datenträgern zugewiesen und in den Controller geladen werden.
- Bei den Lesern der Serie GAT SR/SLR 73xx und GR7 sind die RFID Technologien LEGIC prime, LEGIC advant, ISO 14443A und ISO 15693 aktiviert.
- Der Relaisausgang 1 ist im Auslieferzustand als Entriegelungsrelais für die Tür 1 und der Optokopplereingang 1 als Türrückmeldung der Tür 1 vordefiniert. Dasselbe gilt für Tür 2, 3 und 4 mit den Relais und Optokopplern 2, 3 und 4.

- Die Zeitzone ist auf UTC +01:00 gesetzt und die europäische Sommer-/Winterzeitumschaltung ist eingeschaltet.
- DHCP ist eingeschaltet, um automatisch eine IP-Adresse im Netzwerk zu beziehen. Der Netzwerkname des GAT DC 7200 ist auf den Default:

  `DC7x_nnnnnnnnnn`

  eingestellt, wobei nnnnnnnnnn die Seriennummer des jeweiligen Gerätes ist. Die Seriennummer finden Sie auf der Geräterückseite oder auf der Verpackung. Somit kann jedes Gerät im Netzwerk eindeutig angesprochen werden.
- Der Standardport für die Kommunikation mit GAT ACE 7000 ist Port 8000 (dieser Port ist parametrierbar im GAT DC 7200 und in GAT ACE 7000).
- Standardports für FTP sind 20 und 21. Ab Version 2.0 der GAT ACE 7000 Software wird kein FTP mehr benötigt.
- Standard Webserverport für den Zugriff auf die GAT DC 7200 Konfigurationsseite ist ab Version 3.0 der GAT DC 7200 Firmware der Port 443 (verschlüsselte Verbindung über TLS/SSL). Bei älteren Versionen ohne TLS/SSL wird Port 80 verwendet.
- Der NTP Port für Zeitsynchronisation ist 123 (UDP) ausgehend.
- Der Standardport für GAT DIRECT.Connect ist 8239.

6.4 Konfiguration

Die Konfiguration erfolgt mittels Internetbrowser über eine Web-Oberfläche. Als Internetbrowser kann jeder aktuelle Browser sowohl auf dem Desktop als auch in der mobilen Variante z. B. auf Smartphones oder Tablets benutzt werden. GANTNER Electronic GmbH empfiehlt, für die Konfiguration den Firefox oder Chrome Browser in der aktuellen Version zu verwenden.

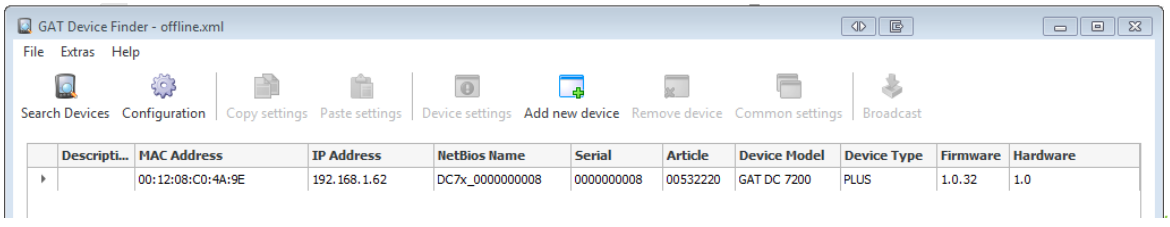
Die Konfiguration mit der GAT ACE 7000 Software erfolgt ebenfalls über dieselbe Web-Oberfläche.

► Geben Sie im Internetbrowser folgende Adresse ein, um die Web-Oberfläche zur Konfiguration des GAT DC 7200 zu öffnen. Die Verbindung erfolgt ab Version 3.0 der Firmware im GAT DC 7200 standardmäßig verschlüsselt über TLS/SSL (siehe folgenden Abschnitt "6.4.1. Zertifikat für TLS/SSL Verbindung"):

`https://DC7x_nnnnnnnnnn` (wobei nnnnnnnnnn die Seriennummer des Gerätes ist) oder
`https://<IP-Adresse>` (wobei <IP-Adresse> die IPv4 Adresse des GAT DC 7200 im Netzwerk ist).

Hinweis: Ab der Firmware Version 3.0 wird beim Aufruf der Seite ein Hinweis im Browser angezeigt, dass es sich um keine Sichere Verbindung handelt, wenn das Zertifikat für die https Verbindung noch nicht installiert ist. Sie können diesen Hinweis überspringen, um auf die Konfigurationsseite zuzugreifen und das Zertifikat zu installieren. Nähere Infos siehe "6.4.1. Zertifikat für TLS/SSL Verbindung einrichten".

Der GAT DC 7200 verwendet DHCP, um beim Hochstart autmatisch eine IP-Adresse aus dem Netzwerk zu beziehen. Die IP-Adresse des GAT DC 7200 können Sie z. B. mit der GANTNER Software GAT Device Finder finden.



- Es wird ein Popup-Anmeldefenster angezeigt.

► Geben Sie im Anmeldefenster den Benutzernamen und das Passwort ein, um sich am GAT DC 7200 anzumelden.

HINWEIS! Bei Auslieferung ist der Benutzername auf "admin" und das Passwort auf "GAT" gesetzt. Sie müssen das Passwort nach der ersten Anmeldung aus Sicherheitsgründen auf ein geheimes Passwort ändern (siehe "6.4.5. Benutzer"). Bewahren Sie das Passwort an einem Sicheren Ort (z.B. Passwort-Tresor) auf.

► Klicken Sie "OK"

- Das Hauptfenster mit dem Live View der Türen wird in der Web-Oberfläche geöffnet (siehe Bild 6.11). Weitere Web-Interface Funktionen können über das Menü links aufgerufen werden.

HINWEIS! Wenn für 15 Minuten keine Bedienung in der Web-Oberfläche erfolgt, wird der aktuelle Benutzer aus Sicherheitsgründen abgemeldet.

6.4.1 Zertifikat für TLS/SSL Verbindung einrichten

Die Verbindung zum GAT DC 7200 über die Webschnittstelle erfolgt ab Version 3.0 des GAT DC 7200 standardmäßig mittels TLS Verschlüsselung. Diese Verschlüsselung wird auch für die Kommunikation mit GAT ACE 7000 ab Version 2.0.0 verwendet. Vor dieser Version verwendete GAT ACE 7000 zur Kommunikation mit dem GAT DC 7200 noch kein TLS.

Wenn die Konfigurationsseite von GAT DC 7200 auf einem PC das erste Mal aufgerufen wird, wird eine Meldung angezeigt, dass die Seite unsicher ist.

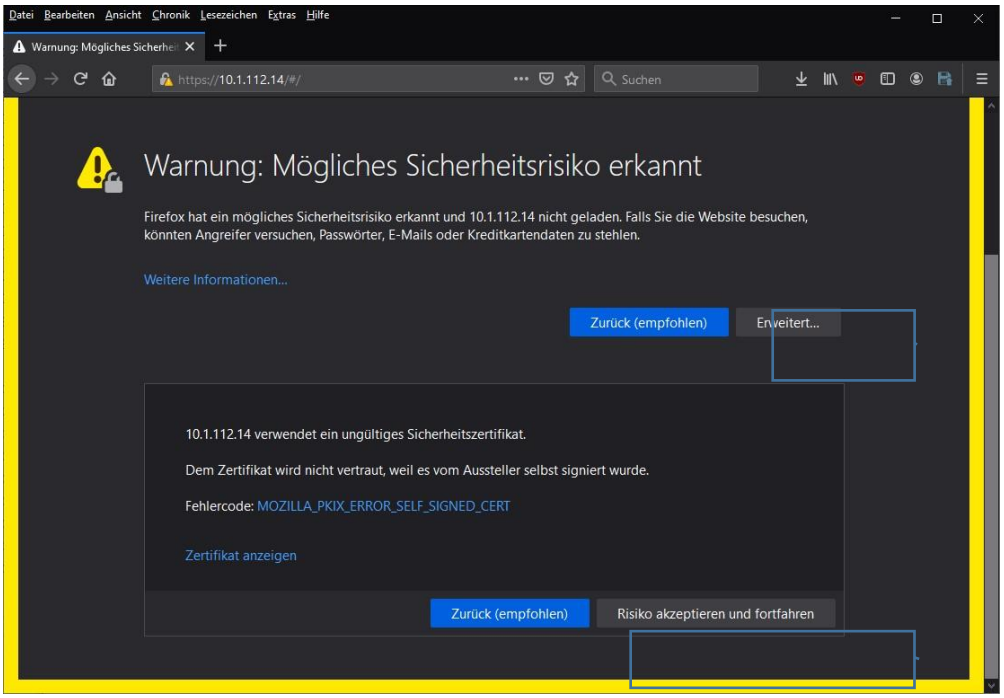


***Bild 6.1** – Meldung zur Verbindung mit SSL/TLS*

Diese Meldung erscheint (Beispiel Firefox-Browser), weil am PC noch kein Zertifikat installiert ist, das die Sicherheit der Konfigurationsseite bestätigt. Es ist möglich, mit dem GAT DC 7200 selbst ein Zertifikat auszustellen, das am PC installiert werden kann. Führen Sie folgende Schritte aus.

► Wenn Sie sicher sind, dass die Internet-Adresse des GAT DC 7200 korrekt eingegeben wurde, wählen Sie bei dieser Sicherheitswarnung "Erweitert …"

► Wählen Sie dann "Risiko akzeptieren und fortfahren“.

  o Sie können die Verbindung zum GAT DC 7200 aufbauen. Es erscheint das Anmeldefenster.

► Melden Sie sich hier mit Benutzername und Passwort an (siehe vorige Seite).

  o Die Konfigurationsseite des GAT DC 7200 wird angezeigt. Sie sehen in der Adressleiste, dass die Verbindung mit https erfolgt aber als unsicher gekennzeichnet ist.

► Wechseln Sie im Menü links auf "Konfiguration" -> "Sicherheit und Benutzer".

► In der Registerkarte "Allgemein" müssen für die sichere Konfiguration via SSL unter "Host-Interface-Einstellungen" die Option "Sichere Verbindung verwenden (TLS/SSL)" aktiviert sein.

► Wechseln Sie hier auf die Registerkarte "Zertifikate".

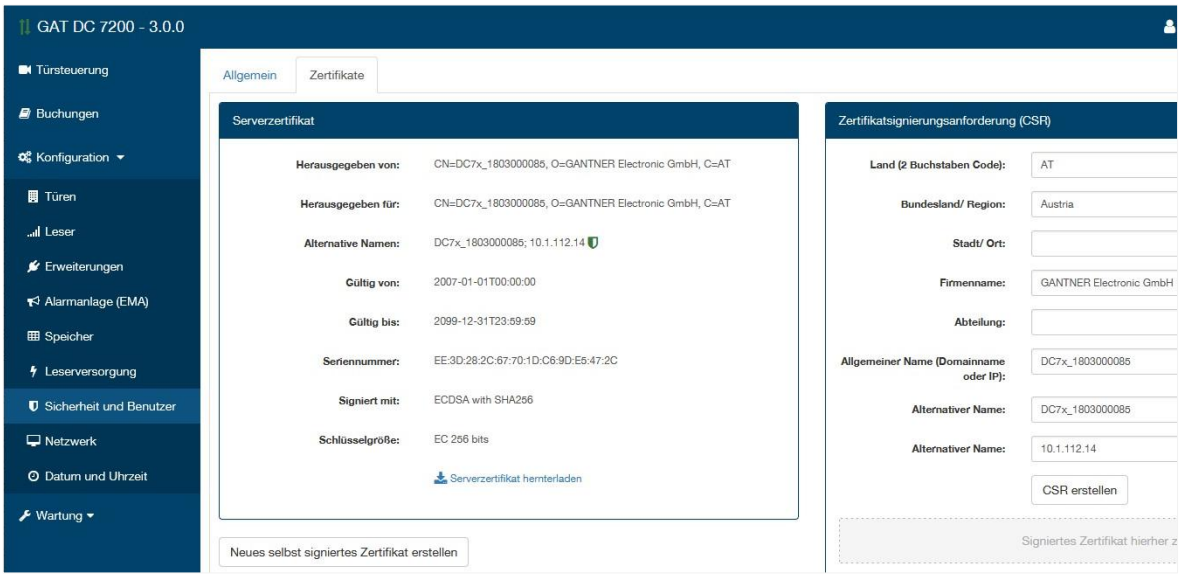


***Bild 6.2** – Zertifikat erstellen*

► Prüfen Sie, ob im verwendeten Zertifikat die richtige IP-Adresse und der richtige NetBios Name eingetragen sind (Symbol hinter "Alternative Namen"). Falls nicht, klicken Sie auf "Neues selbst signiertes Zertifikat erstellen".

Hinweis: Windows 8.0 oder frühere Windows Versionen unterstützen keinen "Alternativer Name".

Hinweis: Der Firefox Browser verwendet einen eigenen Zertifikatspeicher.

► Klicken Sie anschließend auf "Kontroller neu starten".

  o Warten Sie ca. 30 Sekunden, bis der Türcontroller neu gestartet ist. Die Verbindung wird automatisch wieder hergestellt.

► Sie müssen nun das erstellte Zertifikat vom GAT DC 7200 auf den PC laden. Dazu habe Sie 2 Möglichkeiten:

Möglichkeit 1 – Zertifikat via Web-Oberfläche laden:

(empfohlen – Firefox, Internet Explorer)

► Klicken Sie auf "Serverzertifikat herunterladen".

- Es öffnet sich ein Dateifenster, in dem Sie den Speicherort und Namen für die Zertifikatsdatei wählen können. Das Zertifikat wird im Format "`server_Name.cer`" gespeichert.

Möglichkeit 2 – Zertifkat mittels Browserfunktion laden:

Wenn der Browser das direkte Herunterladen via Web-Oberfläche nicht unterstützt (z. B. Microsoft Edge), wird eine Fehlermeldung beim Klick auf "Serverzertifikat herunterladen" angezeigt. Sie können das Zertifikat auch mittels Browser-Funktion herunterladen. Dies ist abhängig vom Browser und kann z. B. für den Edge Browser wie folgt durchgeführt werden.

► Klicken Sie auf "Nicht sicher" und wählen Sie dann "Die Verbindung mit dieser Website ist nicht sicher".

► Im daraufhin angezeigten Meldungsfenster klicken Sie auf das Symbol rechts oben.

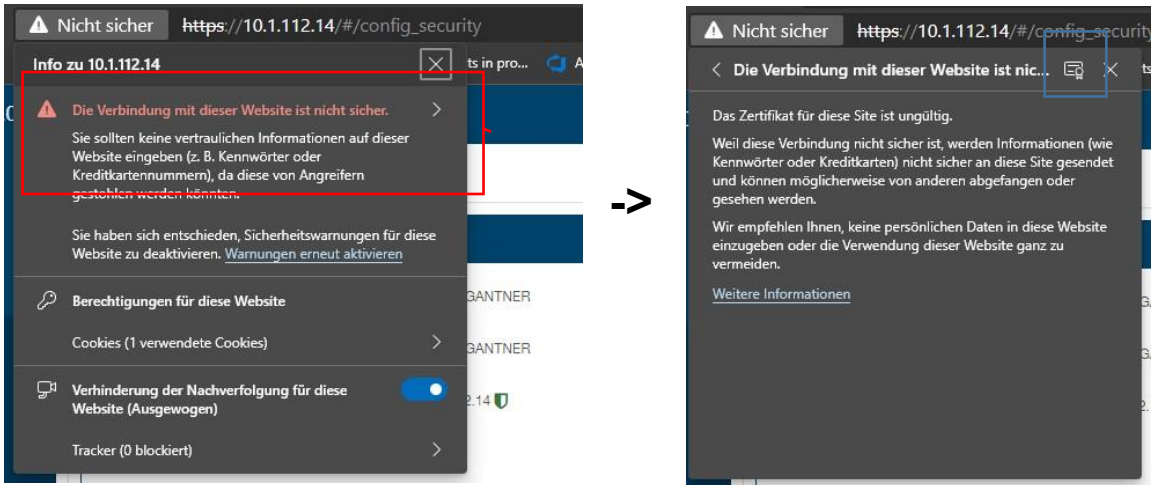


***Bild 6.3** – Zertifikat öffnen*

- Das vom GAT DC 7200 generierte Zertifikat wird im Fenster "Zertifikat" angezeigt.

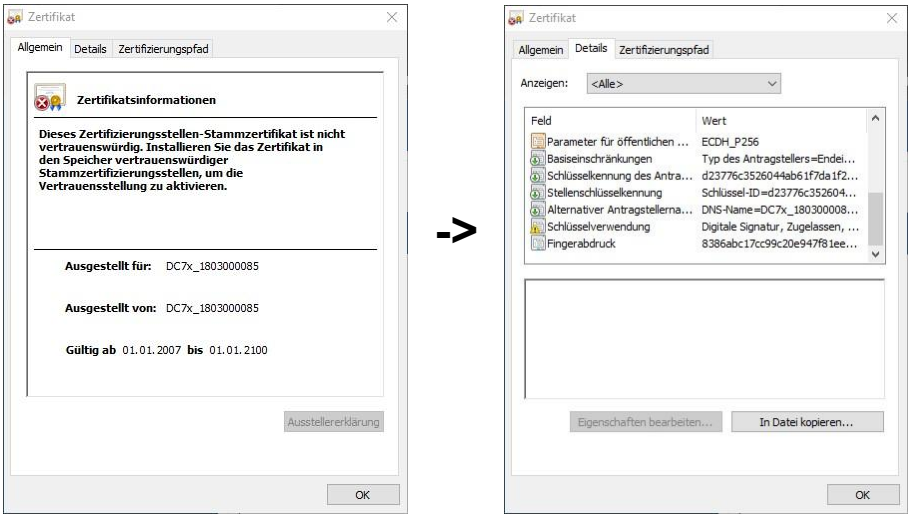


***Bild 6.4** – Zertifikat anzeigen*

► Wechseln Sie auf die Registerkarte "Details".

► Wählen Sie "In Datei kopieren …".

  ○ Es wird das Fenster des Zertifikatsexport-Assistent angezeigt.

► Klicken Sie auf "Weiter" und wählen Sie dann die Option "DER-codiert-binär X.509 (.CER)".

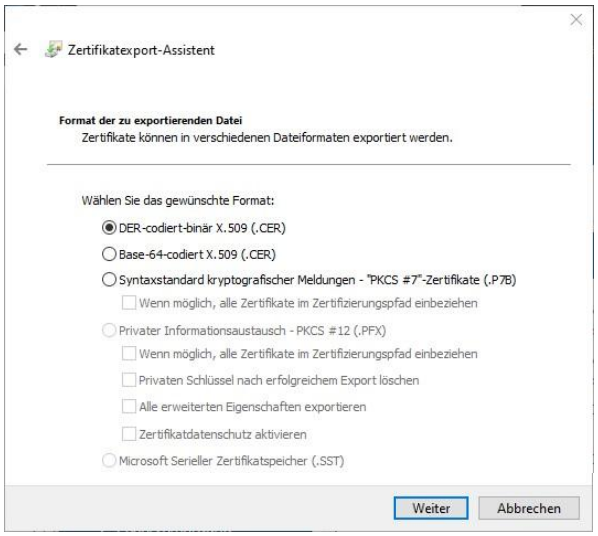


***Bild 6.5** – Zertifikat exportieren*

► Mit Weiter können Sie einen Dateinamen auswählen und die Zertifikatsdatei auf dem PC speichern.

<u>Zertifikat auf PC installieren:</u>

Nachdem Sie die Zertifikatsdatei (.cer) vom GAT DC 7200 auf den PC kopiert haben, installieren Sie diese in Windows wie folgt.

► Doppelklicken Sie auf das Zertifikat (Datei mit Endung .cer).

  ○ Es wird das Fenster "Zertifikat" angezeigt.

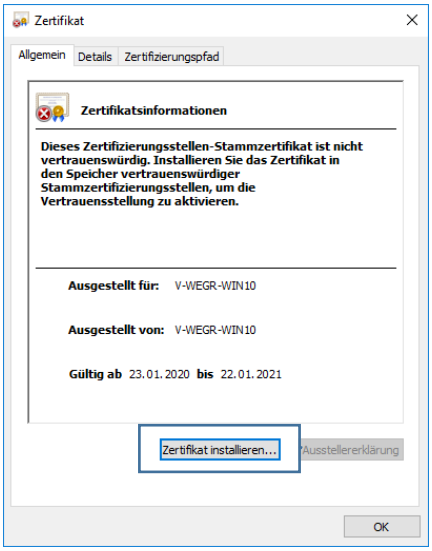


***Bild 6.6** – "Zertifikat" Fenster*

► Klicken Sie auf "Zertifikat installieren".

  ○ Das Fenster “Zertifikatimport-Assistent” wird geöffnet.

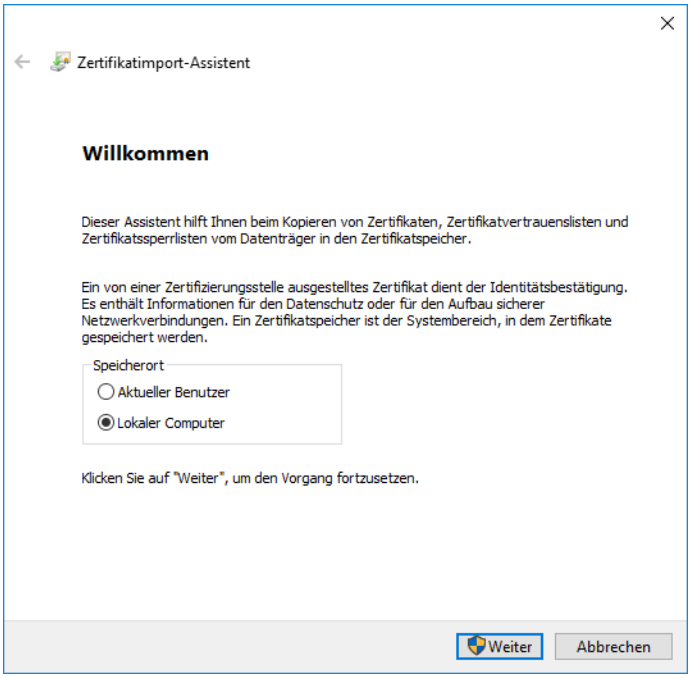


***Bild 6.7** – “Zertifikatimport-Assistent” – Schritt 1*

► Wählen Sie den zu verwendenden Zertifikatsspeicher (“Aktueller Benutzer” oder “Lokaler Computer”) und klicken Sie "Weiter".
Hinweis: Auf dem PC, auf dem nur mittels Viewer auf GAT ACE 7000 zugegriffen werden soll oder auf dem Sie den GAT DC 7200 mittels Webbrowser konfigurieren, wählen Sie bitte "Lokaler Computer". Auf dem PC, auf dem der GAT ACE 7000 Dienst läuft, wählen Sie bitte "Aktueller Benutzer" und installieren Sie das Zertifikat zusätzlich auch mit "Lokaler Computer", wenn der GAT ACE 7000 Viewer benutzt werden soll.

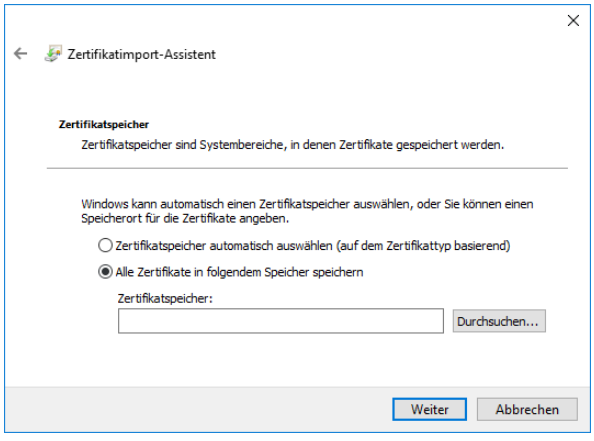


***Bild 6.8** – “ Zertifikatimport-Assistent” – Schritt 2*

► Wählen Sie “Alle Zertifikate in folgendem Speicher speichern" und klicken Sie auf "Durchsuchen…".

► Im Fenster “Zertifikatspeicher auswählen” wählen Sie “Vertrauenswürdige Stammzertifizierungsstellen” und klicken Sie auf “OK”.

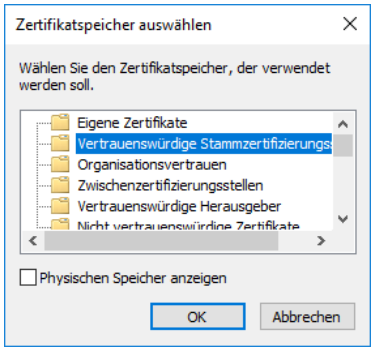


Bild 6.9 *– "Zertifikatimport-Assistent" – Schritt 3*

► Klicken Sie dann auf "Fertig stellen" und bestätigen Sie das nachfolgende Meldungsfenster mit Klick auf "Weiter".

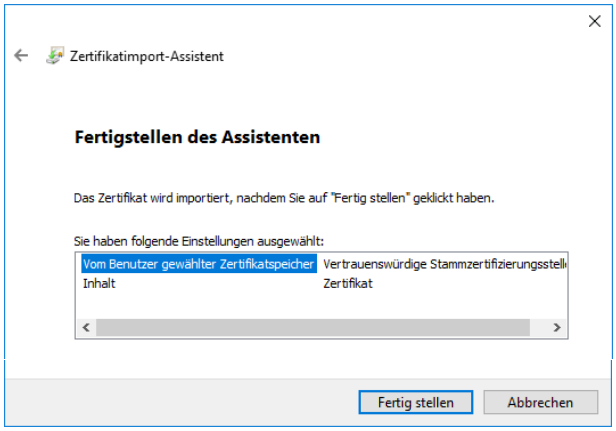


Bild 6.10 *– "Zertifikatimport-Assistent" – Schritt 4*

6.4.2 Live-Ansicht mit Statusanzeige und Türsteuerung

Wenn bereits Türen konfiguriert sind, werden die Statusinformationen der Türen und die Sicherheitsstatus in der Live-Ansicht angezeigt.

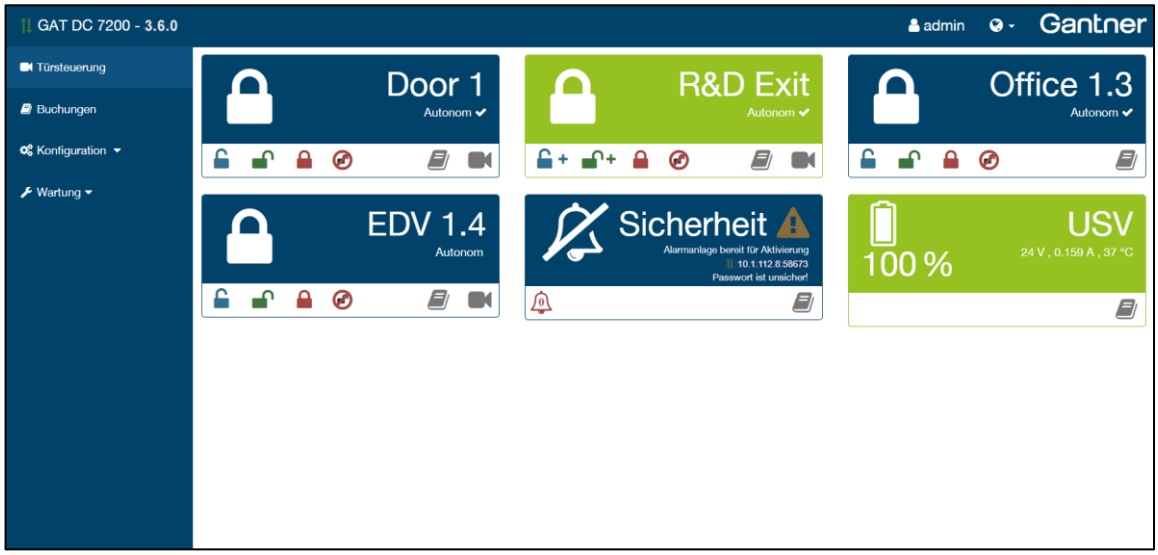
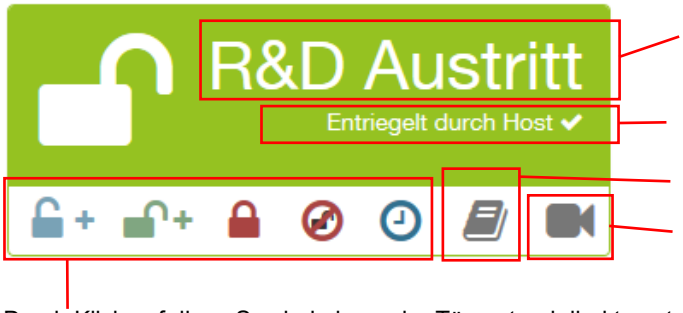


***Bild 6.11** – Konfiguration des GAT DC 7200 – Hauptfenster Web-Oberfläche*

Die folgenden Informationen werden bei jeder Tür angezeigt:



Der Name der Tür laut Türkonfiguration (siehe “6.4.7. Türkonfiguration”).

Information über den Türstatus.

Anzeige der Buchungen an der Tür.

Live-Anzeige der Videokamera (falls verwendet, siehe "6.4.9. Hardware Erweiterungen").

Durch Klick auf diese Symbole kann der Türzustand direkt gesteuert und Alarme bedient werden:

= entriegelt die Tür einmalig für das Öffnen ohne Datenträger. Nach Schließen ist die Tür wieder versperrt. Klick auf das "+" Symbol steuert zusätzlich das Sonderrelais an (Ausgang muss als Sonderrelais definiert sein).

= entriegelt die Tür durchgehend. Die Tür kann ohne Datenträger beliebig oft geöffnet und geschlossen werden. Klick auf das "+" Symbol steuert zusätzlich das Sonderrelais an (Ausgang muss als Sonderrelais definiert sein).

= versperrt die Tür durchgehend. Ein Zutritt ist auch mit gültigem Datenträger nicht möglich.

= Generell-Offen Funktion unterdrücken. Wenn die Tür mittels Generell-Offen Funktion generell entriegelt ist, wird sie hiermit versperrt, kann aber mittels gültigem Datenträger geöffnet werden.

= setzt die Tür auf autonome Steuerung zurück. Damit wird die Tür anhand der Berechtigungsdaten gesteuert.

= rücksetzen eines Alarms (z.B. Tür-zu-lange-offen), angezeigt durch einen roten Hintergrund.

Wenn eine Türrückmeldung konfiguriert ist, kann der Türzustand (offen, geschlossen) angezeigt werden. Für den Fall, dass ein Alarm an dieser Türe ansteht, wird dieser hier angezeigt. Weiter ist in der Live Statusanzeige ersichtlich, ob die Türe autonom über die Zutrittsberechtigung entscheidet und ob ein Leser verbunden ist.

Im Feld für die Sicherheitsanzeige ist ersichtlich, ob die Alarmanlage scharf oder unscharf ist bzw. scharf geschaltet werden kann.

Das Symbol signalisiert, dass die Verbindung zwischen PC und GAT DC 7200 sicher ist. Infos dazu finden Sie in den folgenden Kapiteln.

Wird statt diesem Symbol das Zeichen angezeigt, sind nicht alle Sicherheitseinstellungen optimal gesetzt (z. B. das Standard-Passwort ist noch vorhanden).

Sobald eine Verbindung zum PC hergestellt ist, wird die IP-Adresse des Host-Computers neben dem Symbol angezeigt.

6.4.3 USV Stromversorgung

Wenn eine USV (Notstromversorgung) am GAT DC 7200 angeschlossen ist, wird der Ladezustand der USV in der Live-Ansicht angezeigt. Die USV wird automatisch erkannt, wenn diese beim Start des Controllers an der „Sub“ Schnittstelle angeschlossen ist.

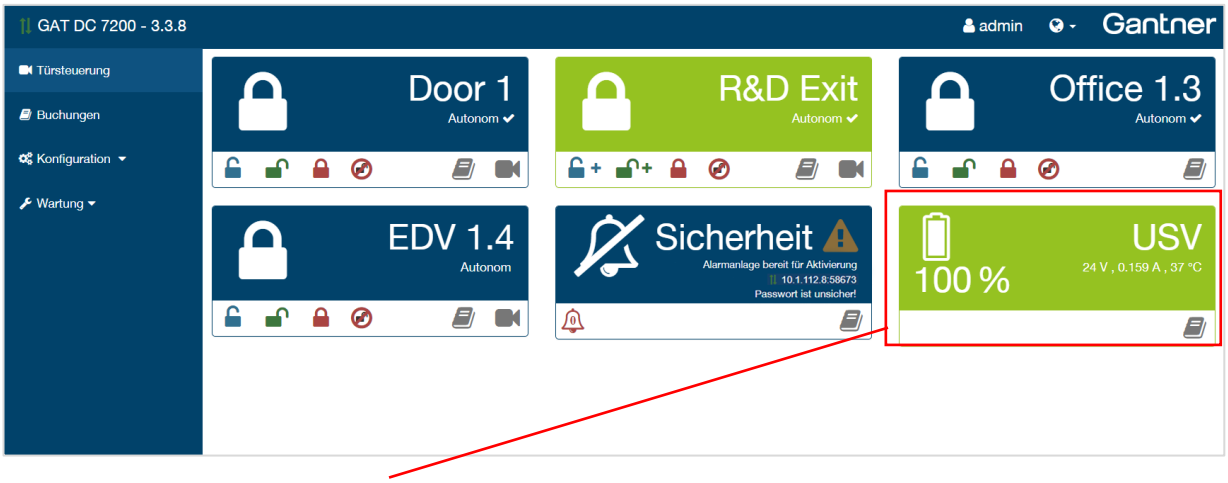


***Bild 6.12** – Web-Oberfläche – USV Ladeanzeige in der Live-Ansicht*

HINWEIS! Die gleichzeitige Verwendung der USV und anderer Komponenten an der SUB Schnittstelle ist nicht möglich.

6.4.4 Allgemeine Bemerkungen

Während der Konfiguration des GAT DC 7200 können zahlreiche Parameter verändert werden. Diese müssen im GAT DC 7200 gespeichert werden damit diese aktiv werden. Die Funktion zum Speichern bezieht sich immer auf einzelne Parametergruppen, die in einem Zusammenhang stehen. Wird ein Wert einer solchen Parametergruppe geändert, so wird die Schaltfläche "Save“ grün und das zugehörige Menü wird rot und mit einem Symbol markiert. Dadurch ist sofort ersichtlich, dass hier Änderungen gemacht wurden, die noch nicht gespeichert sind. Sobald die Werte gespeichert sind, wird die Schaltfläche "Save“ weiß und die Markierung im Menü verschwindet.

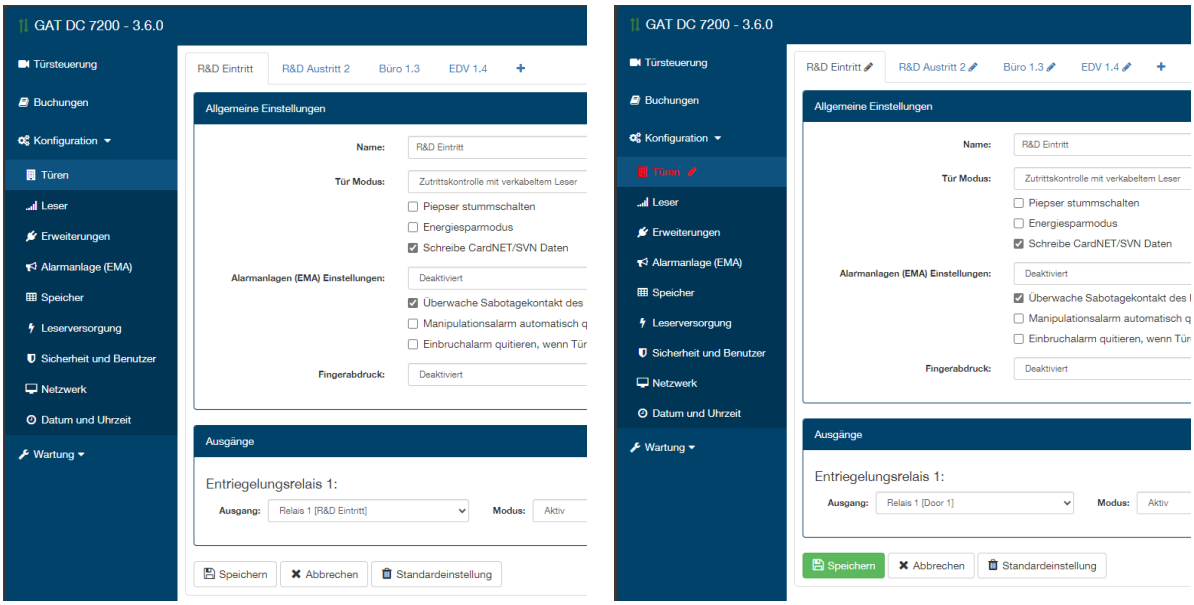


***Bild 6.13** – Web-Oberfläche – Anzeige von ungespeicherten Änderungen (rechts)*

Wurden Änderungen noch nicht gespeichert und Sie verlassen die Konfigurationsoberfläche des GAT DC 7200, so wird ein Warnhinweis ausgegeben.

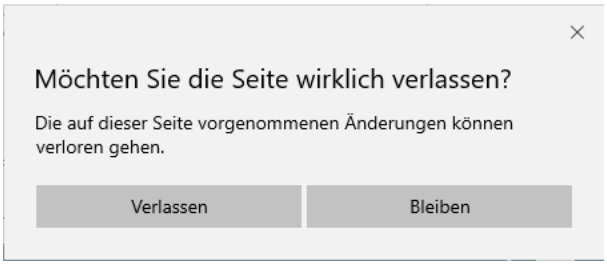


***Bild 6.14** – Web-Oberfläche – Warnhinweis für ungespeicherte Änderungen*

- ► Wenn Sie die Änderungen nicht verlieren möchten, wählen Sie "Bleiben" und speichern Sie die Änderungen.
- ► Wenn Sie die Seite mit "Verlassen" trotzdem schließen, so werden die Änderungen nicht gespeichert!

6.4.5 Benutzer

Links neben dem GANTNER Logo wird der angemeldete Benutzer angezeigt.

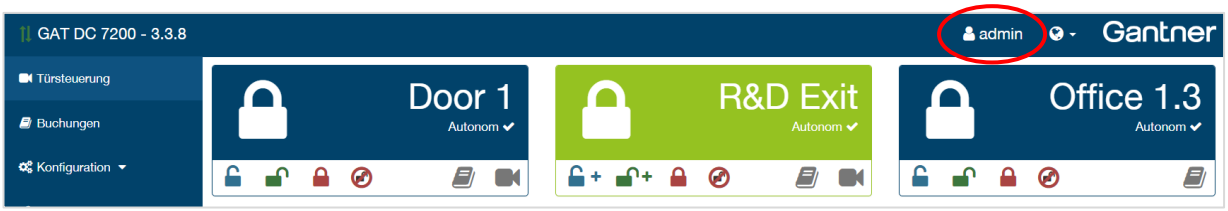


***Bild 6.15** – Web-Oberfläche – Benutzername des eingeloggten Benutzers*

► Durch Klicken auf den angezeigten Benutzer kann das Passwort des Benutzers geändert werden.

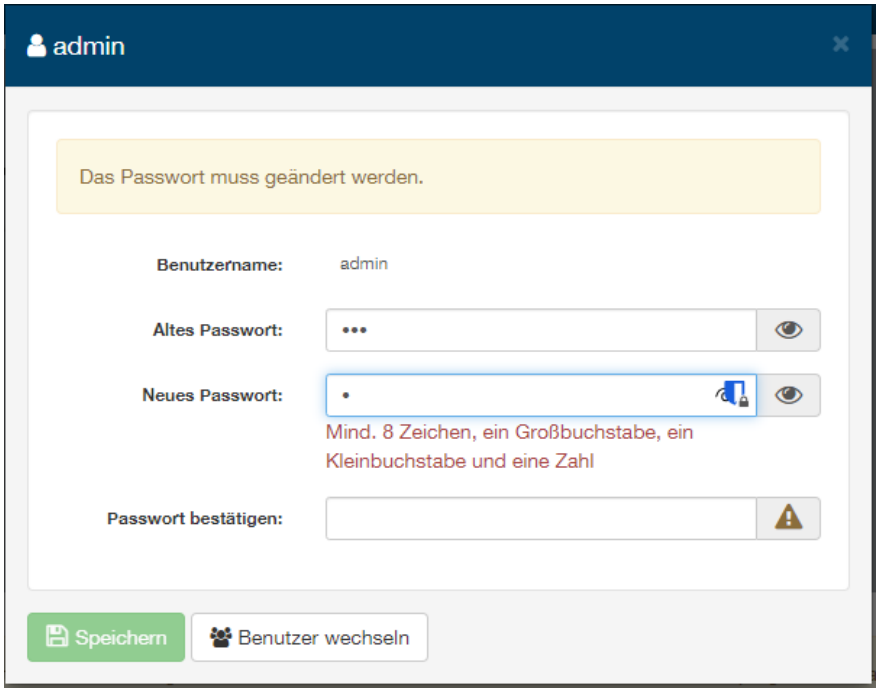


***Bild 6.16** – Web-Oberfläche – Benutzerpasswort ändern*

Hinweis: Nach der ersten Anmeldung in GAT DC 7200 wird im Passwort-Fenster der gelbe Hinweistext (siehe Bild) angezeigt, weil ab Firmware Version 3.6 es erforderlich ist, nach der ersten Anmeldung das Standard-Passwort in ein neues, geheimes Passwort zu ändern. Der Text wird nach erster Änderung des Passworts nicht mehr angezeigt.

► Geben Sie das aktuell verwendete Passwort des Benutzers im Feld "Altes Password" ein.
► Geben Sie dann ein neues, sicheres Passwort in den Feldern "Neues Passwort" und "Passwort bestätigen" ein. Das neue Passwort muss mind. 8 Zeichen lang sein und mind. einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten.

Über den Button "Benutzer wechseln" kann die Bedienung als anderer Benutzer mit eingeschränkten Berechtigungen vorgenommen werden. Dazu müssen die Benutzer in der Konfiguration jedoch zuerst freigeschaltet werden.

6.4.6 Sprache der Weboberfläche

In der Kopfzeile befindet sich ein Globus-Symbol, mit dem Sie die Anzeigesprache der GAT DC 7200 Konfigurationsoberfläche ändern können.

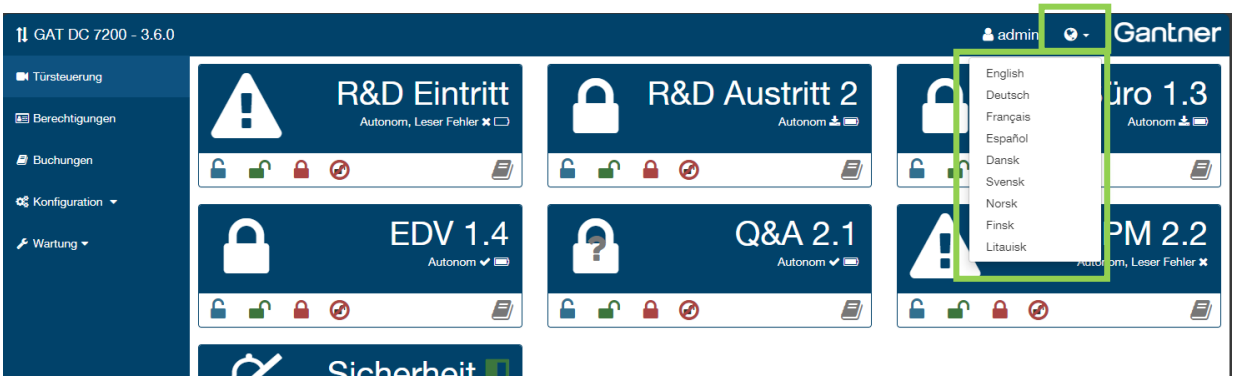


***Bild 6.17** – Web-Oberfläche – Ändern der Anzeigesprache*

► Nach Auswahl der gewünschten Anzeigesprache wird die Sprache sofort umgestellt. Manuell eingetragene Bezeichnungen wie die Bezeichnungen der Türen bleiben in der ursprünglichen Sprache.

6.4.7 Türkonfiguration

Bei Auslieferung des GAT DC 7200 sind 4 Türen (Door 1 bis Door 4) standardmäßig angelegt. Unter "Configuration" –> "Doors“ können diese auf die eigenen Anforderungen konfiguriert werden.

► Wählen Sie unter "Door 1" die für Ihren Zweck passenden Parameter aus

► Benennen Sie die Türe der Verwendung entsprechend (z. B. Haupteingang).

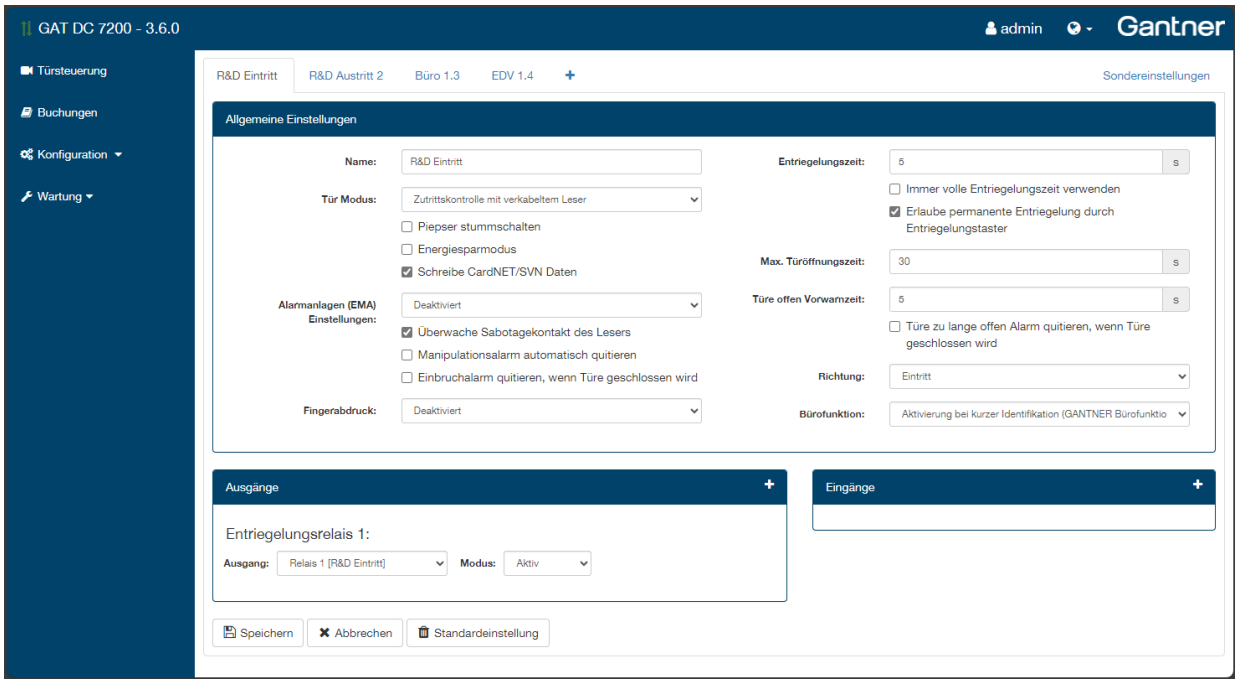


***Bild 6.18** – Web-Oberfläche – Türeinstellungen*

Allgemeine Einstellungen

- Tür Modus: Hier kann der Betriebsmodus der Türe eingestellt werden. Mögliche Werte sind:
  - Deaktiviert: Die Tür wird nicht verwendet, wenn dieser Modus gewählt ist.
  - Zutrittskontrolle mit verkabeltem Leser: Bei Verwendung eines verkabelten Lesers, wie z.B. ein GAT SR 73xx, GAT SLR 73xx, GAT SR 7xxx oder GR7 oder eines funkgesteuerten Schlosses GDL7m.
  - WiNET High Security: Mit dieser Einstellung für die Funkschlösser mit WiNET Funktion führt der GAT DC 7200 die Berechtigungsprüfung durch, sobald ein Datenträger an der Tür gelesen wird. Dies ist die sicherste Version von WiNET, aber es ist eine stabile Funkverbindung notwendig.
  - WiNET Comfort: Die Zutrittsberechtigungen werden bei erster Benutzung in den Funkschlösser mit WiNET Funktion gespeichert. Eine stabile Funkverbindung ist für weitere Berechtigungsprüfungen nicht notwendig. Aktualisierungen der Zutrittsberechtigungen werden alle 10 Minuten an die Schlösser gesendet.
  - Schließfachsteuerung: Wenn der Controller für die Steuerung einer Schließfachanlage (elektronische Schrankschlösser) verwendet wird, wählen Sie diese Option. Dafür wird eine passende Lizenz benötigt (siehe Bestellhinweise). Bei der Schließfachsteuerung können einer Person Berechtigungen

für ein oder mehrere Schließfächer zugewiesen werden. Nach einer Identifikation kann die Person durch Eingabe einer Schließfachnummer das gewünschte Fach geöffnet werden.
Ab der Firmware Version 3.5.0 ist eine optimierte Bedienung möglich, bei der das Schließfach nach einer Identifikation sofort geöffnet wird, wenn nur für ein Schließfach eine Berechtigung vorhanden ist. Sind mehrere Berechtigungen vorhanden, muss nach der Identifikation auch wieder die Schließfachnummer eingegeben werden.

- Anwesenheitsüberwachg: Mit dieser Einstellung wird die Tür geöffnet (bzw. das Relais angesteuert), wenn ein gültiger Datenträger gelesen wird. Die Ansteuerung bleibt so lange aufrecht, wie der Datenträger am Leser gehalten wird. Dieser Modus kann z.B. verwendet werden, um die Stromversorgung in einem Hotelzimmer bei Anwesenheit des Gastes zu aktivieren oder um eine Maschine nur einzuschalten, wenn der Bediener sich an der Maschine befindet.
- "GAT SMART.Lock": Die Modi "Zutrittskontrolle (GAT SMART.Lock)" und "Schließfachsteuerung (GAT SMART.Lock)" sind analog zu den gleichnamigen zuvor beschriebenen Modi. Der Unterschied liegt darin, dass GAT SMART.Lock Schrankschlösser angesteuert werden. In diesen Betriebsmodi wird die Entriegelungszeit automatisch auf das GAT SMART.Lock konfiguriert. Es sind keine Generell-Offen Funktionen möglich, um das GAT SMART.Lock nicht zu beschädigen.

- Piepser stummschalten: Wird diese Option aktiviert, wird der Piepser am Leser deaktiviert. Für Leser, die diese Funktion nicht unterstützen, ist die akustische Rückmeldung auch im Silent Mode zu hören.
- Energiesparmodus: Diese Option setzt die Tür während Perioden der Inaktivität in den Energiesparmodus, um die Stromaufnahme zu minimieren. Die LED's am Leser werden nach 1 Minute Inaktivität ausgeschaltet. Der Leser ist weiterhin aktiv. Die LEDs werden wieder eingeschaltet, wenn eine Aktion am Leser stattfindet oder sich der Status des Lesers ändert (z.B. Fernöffnung).
- Schreibe CardNET/SVN Daten: Wenn diese Option aktiviert ist, werden von diesem Türcontroller CardNET Daten und/oder SVN Daten (Salto Virtual Network) auf die Datenträger geschrieben und gelesen. D.h. beim Lesen eines Datenträgers an einem Leser schreibt der Türcontroller automatisch die betreffenden, von der Zutrittskontrollsoftware gesendeten, CardNET bzw. SVN Daten für den Datenträger auf diesen. Wenn die Option nicht aktiv ist, werden von diesem Türcontroller keine CardNET bzw. SVN Daten geschrieben.
  HINWEIS! Die CardNET/SVN Funktion muss für den Türcontroller aktiviert sein, ansonsten wird diese Option nicht angezeigt (siehe "6.4.8. Leserkonfiguration").
- Alarmanlagen (EMA) Einstellungen:
  Mit dieser Einstellung können Sie festlegen, ob die Einbruchmeldeanlage an dieser Türe scharf- und unscharf geschaltet werden kann. Es können bis zu 4 verschiedene Alarmsystem-Bereiche durch Auswahl aus der Liste kontrolliert werden. Ist die Beeinflussung der EMA konfiguriert, wird gleichzeitig bei scharfgeschalteter EMA der Zutritt verhindert, um einen Alarm durch eine Türöffnung bei gültiger Identifikation zu vermeiden. Weiter kann ausgewählt werden, ob der Zustand der EMA am Leserpunkt angezeigt werden soll. Die Anzeigefarben werden im Menü "Alarmanlage (EMA)" in der Web-Oberfläche eingestellt (siehe "6.4.10. Alarmsystemeinstellungen").
- Überwache Sabotagekontakt des Lesers:
  Der Sabotagekontakt eines Lesers registriert, wenn eine unautorisierte Aktion am Leser durchgeführt wird (z. B. Gehäuseaufbruch). Bei Aktivierung dieser Funktion wird der Leser auf diese Aktionen hin überwacht.
  HINWEIS! Der Sabotagekontakt ist nicht bei allen Lesern vorhanden.
- Manipulationsalarm automatisch quittieren:
  Ist diese Funktion aktiviert, dann wird ein Manipulationsalarm (z. B. zu lange Türöffnung oder Öffnung ohne Berechtigung) automatisch wieder deaktiviert, sobald der Grund für die

Auslösung des Alarms nicht mehr besteht (z. B. wenn die Türe nach zu langer Öffnung wieder geschlossen wird).

Wenn die Option nicht aktiviert ist, dann bleibt der Alarm bestehen, bis er manuell von einer befugten Stelle quittiert wird.

In zweiterem Fall würde ein mehrfaches Auftreten der Manipulation nicht erneut z. B. bei einem Leitstand übertragen, da der zuvor anstehende Alarm nicht verarbeitet wurde.

- Einbruchalarm quittieren, wenn Türe geschlossen wird:

  Ein Einbruchalarm kann z.B. durch unautorisierte Türöffnung/Aufbruch ausgelöst werden. Ist diese Option markiert, so kann ein ausgelöster Einbruchsalarm durch Schließen der Tür automatisch wieder gelöscht/quittiert werden. Der Alarm wird jedoch in den Buchungen protokolliert.

- Fingerabdruck: Hier kann festgelegt werden, ob Fingerabdrücke für die Verifikation oder für Identifikation verwendet werden sollen oder ob diese an der Türe nicht verwendet werden.

- Entriegelungszeit: Diese Zeit legt fest, wie lange das Schloss bei gültigem Zutritt entriegelt werden soll. Zusätzlich kann mit Aktivierung der Option "Immer volle Entriegelungszeit verwenden“ eingestellt werden, dass das Schloss die gesamte Entriegelungszeit angesteuert wird. Anderenfalls endet die Entriegelungszeit, sobald die Türe als offen erkannt wird.

- Erlaube permanente Entriegelung durch Entriegelungstaster:

  Diese Option ermöglicht es, die Tür durch ein externes Signal (z. B. Portiertaste) auf Dauer-offen zu stellen. Ist diese Funktion nicht aktiviert, ist die Öffnung durch dieses Signal nur für die Entriegelungszeit möglich. Für eine neuerliche Entriegelung muss das Signal zuerst abfallen, bevor eine neuerliche Entriegelung möglich ist.

- Max. Türöffnungszeit: Diese Zeit legt fest, wie lange eine Türe maximal offen sein darf, bis eine Signalisierung erfolgt. Die Signalisierung kann mit einem Relais Ausgang oder einer Benachrichtigung im Gebäudeleitstand realisiert werden. Die Signalisierung erfolgt dann für die mit "Türe offen Vorwarnzeit" eingestellte Zeitspanne. Wird innerhalb dieser Zeit die Türe nicht geschlossen, wird ein "Türe-zu-lange-offen Alarm" ausgelöst.

- Tür-zu-lange-offen Alarm quittieren, wenn Türe geschlossen wird:

  Wenn diese Option markiert ist, kann ein ausgelöster Tür-zu-lange-offen Alarm durch Schließen der Tür quittiert werden. Andernfalls bleibt der Alarm beim Schließen der Tür bestehen und muss in der Live Anzeige oder im Gebäudeleitstand manuell quittiert werden.

- Richtung: Hier können Sie wählen, ob es sich um einen Eintritt oder einen Austritt handelt. Diese Information wird in den Buchungen angezeigt.

- Bürofunktion: Ist die Bürofunktion für eine Tür in der GAT Matrix aktiviert (siehe Anleitung im GAT Matrix Handbuch), kann die Tür durch das Lesen eines gültigen Datenträgers dauerhaft entriegelt werden. Der Vorgang kann danach wiederholt werden, um die Bürounktion für die Tür zu deaktivieren und die Tür wieder in den zeitplangesteuerten Modus zu setzen.

  Wählen Sie im Menü aus, wie die Bürounktion aktiviert werden soll. Wählen Sie entweder die Aktivierung über eine kurze Identifikation (Standardeinstellung) oder die Aktivierung über eine lange Identifikation, d.h. der Datenträger muss mindestens 3 Sekunden lang gelesen werden.

Sie können die kurze oder lange Identifikation auch mit einer Freischaltung für Personen mit besonderer Berechtigung (auch "Sonderrechte" genannt) kombinieren, so dass nicht alle Personen die Bürounktion aktivieren können. Die Sonderrechte müssen für die jeweiligen Personen in GAT Matrix (über die Option "Sonderberechtigung für Bürofunktion") für jede Tür aktiviert und dem/den Controller(n) zugewiesen werden. Weitere Informationen finden Sie im GAT Matrix Handbuch.

Einstellungen "Ausgänge" und "Eingänge"

Hier können logische Signale und Zustände auf elektrische Signale umgesetzt werden.

Im GAT DC 7200 sind 6 digitale Optokopplereingänge und 6 Relaisausgänge integriert und es gibt unterschiedliche Funktionen (siehe Tabelle unten), die diese Ein-/Ausgänge ausführen können. Bei den Türeinstellungen kann für jede Tür jeder dieser Funktionen, falls gewünscht, ein Optokopplereingang bzw. Relaisausgang zugewiesen werden. Damit lässt sich das GAT DC 7200 exakt an den gewünschten Einsatzzweck anpassen.

Die Verwendung des gleichen Relais oder Optokopplers für verschiedene Türen ist möglich. So können z. B. Sammelalarme (Manipulationsalarm von allen Türen wird auf einem Relaiskontakt ausgegeben) oder eine Sammelsteuerung (ein Signal entriegelt mehrere Türen) einfach realisiert werden. Es ist jedoch darauf zu achten, dass sich manche Verwendungen gegenseitig ausschließen oder praktisch keinen Sinn machen. Solche Konfigurationen sind zu vermeiden.

***Bild 6.19** – Web-Oberfläche – Eingangs- und Ausgangseinstellungen*

Funktionen der Relaisausgänge

Für die nachfolgend beschriebenen Funktionen kann jeweils der Modus "Aktiv" oder "Passiv" gewählt werden. Damit kann die Ausführung der Funktionen der jeweiligen Relaisbeschaltung angepasst werden. Aktiv bedeutet, dass das Relais angesteuert (bestromt) wird, wenn die Funktion aktiv ist (z.B. im Fall des Entriegelungsrelais, wenn eine gültige Identifikation erfolgte und die Türe entriegelt werden soll). Passiv bedeutet, dass das Relais im Ruhezustand angesteuert (bestromt) ist, und wenn die betreffende Funktion aktiv ist, ist das Relais unbestromt.

Einstellung im GAT DC 7200	Bedeutung
Entriegelungsrelais X	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. 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. Wenn 2 oder mehrere Entriegelungsrelais definiert sind, kann für die Relais eine Verzögerungszeit in Sekunden eingegeben werden, um die Relais zeitversetzt zu aktivieren. Bei Eingabe von "0" wird das Relais zeitgleich mit dem ersten Entriegelungsrelais aktiviert.
Entriegelungsimpuls / Verriegelungsimpuls	Diese Funktionen werden verwendet, um ein kurzes Signal (Impuls) vom Relais zu senden, um ein Schloss zu ver- oder entriegeln. Diese Relais sind für Schlösser vorgesehen, bei denen ein solcher kurzer Impuls z. B. an einem Eingang des Steuergeräts zum Entriegeln und ein Impuls an einem anderen Eingang des Steuergeräts zum Beenden der Entriegelung gesendet werden muss. Die Zeit bei dieser Funktion bestimmt die Dauer der Aktivierung.
Sonderrelais	Wenn für eine Person an der Türe die Sonderberechtigung definiert ist, so ist diese Funktion bei einer gültigen Identifikation aktiv. Das Sonderrelais wird parallel zum Entriegelungsrelais mit angesteuert. Wie lange diese Funktion aktiv bleibt, kann mit der Zeitangabe neben der Funktion festgelegt werden.
Nicht berechtigt	Diese Funktion wird aktiviert, wenn eine Identifikation erfolgte, aber die Person bzw. der Datenträger nicht zutrittsberechtigt ist. Die Zeit bei dieser Funktion bestimmt die Dauer der Aktivierung.
Einbruchsalarm	Diese Funktion ist aktiv, wenn die Tür ohne Berechtigung geöffnet wird. Dazu muss der Türzustand mittels Optokopplereingang überwacht werden. Die Zeit bei dieser Funktion bestimmt, wie lange der Alarm aktiv bleibt. Bei einem Wert größer Null wird der Ausgang für die eingegebene Zeit aktiviert. Mit dem Wert "0" bleibt der Alarm so lange bestehen, bis der Alarm quittiert/zurückgesetzt wird.
Einbruchsalarm unterdrücken Relais	Dieses Relais 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).
Manipulationsalarm	Diese Funktion wird aktiviert, wenn das Gehäuse eines angeschlossenen Lesers unerlaubterweise geöffnet wird oder die Verbindung zwischen einem Leser und GAT DC 7200 getrennt wird. Die Zeit bei dieser Funktion bestimmt, wie lange der Ausgang aktiv bleibt. Bei einem Wert größer Null wird der Alarm für die eingegebene Zeit aktiviert. Mit dem Wert "0" bleibt der Alarm so lange bestehen, bis der Alarm quittiert/zurückgesetzt wird.

Bedrohungsalarm	Diese Funktion kann vom Benutzer aktiviert werden, wenn er sich bei der Identifikation bedroht oder genötigt fühlt, z. B. beim Betreten des Gebäudes. Je nach Konfiguration kann der Benutzer den Bedrohungsalarm unterschiedlich auslösen. Eine Möglichkeit ist die Eingabe eines Bedrohungs-PIN-Codes während des Zutritts anstelle des persönlichen PIN-Codes, eine andere Möglichkeit ist durch die Identifizierung mit dem definierten Bedrohungs-Fingerabdruck oder weiters ist auch das Drücken der F1-Taste am Leser GR7.2310 vor der Identifizierung möglich. Siehe Kapitel "6.4.10 Alarmsystemeinstellungen" für weitere Informationen. Die Zeit bei dieser Funktion bestimmt, wie lange das Relais aktiviert bleibt. Bei einem Wert größer Null wird der Ausgang für die eingegebene Zeit aktiviert. Mit dem Wert "0" bleibt der Alarm so lange bestehen, bis der Alarm quittiert/zurückgesetzt wird.
Türe zu lange offen Warnung	Wird ein Optokopplereingang als Türrückmeldung ("Türkontakt") definiert, so wird bei einem gültigen Zutritt die Öffnungszeit der Tür gemessen. Ist die Türe länger als die definierte Max. Türoffenzeit geöffnet, so wird diese Funktion aktiviert. Die Zeit bei dieser Funktion bestimmt, wie lange die Warnung angezeigt wird. Wird die Tür nach Ablauf dieser Zeit nicht geschlossen, wird ein Türe zu lange offen Alarm ausgelöst.
Türe zu lange offen Alarm	Diese Funktion wird aktiviert, d.h. der Türe zu lange offen Alarm ausgelöst, wenn die Tür nach einer gültigen Öffnung länger als die definierte Max. Türöffenzeit + der Türe zu lange offen Warnung (falls definiert, siehe voriger Punkt) geöffnet bleibt. Die Zeit bei dieser Funktion bestimmt, wie lang das Alarmrelais aktiviert bleibt. Bei einem Wert größer Null wird der Ausgang für die eingegebene Zeit aktiviert. Mit dem Wert "0" bleibt der Alarm so lange bestehen, bis der Alarm quittiert/zurückgesetzt wird.

***Tabelle 6.1** – Funktionen der digitalen Ausgänge des GAT DC 7200*

Funktionen der Optokopplereingänge

Für die nachfolgend beschriebenen Funktionen kann jeweils der Modus "Aktiv" oder "Passiv" gewählt werden. Damit kann die interne Verarbeitung der Funktionen der jeweiligen Beschaltung der Eingänge angepasst werden. Aktiv bedeutet, dass die betreffende Funktion aktiv ist, wenn der Eingang bestromt ist. Passiv bedeutet, dass die Funktion aktiv, wenn keine Bestromung am Eingang anliegt. Bei Bestromung ist die Funktion passiv.

Einstellung im GAT DC 7200	Bedeutung
Türkontakt	Über diesen Eingang wird dem Controller signalisiert, ob die Türe offen ist. 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 weder eine Identifikation noch eine Tasteröffnung oder Fernsteuerung per Kommando und wird über den Eingang dennoch eine Türöffnung gemeldet, so führt dies zu einem Einbruchsalarm (sofern nicht im Türzeitplan unterdrückt). Bei einer normalen Türöffnung wird über diesen Eingang auch die max. Türoffenhaltezeit überwacht (sofern nicht im Türzeitplan unterdrückt) und damit bei zu langer Türöffnung eine Türe-zu-lange-offen Warnung und/oder ein Türe-zu-lange-offen Alarm ausgelöst.
Entriegeln x	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. Wenn die Option "Erlaube permanente Entriegelung durch Entriegelungstaster" in den allgemeinen Türeinstellungen nicht aktiviert ist, so setzt sich die

	Entriegelungsdauer aus der Dauer des Signals an diesem Eingang plus der eingestellten Entriegelungszeit zusammen. Ist die Option aktiviert, so ist die Entriegelungsdauer so lange, wie das Signal am Eingang anliegt (z.B. so lange, wie die Taste am Eingang gedrückt bleibt).
Dauerhaft verriegeln	Ist diese Funktion aktiv, so ist auch mit gültiger Identifikation 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. Eine dauerhafte Verriegelung kann auch durch eine Alarmanlage mit Verwendung der Blockschlossfunktion erfolgen (siehe "6.4.10. Alarmsystemeinstellungen").
Sabotagekontakt	An diesem Eingang kann ein externer Sabotagekontakt, z. B. ein GR7.23xx Leser, der in einer GR7m.2001 Einbaudose montiert ist, zur Sabotage-/Aufbruchüberwachung angeschlossen werden. Der Sabotagekontakt muss entsprechend der Moduseinstellung Aktiv oder Passiv verschaltet werden, so dass die Sabotagefunktion bei Bestromung oder Stromunterbrechung entsprechend korrekt aktiviert wird.
Generell Offen unterdrücken	Wenn diese Funktion aktiv ist, wird ein gerade aktiver Generell Offen Plan deaktiviert, so dass die reguläre Zutrittsberechtigung gilt. Für einen Eintritt ist dann eine gültige Identifikation notwendig.

***Tabelle 6.2** – Funktionen der digitalen Eingänge des GAT DC 7200*

Sondereinstellungen (Verzögerungszeiten)

Mit der Registerkarte "Sondereinstellungen" im rechten oberen Eck des Fensters öffnen Sie zusätzliche Zeiteinstellungen für die Türen. Die hier getätigten Einstellungen gelten für alle im GAT DC 7200 angelegten Türen.

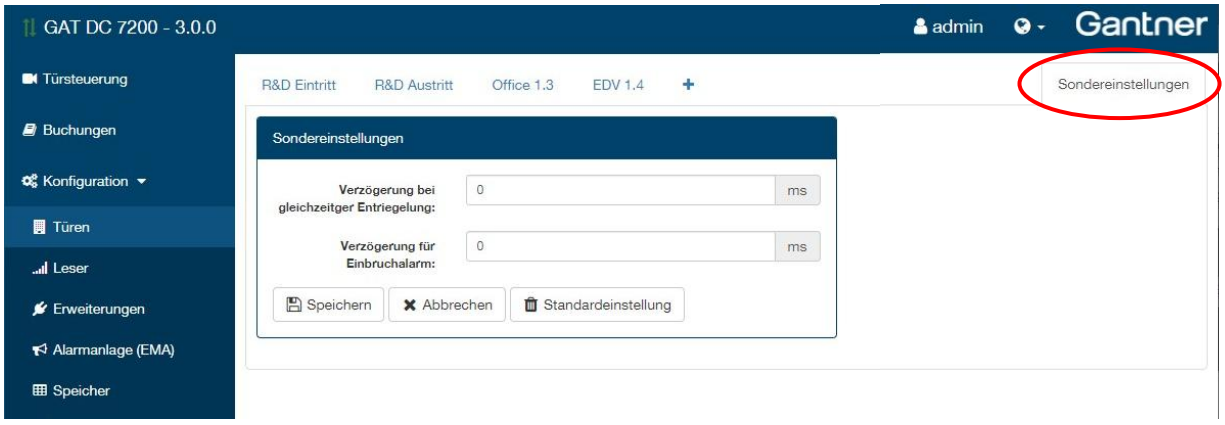


***Bild 6.20** – Web-Oberfläche – Sondereinstellungen für die Türen*

- Verzögerung bei gleichzeitiger Entriegelung: Wenn hier eine Zeit eingetragen ist (Wert in Millisekunden), werden bei einer Entriegelung von mehreren Türen, d.h. Ansteuerung von mehreren Relais, diese mit der hier eingetragenen Zeit versetzt angesteuert. Mit dem Wert "0" erfolgt die Ansteuerung gleichzeitig.
- Verzögerung für Einbruchalarm: Hier kann eine Zeit eingegeben werden (Wert in Millisekunden), um die bei einem Aufbruch der Schranktür ein Alarm zeitversetzt ausgelöst werden soll. Beim Wert "0" erfolgt die Auslösung ohne Verzögerung.

6.4.8 Leserkonfiguration

Die Konfiguration der Leser ist sehr universell, so dass zahlreiche Datenträger und Leser am GAT DC 7200 verwendet werden können. Am einfachsten ist die Konfiguration, wenn Leser der Serie GR7 und Datenträger mit einer GANTNER Codierung verwendet werden. Die Lesereinstellungen sind in verschiedenen Registerkarten unterteilt. Diese sind auf den folgenden Seiten beschrieben.

Registerkarte "Allgemein"

Folgende Einstellungen können auf der Registerkarte "Allgemein" definiert werden.

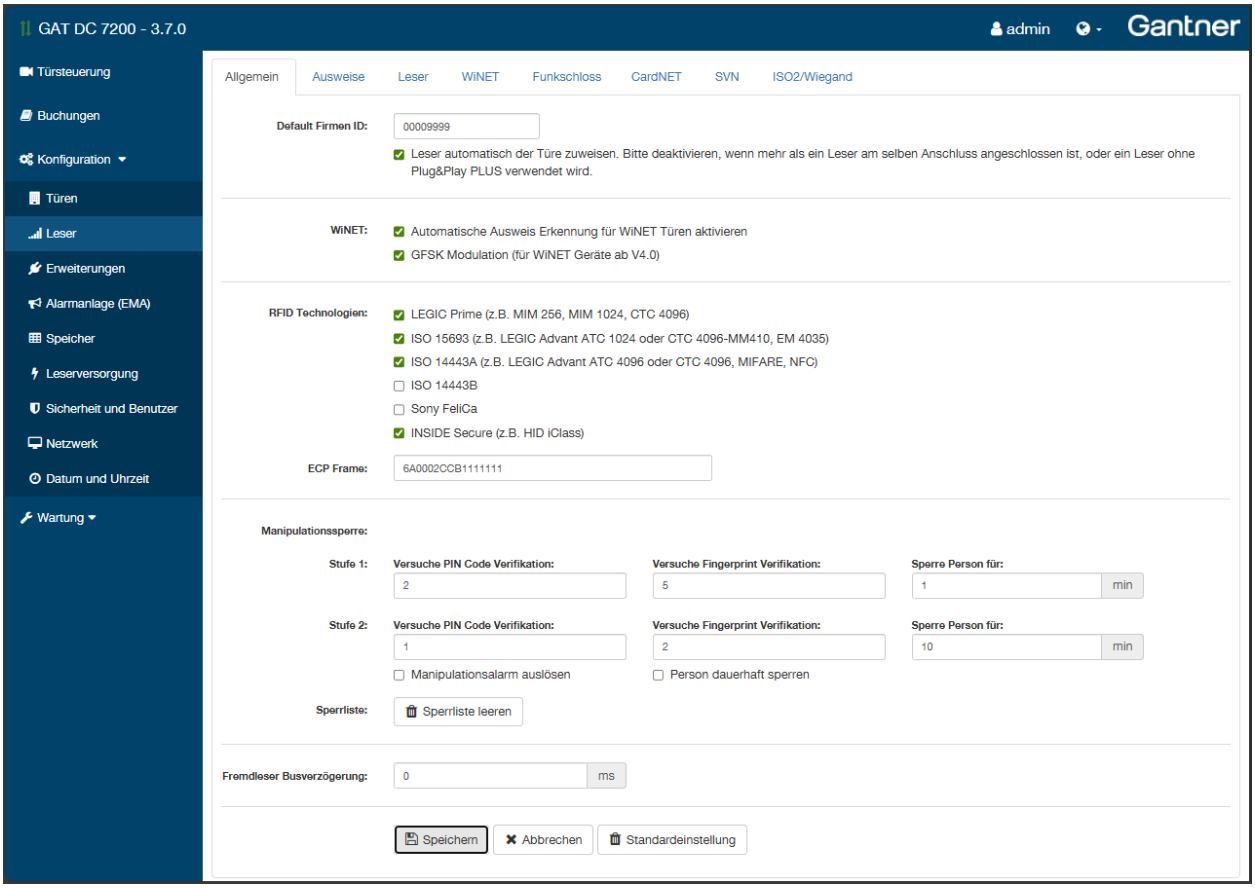


***Bild 6.21** – Web-Oberfläche – Grundeinstellungen für die Leser*

- Default Firmen ID: Tragen Sie in hier ihre Anlagennummer ein, die Sie mit der Lieferung der Ausweise erhalten haben.
- Leser automatisch der Tür zuweisen: Diese Option aktiviert die Plug&Play PLUS Funktion, die die automatische Erkennung von Lesern ermöglicht. Werden Leser verwendet, die diese Funktion nicht unterstützen oder werden mehrere Leser an einen Reader Port angeschlossen, so ist diese Funktion zu deaktivieren und die Zuweisung muss manuell erfolgen.
- WiNET: - "Automatische Ausweis Erkennung für WiNET Türen aktivieren":
  Wenn die Option aktiviert ist, prüft das WiNET Schloss regelmäßig, ob sich ein Datenträger im Lesefeld befindet. Andernfalls muss das Schloss zum Lesen erst aufgeweckt werden, so dass das Lesefeld aktiviert wird. Dies kann je nach Schloss auf unterschiedliche Weise erfolgen

(z.B. beim GAT DL 320 durch Drehen des Knopfs). Die Aktivierung dieser Option verkürzt die Batterielebensdauer, da mehr Energie benötigt wird.

- "GFSK Modulation":
Diese Funktion ist bei WiNET Schlössern ab Firmware Version 4.0 möglich. Diese Einstellung aktiviert die Kompatibilität zur RED (Radio Equipment Directive), die seit 2017 für Neuinstallationen gültig ist. Für Systeme, die vor dem Inkrafttreten der RED installiert wurden, kann auch der frühere Standard verwendet werden, in dem die Einstellung GFSK deaktivert wird.

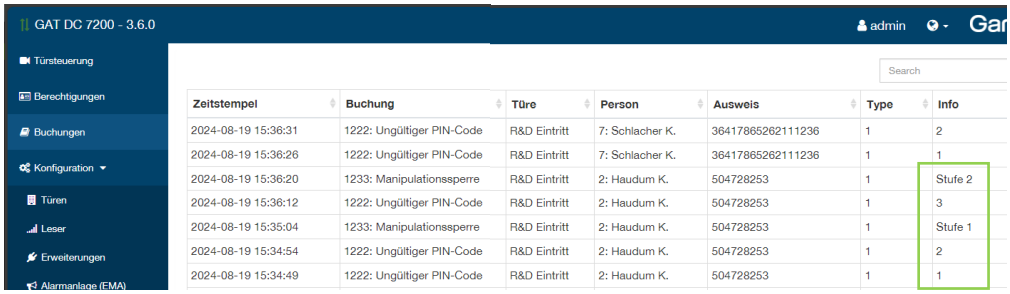
- RFID Technologien: Wählen Sie bitte die RFID-Technologien bzw. ISO Standards, die für Ihre Datenträger passend sind. Die Aktivierung und Deaktivierung der Technologien ist nur bei Lesern möglich, die diese Funktion unterstützen.

- ECP Frame: Diese Einstellung ist für die "Mobile Credential" Funktion notwendig. Das Feld wird nur angezeigt, wenn die Mobile Credential Lizenz aktiviert ist. Geben Sie dann hier die passende Nummer des ECP Frame ein. Eingabe erfolgt in Hexadezimalformat. Die Nummer erhalten Sie vom Lieferanten der Wallet Credentials.
Über den ECP Fram

- e kann unter anderem auch festgelegt werden, ob für die Verwendung des Mobile Credentials eine Verifikation (Gesicht, Fingerabdruck oder PIN-Code) erforderlich ist oder ob das Mobile Credential auch ohne Verifikation ("Express Mode") verwendet werden kann.
HINWEIS: Informationen zu den notwendigen Konfigurationsschritten für Mobile Credential finden Sie im Kapitel "6.5. Mobile Credential konfigurieren".

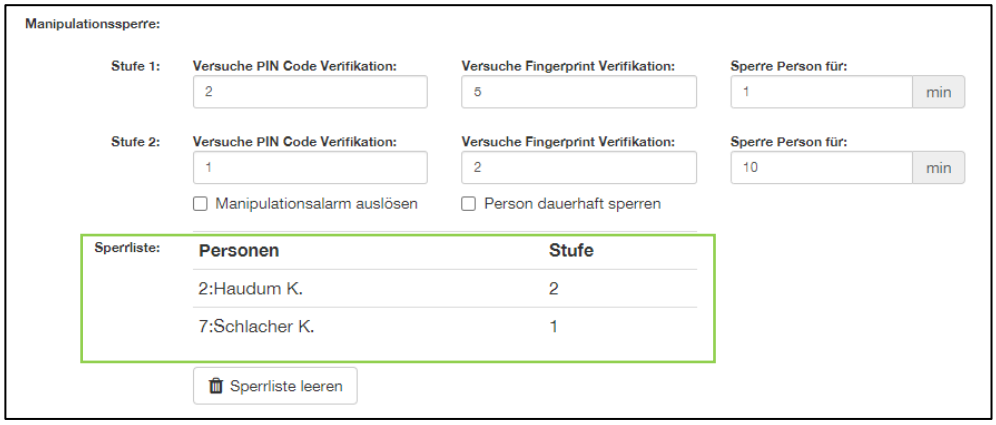
- Manipulationssperre: Hier können Sie einstellen, wieviel falsche Verifikationen mittels PIN-Code und Fingerabdruck zulässig sind, bevor der Zutritt für diese Person für die eingestellte Zeit unmöglich wird.

  Zuerst werden die Anzahl falscher PIN Code oder Fingerprint Verifikationen in der Zeile "Stufe 1" gezählt und bei Erreichen der eingegeben Werte wird die Person für die in dieser Zeile definierte Zeit bei allen Türen am Controller gesperrt.
  Nach Ablauf dieser Sperrzeit werden die Fehlversuche anhand der Eingaben in "Stufe 2" gezählt. Diese Werte können sich von Stufe 1 unterscheiden. Werden auch diese Anzahl Fehlversuche erreicht so wird die Person für die in Stufe 2 definierte Sperrzeit bei allen Türen am Controller gesperrt.
  Nach Ablauf dieser Zeit kann die Person erneut eine Identifikation mit Verifikation durchführen, sofern die Person nicht mit der Funktion "Person dauerhaft sperren" gesperrt wurde (siehe weiter unten).
  In den Buchungen werden falsche Verifikationen der Personen wie folgt angezeigt (im Beispiel für "Haudum K." zuerst 2 Fehlversuche (1, 2) und Stufe 1 aktiviert, nach 1 Minute dann eine erneute Fehlverifikation (3) und Stufe 2 ist aktiv).



Zeitstempel	Buchung	Türe	Person	Ausweis	Type	Info
2024-08-19 15:36:31	1222: Ungültiger PIN-Code	R&D Eintritt	7: Schlacher K.	36417865262111236	1	2
2024-08-19 15:36:26	1222: Ungültiger PIN-Code	R&D Eintritt	7: Schlacher K.	36417865262111236	1	1
2024-08-19 15:36:20	1233: Manipulationssperre	R&D Eintritt	2: Haudum K.	504728253	1	Stufe 2
2024-08-19 15:36:12	1222: Ungültiger PIN-Code	R&D Eintritt	2: Haudum K.	504728253	1	3
2024-08-19 15:35:04	1233: Manipulationssperre	R&D Eintritt	2: Haudum K.	504728253	1	Stufe 1
2024-08-19 15:34:54	1222: Ungültiger PIN-Code	R&D Eintritt	2: Haudum K.	504728253	1	2
2024-08-19 15:34:49	1222: Ungültiger PIN-Code	R&D Eintritt	2: Haudum K.	504728253	1	1

Haben Personen falsche Verifikationen durchgeführt, werden diese in der "Sperrliste" angezeigt. Die Stufe, in der sich die Personen befinden, werden hier ebenfalls angezeigt.

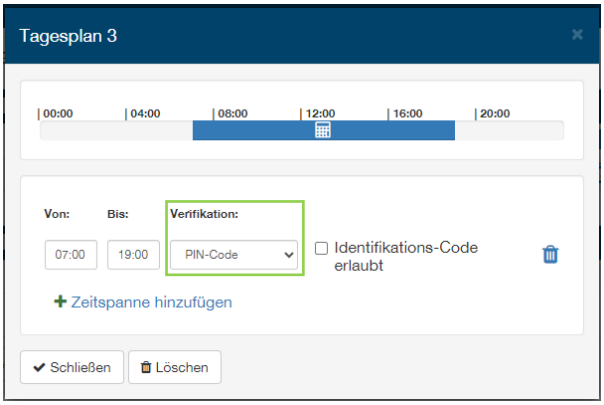


Mit Klick auf "Sperrliste leeren" können die gesperrten Personen freigegeben werden, bevor die eingestellte Sperrzeit von Stufe 2 abgelaufen ist.

Mit den 2 Optionen "Manipulationsalarm auslösen" und "Person dauerhaft sperren" können zusätzliche Funktionen aktiviert werden.

- "Manipulationsalarm auslösen": Nach Erreichen der Fehlversuche von Stufe 2 wird ein Signal an einem Relais, das für Manipulationsalarm definiert ist (siehe "6.4.7. Türkonfiguration"), ausgegeben. Damit kann z. B. eine Signalisierung vor Ort erfolgen.
- Person dauerhaft sperren: Wird diese Option markiert, so wird eine Person nach Überschreiten der Fehlversuche aus Schritt 2 für weitere Zutritte dauerhaft gesperrt. Diese Sperre bezieht sich auf den aktuellen Controller und die von ihm überwachten Türen. In der gesamten Zutrittsanlage ist die Person nicht gesperrt, d.h. an anderen Controllern ist weiterhin ein Zutrittsversuch möglich.

HINWEIS: Die Verifikations-Funktion kann bei einem Benutzer in den Tagesplänen aktiviert und eingestellt werden. Falls der Standalone Modus verwendet wird, ist das direkt am GAT DC 7200 im Menü "Berechtigungen" möglich (siehe "8.3. Berechtigungen verwalten").



- Fremdleser Busverzögerung: Die Standardeinstellung ist hier 0 ms. Diese Einstellung ist zu verwenden, wenn nur GANTNER Leser verwendet werden. Wenn Leser von anderen Herstellern angeschlossen werden, muss hier der korrekte Wert für die Verzögerung der Kommunikation auf der Busverbindung angegeben werden (siehe Angaben des Leserherstellers).

Registerkarte "Ausweise"

Tragen sie auf der Registerkarte "Ausweise" die Einstellungen der verwendeten Datenträger ein.

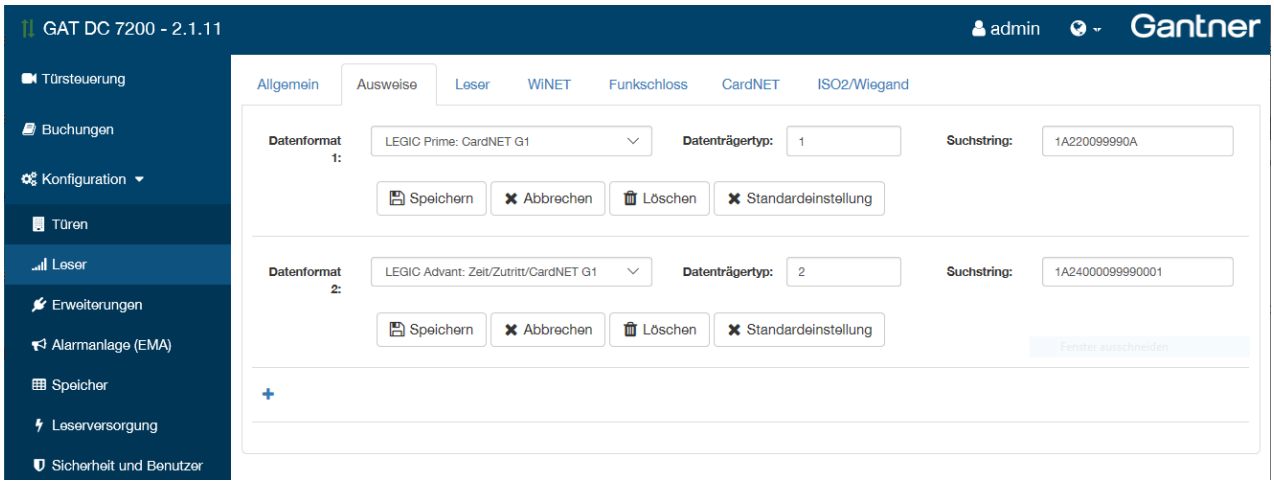


***Bild 6.22** – Web-Oberfläche – Datenträger Einstellungen für die Leser*

Für häufig verwendete Datenträger Codierungen sind einfache Einstellungen vorhanden und einfache Defaults werden automatisch vorgeschlagen. Ändern Sie diese nur ab, wenn Sie die Bedeutung kennen. Anderenfalls wenden Sie sich bitte an Ihren Lieferanten oder einen Spezialisten von GANTNER Electronic GmbH.

Kundenspezifische Ausweiscodierungen können in vielen Fällen ebenfalls verwendet werden, wenn die Informationen zur Codierung vorliegen. Hier ist es aber bevor das Projekt realisiert wird notwendig, die Datenträger auf Verwendbarkeit zu prüfen.

Eine einfach anzuwendende Methode ist die Verwendung der Unikatsnummer von Datenträgern. Dies können Sie durch Auswahl von "Unikatsnummer" oder "Unikatsnummer: Kundenspezifisch" einstellen. Dabei ist zu beachten, dass die Sicherheit der Ausweise nicht so hoch ist, wie dies bei codierten Ausweisen der Fall ist.

Für die Verwendung von Mobile Credentials müssen hier ebenfalls die Ausweisinformationen für das Datenformat "LEGIC Connect: Apple Wallet" und/oder "LEGIC Connect: Google Wallet" eingetragen werden. Die "Einstellungen" müssen passend für die Anlage gesetzt werden. Sie erhalten diese Information von ihrem Vertriebspartner.

***Hinweis:** Wenn die VCP Datei aus den Lesern gelöscht wird (siehe nächster Abschnitt "Registerkarte "Leser""), dann bleiben die Einstellungen hier bestehen (für eine eventuelle spätere Wiederverwendung), allerdings wird das Feld "Datenformat" gelöscht, so dass dieses Ausweisformat aktuell nicht mehr verwendet werden kann.*

Registerkarte "Leser"

Hier werden die durch Plug&Play PLUS erkannten und zugewiesenen Leser dargestellt. Beachten Sie, dass Leser vom Typ GAT SR 380 am GAT DC 7200 nicht verwendet werden können!

HINWEIS: Bitte beachten Sie, dass für GANTNER SVN die GAT Authorization Tag 400 BA benötigt wird.

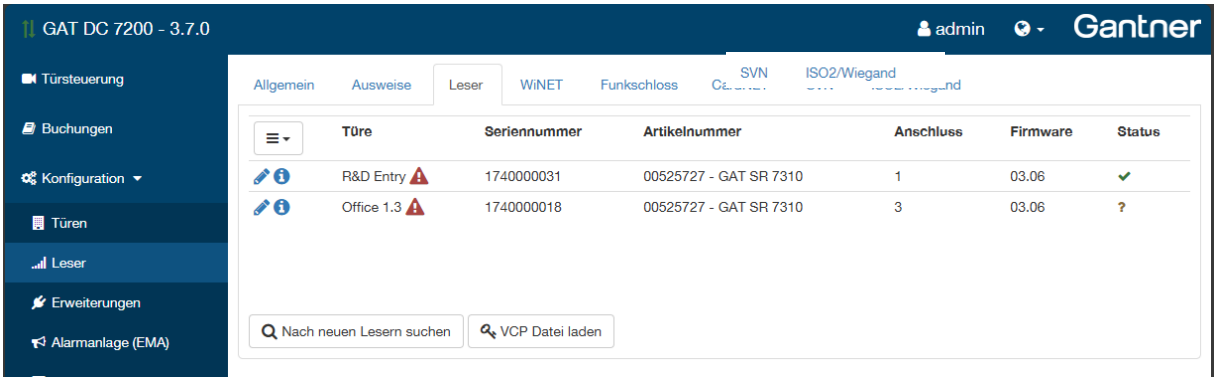


***Bild 6.23** – Web-Oberfläche – Übersicht der angeschlossenen Leser*

► Ist Plug&Play PLUS nicht aktiviert, können die Leser mit "Nach neuen Lesern suchen" manuell gesucht und dann den Türen zugewiesen werden.

Leser initialisieren für CardNET Funktion:
Leser, die für die CardNET Funktion verwendet werden, müssen einmalig initialisiert werden. Dies ist notwendig, damit die Zutrittsberechtigungen vom Leser auf die Datenträger geschrieben werden können.

► Zur Initialisierung eines Lesers halten sie den Initialisierungsdatenträger für Ihre Anlage (GAT Authorisation Tag 400 B oder BA) an den Leser, bis die Initialisierung abgeschlossen ist (ca. 15 Sekunden).
  - Während der Initialisierung blinkt die Leuchtanzeige abwechselnd rot und grün.

► Die Initialisierung der Leser mit einem GAT Authorisation Tag 400 BA ist auch für MIFARE DESFire Systeme und für GANTNER SVN notwendig.

► Um festzustellen, ob ein Leser initialisiert ist, klicken Sie auf das "i" Symbol bei einem Leser.
  - Es öffnet sich folgendes Fenster.

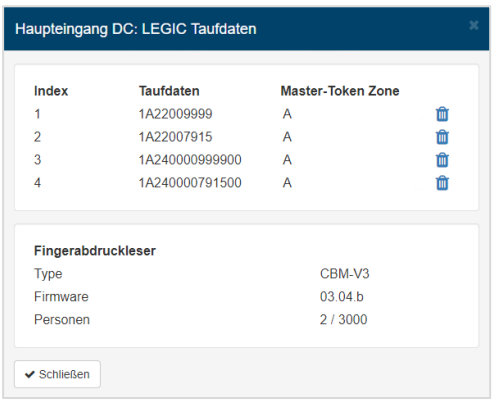


***Bild 6.24** – Web-Oberfläche – Leserinformationen anzeigen*

  - Wenn der Leser initialisiert ist, werden im oberen Bereich die Initialisierungsdaten ("Taufdaten") angezeigt.

- Die in der Spalte "Master-Token Zone" angezeigten Informationen sind für Installationen relevant, die das LEGIC Master-Token System verwenden. Die verschiedenen Zonen werden je nach verwendetem Datenträger eingestellt, was zur langfristigen Nutzung des Zutrittskontrollsystems beiträgt (weitere Informationen finden Sie auf der LEGIC Website).

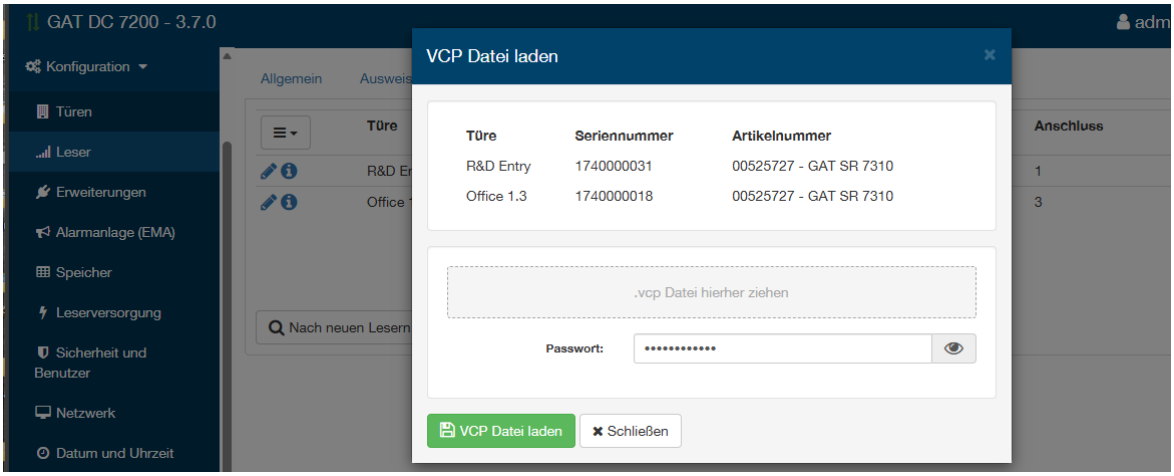
► Falls gewünscht, können Sie die Initialisierungsdaten (Taufdaten) mit Klick auf das Symbol löschen.

- Der Abschnitt "Fingerabdruckleser" wird nur angezeigt, wenn ein Fingerabdruckleser am Leser verwendet wird. Hier sehen Sie den Typ des Fingerabdrucklesers, die installierte Firmware und die Anzahl erfasster und max. möglicher Personen (Fingerabdrücke).

VCP Datei laden (für Mobile Credential):
Für die Mobile Credential Funktion ist es notwendig, eine VCP Datei in die angeschlossenen Leser zu laden. Die Datei enthält bestimmte LEGIC-Konfigurationsparameter, wodurch bei diesen Lesern die Verwendung von Mobile Credential ermöglicht wird. Siehe auch "6.5. Mobile Credential konfigurieren". Die VCP Datei erhalten Sie von ihrem Lieferanten der Wallet Credentials. Für die GR7 und S(L)R 73xx Leser sind VCP's für SM-4xxx Chips erforderlich.
Aus Sicherheitsgründen ist für das Laden und Aktivieren der VCP Datei ein Passwort notwendig.

► Klicken Sie auf die Schaltfläche "VCP Datei laden".

- Es wird ein Pop-up-Fenster geöffnet.

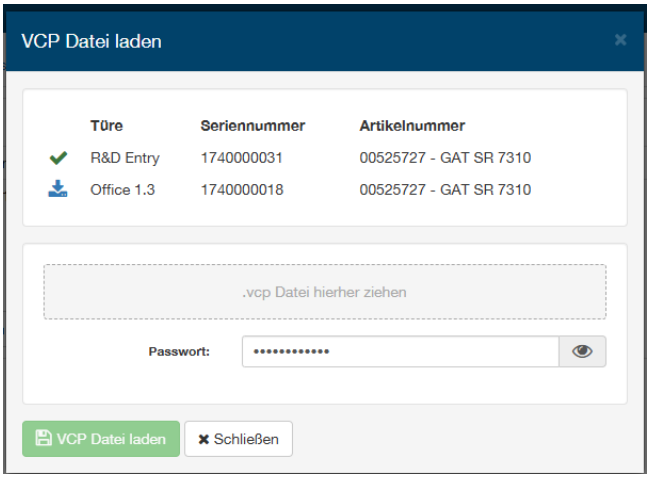


► Ziehen Sie die VCP Datei (Dateiendung .vcp) in das hier gekennzeichnete Feld.

► Geben Sie das passende Passwort in das Feld "Passwort" ein.

► Klicken Sie auf "VCP Datei laden".

- Die Datei wird in die angezeigten Leser geladen und aktiviert. Wenn die Datei erfolgreich aktiviert wurde, sehen Sie beim betreffenden Leser ein grünes Haken-Symbol.



HINWEIS: Um ein geladenes VCP von einem Leser zu entfernen, muss ein "Remove VCP" geladen werden. Dies erfolgt ebenfalls auf dieser Seite. Nähere Informationen dazu siehe "6.5.1. VCP von einem Leser löschen".

Registerkarte "WiNET"

Bei Verwendung von batteriebetriebenen Schlössern im WiNET Mode werden die erkannten Access Points (z. B. GAT DL 091 RS485) und die Schlösser, die sich in Funkreichweite befinden, dargestellt. Die Schlösser können anhand ihrer Seriennummern den Türen zugewiesen werden.

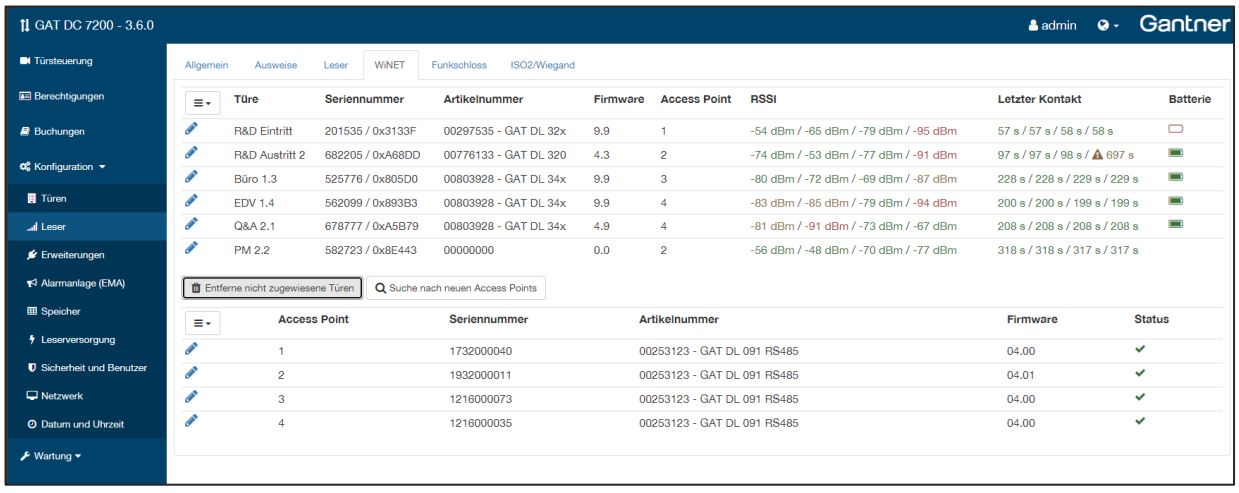
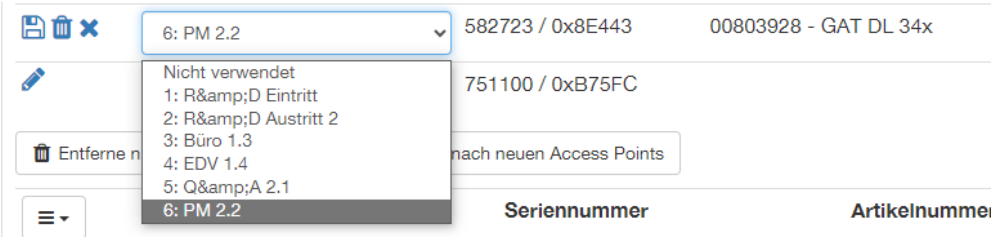


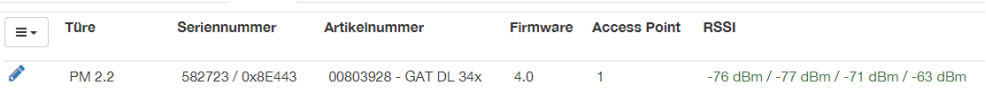
***Bild 6.25** – Web-Oberfläche – WiNET Einstellungen*

- Türen, Schlösser: Wenn Access Points verbunden sind, sehen Sie in der oberen Liste die erkannten Schlösser mit Seriennummer und Artikelnummer + Typenbezeichnung. Um ein Schloss einer im GAT DC 7200 konfigurierten Tür zuzuweisen (siehe voriges Kapitel), klicken Sie auf das Editieren-Symbol des Schlosses, wählen Sie die gewünschte Tür aus der Liste aus und klicken Sie auf das Speichern Symbol.



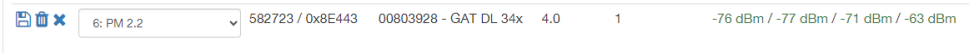
HINWEIS: Sollte hinter einem Schlossnamen ein Ausrufezeichen angezeigt werden (z. B. Büro 1.3), so ist möglicherweise an der Tür, die dem Schloss zugeordnet ist, ein weiterer Leser zugeordnet (Registerkarte "Leser").

HINWEIS: Es kann vorkommen, dass die Signalstärke eines Access Points, mit dem ein Schloss verbunden ist, schwächer wird als das Signal eines anderen Access Points. In diesem Fall wird beim Editieren und anschließendem Speichern des Schlosses automatisch auf den Access Point mit der besten Signalstärke gewechselt. Im folgenden Beispiel ist das Schloss mit Seriennummer 582723 mit Access Point 1 verbunden, aber das Signal von Access Point 4 ist stärker (-78 dBm bei AP1 und -63 dBm bei AP4) …



Türe	Seriennummer	Artikelnummer	Firmware	Access Point	RSSI
PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	1	-76 dBm / -77 dBm / -71 dBm / -63 dBm

… nach dem Editieren und Speichern …



6: PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	1	-76 dBm / -77 dBm / -71 dBm / -63 dBm

… ist das Schloss dem Access Point 4 zugewiesen mit -63 dBm Signalstärke.

PM 2.2	582723 / 0x8E443	00803928 - GAT DL 34x	4.0	4	-76 dBm / -77 dBm / -71 dBm / -63 dBm

Dieser manuelle Eingriff wird nur benötigt, wenn zwei Access Points eine Verbindung zum Schloss haben und ein Wechsel zum besseren Access Point nicht automatisch erfolgen kann.

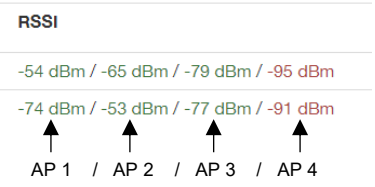
- RSSI: Über die Werte in der Spalte "RSSI" (grün – orange – rot) wird dargestellt, wie gut die Funkverbindung bei der letzten Verbindung es jeweiligen Schlosses mit den Access Points ist. Dies ermöglicht bei der Inbetriebnahme die passende Platzierung der Access Points zu definieren. Bitte beachten Sie, dass das Schloss wenn es nicht betätigt wird ca. alle 15 Minuten einen Status "betriebsbereit" versendet. Da kein Datenträger oder Person vor dem Schloss steht, werden die RSSI Werte hier besser angezeigt. Wenn eine Person und Datenträger vor dem Schloss steht, werden die RSSI Werte schlechter, daher muss bei der Projektierung gezielt darauf geachtet werden.

= Gute Funkverbindung.

= Schwache Funkverbindung. Positionieren Sie den Access Point wenn möglich neu.

= Schlechte Funkverbindung. Der Access Point muss neu positioniert werden.

Wenn mehrere Access Points angeschlossen sind, werden dessen Werte durch Querstriche "/" getrennt hintereinander angezeigt (von links nach rechts Access Point 1, 2, 3, …).



- Letzter Kontakt: In dieser Spalte wird angezeigt, wie lange das Schloss nicht mehr mit dem GAT DC 7200 kommuniziert hat.
- Batterie: Der Batteriezustand des Schlosses wird in dieser Spalte angezeigt.
   = Batteriezustand schwach. Die Batterie sollte bald gewechselt werden.
   = Batterie ist leer. Die Batterie muss gewechselt werden.
- Weitere Informationen in der Türliste:
  Mit dem Symbol ≡▾ können weitere Informationen für die Türen eingeblendet werden:
  - Hardware: Zeigt die Hardwareversion des Türschlosses an.
  - LQI: Der LQI Wert ist ein Maß für die Übertragungsqualität eines Funkschlosses in Werten von 0 (schlecht) bis 255 (sehr gut).
  - Client RSSI: Analog zu den "RSSI" Werten sind dies die Empfangsstärken zwischen Access Point und den Funkschlössern. Der Client-Wert gibt den Empfangswert vom Access Point aus Sicht des Funkschlosses an.
  - Client LQI: Analog zu den "LQI" Werten sind dies die Übertragungsqualitäten der Datenpakete von 0 bis 255. Der Client-Wert gibt jedoch den Wert Access Point aus Sicht der Funkschlösser an.
- Access Point: Am GAT DC 7200 können maximal 4 Access Points GAT DL 091 RS485 angeschlossen werden. Diese werden in der unteren Liste angezeigt.

  Mit Klick auf "Suche nach neuen Access Points" wird nach neu angeschlossenen Access Points gesucht und alle erkannten Access Points werden in der Liste mit fortlaufender Nummerierung angezeigt. Diese Nummern werden dann in der Spalte "Access Point" bei der Türenliste angezeigt und zeigen an, mit welchem Access Point eine Tür verbunden ist bzw. kommuniziert.

  Für jeden Access Point sehen Sie in der Liste neben der Nummer auch die Seriennummer, die Typenbezeichnung bzw. Artikelnummer, die Firmwareversion und der Online-Status.
- Weitere Informationen in der Access Point Liste:
  Mit dem Symbol ≡▾ können weitere Informationen für die Access Points eingeblendet werden:
  - Adresse: Die Netzwerkadresse des Access Point
  - Hardware: Die Hardware Versionsnummer des Access Points.

ACHTUNG! Wird ein Access Point erweitert oder ein defekter Access Point durch einen neuen ersetzt, muss nach dem Austausch oder Erweiterung bei allen angeschlossenen Schlössern die WiNET Verbindung getrennt und erneut verbunden werden. Beim WiNET Verbindungsaufbau werden die zuvor Konfigurierten Access Point einmalig in die Schlösser übertragen.

Registerkarte "Funkschloss"

Information über die Funkschlösser (z. B. GDL7m), die mit den Lesern gepaart sind, wird hier angezeigt.

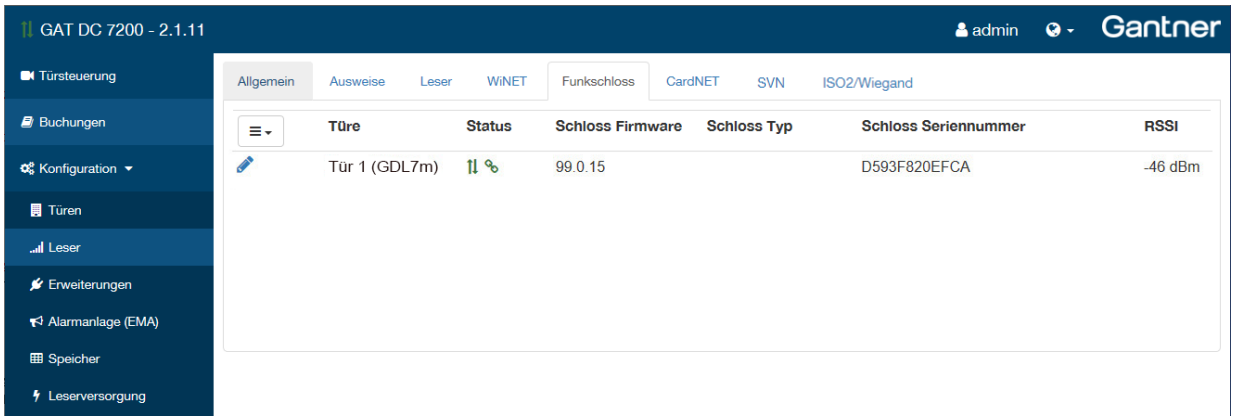


***Bild 6.26** – Web-Oberfläche – Funkschloss Einstellungen*

- Bearbeitensymbol: Das Symbol zum Bearbeiten in der ersten Spalte erlaubt es, die Paarung zwischen dem Funkschloss und dem Leser aufzuheben. Klicken Sie auf das Symbol und danach auf das rote Schloss Symbol , um die Paarung aufzuheben.

  HINWEIS! Drücken Sie das Symbol zur Trennung der Paarung nur, wenn dies unbedingt notwendig ist. Zur Info lesen Sie dazu bitte das Handbuch des Funkschlosses.

- Türe: Dieses Feld zeigt den Namen der Tür, zu der das Funkschloss zugewiesen ist.

- Status: Hier wird eine der folgenden möglichen Statussignale angezeigt:

  Das grüne Pfeilsymbol zeigt an, dass die Kommunikation zwischen dem Funkschloss und Leser aktiv ist. Das grüne Schloss-Symbol zeigt an, dass das Funkschloss mit dem Leser gepaart ist.

  Das rote Achtung-Symbol zeigt an, dass die Kommunikation zwischen dem Funkschloss und dem Leser inaktiv ist (möglicherweise außer Reichweite). Das grüne Schloss-Symbol zeigt an, dass das Funkschloss weiterhin mit dem Leser gepaart ist.

  Ein rotes Schloss-Symbol bedeutet, dass die Paarung und die Kommunikation zwischen dem Funkschloss und dem Leser inaktiv sind.

- Schloss Firmware: Die aktuelle Firmware Version des Funkschlosses.

- Schloss Seriennummer: Die Seriennummer des Funkschlosses.

- RSSI: Der Wert der "RSSI" Spalte zeigt die Stärke der Funkverbindung zwischen dem Funkschloss und dem Leser an. Ein Wert unterhalb von -90 dBm (z.B., -100 dBm) bedeutet eine schlechte Verbindung und mögliche Kommunikationsprobleme. Wenn der Leser innerhalb der empfohlenen 2 Meter Abstand installiert ist, sollte die Signalstärke gut sein.

Registerkarte "CardNET"

Auf dieser Registerkarte kann das CardNET System am GAT DC 7200 aktiviert werden. Dadurch werden Berechtigungen auf Datenträger geschrieben, die dann an batteriebetriebenen Schlössern für die Berechtigungsprüfung verwendet werden.

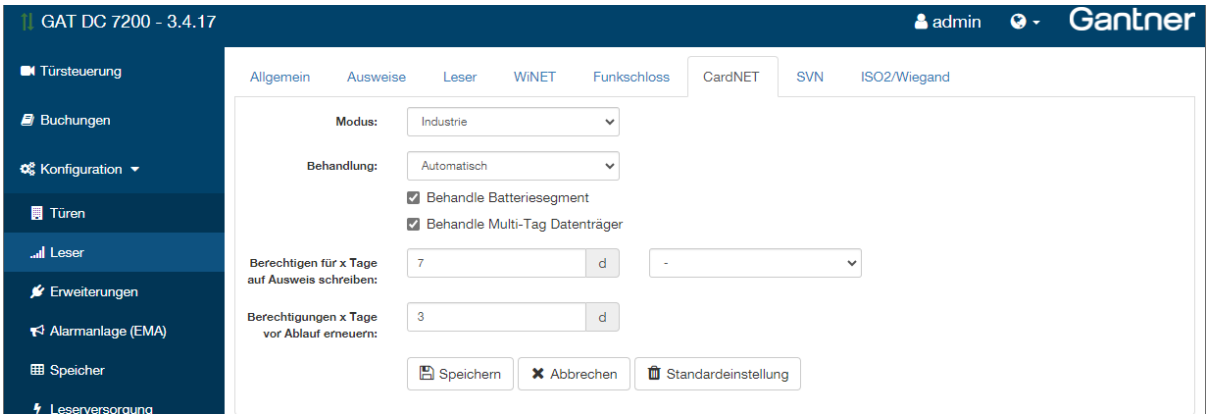


***Bild 6.27** – Web-Oberfläche – CardNET Einstellungen*

Die folgenden Einstellungen sind möglich.

- Modus: Definiert den Betriebsmodus des CardNET Systems. Wählen Sie eine der folgenden Optionen:
  - Industrie: Wählen Sie diese Einstellung für CardNET G2 Datenträger oder für CardNET G1 Datenträger, die mit einem Segment mit Namen “Offline 1 (0A)" codiert sind, was auch der Standard für die meisten Datenträger ist.
  - Hotel: Wählen Sie diesen Modus, wenn der CardNET G1 Datenträger mit einem Segment "Hotel (0C)" codiert ist. Der Modus "Hotel" ist nur für Datenträger möglich, die als CardNET G1 codiert sind
  - Deaktiviert: Wählen Sie diesen Modus, wenn CardNET G1 nicht verwendet wird.
- Behandlung: Diese Einstellung legt fest, wie die CardNET Datenträger auf die Datenträger geschrieben werden.
  - Automatisch: Die CardNET Daten werden automatisch geschrieben, wenn ein Datenträger gelesen wird. Voraussetzung ist, dass das Schreiben bei der Tür aktiviert ist (siehe "6.4.7. Türkonfiguration") und dass laut Zeiteinstellungen die Daten auch geschrieben/erneuert werden sollen (siehe Einstellung weiter unten).
  - Manuell: Es muss zum Schreiben der CardNET Daten auf einen Datenträger zuerst am Leser die "Kommen" Taste gedrückt und danach der Datenträger ans Lesefeld gehalten werden. Mit Druck auf die "Gehen" Taste am Leser können die CardNET Daten wieder vom Datenträger gelöscht werden.
  - Automatisch und manuell: Das Schreiben der CardNET Daten erfolgt automatisch beim Lesen eines Datenträgers. Mit Druck auf die "Gehen" Taste können die CardNET Daten wieder vom Datenträger gelöscht werden.
- Behandle Batteriesegment: Markieren Sie diese Option, um den Batteriestatus aus den Schlössern auszulesen und an eine übergeordnete Software weiterzuleiten.
- Behandle Multi-Tag Datenträger: Markieren Sie diese Option, um Datenträger mit mehreren Technologien beschreiben zu können.

  HINWEIS! Verwenden Sie diese Funktion nicht, wenn verschiedene Datenträgertypen verwendet werden, die aber nicht auf einem Datenträger kombiniert sind.
- Berechtigung für x Tage auf Ausweis schreiben/x Tage vor Ablauf erneuern: Legen Sie hier fest, für wie lange die Berechtigungen erstellt werden sollen und wann diese erneuert werden sollen.

Registerkarte "SVN"

SALTO Produkte verwenden für den Transport der Zutrittsberechtigungen die Salto Virtual Network (SVN) Technologie. Zusammen mit Datenträgern mit einer GANTNER-Codierung entsteht die "GANTNER SVN" Technik, die vergleichbar mit der bekannten CardNET Technik ist. Somit können Datenträger und Schlösser von SALTO und GANTNER im gemeinsamen System genutzt werden. Auf der Registerkarte "SVN" kann die GANTNER SVN Funktion am GAT DC 7200 aktiviert werden. Diese betrifft global alle am GAT DC 7200 angeschlossenen Leser.

Um die GANTNER SVN Funktion nutzen zu können, sind bestimmte Voraussetzungen zu erfüllen:
- SALTO ProAccess SPACE mind. Version 6.8
- GAT ACE 7000 mind. Version 2.2
- Firmware der angeschlossenen Leser mind. 3.4.0
- Datenträger müssen entsprechend codiert sein
Nähere Informationen zu dieser Funktion siehe auch Kapitel "7. BERECHTIGUNGSVERGABE*".*

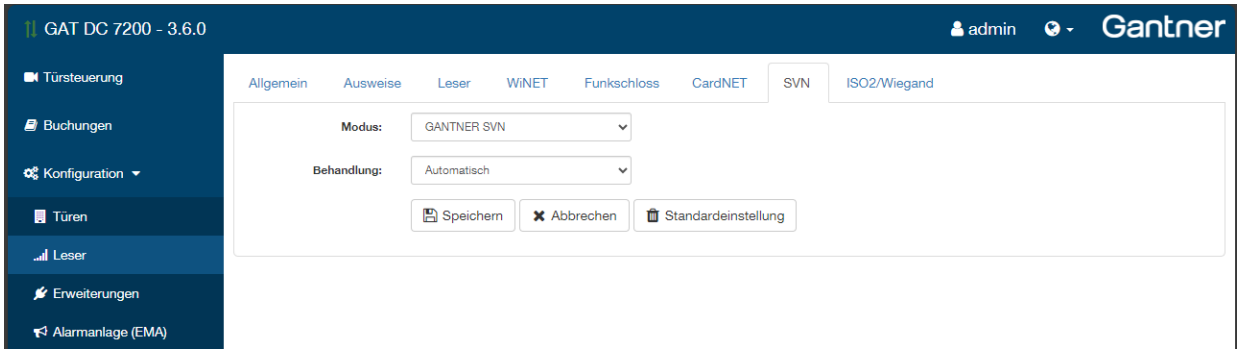


***Bild 6.28** – Web-Oberfläche – SVN Einstellungen*

Die folgenden Einstellungen sind möglich.

- Modus: Hier kann die SVN Funktion aktiviert werden:
  - Deaktiviert: Wählen Sie diesen Modus, wenn SVN nicht verwendet werden soll.
  - GANTNER SVN: Wählen Sie diesen Modus, wenn Sie SVN verwenden möchten, d.h. wenn an den Lesern am GAT DC 7200 die SVN Daten geschrieben und gelesen werden sollen.
- Behandlung: Diese Einstellung legt fest, wie der Vorgang beim Schreiben und Lesen der SVN Daten auf die Datenträger ablaufen soll.
  - Automatisch: Die SVN Daten werden automatisch auf die erkannten Datenträger geschrieben und die Buchungen von den Datenträgern gelesen. Voraussetzung ist, dass das Schreiben bei der Tür aktiviert ist (siehe "6.4.7. Türkonfiguration").
  - Manuell *: Es muss zum Schreiben der SVN Daten auf einen Datenträger zuerst am Leser die "F1" Taste gedrückt und danach der Datenträger ans Lesefeld gehalten werden. Mit Druck auf die "F2" Taste am Leser können die SVN Daten wieder vom Datenträger gelöscht werden.

- Automatisch und manuell *:

  Das Schreiben der SVN Daten erfolgt automatisch beim Lesen eines Datenträgers. Mit Druck auf die "F2" Taste können die SVN Daten wieder vom Datenträger gelöscht werden.

* **HINWEIS!** Für die beiden Einstellungen "manuell" ist zu beachten, dass bei der Alarmanlagenkonfiguration (siehe "6.4.10. Alarmsystemeinstellungen") für die Funktion "Bedrohungsalarm auslösen" NICHT die Funktion "F1 + Identifikation" gewählt werden darf. Dies kann zu Überschneidungen mit der SVN Funktion führen wodurch diese nicht korrekt ausgeführt wird.

Registerkarte "ISO2/Wiegand"

Im Register ISO2/Wiegand können Einstellungen für Longrange Leser, Leser mit anderen RFID Technologien (z. B. PROXY 125 kHz Leser) und benutzerdefinierte Formate z.B. für KFZ-Erkennungen definiert werden.

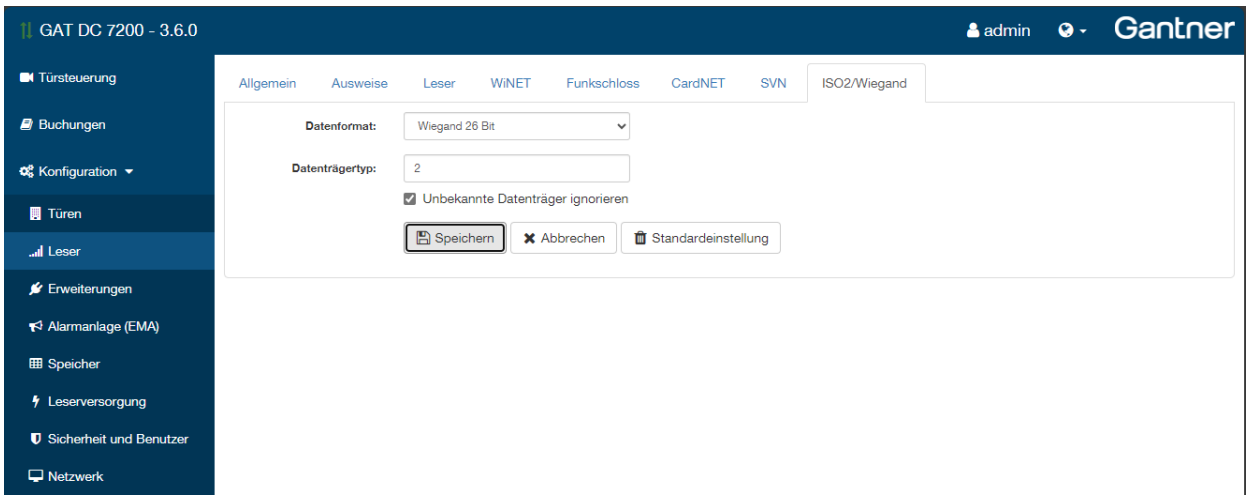
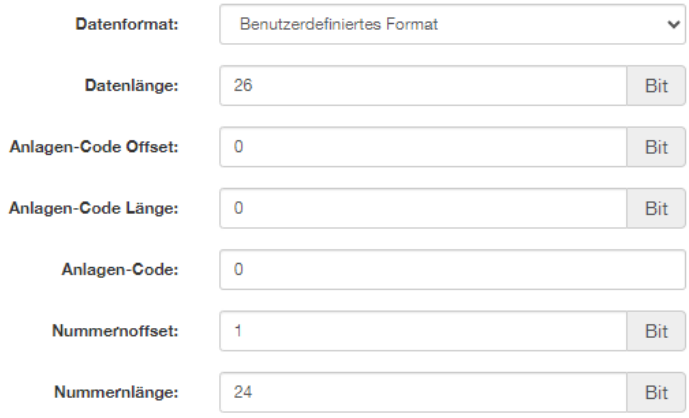


***Bild 6.29** – Web-Oberfläche – ISO2/Wiegand Einstellungen*

Es stehen hier verschiedene Datenformate und Konfigurationsmöglichkeiten für Wiegand- oder Omron-Leser zur Verfügung, die über die "Sub-Schnittstelle" angeschlossen werden (siehe "4.3.3. Beispiel: Anschluss eines GR7.13xx und GAT SR 7000 Wiegand an Tür"). Wählen Sie eines der folgenden Datenformate aus:

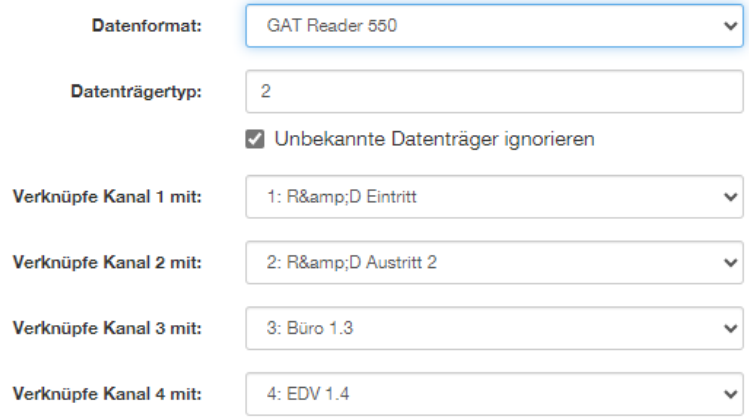
- ISO2 (Omron): Für Leser mit Anschluss über die Omron-Schntittstelle.
- Wiegand 26 Bit / 37 Bit (mit Anlagen-Code):
  Für Leser die die Wiegand-Schnittstelle verwenden (26 Bit oder 37 Bit). Mit den zusätzlichen Eingaben "Anlagen-Code" wird auch ein anlagenabhängiger Code berücksichtigt. Dieser kann im angezeigten Feld eingegeben werden.

- Benutzerdefiniertes Format: Mit dieser Einstellung lässt sich ein eigenes Datenformat für die Schnittstelle zu einem Leser definieren, z. B. bei Anschluss eines Wiegand-Lesers mit speziellem Datenformat. Geben Sie die Offsets und Längen der einzelnen Datenfelder laut der vom Leser vorgegebenen Kommunikationseinstellungen ein.



- GAT Reader 550: Wählen Sie dieses Format für den GANTNER Leser GAT Reader 550. In den Feldern "Verknüpfe Kanal 1/2/3/4 mit" können Sie je eine der in GAT DC 7200

definierten Türen auswählen, um den entsprechenden Kanal des GAT Reader 550 dieser gewählten Tür zuzuweisen.



- GAT Reader 405 AP / 500 UP: Wählen Sie dieses Format für die GANTNER Leser GAT Reader 405 AP oder 500 UP.
- GAT Reader 86x / 900: Dieses Datenformat ist für die Longrange Leser von GANTNER vorgesehen.

- Datenträgertyp: Dieses Feld ist bei allen Datenformaten vorhanden. Mit Datenträgertypen lassen sich verschiedene Arten von Datenträgern, die sich in Technologie (LEGIC prime, LEGIC advante, etc.), in der CardNET Genration oder in der Verwendung für Salto ProAccess SPACE unterscheiden, gemeinsam in einer Anlage nutzen. Wählen Sie hier aus, welchem definierten Datenträgertyp das betreffende Datenformat zugewiesen sein soll. Nähre Infos zu den Datenträgertypen finden Sie in der Beschreibung von GAT Matrix.
- Unbekannte Datenträger ignorieren:
  Wird diese Einstellung aktiviert, werden für alle unbekannte Datenträger, die über das Wiegand Protokoll gesendet werden, keine Buchungen im GAT DC 7200 gespeichert. Diese Aktivierung dieser Option wird z. B. für die KFZ-Kennzeichen-erkennung empfohlen. Es werden dann nur die gültigen bzw. bekannten Kennzeichen dokumentiert und nicht unnötige Buchungen für z. B. Besucher- oder Gästekennzeichen gespeichert.

6.4.9 Hardware Erweiterungen

Im Menüpunkt "Erweiterungen" können Hardwareerweiterungen wie Liftsteuerungen, Schließfachsteuerungen, die Bilder von Videokameras oder Online Zutrittsmanagement und Anti-Pass-Back Funktionen für Türen verwaltet werden.

Registerkarte "Relaisexpander"

Hier werden die Relais von den am GAT DC 7200 angeschlossenen Expandern angezeigt. Es können bis zu zwei GAT IO 055 oder bis zu 8 GAT IO 7054 bzw. GAT IO 7055 verwendet werden.

HINWEIS: Ein Mischbetrieb mit GAT IO 055 und GAT IO 705x ist möglich. Die Gesamtanzahl an Relais-ausgängen von 64 darf aber nicht überschritten werden.

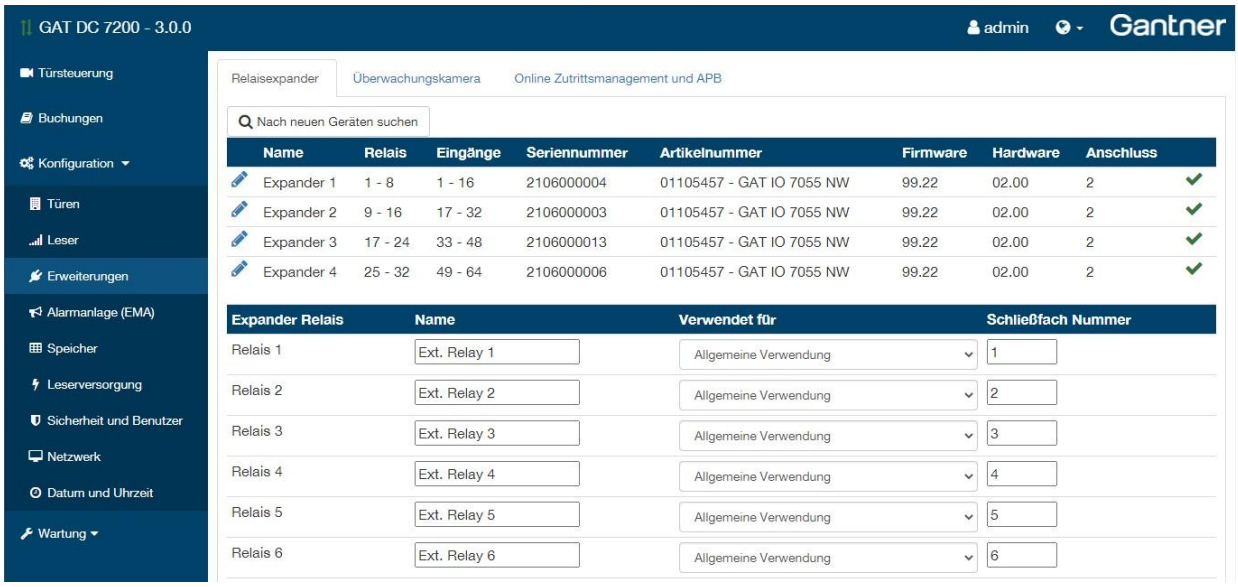


***Bild 6.30** – Web-Oberfläche – Relaisexpander Einstellungen*

- ► Um die am GAT DC 7200 angeschlossenen Relaisexpander zu erkennen, klicken Sie auf "Nach neuen Geräten suchen".
  - o Die gefundenen Expander werden im oberen Bereich des Fensters aufgelistet (im Beispielbild werden 4 Relaisexpander GAT IO 7055 NW verwendet).
- ► Sie können den Namen sowie die Relais- und Optokoppler ID-Nummern bearbeiten. Klicken Sie dazu auf das Editier-Symbol (🖉) vor einem Relaisexpander.
  - o Es öffnet sich folgendes Fenster.

***Bild 6.31** – Relaisexpander Details*

- ► Sie können hier dem Relaisexpander einen Namen geben bzw. den Standardnamen umbenennen.
- ► Die Zahlen in den Feldern "Relais Start-ID" und "Eingang Start-ID" legen die Anfangsnummern der Relaisausgänge und Statuseingänge fest.
  - o Je nach Anzahl von Ein- und Ausgängen werden die restlichen Ein-/Ausgänge dann aufsteigend durchnummeriert.

Alle Relais der angeschlossenen Relaisexpander werden in einer Liste angezeigt. In der Spalte "Expander Relais" sehen Sie die ID-Nummern der Relais entsprechend der automatischen Nummerierung beginnend bei der eingestellten ID-Startnummer.

- ► In der Spalte "Name" können Sie für jedes Relais eine Bezeichnung, z. B. für die Verwendung, eingegeben. Der Name wird dann auch in der GAT Matrix bei der Definition der Relaispläne angezeigt.
- ► Wählen Sie in der Spalte "Verwendet für" die gewünschte Funktion der Relais:
  - ➔ "Allgemeine Verwendung", um das/die Relais für allgemeine Zwecke zu konfigurieren.

    Jedes Relais mit dieser Einstellung kann für die Türkonfiguration oder bei der Konfiguration des Alarmsystem ausgewählt werden.
  - ➔ "Türname", um das/die Relais einer Tür zuzuweisen.

    Das Relais steht dann für die Auswahl bei einer anderen Tür nicht zur Verfügung.
- ► Wenn am GAT DC 7200 eine Elevator Lizenz eingespielt wurde, können die Relais auch für Liftsteuerungen oder für Schließfachsteuerungen verwendet werden.
- ► Um die Schließfachsteuerung zu konfigurieren, gehen Sie gleich wie bei der Liftsteuerung vor, wählen aber in der Türkonfiguration im Feld "Tür Modus" die Funktion "Schließfachsteuerung".

Registerkarte "Überwachungskamera"

Hier kann pro Türe eine Videokamera konfiguriert werden. Das Bild dieser Videokamera ist dann in der "Live-Ansicht“ der Türen darstellbar.

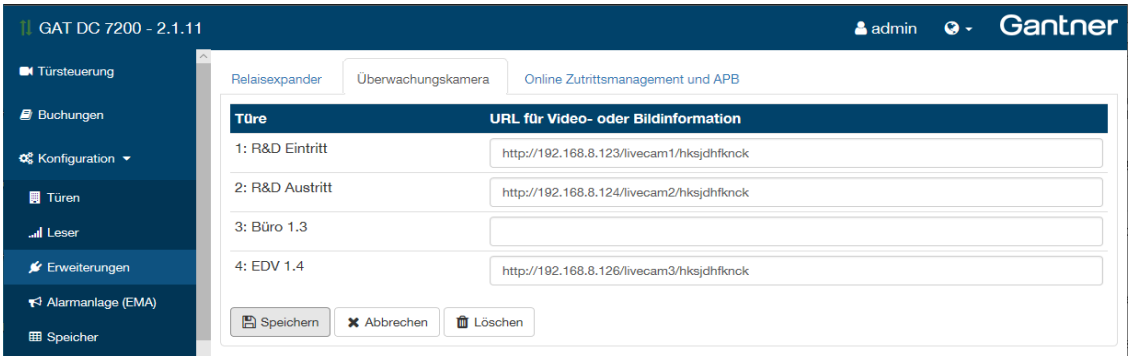


***Bild 6.32** – Web-Oberfläche – Einstellungen für Überwachungskameras*

- ► Tragen Sie in den Feldern "URL" den URL-Link zum Videostream der verwendeten Videokamera ein. Die erforderlichen Werte finden Sie im Handbuch der Kamera.

Wird die Kamera auf "Livestream" eingestellt, so wird im "Live-Ansicht" dieser wiedergegeben. Wird nur ein Einzelbild konfiguriert, so kann im Browser mit F5 (aktualisieren) das aktuelle Bild dargestellt werden.

Registerkarte "Online Zutrittsmanagement und APB"

Auf dieser Registerkarte sind für jede Tür 2 Optionen auswählbar, um das Online Zutrittsmanagement und die Anti-Pass-Back Funktion (APB) zu aktivieren.

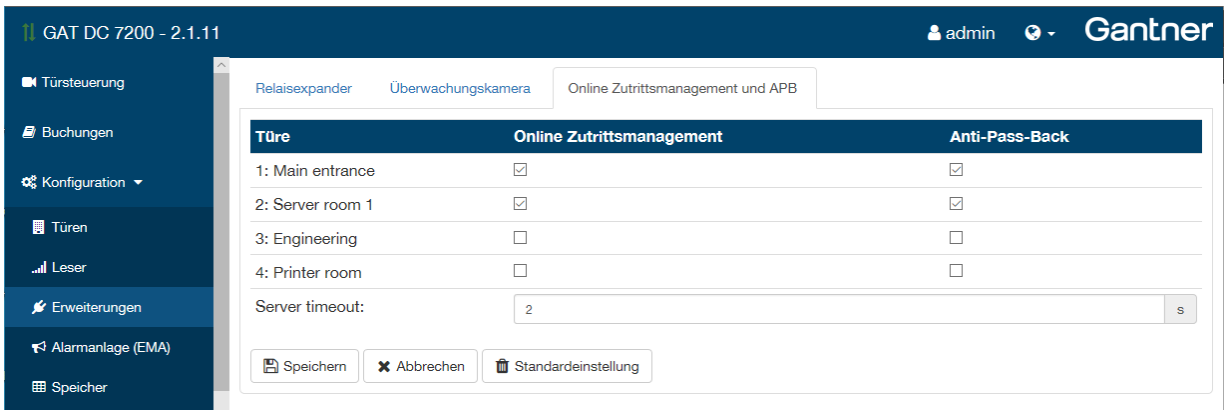


***Bild 6.33** – Web-Oberfläche – Einstellungen für Online Zutrittsmanagement und Anti-Pass-Back (APB)*

Das Online Zutrittsmanagement ist nur für Personen wirksam, die im GAT DC 7200 unbekannt sind. Bei einer Identifikation einer solchen Person werden deren Informationen an die GAT ACE 7000 Software weitergeleitet und eine Software am Server muss entscheiden, ob die Person zutrittsberechtigt ist. Diese Serversoftware kann eine Besucherverwaltung, eine Ticketing-Lösung oder eine andere Zutrittskontrollsoftware sein, die mit GAT ACE 7000 verbunden ist.

Anti-Pass-Back wird verwendet, um wiederholte Eintritte mit demselben Datenträger zu kontrollieren. Ein Austritt ist nur erlaubt, wenn zuvor ein Eintritt durchgeführt wurde und umgekehrt. Die APB Prüfung ist nur möglich für Personen, die dem GAT DC 7200 bekannt sind, wenn die GAT ACE 7000 APB Software installiert und konfiguriert ist und alle Controller einer Zutritts-Zone online sind.

HINWEIS! Wird die Anti-Pass-Back Funktion verwendet, können die Buchungen nicht anonymisiert werden, weil die GAT ACE 7000 APB nur anonyme Buchungen empfangen würde, und damit keine APB-Prüfung möglich sind.

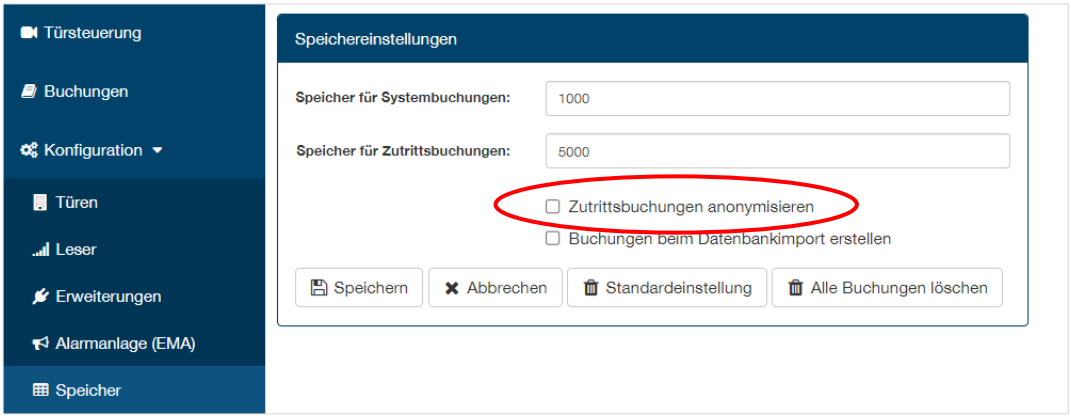


***Bild 6.34** – Personenbuchungen können nicht anonymisiert werden, wenn APB verwendet wird*

Wenn Buchungen anonymisiert werden, ist das Online Zutrittsmanagement möglich, da nur unbekannte Personen über das Online Zutrittsmanagement gesendet werden. Diese Personen sind dem GAT DC 7200 nicht bekannt (anonymisiert) und die Software, die die Zutrittsprüfung durchführt, kann die Buchungen, wenn gewünscht, selbst anonymisieren.

6.4.10 Alarmsystemeinstellungen

Die Einstellungen für die Behandlung eines in der Anlage vorhandenen Alarmsystems sind allgemein für den GAT DC 7200 gültig und beziehen sich nicht auf eine spezielle Tür, sondern auf den gesamten Controller. In der Türkonfiguration kann gewählt werden, welche Türen durch die Einbruchmeldeanlage beeinflusst werden bzw. welche diese beeinflussen kann.

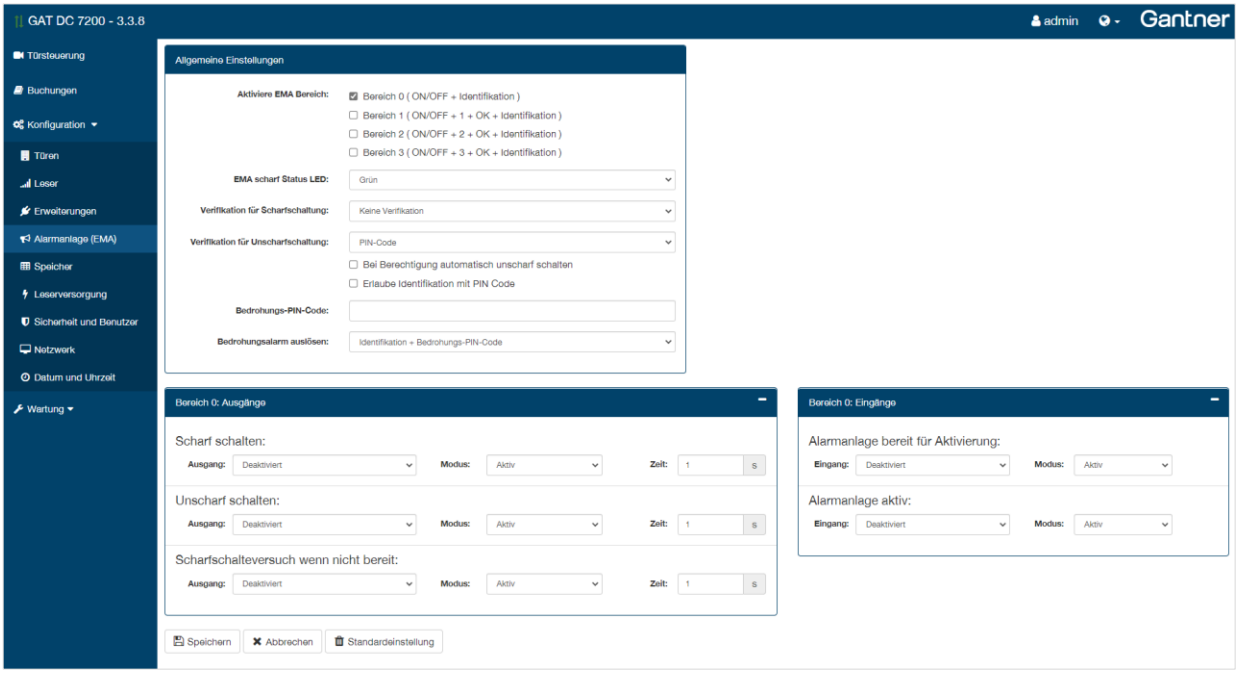


***Bild 6.35** – Web-Oberfläche – Einstellungen zum Alarmsystemverhalten*

Hier können Sie folgende Einstellungen definieren:

- Aktiviere EMA Bereich: Hier können Sie das Alarmsystem für die verschiedenen Bereiche aktivieren.
- EMA scharf Status LED: Wählen Sie hier die Farbe der LED, die bei aktivierter Alarmanlage angezeigt werden soll.
- Verifikation für (Un)Scharfschaltung: Wählen Sie hier, ob für das Ein- und Ausschalten der Alarmanlage eine Verifikation am GAT DC 7200 notwendig sein soll, und falls ja, wie die Verifikation erfolgen soll.
  "Bei Berechtigung automatisch unscharf schalten": Ist diese Option markiert, wird ein aktiver Alarm bei einer gültigen Identifikation, z. B. für einen Zutritt, automatisch deaktiviert.
  "Erlaube Identifikation mit PIN Code": Wenn diese Option aktiviert ist, kann ein Alarm durch eine gültige Identifikation mit PIN Code deaktiviert werden.
- Bedrohungs-PIN-Code: Hier kann ein Bedrohungs-PIN-Code für den Controller definiert werden, mit dem alle berechtigten Personen im Falle einer Bedrohung oder eines Angriffs einen stillen Alarm auslösen können. Die Eingabe des Bedrohungscodes muss 8 Zeichen lang sein. Die Zeichen "x" oder "*" können als Platzhalter verwendet werden. Es werden nur einige Ziffern des Bedrohungscodes definiert, die restlichen Ziffern werden durch einen Platzhalter dargestellt.

Beispiel:

Persönlicher PIN-Code	-	-	-	-	1	2	3	4
Bedrohungs-PIN-Code	x	x	x	9	x	x	x	9
PIN-Code zum Auslösen des Bedrohungsalarms	-	-	-	9	1	2	3	9

Um den Bedrohungsalarm auszulösen, muss der Benutzer anstelle des Platzhalters die entsprechende Ziffer seines persönlichen PIN-Codes eingeben. Führende Nullen müssen nicht eingegeben werden.

HINWEIS!

- Stellen Sie sicher, dass der persönliche PIN-Code einer Person nicht mit dem Bedrohungs-PIN-Code identisch ist, da dies jedes Mal einen Alarm auslösen würde, wenn der persönliche PIN-Code eingegeben wird.
- Der Bedrohungs-PIN-Code kann nur eingegeben werden, wenn die PIN-Code-Eingabe für den regulären Zugang aktiviert ist.

- Bedrohungsalarm auslösen:

Wählen Sie hier aus, wie der Benutzer den stillen Bedrohungsalarm auslösen kann. Es stehen zwei Optionen zur Verfügung:

Identifikation + Bedrohungs-PIN-Code: Standardoption. Um den Bedrohungsalarm auszulösen, muss der Benutzer seinen Bedrohungs-PIN-Code eingeben, wie in der vorherigen Einstellung "Bedrohungs-Pin-Code" definiert.

F1 + Identifikation: Um den Bedrohungsalarm auszulösen, muss der Benutzer die Taste F1 auf der GR7.2310 Tastatur drücken, bevor die Identifizierung abgeschlossen ist. Diese Option kann verwendet werden, wenn die PIN-Code-Eingabeeinstellung nicht dauerhaft aktiviert ist.

HINWEISE zur Option F1 + Identifikation:

1. Diese Option ist nur für GR7.2310 Leser verfügbar, die an den GAT DC 7200 angeschlossen sind.
2. Auf der Seite "Konfiguration -> "Leser" -> "CardNET" muss für die Option "Behandlung" die Einstellung "Automatisch" gewählt sein. Ist dies nicht der Fall, wird eine entsprechende Meldung angezeigt, wenn die Option "F1 + Identifikation" verwendet wird.

- Ausgänge:

Zum Ein- und Ausschalten der Alarmanlage können für die Relaisausgänge mit den Bezeichnungen "Scharf schalten" und "Unscharf schalten" des GAT DC 7200 oder der angeschlossenen Leser die betreffenden Funktionen zugeordnet werden. Für das Scharfschalten und Unscharfschalten der Alarmanlage zwei getrennte oder derselbe Ausgang zu verwenden.

Der Ausgang "Scharfschaltversuch wenn nicht bereit" kann verwendet werden, um einen Scharfschaltversuch der Alarmanlage zu protokollieren, wenn die Alarmanlage nicht bereit ist. In diesem Fall wird ein Signal an die Alarmanlage gesendet, in dem der Scharfschaltversuch protokolliert wird, was in Fällen, in denen Polizei und Versicherungen involviert sind, als Beweis verwendet werden kann. Auch für diesen Ausgang kann das gleiche Relais wie für den Ausgang "Scharf schalten" definiert werden, so dass nur ein Kontakt mit der Alarmanlage verdrahtet werden muss.

HINWEIS! Der Eingang "Alarmanlage bereit für Aktivierung" sollte weiterhin verwendet werden, damit der Benutzer informiert wird, ob die Alarmanlage bereit ist oder nicht.

Für alle Relaisausgänge kann eine Zeit beim Scharf- und/oder Unscharfschalten eingestellt werden. Mit einer Zeit größer Null wird nur ein Impuls mit der eingegebenen Zeit abgesetzt. Wenn für die Zeit "0“ eingegeben wird, wird hingegen ein durchgehendes Signal erzeugt (z. B. Ausgang aktiviert, solange die Alarmanlage scharf geschaltet ist). Der Modus "Aktiv" bedeutet, dass der Ausgang bei aktiver Funktion aktiviert wird. "Passiv" bedeutet, der Ausgang wird aktiviert, wenn die Funktion nicht aktiv ist.

- Eingänge: Für die Statuserfassung der Alarmanlage können Optokopplereingänge des GAT DC 7200 oder der angeschlossenen Leser den betreffenden Funktionen zugeordnet werden. Mit der Funktion "Alarmanlage bereit für Aktivierung" die Aktivierung der Alarmanlage vom Zustand dieses Eingangssignals abhängig gemacht werden. Damit kann verhindert werden, dass die Alarmanlage in bestimmten Fällen scharf geschaltet werden kann (d.h. solange die Funktion nicht aktiviert ist). Mit dem Eingang "Alarmanlage aktiv" kann die Alarmanlage durch ein Signal aktiviert werden. Der Modus "Aktiv" bedeutet jeweils, dass die betreffende Funktion nur aktiv ist, wenn ein Signal angelegt wird. Mit dem Modus "Passiv" ist die Funktion nur aktiv, wenn kein Signal angelegt ist.

6.4.11 Speichereinstellungen

Unter dem Menüpunkt "Speicher" kann angegeben werden, wie groß der Speicher für Systemereignisse und für Personen- und Türbezogene Buchungen sein soll. Beide Speicher sind als Ringspeicher ausgelegt, bei denen das älteste Ereignis überschrieben wird, wenn der Speicher voll ist.

***Bild 6.36** – Web-Oberfläche – Speichereinstellungen*

Unabhängig von diesen Einstellungen werden in der Buchungsanzeige am GAT DC 7200 immer nur die letzten 1000 Buchungen dargestellt. Lediglich über die Schnittstelle können mehr Buchungen abgeholt werden.

Mit der Funktion "Zutrittsberechtigungen anonymisieren" kann eingestellt werden, dass bei den personenbezogenen Buchungen kein Name oder keine Personalinformation angezeigt wird. Wird die Funktion wieder deaktiviert, so werden die Informationen in der Auswertung wieder zur Verfügung gestellt. Beachten Sie dazu den Hinweis für die Anti-Pass-Back Einstellung (siehe "Registerkarte "Online Zutrittsmanagement und APB"").

Wenn die Option "Buchungen beim Datenbankimport erstellen" aktiviert ist, wird für Dokumentationszwecke eine Buchung erzeugt, wenn der Controller mit neuen Daten geladen wurde (Datenbankimport). Die Datenbankimport-Buchung wird auf der Seite "Buchungen" angezeigt (siehe Kapitel "6.6 Buchungen").

6.4.12 Leserversorgung

Mit dieser Konfiguration ist es möglich, die Spannungsversorgung auf den "Reader" Anschlüssen und auf dem "Sub" Anschluss ein- und auszuschalten. Auf diesem Weg kann ein Leser oder ein angeschlossenes Gerät wie z. B. ein Relaisexpander GAT IO 705x stromlos gemacht werden (z. B. um es zu deaktivieren oder neu zu starten).

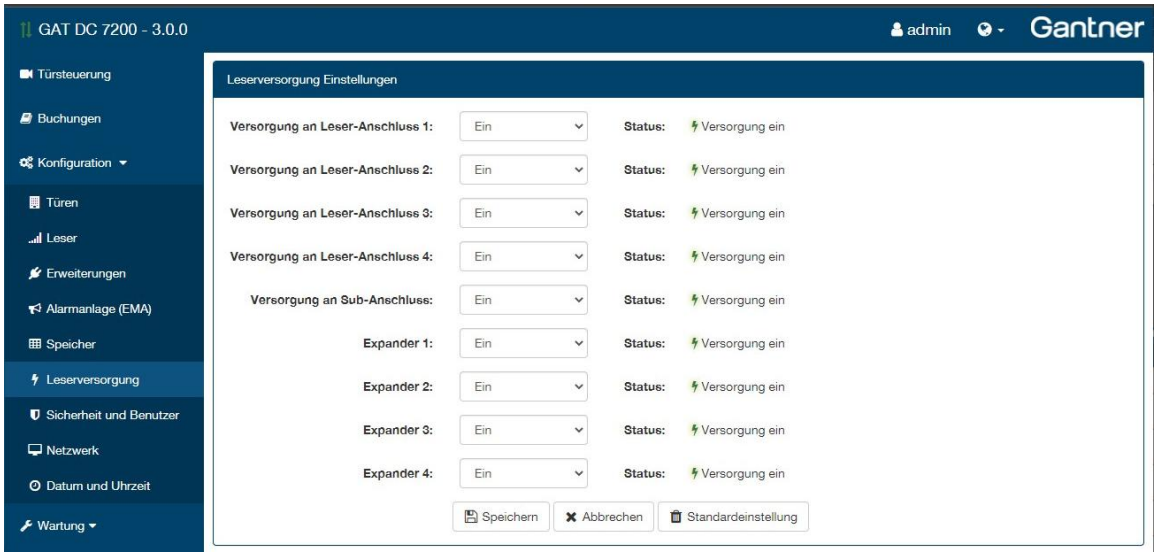


***Bild 6.37** – Web-Oberfläche – Leserversorgung*

Bei einem Kurzschluss oder einer Überlast am Anschluss wird die Spannungsversorgung zum Schutz des GAT DC 7200 und der angeschlossenen Geräte automatisch ausgeschaltet. Der aktuelle Status wird dargestellt.

6.4.13 Sicherheit und Benutzer

Im Menü "Sicherheit und Benutzer" können zahlreiche Sicherheitseinstellungen vorgenommen und weitere Benutzer angelegt werden.

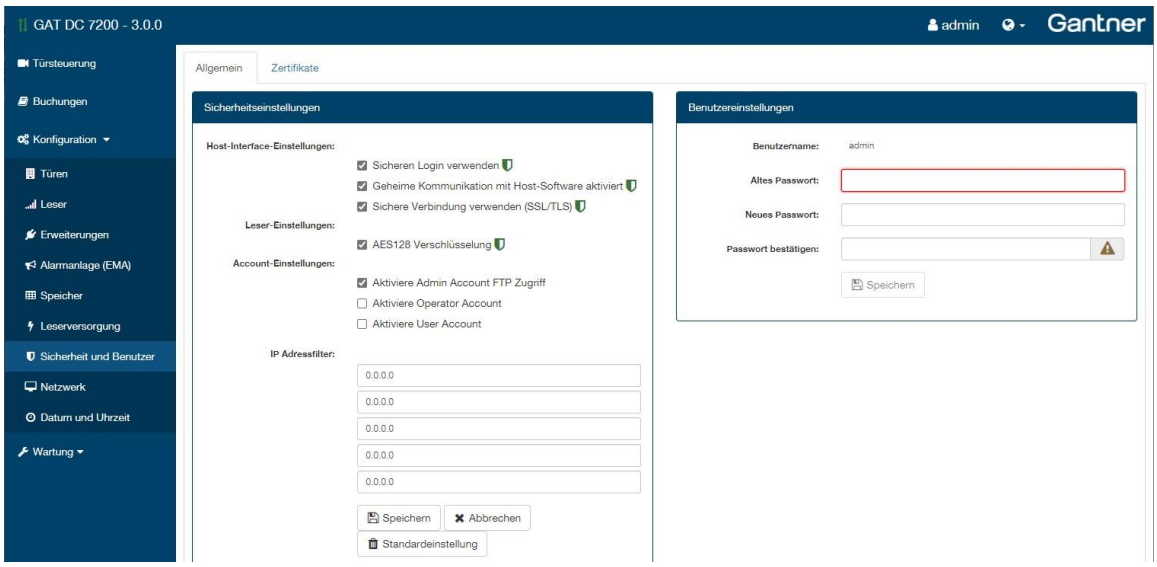


***Bild 6.38** – Web-Oberfläche – Sicherheits- und Benutzereinstellungen*

Registerkarte "Allgemein" -> "Sicherheitseinstellungen"

- Sicheren Login verwenden: Diese Funktion verlangt beim Verbindungsaufbau mit GAT Matrix nach einem mehrstufigen Verfahren zur wechselseitigen Authentifizierung, um eine sichere Verbindung herzustellen. Diese Methode ist dringend empfohlen und sollte nur für den Fall, dass die Zutrittssoftware diese Methode nicht unterstützt, deaktiviert werden.
- Geheime Kommunikation mit Host-Software aktivieren:

  Die Markierung zeigt an, dass die Zutrittssoftware das Passwort für die Host-kommunikation verändert hat. Wird die Zutrittssoftware verändert, kann durch Deaktivieren dieser Funktion das Passwort für die Hostkommunikation wieder auf den Default zurückgesetzt werden, sodass eine neue Verbindung ermöglicht wird.

  HINWEIS! Diese Einstellung ist im Stand-Alone Modus des GAT DC 7200 nicht verfügbar.
- Sichere Verbindung verwenden (SSL/TLS):

  Die Verbindung zur GAT ACE 7000 kann zur Erhöhung der Abhörsicherheit mittels TLS Verbindung verschlüsselt erfolgen. Dazu markieren Sie diese Option. Am PC muss das gültige Zertifikat für die TLS Verbindung (GAT ACE 7000 und Konfigurationswebseite) installiert werden (siehe "6.4.1. Zertifikat für TLS/SSL Verbindung einrichten").
  HINWEIS! GANTNER empfiehlt aus Sicherheitsgründen, diese Einstellung zu aktivieren.
- AES 128 Verschlüsselung: Diese Einstellung sorgt für eine verschlüsselte Kommunikation zwischen Lesern und GAT DC 7200. Diese Funktion sollte nur deaktiviert werden, wenn Leser angeschlossen sind, die die verschlüsselte Kommunikation nicht unterstützen.
- Aktiviere Admin Account FTP Zugriff: Diese Funktion legt fest, ob der Benutzer "Admin" per FTP auf den GAT DC 7200 zugreifen kann, um Dateien auf diesem Weg auszutauschen.
- Aktiviere Operator/User Account: Diese Funktionen geben an, ob die Benutzer "Operator" und "User" verfügbar sein sollen. Dem Benutzer "Operator" stehen die Menüs "Türsteuerung", "Buchungen" und im Stand-Alone Modus "Zutrittsrechte" zur Verfügung, er kann aber keine Konfiguration und Wartungsarbeiten erledigen. Dem Benutzer "User" steht nur das Menü "Türsteuerung" zur Verfügung. Die Passwörter müssen bestimmten Vorgaben genügen (siehe nächste Seite).
- "IP Adressfilter": Legen Sie hier fest, ob von beliebigen Rechnern auf den GAT DC 7200 zugegriffen werden kann (alle Felder 0.0.0.0) oder ob nur die hier festgelegten Rechner (IP Adressen) Zugriff erhalten.
  HINWEIS! Werden die IP-Adressen Filter konfiguriert muss sowohl der Rechner, über den die Konfiguration gemacht wird, als auch der Rechner, über den die Software kommuniziert, eingestellt sein.

Registerkarte "Allgemein" -> "Benutzereinstellungen"

In diesem Bereich kann das Passwort des Administrators und der Benutzer geändert werden.

HINWEIS! Ab Firmware Version 3.6 ist es zwingend notwendig, das Standard-Passwort gegen ein sicheres Passwort zu tauschen!

Für die Benutzer "Operator" und "User" sind die Standard-Passwörter "GAT".

HINWEIS! Auch für diese Benutzer ist es zwingend vorgegeben, die Standard-Passwörter durch sichere Passwörter zu ersetzen. Der Benutzer "Administrator" kann die Passwörter für diese beiden Benutzer überschreiben und sie so ersetzen.

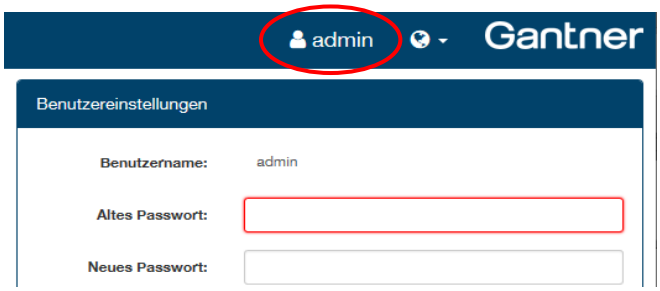


***Bild 6.39** – Aktueller Benutzer*

- ► Durch Klick auf die Anzeige des angemeldeten Benutzers (rechts oben neben dem Logo) öffnet sich ein Fenster, in dem der Benutzer selbst sein Passwort ändern kann.

  HINWEIS: Das Passwort muss mindestens 8 Zeichen lang sein und mindestens 1 Großbuchstabe, ein Kleinbuchstabe und eine Ziffer enthalten.
- ► Über die Funktion "Benutzer wechseln" in diesem Fenster kann der angemeldete Benutzer gewechselte werden.

Im der Live-Ansicht wird durch das Symbol Security angezeigt, dass alle Sicherheitseinstellungen optimal gesetzt sind. Ist eine der Sicherheitseinstellungen nicht aktiviert oder ist das Passwort des Benutzers "Admin" noch auf den Standard eingestellt, so wird dies durch das Symbol Security angezeigt.

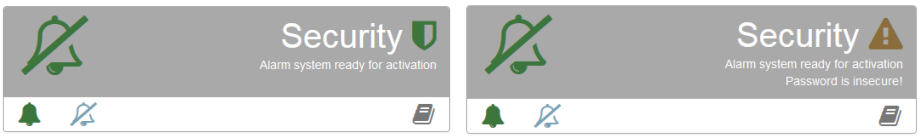


***Bild 6.40** – Qualität der Sicherheitseinstellungen*

Registerkarte "Zertifikate"

In diesem Bereich kann ein Zertifikat vom GAT DC 7200 erstellt und heruntergeladen werden. Dieses wird benötigt, um die Konfiguration und Kommunikation mit GAT ACE über die gesicherte TLS/SSL Verbindung durchzuführen. Eine Anleitung der dafür notwendigen Einstellungen in GAT ACE finden Sie im Handbuch der GAT ACE Software.

Hinweis: Es wird empfohlen, den Firefox Browser oder Microsoft Edge zu verwendet werden. Mit anderen Browsern ist das Herunterladen eventuell nur über Umwege möglich (siehe "6.4.1. Zertifikat für TLS/SSL Verbindung einrichten").

Zum Erstellen eines Zertifikats haben Sie grundsätzlich 2 Möglichkeiten.

a) Sie können ein Zertifikat vom GAT DC 7200 erstellen lassen, oder

b) eine Zertifikatsanforderung erstellen, die Sie bei einer eingetragenen Zertifizierungsstelle signieren lassen.

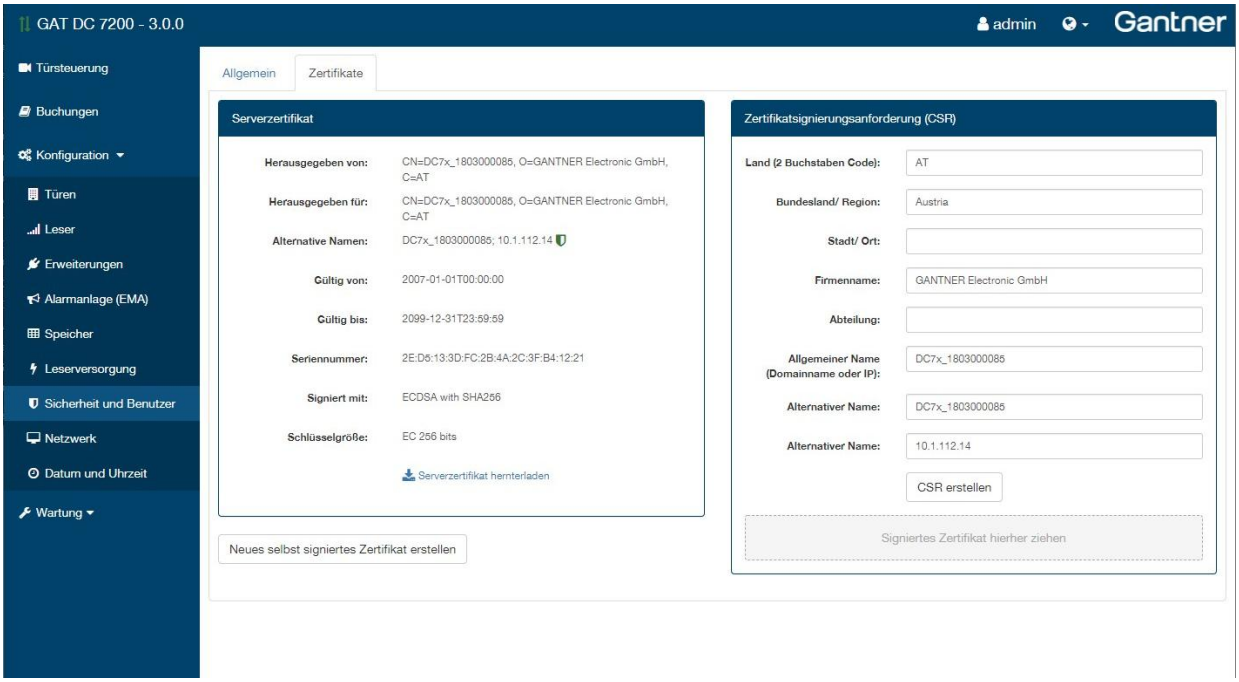


***Bild 6.41** – Zertifikat für TLS erstellen*

a) Selbst signiertes Zertifikat erstellen:

Im Feld "Serverzertifikat" sehen Sie die Daten, die für das Zertifikat verwendet werden, wenn der GAT DC 7200 das Zertifikat erstellt.

► Um das Zertifikat durch den GAT DC 7200 zu erstellen, klicken Sie auf "Neues selbst signiertes Zertifikat erstellen".

► Klicken Sie auf "Serverzertifikat herunterladen".

- Sie können damit das erstelle Zertifikat als .cer Datei auf den Computer laden. Diese Datei muss dann auf dem PC installiert werden. Dies ist in Abschnitt "6.4.1. Zertifikat für TLS/SSL Verbindung einrichten" sowie für GAT ACE auch im GAT ACE Handbuch beschrieben.
  Hinweis: Auf dem PC, auf dem nur mittels Viewer auf GAT ACE 7000 zugegriffen werden soll oder auf dem Sie den GAT DC 7200 mittels Webbrowser konfigurieren, wählen Sie bitte "Lokaler Computer". Auf dem PC, auf dem der GAT ACE 7000 Dienst läuft, wählen Sie bitte "Aktueller Benutzer" und installieren Sie das Zertifikat zusätzlich auch mit "Lokaler Computer", wenn der GAT ACE 7000 Viewer benutzt werden soll.

b) Zertifikatsanforderung für Zertifizierungsstelle erstellen:

Im Bereich "Zertifikatsignierungsanforderung (CSR)" können Sie die Daten für das Zertifikat eingeben.

► Tragen Sie hier die Daten für Ihr Unternehmen und den Türcontroller ein.

► In den Feldern "Alternativer Name" können Sie z. B. den Netzwerknamen eintragen. Wenn die IP-Adresse sich ändert, kann damit über den Netzwerknamen die TLS Verbindung immer noch aufgebaut werden.

Hinweis: Windows 8.1 oder frühere Windows Versionen unterstützen keine IP-Adressen in den alternativen Namen.

► Klicken Sie auf "CSR erstellen".

- Die Anforderungsdatei wird als CSR Datei auf den PC geladen.

► Geben Sie im Dateifenster den Speicherort an.

► Senden Sie die Datei an die Zertifizierungsstelle.

► Am PC installieren Sie dann das Root Zertifikat der Zertifizierungsstelle wie unter "6.4.1. Zertifikat für TLS/SSL Verbindung einrichten" beschrieben.

► Das von der Zertifizierungsstelle erhaltene Zertifikat (im PEM oder DER Format) installieren Sie dann im GAT DC 7200. Ziehen Sie dazu die Zertifikatsdatei in das Feld "Signiertes Zertifikat hierherziehen".

- Das Zertifikat wird im GAT DC 7200 installiert und der Controller muss neu gestartet werden.

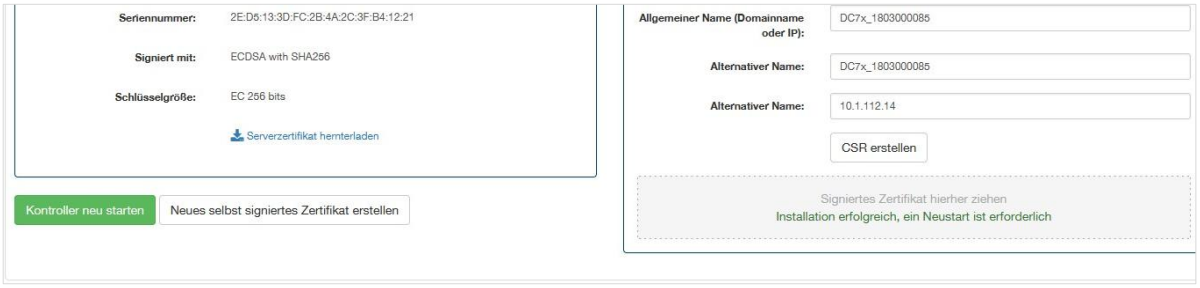


***Bild 6.42** – Zertifikat für TLS erstellen*

► Klicken Sie auf "Kontroller neu starten".

- Der Controller wird automatisch neu gestartet und nach ca. 30 Sekunden befinden Sie sich wieder in der Konfigurationsoberfläche.

6.4.14 Netzwerkeinstellungen

Mit dem Menüpunkt "Netzwerk" können die Netzwerkeinstellungen des GAT DC 7200 verändert werden.

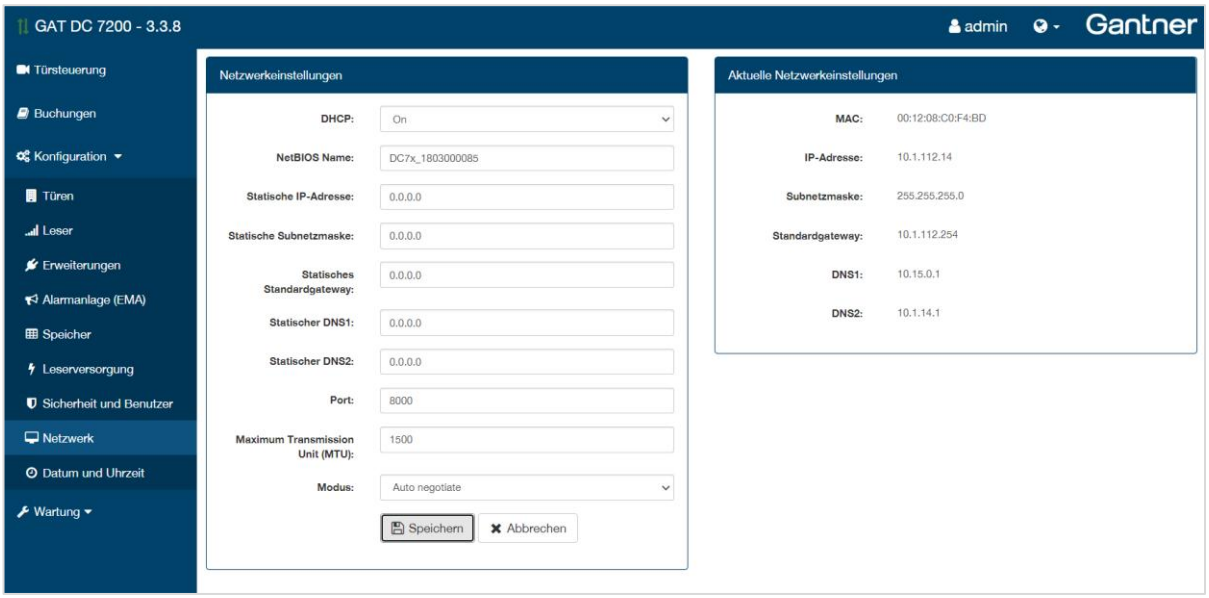


***Bild 6.43** – Web-Oberfläche - Netzwerkeinstellungen*

Auf der rechten Seite unter "Aktuelle Netzwerkeinstellungen" sehen Sie die aktuellen Netzwerkeinstellungen des GAT DC 7200. In der linken Seite unter "Netzwerkeinstellungen" können diese Einstellungen bearbeitet werden.

- DHCP: Im Auslieferzustand ist am GAT DC 7200 die DHCP Funktion aktiviert. Sie können die Verwendung von DHCP hier auch deaktivieren oder aktivieren.
- NetBIOS Name: Der Netzwerkname des GAT DC 7200. Dieser ist standardmäßig auf "DC7x_nnnnnnnnnn" eingestellt, wobei nnnnnnnnnn die Seriennummer des Controllers ist. Die Seriennummer finden Sie auf dem Typenschild oder auf der Verpackung.
  Bei Netzwerken, die DHCP verwenden, können Sie folgenden Netzwerknamen verwenden, um auf die Konfiguration des GAT DC 7200 zuzugreifen:
  `http://DC7x_nnnnnnnnnn`
- IP-Adresse, Subnetzmaske, Gateway, DNS: Hier können Sie die IP-Adresse des Controllers, das Gateway und den Domain Name Service eingeben sowie die Subnetzmaske definieren. Diese Einstellungen hängen von ihrer Netzwerkkonfiguration ab. Bei Verwendung eines DHCP Servers wird die IP-Adresse des Controllers durch diesen Server gesetzt. In Netzwerken ohne DHCP Server können Sie mit der Software GAT Device Finder den Controller suchen und die Netzwerkeinstellungen auf die gewünschten Werte ändern.
- Port: Setzten Sie die Portnummer, die für die Kommunikation mit GAT ACE 7000 verwendet wird. Die folgenden Standardports werden für die Kommunikation verwendet:
  - GAT ACE 7000 Port: 8000
  - FTP: 20 und 21 (ab Version 2.0 von GAT ACE 7000 wird kein FTP mehr benötigt)
  - Webserver (Zugriff auf Konfigurationsoberfläche): ab Version 3.0 der GAT DC 7200 Firmware der Port 443 (verschlüsselte Verbindung über TLS/SSL). Bei älteren Versionen wurde noch Port 80 verwendet.
  - NTP Port für Zeitsynchronisation: 123 UDP ausgehend.
  - GAT DIRECT.Connect: Standard 8239
- Maximum Transmission Unit (MTU):
  In Kundennetzwerken oder wenn versucht wird, eine Verbindung zum Server über ein virtuelles privates Netzwerk (VPN) herzustellen, kann es zu Problemen bei der Kommunikation mit dem GAT DC 7200 kommen. Dies liegt daran, dass die Paketgröße der Schnittstelle zu groß eingestellt ist, so dass bei VPN- oder VLAN-Verbindungen die vom Router erlaubte Paketgröße überschritten wird. Die Kommunikation des GAT DC 7200 basiert auf dem IEEE 802.3 Ethernet Standard (10/100 Mbit), bei dem die max. Paketgröße 1472 Byte beträgt.
  Die Reduzierung des MTU-Werts (Maximum Transmission Unit) des Servers, sodass die maximale Paketgröße des VPN nicht überschritten wird, kann dieses Problem lösen.
- Modus: Wählen Sie die Kommunikationseinstellung (Geschwindigkeit und Duplex). Mit der Einstellung "Auto negotiate" wird diese Einstellung automatisch ermittelt und gesetzt.

6.4.15 Datum und Uhrzeit

Im Menü "Datum und Uhrzeit" können Datum und Uhrzeit des GAT DC 7200 gesetzt werden und Einstellungen für automatische Zeitsynchronisation definiert werden.

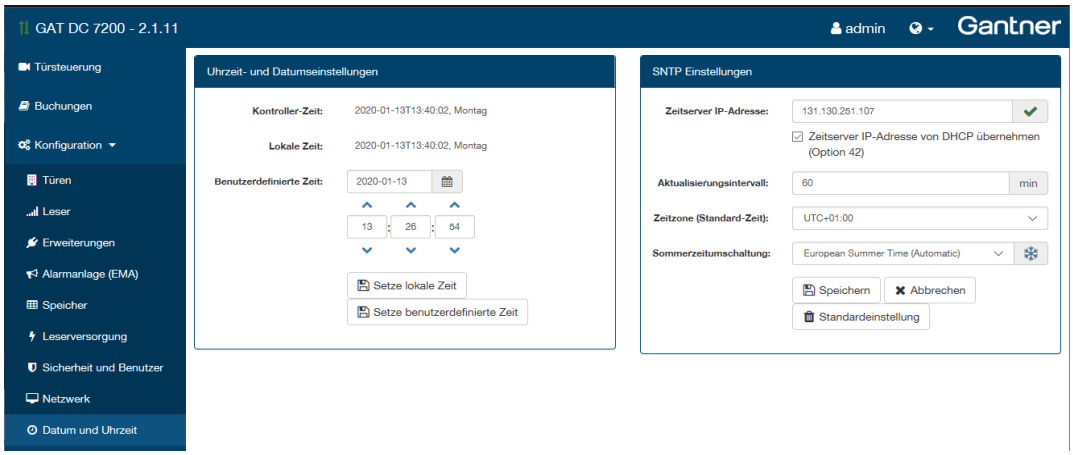


***Bild 6.44** – Web-Oberfläche – Datum & Uhrzeit*

Im linken Bereich "Uhrzeit- und Datumseinstellungen" gibt zwei Möglichkeiten, Datum/Uhrzeit des Controllers zu setzen:

- Setze lokale Zeit: Mit dieser Schaltfläche kann Datum und Uhrzeit des GAT DC 7200 auf die Werte des aktuellen Rechners gesetzt werden. Diese wird hinter "Lokale Zeit“ angezeigt.
- Setze benutzerdefinierte Zeit: Mit dieser Schaltfläche kann eine individuelle Uhrzeit und Datum am GAT DC 7200 gesetzt werden. Geben Sie dazu das gewünschte Datum und die Zeit hinter "Benutzerdefinierte Zeit" ein.

Der übliche Weg ist die Konfiguration eines Zeitservers von dem in regelmäßigen Abständen oder beim Neustart des GAT DC 7200 die Uhrzeit und das Datum geholt und am GAT DC 7200 gesetzt wird. Die Konfiguration dieses Zeitservers erfolgt im Bereich "SNTP Einstellungen".

- Zeitserver IP-Adresse: Die Adresse des Zeitservers können Sie hier eintragen oder alternativ vom DHCP Server über die Option "Zeitserver IP-Adresse von DHCP übernehmen (Option 42)" beziehen (sofern dies der verwendete DHCP Server anbietet).

Setzten Sie die Zeitzone und die Sommer-/Winterzeitumschaltung entsprechend ihrem Standort.

Rechts neben der Sommer-/Winterzeiteinstellung wird mittels Symbols angezeigt, ob sich der Controller aktuell in der Winterzeit (Schneeflocke) oder Sommerzeit (Sonne) befindet.

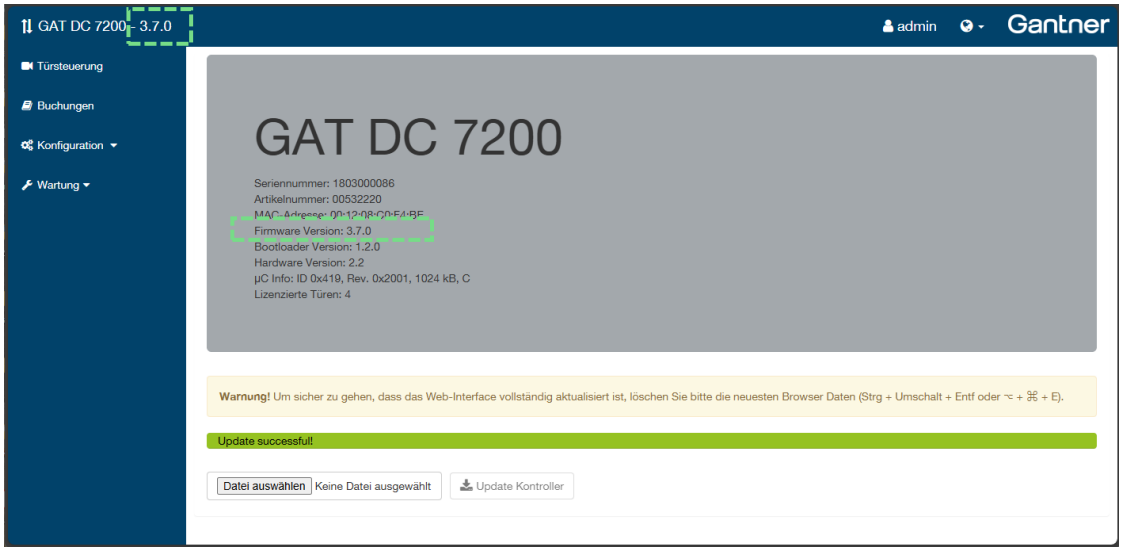
6.5 Mobile Credential konfigurieren

Um Mobile Credential mit einem GAT DC 7200 und angeschlossenem Leser nutzen zu können, ist die passende Lizenz und einige Konfigurationsschritte notwendig. Anschließend ist es möglich, dass sich Benutzer mit ihrem Mobilgerät wie z. B. einem Smartphone oder Smartwatch und dem darauf gespeicherten Berechtigungsausweis in der Zutrittsanlage identifizieren können.

In diesem Abschnitt finden Sie die Konfigurationsschritte, die für die Verwendung von Mobile Credential notwendig sind. Beachten Sie bitte auch die notwendigen Voraussetzungen für Mobile Credential (siehe "2.7. Mobile Credential").

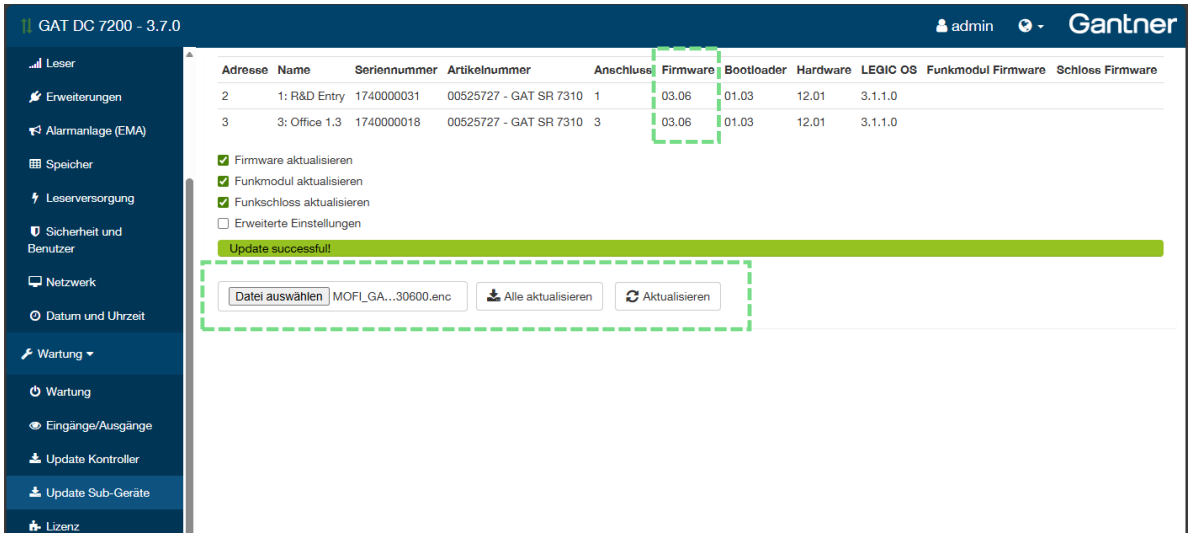
Die nachfolgende Beschreibung geht davon aus, dass die Mobile Credentials über LEGIC Connect erstellt wurden. In diesem Fall können alle erforderlichen Einstellungen wie beschrieben angewendet werden und die benötigten Parameter können über LEGIC Connect erzeugt und zur Verfügung gestellt werden.
Sollen Mobile Credentials verwendet werden, die über andere Plattformen erstellt wurden, müssen die Parameter über diese Plattform in einer vergleichbaren Weise zur Verfügung gestellt werden. Es wird empfohlen, die Kompatibilität der Credentials im Zuge der Projektplanung zu überprüfen.

► Die Firmware des Controllers muss mind. Version 3.7 sein. Sie sehen die Versionsnummer in der Kopfzeile der Webschnittstelle. Sie können die Firmware mit dem Menü "Update Kontroller" im Abschnitt "Wartung" aktualisieren. Dazu brauchen Sie die passende Firmware-Datei von der Gantner Partner-Page.



Nach dem Laden in den Controller wird dieser neu gestartet und die neue Versionsnummer wird angezeigt. Siehe "6.7.3. Update Kontroller".

► Die Leser, an denen die Mobile Credential Funktion verwendet werden soll, müssen mindestens Firmware Version 3.06 verwenden. Sie können die Leser im Menü "Update Sub-Geräte" aktualisieren. Dort wird auch die aktuelle Firmware-Version der Leser angezeigt.



In der Liste sehen Sie alle angeschlossenen Leser. In der Spalte "Firmware" wird die Firmware-Version der Leser angezeigt.

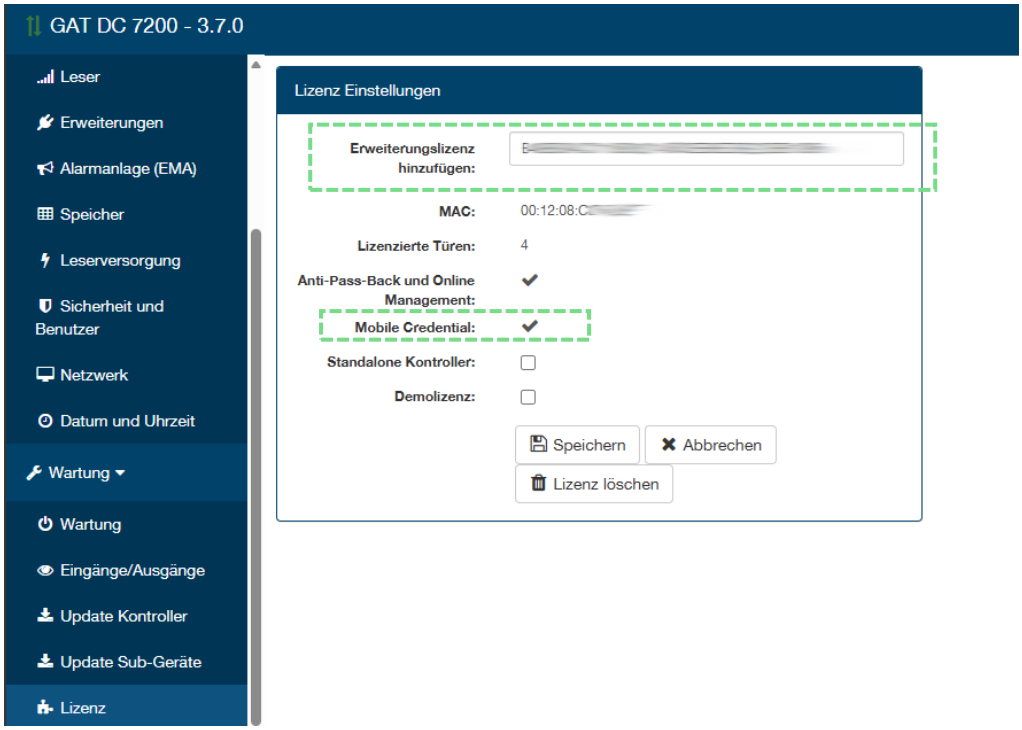
Um die Firmware eines oder aller Leser zu aktualisieren, laden Sie die aktuelle Leser-Firmware von der Gantner Partner-Page. Wählen Sie dann diese Datei (Endung "`.enc`") mit Klick auf "Datei auswählen" und laden Sie die neue Firmwaredatei in die Leser. Drücken Sie dazu auf "Alle aktualisieren". Während dem Update blinken die LED Anzeigen an den Lesern in buntem Lauflicht. Nähere Informationen dazu finden Sie unter "6.7.4. Update Sub-Geräte".

► Das OS (Betriebssystem) des LEGIC Chips muss mindestens Version 5.3.1 sein. Diese Version sehen Sie ebenfalls auf der Seite "Update Sub-Geräte" im Abschnitt "Wartung" und hier in der Spalte "LEGIC OS". Um diese OS Version zu aktualisieren, können Sie die passende Update-Datei (Endung "`.bin`") analog zum Firmware-Update in die Leser laden. Während dem Update wird ein abwechselnd rot/grün leuchtendes Lauflicht an den Lesern angezeigt.

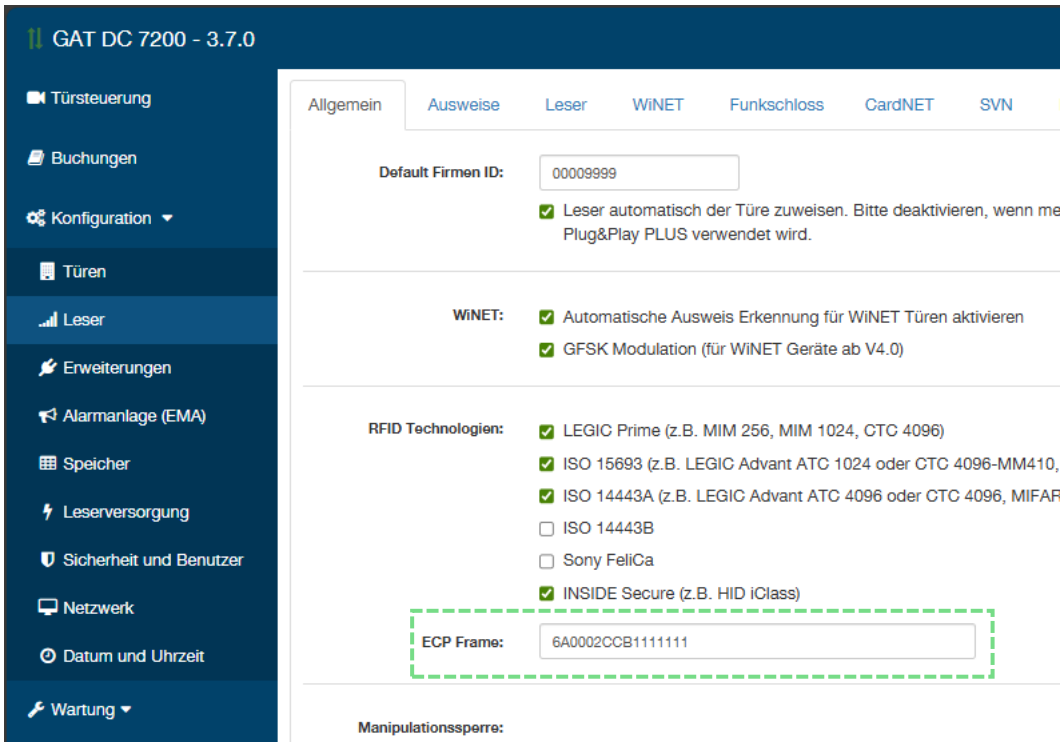
► Nun müssen Sie die Mobile Credential Lizenz aktivieren. Gehen Sie dazu auf die Seite "Lizenz" im Abschnitt "Wartung". Im Feld "Erweiterungslizenz hinzufügen" geben Sie den Lizenzcode für die Mobile Credential Lizenz ein. Klicken Sie dann auf "Speichern".

Wenn die Mobile Credential Lizenz aktiviert ist, wird, wie im folgenden Bild gezeigt, der gleichnamige Eintrag mit Haken-Symbol angezeigt. Ansonsten ist diese Zeile ausgeblendet.

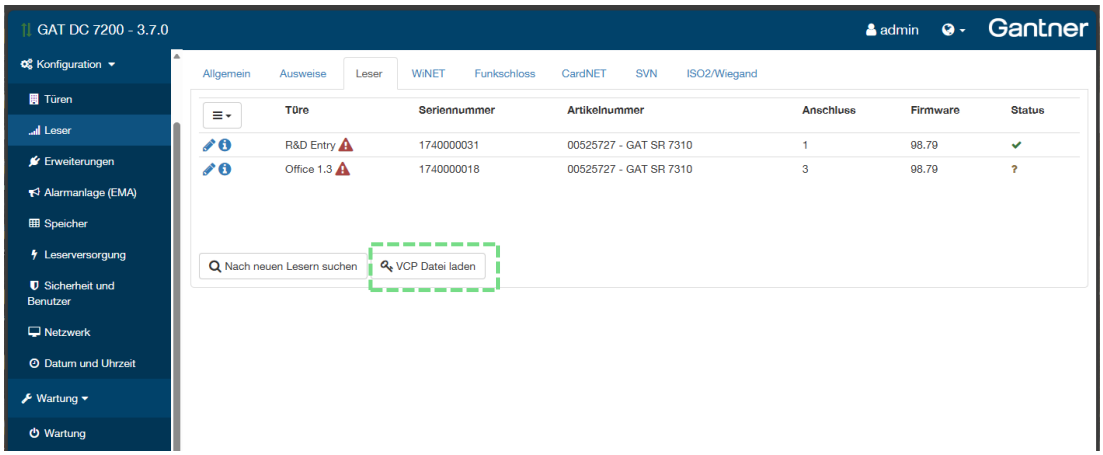
HINWEIS: Mit Aktivieren der Demolizenz kann getestet werden, ob Mobile Credentials die nicht über LEGIC Connect ausgestellt wurden, am Controller und den Lesern verwendet werden können. Dadurch können die erforderlichen Einstellungen für 4 Tage freigeschaltet werden, ohne dass eine Mobile Credential Lizenz bestellt werden muss.



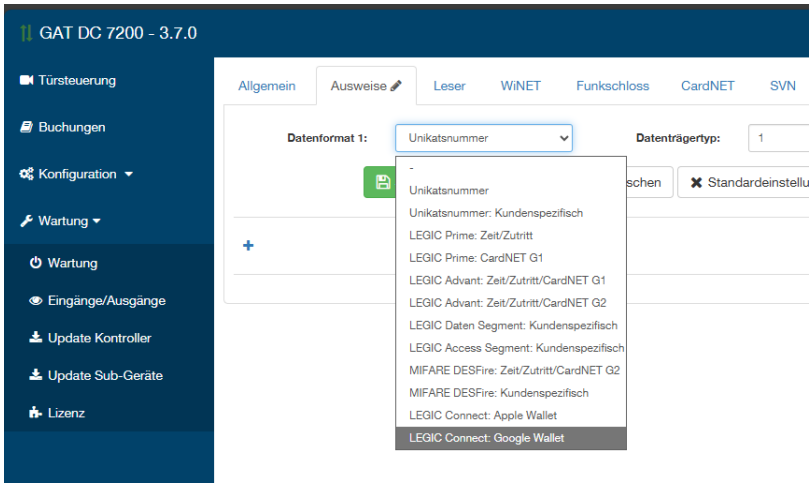
► Nach Aktivieren der Mobile Credential Lizenz wird bei den Lesereinstellungen (Seite "Leser - Allgemein" im Abschnitt "Konfiguration") ein zusätzliches Feld "ECP Frame" angezeigt. Geben Sie dort die Nummer für den ECP Frame (im Hexadezimalformat) ein und bestätigen Sie mit Klick auf "Speichern". Siehe auch "6.4.8. Leserkonfiguration".

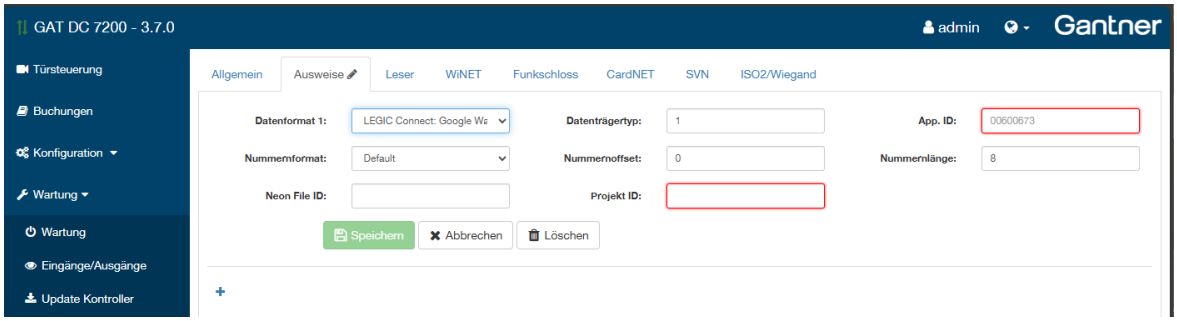


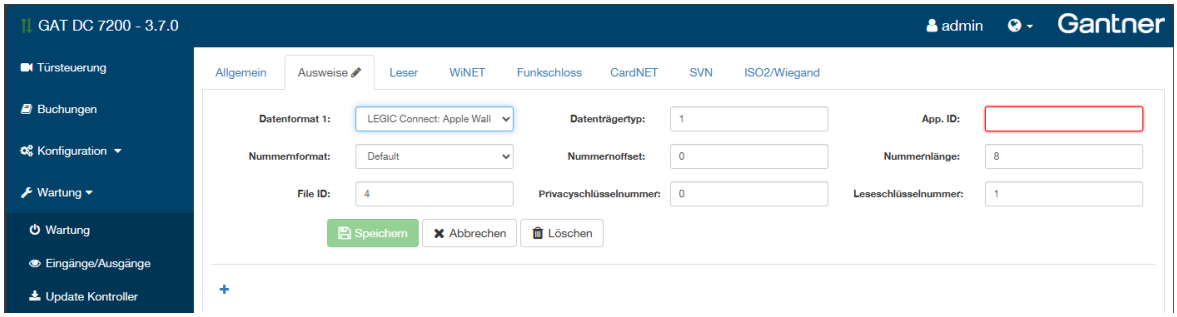
► Nun muss in den Lesern die VCP Datei geladen werden. Diese enthält die LEGIC Konfigurationsparameter für die Leser. Gehen Sie dazu in Abschnitt "Konfiguration", Menü "Leser", Registerkarte "Leser".
Erst nach dem Laden der VCP Datei wird das Lesen der Mobile Credentials am Leser ermöglicht. Aus Sicherheitsgründen muss für die Aktivierung der VCP Parameter in einem Leser ein Passwort eingegeben werden.
Das erfolgreiche Laden wird dann mit einem grünen Haken beim jeweiligen Leser angezeigt. Für mehr Details siehe auch "6.4.8. Leserkonfiguration".
HINWEIS: Für GR7 und GAT S(L)R 73xx Leser werden VCP Dateien für SM-4xxx Chips benötigt.



► Als nächsten Schritt konfigurieren Sie die Einstellungen für die Mobile Credential Ausweise, damit die Ausweisdaten aus den Mobile Credentials richtig verarbeitet und gelesen werden. Gehen Sie dazu auf den Bereich "Konfiguration", Seite "Leser", Registerkarte "Ausweise".
Hier ist für jeden Datenträgertyp ein Datenformat notwendig, das entsprechend konfiguriert ist. Im Falle von Mobile Credential fügen Sie ein neues Datenformat hinzu (Schaltfläche "+") und wählen Sie dann "LEGIC Connect: Apple Wallet" oder "LEGIC Connect: Google Wallet". Die Einstellungen in diesen Datenformaten muss richtig gesetzt werden. Siehe Beispiel und "6.4.8. Leserkonfiguration" – Register "Ausweise".







- ► Mit den hier beschriebenen Schritten ist der GAT DC 7200 und Lesers für die Verwendung von Mobile Credentials vorbereitet.
- ► Auf dem Mobilgerät müssen die Berechtigungen (Credentials) noch in den Apple oder Google Wallets gespeichert werden.
  Die richtige Vorgehensweise für die Erstellung und Speicherung der Wallet Credentials auf den Mobiltelefonen muss mit dem Aussteller der Wallet Credentials geklärt werden.
  Wallet Credentials können aktuell noch nicht über Gantner Plattformen (z. B. Matrix) ausgestellt werden. Lediglich die Zuordnung von ausgestellten Wallet Credentials zu bestehenden Personen kann in der Matrix oder im Fall des Stand-Alone-Modus in der Weboberfläche des Controllers gemacht werden.

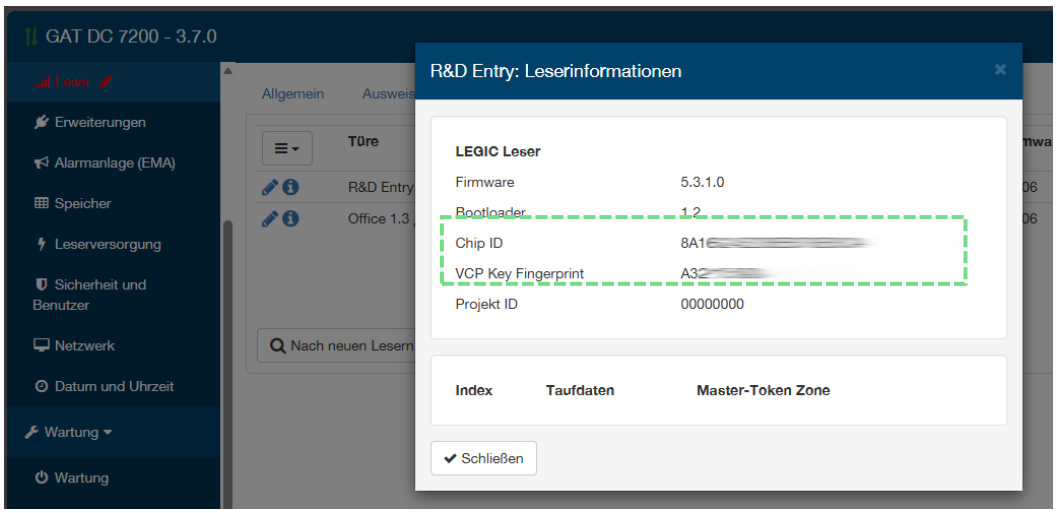
6.5.1 VCP von einem Leser löschen

Um ein geladenes VCP von einem Leser zu entfernen, muss ein "Remove VCP" geladen werden. Dieses erhalten Sie von ihrem Lieferanten der Wallet Credentials.

Beachten Sie, dass im Falle einer Rücksendung eines Lesers an Gantner, z. B. für Reparatur- oder Servicezwecke, unbedingt vor der Rücksendung der VCP im Leser gelöscht werden muss oder ein Remove VCP für die entsprechende Chip ID und das VCP Passwort Gantner zur Verfügung gestellt werden muss.

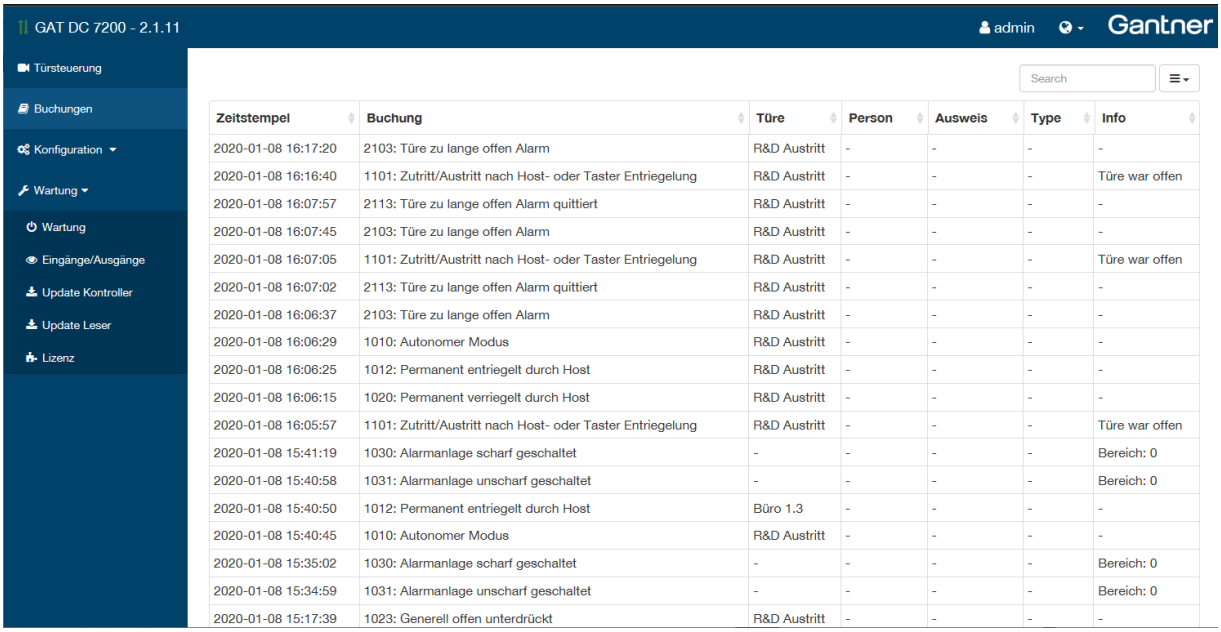
Jedes Remove VCP ist jeweils an die Chip ID eines Leserchips gebunden und muss somit für jeden Leser einzeln erstellt werden.

Zum Löschen eines VCP aus einem Leser wird zusätzlich zum VCP Passwort und der "Chip ID" auch noch der "VCP Key Fingerprint" des Lesers benötigt. Diese Informationen können Sie mit Klick auf das Symbol bei dem betreffenden Leser anzeigen lassen.



6.6 Buchungen

Im Menü "Buchungen" können die Buchungen aller Türen sowie auch systembezogene Buchungen des Controllers dargestellt werden.



Zeitstempel	Buchung	Türe	Person	Ausweis	Type	Info
2020-01-08 16:17:20	2103: Türe zu lange offen Alarm	R&D Austritt	-	-	-	-
2020-01-08 16:16:40	1101: Zutritt/Austritt nach Host- oder Taster Entriegelung	R&D Austritt	-	-	-	Türe war offen
2020-01-08 16:07:57	2113: Türe zu lange offen Alarm quittiert	R&D Austritt	-	-	-	-
2020-01-08 16:07:45	2103: Türe zu lange offen Alarm	R&D Austritt	-	-	-	-
2020-01-08 16:07:05	1101: Zutritt/Austritt nach Host- oder Taster Entriegelung	R&D Austritt	-	-	-	Türe war offen
2020-01-08 16:07:02	2113: Türe zu lange offen Alarm quittiert	R&D Austritt	-	-	-	-
2020-01-08 16:06:37	2103: Türe zu lange offen Alarm	R&D Austritt	-	-	-	-
2020-01-08 16:06:29	1010: Autonomer Modus	R&D Austritt	-	-	-	-
2020-01-08 16:06:25	1012: Permanent entriegelt durch Host	R&D Austritt	-	-	-	-
2020-01-08 16:06:15	1020: Permanent verriegelt durch Host	R&D Austritt	-	-	-	-
2020-01-08 16:05:57	1101: Zutritt/Austritt nach Host- oder Taster Entriegelung	R&D Austritt	-	-	-	Türe war offen
2020-01-08 15:41:19	1030: Alarmanlage scharf geschaltet	-	-	-	-	Bereich: 0
2020-01-08 15:40:58	1031: Alarmanlage unscharf geschaltet	-	-	-	-	Bereich: 0
2020-01-08 15:40:50	1012: Permanent entriegelt durch Host	Büro 1.3	-	-	-	-
2020-01-08 15:40:45	1010: Autonomer Modus	R&D Austritt	-	-	-	-
2020-01-08 15:35:02	1030: Alarmanlage scharf geschaltet	-	-	-	-	Bereich: 0
2020-01-08 15:34:59	1031: Alarmanlage unscharf geschaltet	-	-	-	-	Bereich: 0
2020-01-08 15:17:39	1023: Generell offen unterdrückt	R&D Austritt	-	-	-	-

***Bild 6.45** – Web-Oberfläche – Buchungsanzeige*

In der Buchungsanzeige sehen Sie die am GAT DC 7200 aufgetretenen Aktionen und Zutritte bzw. Zutrittsversuchen mit den jeweiligen Zeiten und betreffender Personenzuordnung (über den Datenträger). Über die Weboberfläche können maximal die letzten 1000 Buchungen dargestellt werden. Möchten Sie weitere Buchungen auswerten, können Sie dies mit der PC-Software GAT Matrix machen.

Über die Schaltfläche ☰ können Sie weitere Spalten mit Informationen ein- und ausblenden.

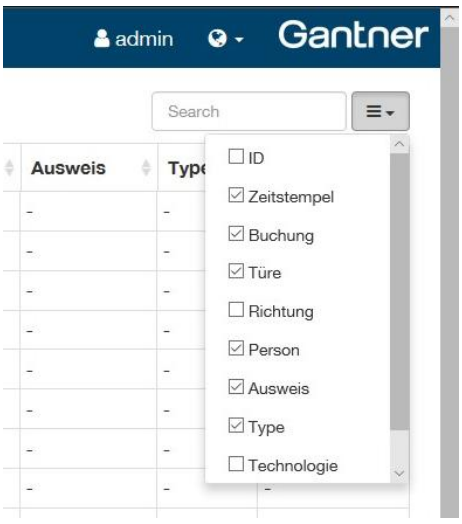


***Bild 6.46** – Web-Oberfläche – Zusätzliche Informationen in der Buchungsanzeige ein-/ausblenden*

6.7 Verwaltung und Wartung

Im Menü "Wartung" bzw. deren Untermenüpunkte können verschiedene Wartungsaufgaben und allgemeine Einstellgen des GAT DC 7200 durchgeführt werden.

6.7.1 Wartung

Registerkarte "Kontroller"

Auf dieser Registerkarte können Sie diverse Informationen wie z. B. die Firmware- und Hardwareversion, Seriennummer, Artikelnummer, Anzahl der lizenzierten Türen und die Speicherauslastung sehen.

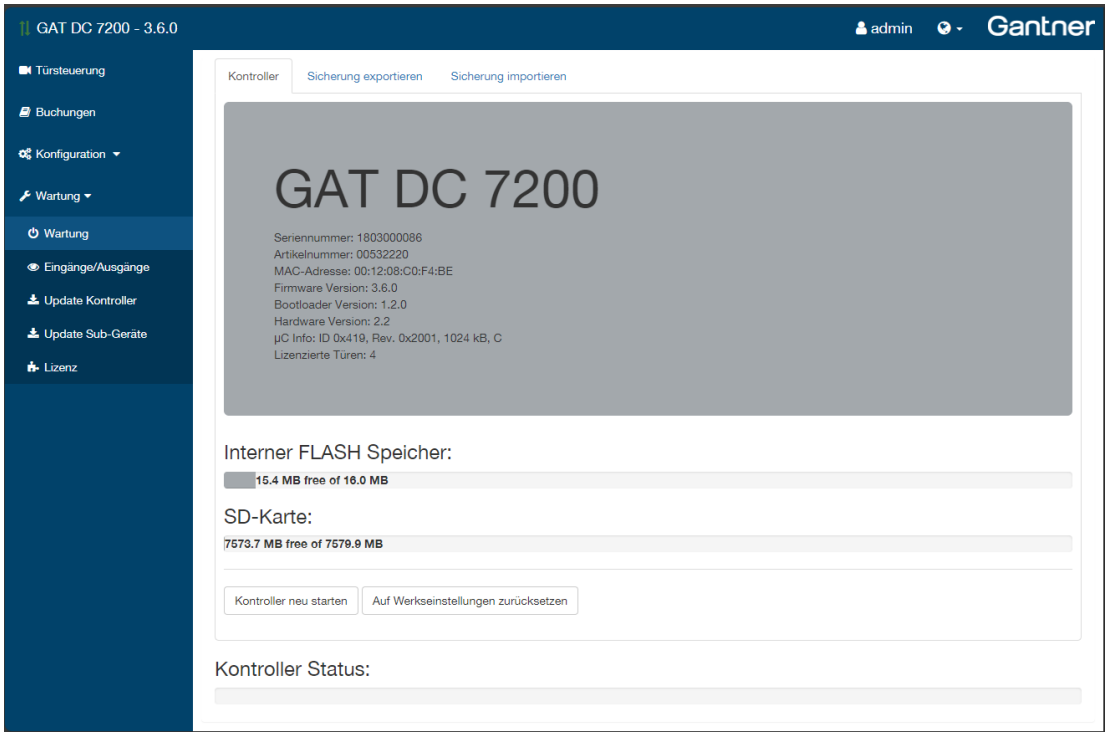


***Bild 6.47** – Web-Oberfläche – Informationen über den GAT DC 7200 anzeigen*

- Kontroller neu starten: Klicken Sie diese Schaltfläche, wenn Sie einen Neustart des Controllers veranlassen möchten.
- Auf Werkseinstellungen zurücksetzen: Wählen Sie diese Schaltfläche, wenn Sie den GAT DC 7200 auf Werkseinstellungen zurücksetzen möchten. Alle seit dem ersten Start durchgeführten Änderungen an den Einstellungen gehen verloren.

Registerkarten "Sicherung exportieren" und "Sicherung importieren"

Auf der Registerkarte "Sicherung exportieren" können Sie alle (oder einige) Einstellungen des GAT DC 7200 verpacken und auf den PC speichern möchten. Diese Datei kann als Datensicherung oder zur Dokumentation eines Zustandes (z. B. bei der Übergabe einer Anlage) verwendet werden.

Bei Verwendung von GAT Matrix oder anderen Zutrittskontroll-Lösungen, die mit GAT ACE 7000 zusammen arbeiten, werden die Backups bei Konfigurationsänderungen von GAT ACE 7000 automatisch erstellt.

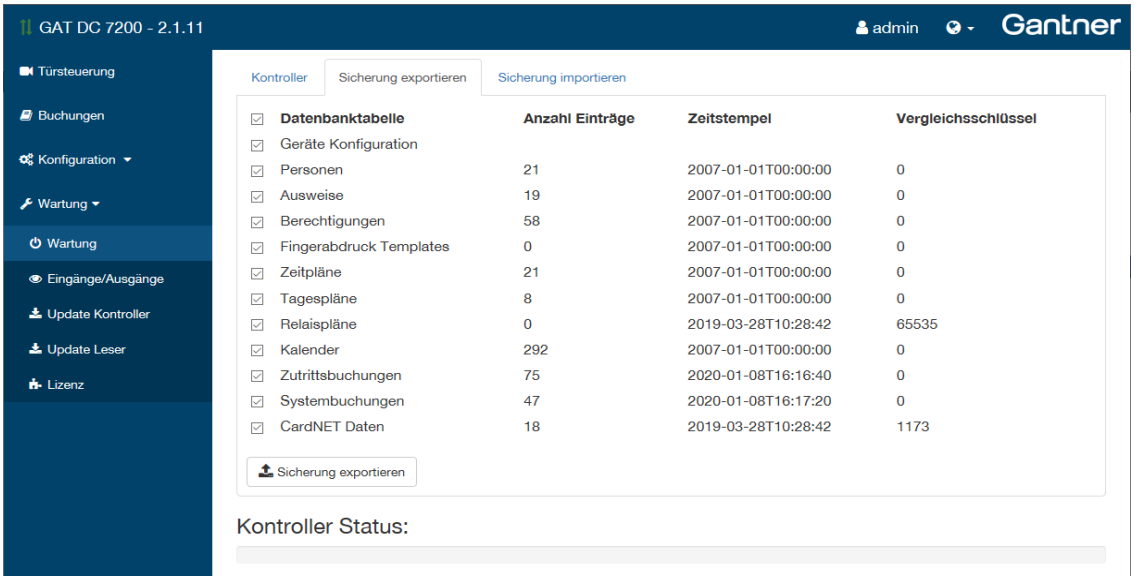
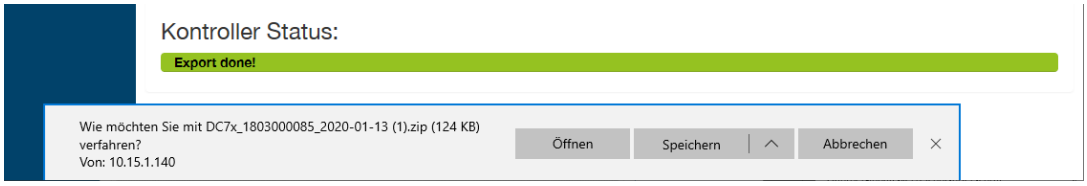


***Bild 6.48** – Web-Oberfläche – Sicherung exportieren*

- ► Gehen Sie zur Registerkarte "Sicherung exportieren".
- ► Markieren Sie hier die gewünschten Daten, die exportiert werden sollen. Standardmäßig werden alle Daten exportiert. Sie können das aber durch Löschen der Markierungen ändern.
- ► Klicken Sie auf "Sicherung exportieren".



  - o Es wird eine ZIP-Datei erstellt, die vom GAT DC 7200 heruntergeladen auf dem PC oder einem Datenträger gespeichert werden kann.
- ► Auf der Registerkarte "Sicherung importieren" können Sie eine gespeicherte Backup-Datei wieder in den GAT DC 7200 zurückladen.

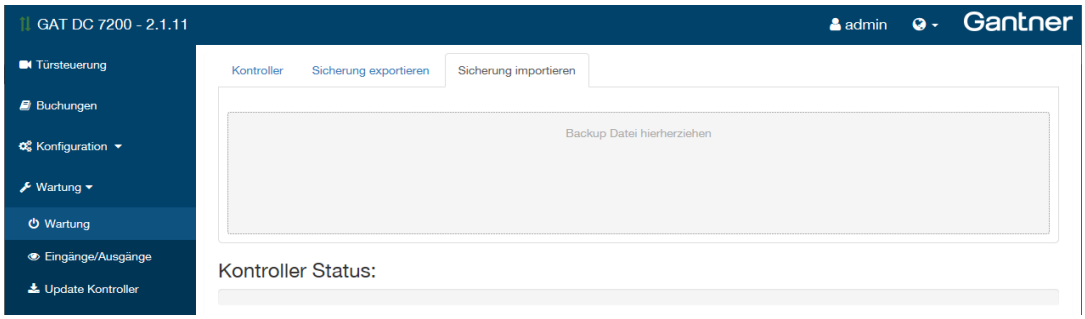


***Bild 6.49** – Web-Oberfläche – Sicherung importieren*

- ► Ziehen Sie die ZIP-Datei der Sicherung in den markierten Bereich.
  - o Sie sehen wieder die Übersicht der gespeicherten Daten.
- ► Markieren Sie die zu importierenden Daten und klicken Sie auf "Sicherung importieren".
  - o Nach erfolgreichem Import wird "Import done" angezeigt und die Einstellungen sind nun importiert.

6.7.2 Ein- und Ausgänge

Im Menü "Eingänge/Ausgänge" können Sie die Zustände der Ein- und Ausgänge des GAT DC 7200 sowie der angeschlossenen Geräte sehen. Ist der Status gesetzt, so ist das Relais derzeit angesteuert bzw. der Eingang derzeit bestromt.

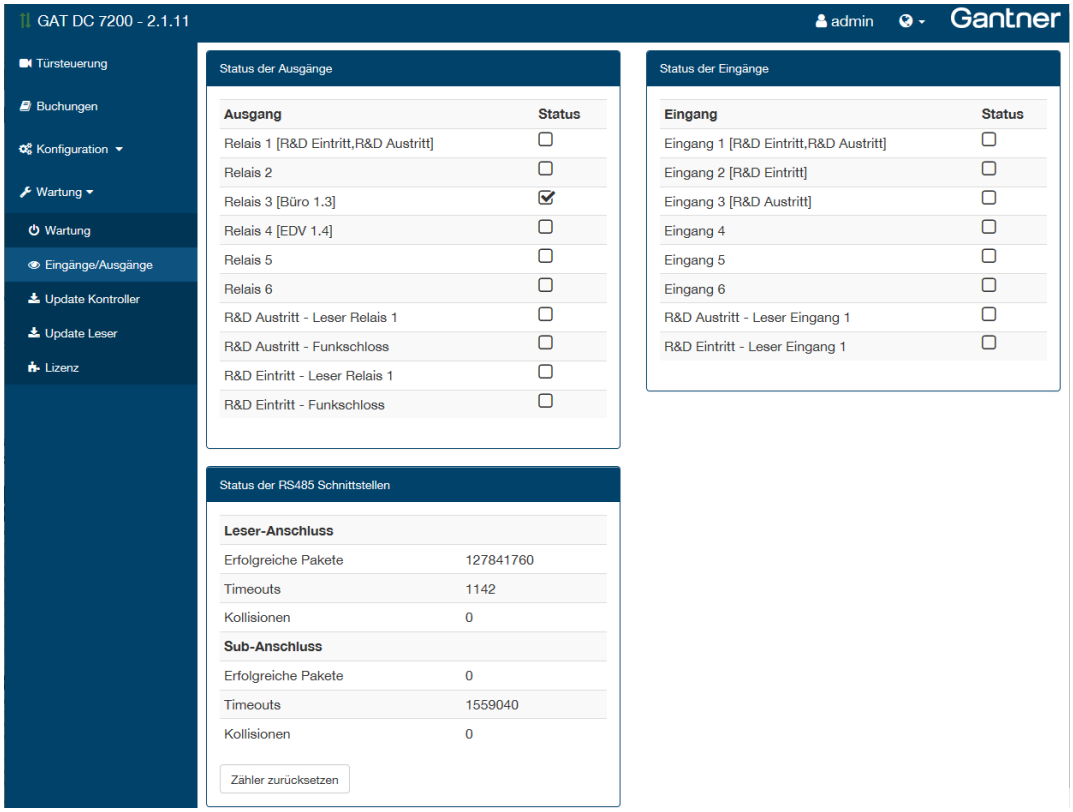


***Bild 6.50** – Web-Oberfläche – Ein- und Ausgänge*

Bei den Ein- und Ausgängen des GAT DC 7200 wird in eckigen Klammern die Türe angegeben, für die dieser Ein- oder Ausgang verwendet wird. Hier können auch mehrere Türen angegeben sein, wenn dieses Signal für mehrere Türen konfiguriert wurde (z. B. Sammelalarm).

Für externe Ein- und Ausgänge wird vor der Nummer des Ein- und Ausgangs die Türbezeichnung angegeben, für die der Leser zugewiesen wurde.

Im Feld "Status der RS 485 Schnittstellen" werden Informationen über die Kommunikation an den Leser- und Sub-Schnittstellen angezeigt. Diese Informationen sind für Servicetechniker hilfreich. Mit der Schaltfläche "Zähler zurücksetzen". Können die gezählten Ereignisse und Informationen auf Null zurückgesetzt werden.

Zum Testen der RS 485 Schnittstelle gehen Sie wie folgt vor:

► Setzen Sie alle Zähler mit der Schaltfläche "Zähler zurücksetzen" auf Null.

► Führen Sie eine 10-minütige Testperiode mit allen Lesern und Access Points durch:

- Die "Timeouts" sollten kleiner als 0,3% der "Erfolgreichen Pakete" sein.
- Es sollten keine "Kollisionen" auftreten. Wenn dieser Wert nicht Null ist, muss ein Widerstand an der betreffenden RS-485 Linie am GAT DC 7200 angeschlossen werden (siehe "4.4. Access Point GAT DL 091").

6.7.3 Update Kontroller

Mit dem Menüpunkt "Update Kontroller" können Sie eine neue Firmware aussuchen und diese auf den Controller laden. Den aktuellen Firmware-Stand sehen Sie unter Maintenance oder in der Titelzeile neben der Produktbezeichnung.

Es wird empfohlen vor dem Update ein Backup zu erstellen!
Beim Update des Controllers werden alle Berechtigungsdaten gelöscht. Der Controller muss nach dem Update unbedingt neu beladen werden! In der Stand-Alone Variante bleiben die Berechtigungsdaten beim Update erhalten.

6.7.4 Update Sub-Geräte

Im Menü "Update Sub-Geräte" werden alle angeschlossenen Leser und externen Geräte wie z. B. Relaisexpander aufgelistet und die Versionen der installierten Firmware werden angezeigt.

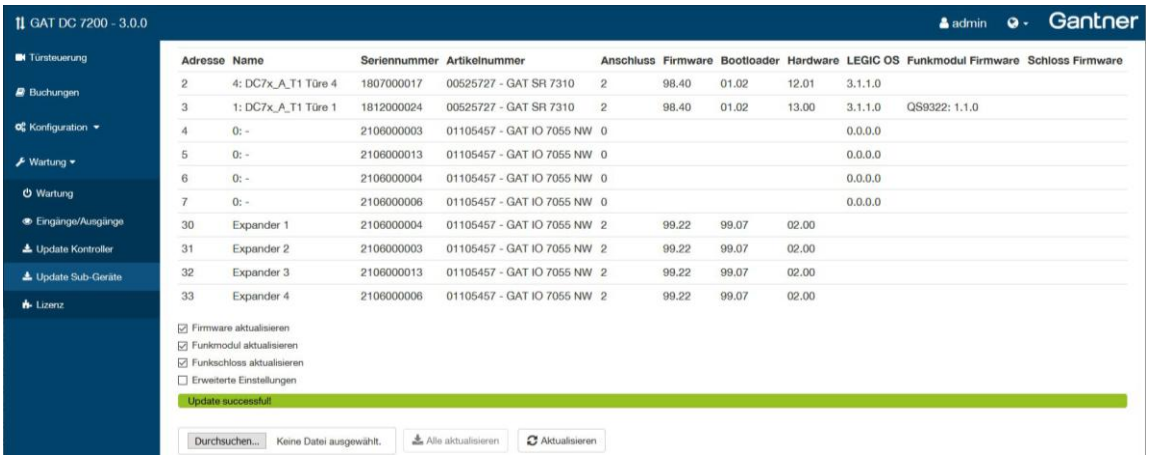


***Bild 6.51** – Web-Oberfläche – Aktualisierungen für Sub-Geräte*

- ► Wählen Sie mit Klick auf "Datei auswählen" eine neue Firmware (.zip Datei) für das Beladen der Sub-Geräte aus.
- ► Zur Aktualisierung der Firmware in einem Gerät markieren Sie die Option "Firmware aktualisieren".
- ► Die Firmware für die Funkmodule und Funkschlösser kann ebenfalls aktualisiert werden, indem die entsprechende Option unterhalb der Leserliste markiert wird. Die Firmware für diese Komponenten ist in der Firmware der GAT SR 73xx enthalten.
- ► Wählen Sie "Erweiterte Einstellungen“ aus, wenn Sie nur bestimmte Leser updaten möchten. Sie können dann eine Adresse eingeben, um nur das Sub-Gerät mit dieser Adresse zu beladen.
- ► Wählen Sie "Erweiterte Einstellungen" nicht aus, werden alle angeschlossenen Leser uns Sub-Geräte nacheinander aktualisiert.
- ► Sind unterschiedliche Leser angeschlossen, die unterschiedliche Firmware Versionen benötigen, so müssen Sie diesen Vorgang für jeden Leser Typ wiederholen, um alle Leser auf den gewünschten Software Stand zu bringen.

6.7.5 Lizenzen

Mit dem Menüpunkt "Lizenzen" können Sie im GAT DC 7200 weitere Softwarefunktionen aktivieren. Das folgende Bild zeigt einen GAT DC 7200, bei dem alle verfügbaren Erweiterungslizenzen aktiviert sind.

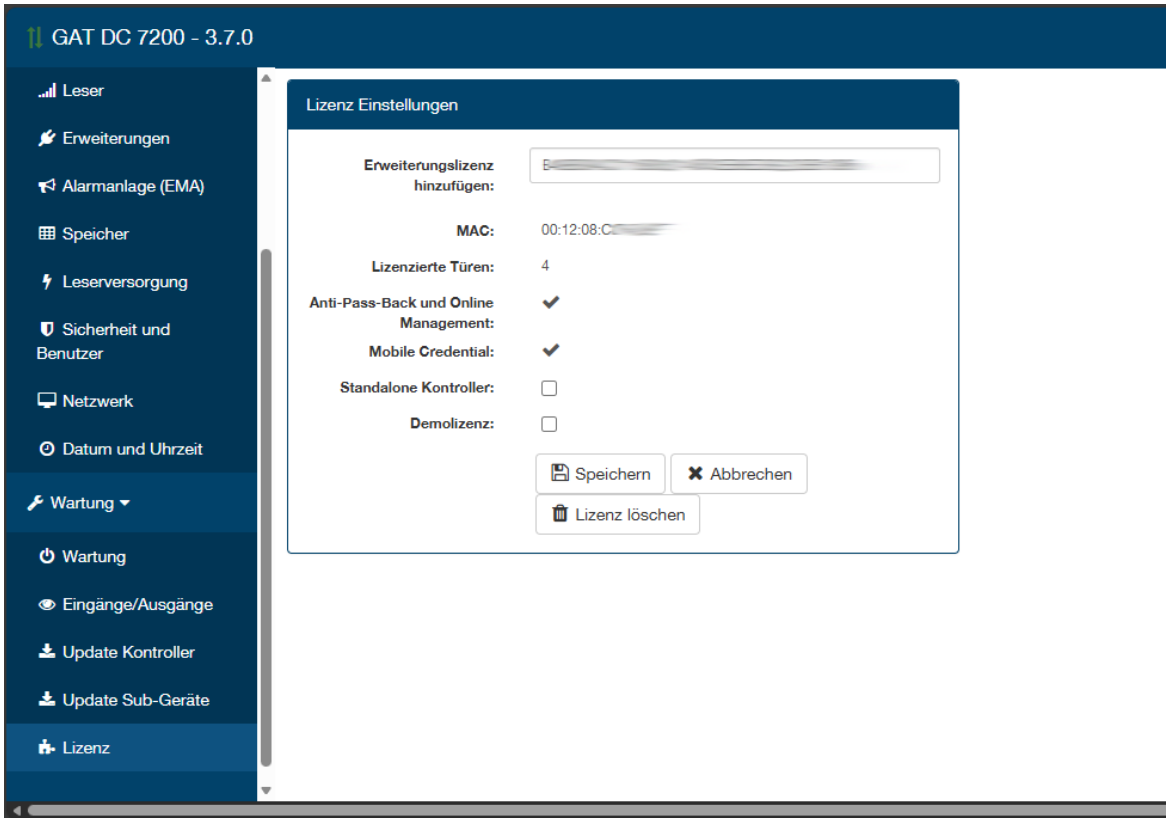


***Bild 6.52** – Web-Oberfläche – Lizenzeinstellungen*

Folgende Lizenzen sind verfügbar:

- Stand-Alone Lizenz: Zum Einsatz des GAT DC 7200 im Stand-Alone Modus. Ab der Version 2.1 ist die Stand-Alone Lizenz automatisch verfügbar. Zum Aktivieren dieser Lizenz markieren Sie die Option "Standalone Kontroller" (siehe "8. STANDALONE MODUS").
- PLUS Lizenz: Zur Erweiterung der steuerbaren Türen von 4 auf 16. Die Anzahl der steuerbaren Türen sehen Sie hinter "Lizenzierte Türen“.
- APB Lizenz: Zur Aktivierung der "Anti-Pass-Back" Funktion, die einen wiederholten Zutritt mit demselben Datenträger (z.B. durch Weitergabe des Datenträgers) verhindert.
  Diese Lizenz beinhaltet auch die Online Management Lizenz. Diese ist notwendig, wenn der GAT DC 7200 mittels der GAT DIRECT.Connect mit einer Drittsoftware verbunden werden soll.
- Liftsteuerung: Zur Ansteuerung von Liftsteuerungen und Schrankschlössern. Diese Funktion ist im Stand-Alone Modus nicht verfügbar.
- Mobile Credential: Mit dieser Funktion können Berechtigungen (Mobile Credentials) auf Mobilgeräten wie Smartphones oder Smartwatches für die Identifikation an Lesern am GAT DC 7200 verwendet werden. Siehe Abschnitt "6.5. Mobile Credential konfigurieren".

Die gewünschte Lizenz kann von GANTNER oder ihrem lokalen Vertriebspartner angefordert werden.

- ► Tragen Sie den Lizenzcode, den Sie per E-Mail oder Karte für Ihren Controller erhalten haben, in das entsprechende Feld ein und speichern Sie die Lizenz durch Klick auf "Speichern".
  - o Die aktivierten Funktionen werden unterhalb der MAC Adresse aufgelistet.
- ► Haben Sie mehrere Lizenzen, die Sie für den Controller aktivieren möchten, so wiederholen Sie den Vorgang für jede Lizenz.
- ► Um den GAT DC 7200 in den Stand-Alone Modus zu setzen, aktivieren Sie die Option "Standalone Kontroller“ (siehe "8. STANDALONE MODUS").
- ► Mit der Option "Demolizenz" können Sie temporär alle Lizenzen aktivieren und somit alle Funktionen wie max. Türanzahl von 16 Türen oder die Liftsteuerung freischalten. Die Demolizenz kann jederzeit aktiviert werden, läuft aber automatisch nach 4 Tagen ab. Das Ablaufdatum wird angezeigt.

  Hinweis: Die Demolizenz ist für Testzwecke hilfreich oder auch wenn Sie weitere Türen oder eine Liftsteuerung außerhalb der Geschäftszeiten konfigurieren und in Betrieb nehmen möchten. Sie können diese dann mit Aktivierung der Demolizenz vorab konfigurieren und in Betrieb nehmen und die notwendige Lizenz später z. B. am nächsten Tag bei GANTNER anfordern und einspielen.

Achten Sie darauf, dass die MAC Adresse des GAT DC 7200 mit der MAC Adresse, die in der Lizenz angegeben ist, übereinstimmen muss.

7 BERECHTIGUNGSVERGABE

Die Berechtigungsdaten beinhalten die Zutrittsberechtigungen und Zeitpläne für die Benutzer der Zutrittsanlage. Diese werden normalerweise mit einer eigenen Software (z. B. GAT Matrix) definiert. In dieser Software definieren Sie z B. die Zeiträume und die Türen, an denen die Personen zutrittsberechtigt sind. Außerdem sind noch viele weitere Funktionen möglich.

Eine detaillierte Beschreibung der Berechtigungsvergabe in der Matrix Software finden Sie im Bedienungshandbuch dieser Software.

Wenn der GAT DC 7200 über die GAT DIRECT.Connect an eine Drittsoftware angebunden wird, kann die Berechtigungsvergabe und Steuerung der Türfreigaben auch über diese Drittsoftware erfolgen. Lesen Sie dazu die Dokumentation dieser Software. Nachfolgend wird die Berechtigungsvergabe mit Blick auf Matrix beschrieben.

Die Berechtigungsdaten werden von der Zutrittskontrollsoftware Matrix über die GAT ACE 7000 Software an das GAT DC 7200 geladen.

Stand-Alone Modus

Für den Fall, dass durch Einspielen einer Lizenz der Stand-Alone Mode des GAT DC 7200 aktiviert wurde, ist die Berechtigungsvergabe und die Kommunikation mit der Software Matrix und GAT ACE 7000 nicht mehr möglich und die Berechtigungsverwaltung erfolgt direkt am GAT DC 7200. Weitere Infos für diesen Fall finden Sie im Kapitel "8. STANDALONE MODUS". Um wieder mit der Software kommunizieren zu können, löschen Sie die Standalone Lizenz!

CardNET

Im CardNET System werden die Berechtigungsdaten von einer Zutrittskontrollsoftware wie z. B. Matrix erstellt und können an einen GAT DC 7200 gesendet werden. Wenn die Schreibfunktion für CardNET im Türcontroller aktiviert ist (siehe "6.4.8. Leserkonfiguration"), werden die CardNET Berechtigungsdaten für einen Datenträger beim Lesen des Datenträgers an einem angeschlossenen Leser auf den Datenträger geschrieben. Außerdem werden auch Buchungen und Informationen wie Batteriewarnungen von den CardNET Datenträgern gelesen und vom Türcontroller an die Berechtigungssoftware gesendet.

Mobile Credential

Mit Mobile Credential ist es möglich, dass sich Benutzer mit ihrem Mobilgerät wie z. B. einem Smartphone oder Smartwatch und dem darauf gespeicherten Berechtigungsausweis (in Google oder Apple Wallet) in der Zutrittsanlage identifizieren können. Um Mobile Credential mit einem GAT DC 7200 und angeschlossenem Leser nutzen zu können, ist die passende Lizenz notwendig. Mehr Informationen siehe "6.5. Mobile Credential konfigurieren".

GANTNER SVN

GANTNER SVN ist eine Kombination aus der Salto Virtual Network (SVN) Technologie und MIFARE DESFire Datenträger mit einer GANTNER Codierung.
Bei der Verwendung von GANTNER SVN (siehe auch "6.4.8. Leserkonfiguration") werden Zutrittsberechtigungen, die in Matrix für SALTO Produkte erstellt werden, an Online-Lesern auf die GANTNER codierten Datenträger geschrieben. Die SALTO Produkte prüfen diese Berechtigungen und speichern die Zutrittsereignisse auf den Datenträgern. Von Online-Lesern werden diese Ereignisse aus den Datenträgern ausgelesen und in die Matrix zurück gemeldet.
Eine Kombination aus GANTNER SVN und CardNET Technologie ist technisch möglich, um gemischte Systeme betreiben zu können.

Voraussetzungen:

- Um die GANTNER SVN Funktion nutzen zu können, sind mind. folgende Softwareversionen notwendig:
  - SALTO ProAccess SPACE - mind. Version 6.8
  - GAT ACE 7000 - mind. Version 2.2
  - Matrix mind. Version 5.2
  - Leser-Firmware mind. Version 3.4.0
- GAT Authorisation Tag 400 BA
- Die notwendigen Einstellungen in Matrix und GAT ACE 7000 sind in den jeweiligen Dokumentationen dieser Software zu finden.
- Es können nur RFID Datenträger vom Typ MIFARE DESFire verwendet werden. Diese müssen mit einem GANTNER SVN File codiert sein. Die Codierung wird für neue Anlagen im Standard codiert. Für bestehende Anlagen können Datenträger bei Neubestellungen diese Codierung zusätzlich erhalten (sprechen Sie dafür mit Ihrem Lieferanten des Zutrittskontrollssystems). Eine Nachcodierung bestehender Ausweise ist oftmals über GT7 Codierstationen möglich.
- Um die GANTNER SVN Daten vor dem Schreiben zu kodieren, ist an mind. einer ProAccess SPACE Installation ein Dongle Encoder notwendig, bei dem mind. Firmware Version 01.12 installiert sein muss. Näheres zu den notwendigen Einstellungen in ProAccess SPACE finden Sie in der Bedienungsanleitung von Matrix.

8 STANDALONE MODUS

Um den GAT DC 7200 ohne Softwareinstallation am PC betreiben zu können, kann dieser in einen Standalone Modus gesetzt werden. In diesem Modus können die Personen und Berechtigungen, Zeit- und Tagespläne sowie der Betriebskalender über die Weboberfläche des GAT DC 7200 verwaltet werden.

Ab Version 2.1 ist die Standalone Lizenz automatisch im GAT DC 7200 verfügbar. Es wird in dem Fall keine zusätzliche Lizenz zur Aktivierung dieser Funktion benötigt.

8.1 Zielgruppe

Dieses Kapitel enthält Informationen für die Administratoren der Zutrittsbrechtigungen. Diese Informationen sind nicht für die Benutzer der Zutrittsanlage bestimmt.

8.2 Standalone Modus aktivieren

Um den GAT DC 7200 in den Standalone Modus zu bringen, stellen Sie sicher, dass auf der "Lizenz“ Seite im Wartungs-Menü die Option "Standalone" markiert ist.

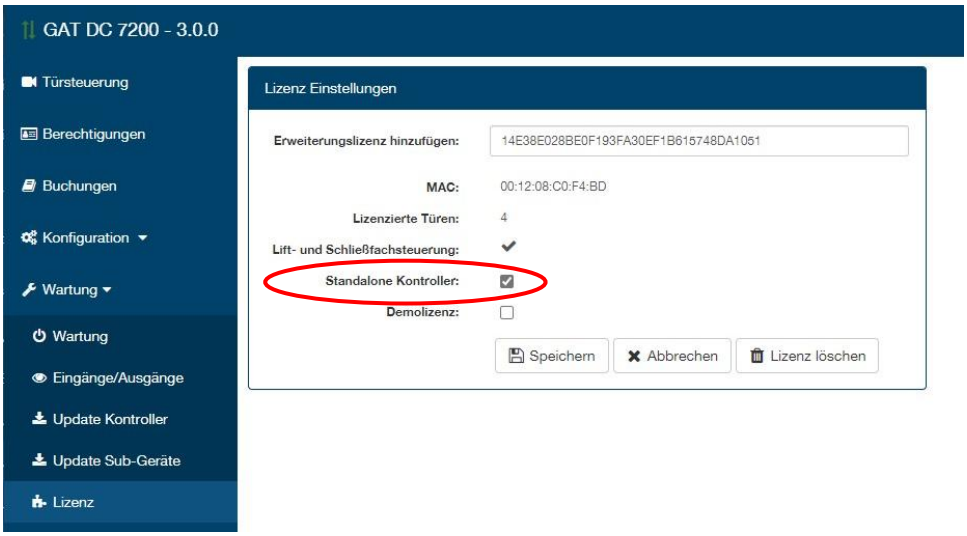


***Figure 8.1** –Web Oberfläche – Standalone Modus aktivieren*

Der Standalone Modus kann auch mit der PLUS Lizenz kombiniert werden, um bis zu 16 Türen verwalten zu können.

Durch Aktivierung des Standalone Modus werden einige Einstellungen des Controllers ausgeblendet, die in der Variante ohne Standalone verfügbar sind. Weiters wird auch die Kommunikation zwischen GAT ACE 7000 und dem GAT DC 7200 durch den Standalone Modus deaktiviert.

8.3 Berechtigungen verwalten

Im Menüpunkt "Berechtigungen“ können Berechtigungen erstellt und verwaltet werden. Dazu zählen Personen mit Ausweisen und Fingerabdrücken, Zeit- und Tagespläne und der Betriebskalender.

HINWEIS! Werden Änderungen an diesen Daten gemacht, müssen diese unbedingt vor dem Verlassen der Seite mit "Änderungen speichern" gespeichert werden. Wird die Seite verlassen oder der Browser geschlossen, so werden die Änderungen nicht gespeichert.

Wurden Änderungen noch nicht gespeichert und Sie verlassen die Konfigurationsoberfläche des GAT DC 7200, so wird ein Warnhinweis ausgegeben.

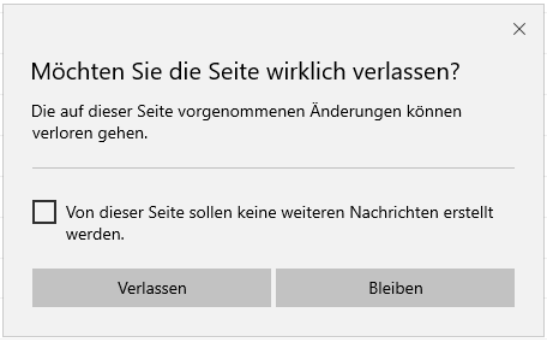
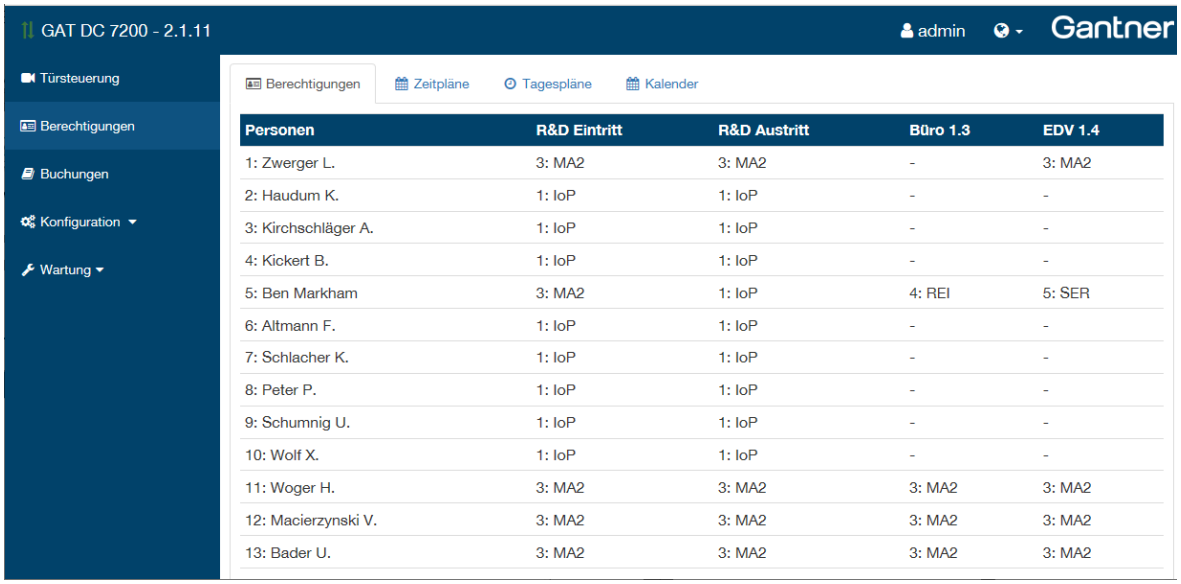


***Bild 8.2** – Warnungsmeldung für noch nicht gespeicherte Einstellungen*

- ► Wenn Sie die Änderungen nicht verlieren möchten, wählen Sie "Bleiben" und speichern Sie die Änderungen.
- ► Wenn Sie die Seite mit "Verlassen" schließen, so werden die Änderungen nicht gespeichert!

8.3.1 Personen und Berechtigungen hinzufügen



Personen	R&D Eintritt	R&D Austritt	Büro 1.3	EDV 1.4
1: Zwerger L.	3: MA2	3: MA2	-	3: MA2
2: Haudum K.	1: IoP	1: IoP	-	-
3: Kirchschläger A.	1: IoP	1: IoP	-	-
4: Kickert B.	1: IoP	1: IoP	-	-
5: Ben Markham	3: MA2	1: IoP	4: REI	5: SER
6: Altmann F.	1: IoP	1: IoP	-	-
7: Schlacher K.	1: IoP	1: IoP	-	-
8: Peter P.	1: IoP	1: IoP	-	-
9: Schumnig U.	1: IoP	1: IoP	-	-
10: Wolf X.	1: IoP	1: IoP	-	-
11: Woger H.	3: MA2	3: MA2	3: MA2	3: MA2
12: Macierzynski V.	3: MA2	3: MA2	3: MA2	3: MA2
13: Bader U.	3: MA2	3: MA2	3: MA2	3: MA2

***Bild 8.3** – Web-Oberfläche – Zutrittsberechtigungen für Standalone Funktion*

► Um zutrittsberechtigte Personen anzulegen und diesen Berechtigungen zuzuweisen, wählen Sie im Menüpunkt "Berechtigungen" auf der gleichnamigen Registerkarte "Berechtigungen" die Funktion "Person hinzufügen“.

- Dadurch öffnet sich das Fenster zur Eingabe von Personendaten.

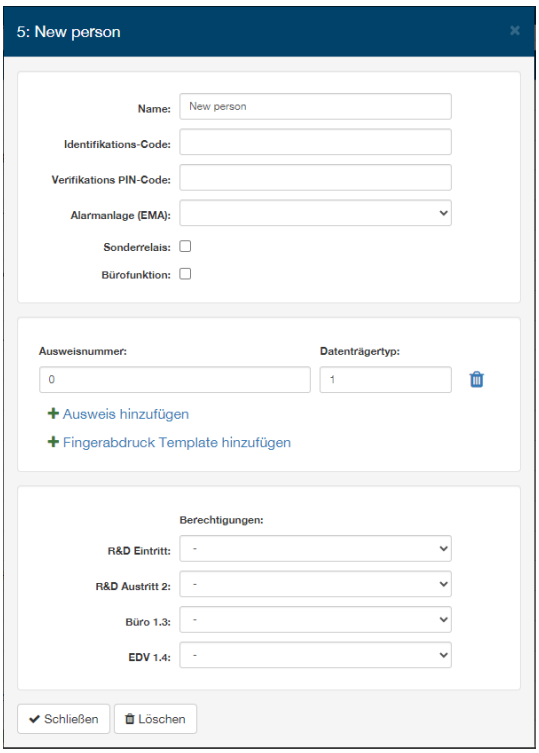


***Bild 8.4** – Web-Oberfläche – Person hinzufügen*

► In diesem Fenster können die Personendaten und die Zutrittsberechtigungen eingegeben werden.

- Name: Geben Sie einen Namen für die Person ein.
- Identifikations-Code: Dieser Code ist eine Nummernkombination, die als Identifikation neben den Datenträgern oder Fingerprints verwendet werden kann. Somit kann eine Türe auch in einer einfachen Codeschloss-Funktion betrieben werden, wobei jede Person einen eigenen Code besitzt und dieser auch zusätzlich mit einem PIN-Code oder Fingerprint kombiniert werden kann. Die Möglichkeit zur Verwendung des Identifikation-Codes muss in den Zeit- und Tagesplänen freigeschaltet werden.
- Verifikations PIN-Code: Dies ist eine geheimer PIN-Code, der zusätzlich zur Identifikation mit dem Datenträger erfasst werden kann, um sicher zu stellen, dass der Inhaber des Datenträgers auch der rechtmäßige Besitzer ist. Die PIN-Code Abfrage kann in den Zeit- und Tagesplänen aktiviert werden.
- Alarmanlage (EMA): Hier kann festgelegt werden, ob die Person berechtigt ist die Einbruchmeldeanlage (EMA) scharf- und unscharf zu schalten.
- Sonderrelais: Diese Einstellung legt fest, ob die Person eine Sonderberechtigung besitzt und das entsprechende Sonderberechtigungsrelais bei einem Zutritt aktiviert werden soll. Die Sonderberechtigung gilt für alle Türen des Controllers.
- Bürofunktion: Wenn Sie diese Einstellung markieren, ist die Bürofunktion für diese Person aktiviert. Bei aktivierter Bürofunktion wird nach gültiger Identifikation des Benutzers an einer Tür diese generell entriegelt (=Bürofunktion aktiv) bis eine weitere Identifikation desselben

Benutzers die Türe wieder verriegelt (in den autonomen Modus setzt). Die Tür kann dann wieder von einem berechtigten Benutzer geöffnet werden.

Bitte beachten Sie, dass abhängig von der Einstellung an der Tür beim Parameter "Bürofunktion" jede Person oder nur berechtigte Personen definiert werden können.

- Ausweis hinzufügen: Mit dieser Schaltfläche können beliebig viele Datenträger für eine Person definiert werden. Neben der Nummer des Datenträgers muss auch der Typ eingegeben werden. Die Definition der Typen erfolgt im Menü "Konfiguration" -> "Leser" -> "Ausweise". Die Nummer eines Datenträgers ist oftmals aufgedruckt oder kann ermittelt werden, indem der Datenträger an einen Leser gehalten wird und die Nummer und der Typ aus der dadurch erstellten Buchung verwendet werden. Alternativ kann die Nummer über einen USB Desktop Reader (Art. Nr. 863231) ausgelesen wird.
- Fingerabdruck Template hinzufügen: Mit dieser Schaltfläche können bis zu zwei Fingerabdrücke pro Person erfasst werden, die dann zur Identifikation oder Verifikation verwendet werden können. Die Auswahl, ob die Finger für Identifikation oder Verifikation verwendet werden sollen, erfolgt im Menü "Konfiguration" -> "Türen" –> "Fingerabdruck".

  Für die Erfassung der Fingerprints ist die Software "GAT FR 010 Scanner" verfügbar, die mit einem GAT FR 010 Fingerprintleser die Templates erfasst und in die Zwischenablage des PCs legt. Aus der Zwischenablage können die Daten in das Feld des Controllers übernommen werden. Die Software kann über den Link neben dem Erfassungsfeld heruntergeladen werden.

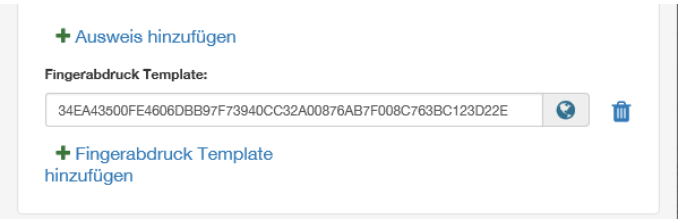


***Bild 8.5** – Web-Oberfläche – Vorlagen für Fingerabdrücke*

  Nach der Installation der Software auf dem PC und dem Anschluss eines Fingerprint Scanners am PC können die Finger eingelesen werden. Legen Sie dazu einen Finger drei Mal auf den Leser, um diesen zu erfassen. Danach werden Sie aufgefordert, den Finger ein weiteres Mal zur Verifizierung auf den Scanner zu legen.

  Ist die Qualität der biometrischen Merkmale ausreichend hoch, wird das erfasste Fingertemplate als Text (Hexadezimal-Zeichenkette) in die Zwischenablage eingefügt. Von dort kann es in das Erfassungsfeld im Browser eingefügt werden, um es im Controller zu speichern. Die Software ist unmittelbar nach der Verifikation für eine weitere Erfassung des nächsten Fingers bereit.
- Berechtigungen: Hier sind die definierten Türen aufgelistet. Pro Türe kann ein Zeitplan ausgewählt werden. Der Zeitplan "Always“ (Immer ohne PIN) ist als Standard-Zeitplan vorhanden und kann sofort verwendet werden. Weitere Zeitpläne können auf der Registerkarte "Zeitpläne" angelegt werden.

► Über "Schließen" verlassen Sie das Eingabefenster.

  - Die Daten werden erst für den GAT DC 7200 wirksam, wenn diese mit "Änderungen speichern" gespeichert werden.

► Sollen Berechtigungen oder Daten einer Person geändert werden, wählen Sie die Person aus, um das Detailfenster erneut zu öffnen.

► Im Fenster können Sie auch die Personen löschen.

8.3.2 Zeitpläne hinzufügen

In der Registerkarte "Zeitpläne“ sind die vorhandenen Zeitpläne aufgelistet.
Es gibt Personen-Zeitpläne und Tür-Zeitpläne. Die obere Tabelle zeigt die Personalzeitpläne. Diese können den Personen, die die Zutrittsanlage benutzen, zugewiesen werden. Als Standard ist der Zeitplan "IoP“ definiert, der an 7 Tagen der Woche, einen 24-Stunden Zutritt ermöglicht. Weitere Zeitpläne können erstellt werden. Die untere Tabelle listet alle Türen auf und zeigt die Zeitpläne, die den Türen zugewiesen ist.
Die Nummern in den Tabellen sind die Nummern der Tagespläne, die den Personen und Türen an den entsprechenden Wochentagen und Sondertagen zugewiesen sind.

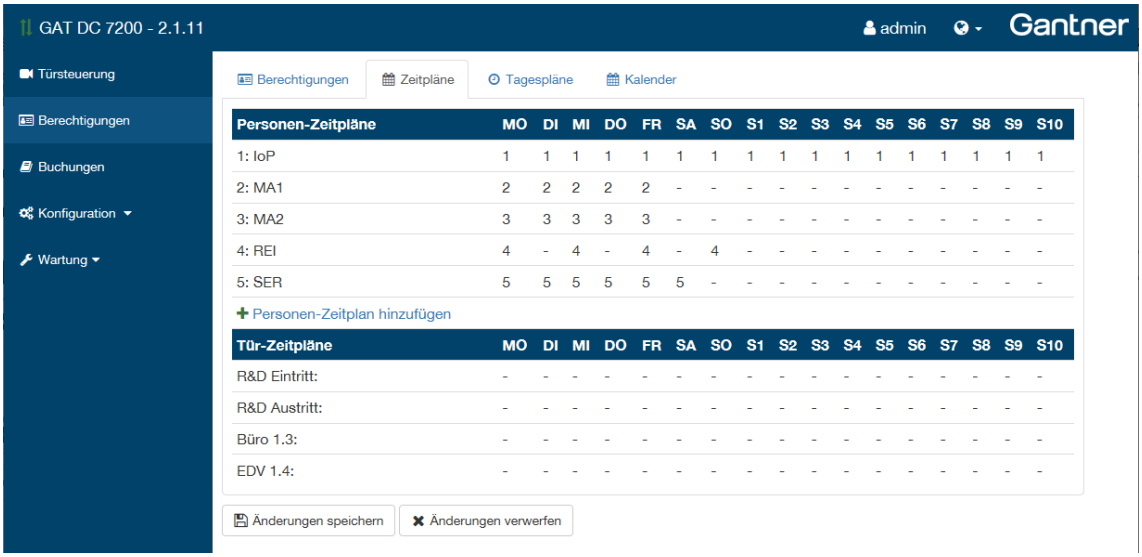


***Bild 8.6** – Web-Oberfläche - Zeitpläne für Standalone Funktion*

Personen-Zeitpläne:

Die Personen-Zeitpläne werden in der oberen Tabelle aufgelistet und erstellt.

► Klicken Sie auf einen Personen-Zeitplan, um diesen zu bearbeiten, oder klicken Sie auf "Personen-Zeitplan hinzufügen“, um weitere Zeitpläne hinzuzufügen.

- Es öffnet sich ein Fenster, in dem der Zeitplan bearbeitet werden kann.

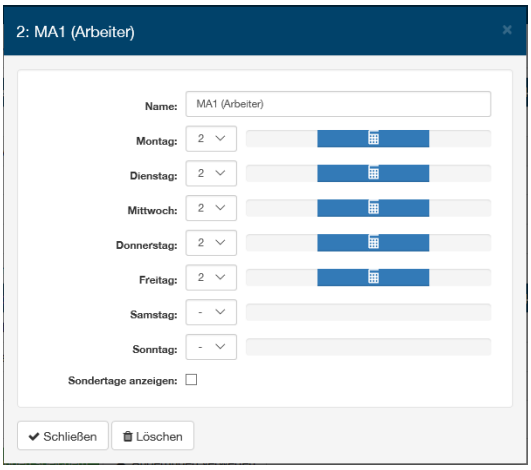


***Bild 8.7** – Web-Oberfläche – Personen-Zeitplan Konfiguration*

- ► Bei "Name" kann ein Name für den Zeitplan vergeben werden.
- ► Pro Wochentag und pro Sondertagetyp kann ein Tagesplan mit zeitlichen Berechtigungen ausgewählt werden. Tagespläne können auf der Registerkarte "Tagespläne" erstellt werden (siehe nächster Abschnitt).
- ► Mit Klick auf "Schließen“ verlassen Sie das Eingabefenster.
  - o Die Daten werden erst für den GAT DC 7200 wirksam, wenn diese mit "Änderungen speichern" gespeichert werden.

Tür-Zeitpläne:

Die Tür-Zeitpläne werden in der unteren Tabelle aufgelistet und erstellt. Hier sind alle Türen aufgelistet.

- ► Klicken Sie auf einen Personen-Zeitplan, um diesen zu bearbeiten, oder klicken Sie auf "Personen-Zeitplan hinzufügen“, um weitere Zeitpläne hinzuzufügen.
  - o Es öffnet sich ein Fenster, in dem der Zeitplan bearbeitet werden kann.

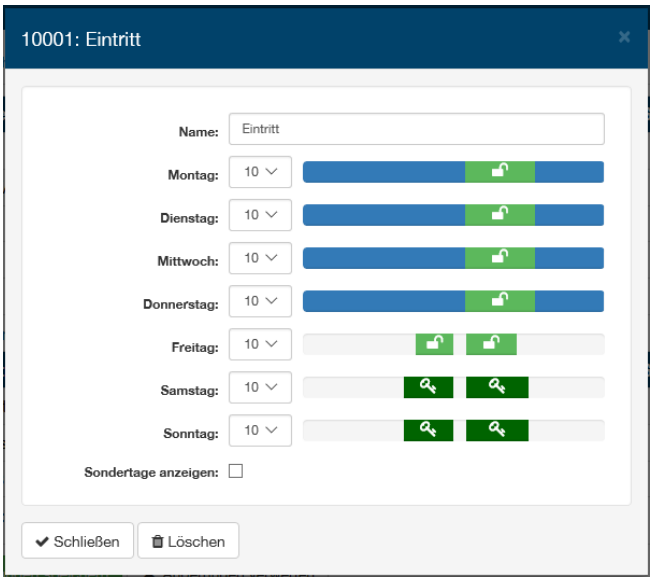


***Bild 8.8** – Web-Oberfläche – Tür-Zeitplan Konfiguration*

- ► Bei "Name" kann ein Name für den Zeitplan vergeben werden.
- ► Pro Wochentag und pro Sondertagetyp kann ein Tagesplan mit zeitlichen Berechtigungen ausgewählt werden.
- ► Tagespläne können auf der Registerkarte "Tagespläne" erstellt werden (siehe nächster Abschnitt).
- ► Mit Klick auf "Schließen“ verlassen Sie das Eingabefenster.
  - o Die Daten werden erst für den GAT DC 7200 wirksam, wenn diese mit "Änderungen speichern" gespeichert werden.

8.3.3 Tagespläne hinzufügen

Im Register "Tagespläne“ sind die vorhandenen Tagespläne aufgelistet. Im Standard ist der Zeitplan 0 – 24 Uhr ohne PIN definiert. Weitere Tagespläne können erstellt werden.

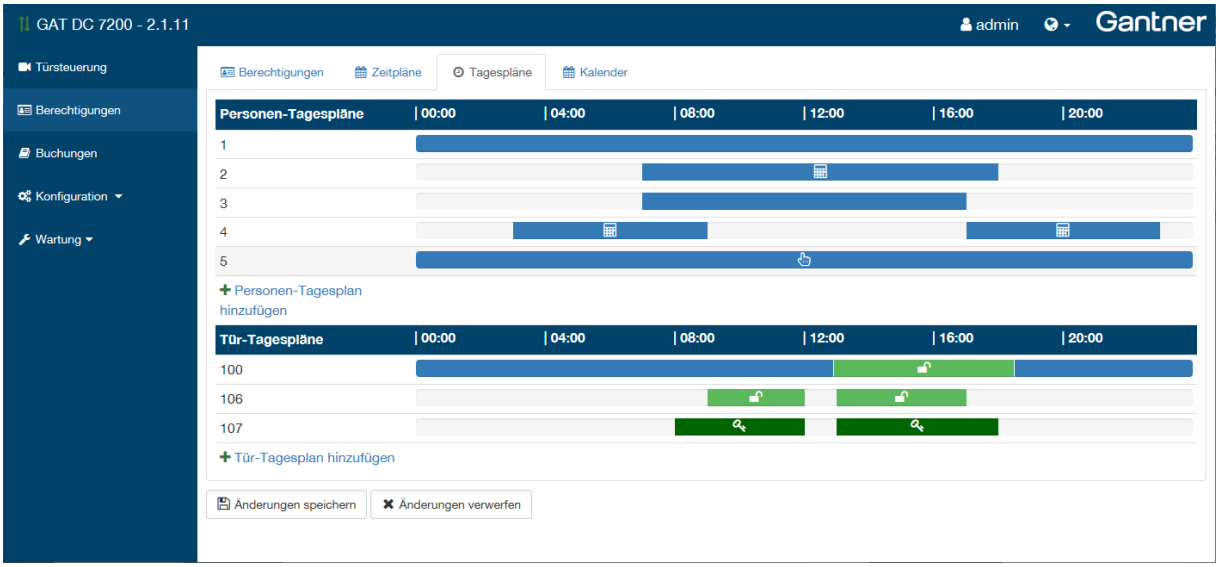


***Bild 8.9** – Web-Oberfläche - Tagespläne*

Personen-Tagespläne:

Die Tagespläne für Personen werden in der oberen Tabelle aufgelistet und erstellt.

► Klicken Sie auf einen Personen-Tagesplan, um diesen zu bearbeiten, oder klicken Sie auf "Personen-Tagesplan hinzufügen“, um weitere Tagespläne hinzuzufügen.

- Es öffnet sich ein Fenster, in dem der Tagesplan bearbeitet werden kann.

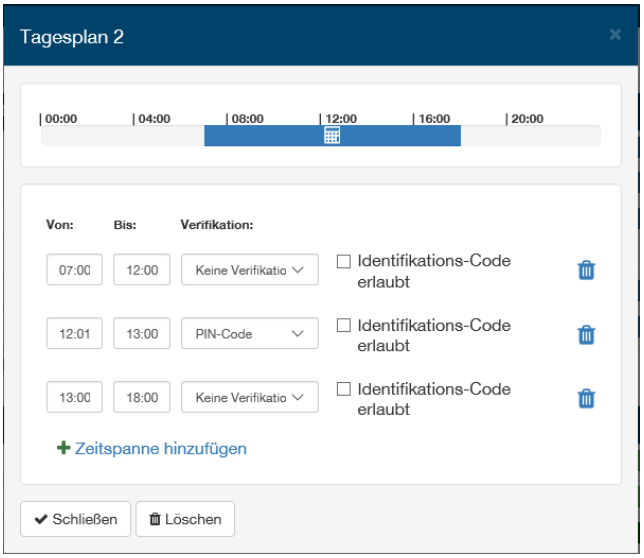


***Bild 8.10** – Web-Oberfläche – Tagesplan für Personen konfigurieren*

► Sie können bis zu 10 Zeitspannen definieren und die Art der Verifikation in jedem Zeitspanne festlegen. Diese Fügen Sie mit der Schaltfläche "Zeitspanne hinzufügen" ein. Folgende Einstellungen sind pro Zeitspanne möglich:

- Von, Bis: Geben Sie hier die Start- und Endzeit der Zeitspanne ein.
- Verifikation: Hier kann festgelegt werden, ob eine Verifikation erforderlich ist und ob diese mittels PIN Code oder Fingerabdruck erfolgen muss.
- Identifikations-Code erlaubt: Hier kann festgelegt werden, ob in dieser Zeitspanne ein Zutritt durch Eingabe des Identifikations-Codes möglich sein soll oder nicht.

► Einzelne Zeitspannen können über das Symbol gelöscht werden.

► Der gesamte Tagesplan kann über "Löschen" gelöscht werden.

► Bestätigen Sie die Eingaben mit Klick auf "Schließen" und anschließend in der Tagesplanübersicht mit "Änderungen speichern", um die Änderungen im GAT DC 7200 zu übernehmen.

Tür-Tagespläne:

Die Tagespläne für Türen werden in der unteren Tabelle aufgelistet und erstellt.

► Klicken Sie auf einen Tür-Tagesplan, um diesen zu bearbeiten, oder klicken Sie auf "Tür-Tagesplan hinzufügen“, um weitere Tagespläne hinzuzufügen.

- Es öffnet sich ein Fenster, in dem der Tagesplan bearbeitet werden kann.

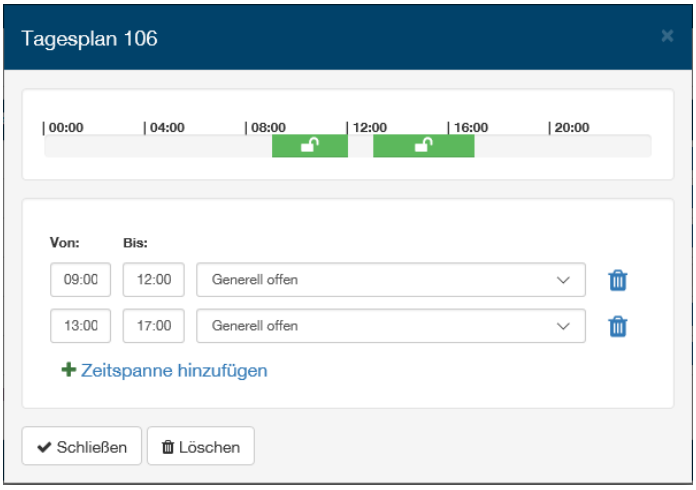


***Bild 8.11** – Web-Oberfläche – Tagesplan für Türen konfigurieren*

► Sie können bis zu 10 Zeitspannen definieren und die Art der Türansteuerung in jedem Zeitspanne festlegen. Diese fügen Sie mit der Schaltfläche "Zeitspanne hinzufügen" ein. Folgende Einstellungen sind pro Zeitspanne möglich:

- Von, Bis: Geben Sie hier die Start- und Endzeit der Zeitspanne ein.
- Funktion: Wählen Sie zwischen:
  - Generell offen: Türe wird entriegelt und kann ohne Identifikation geöffnet werden.
  - Generell offen nach gültigem Zutritt: Wie Funktion zuvor. Aktivierung durch einen gültigen Zutritt.
  - Bürofunktion: Durch jede gültige Identifikation wird zwischen Generell offen und autonom (Öffnen durch gültige Identifikation) gewechselt.
  - Nur Firmen ID prüfen: Es wird nur geprüft, ob der Datenträger zum System zugehörig ist. Diese Funktion kann nur für codierte Ausweise an verkabelten Lesern verwendet werden.
  HINWEIS! Offline Produkte (auch mit WiNET Vernetzung) unterstützen diese Funktion nicht.

- ► Einzelne Zeitspannen können über das Symbol gelöscht werden.
- ► Der gesamte Tagesplan kann über "Löschen" gelöscht werden.
- ► Bestätigen Sie die Eingaben mit Klick auf "Schließen" und anschließend in der Tagesplanübersicht mit "Änderungen speichern", um die Änderungen im GAT DC 7200 zu übernehmen.

8.3.4 Sondertage hinzufügen

Es können in den Kalender des GAT DC 7200 Sondertage eingetragen werden. Über die Zeitpläne kann festgelegt werden, dass an diesen Sondertagen andere Berechtigungen als an normalen Wochentagen gelten.

Dazu sind bis zu 10 verschiedene Arten von Sondertagen (S1 bis S10) möglich. Diese können für beliebig viele Tage im Kalender hinterlegt werden. Der Sondertagetype S1 ist für Feiertage und der Sondertagetyp S2 ist für halbe Feiertage vorgesehen. Die restlichen Typen können kundenspezifisch verwendet werden.

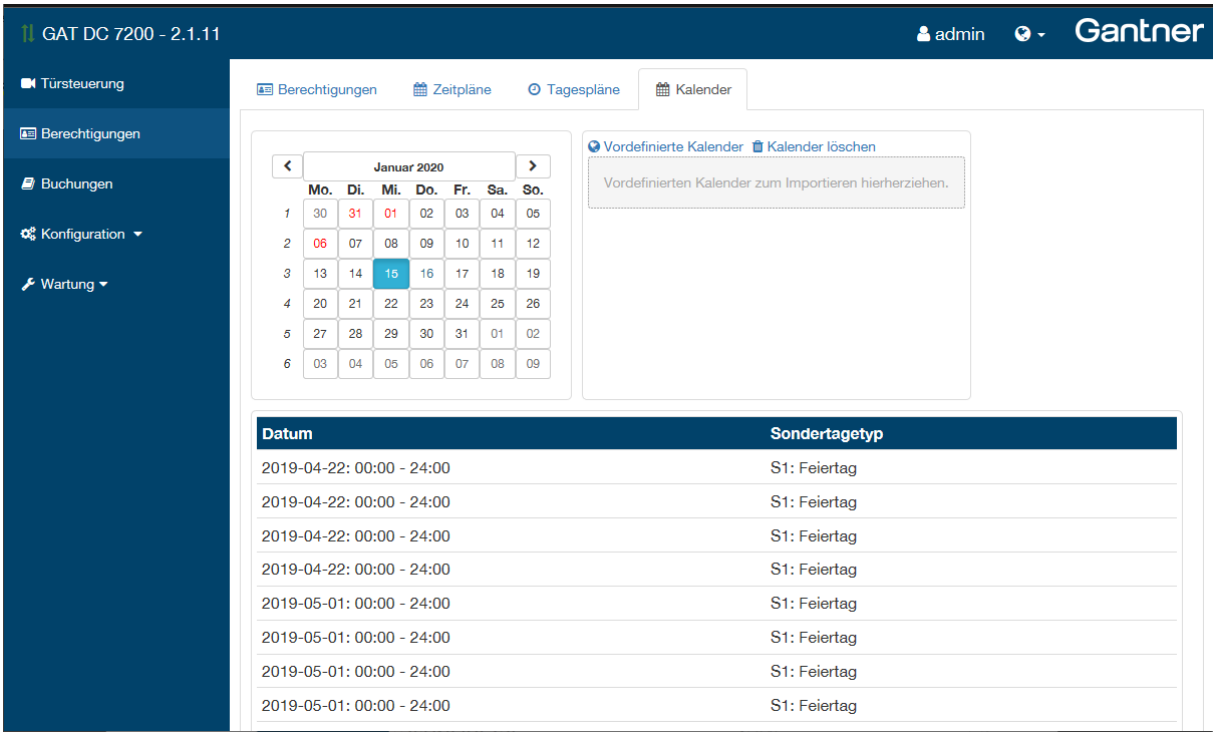
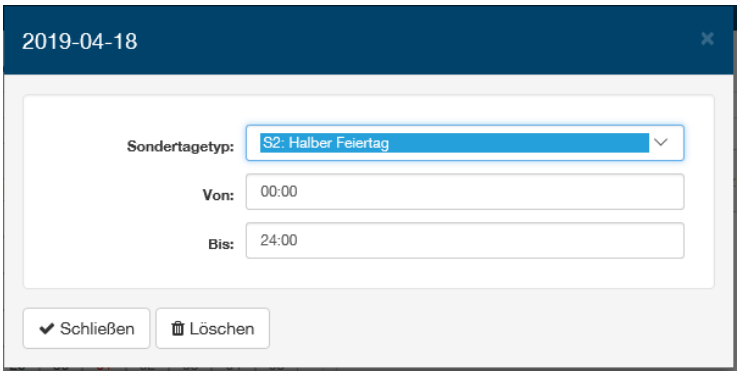


***Bild 8.12** – Web-Oberfläche – Betriebskalender*

- ► Mit der Funktion "Vordefinierte Kalender“ können bereits vorbereitete Kalender von der GANTNER Website geladen werden. Diese Kalender werden in Form eines Files auf den PC geladen und können dann per Drag&Drop auf das vorgesehene Feld im Browser gezogen werden.
  - o Dadurch werden die Sondertage im GAT DC 7200 importiert.
- ► Mit der Schaltfläche "Kalender löschen“ können alle vorhandenen Sondertage gelöscht werden.

► Zum Hinzufügen eines Sondertages wählen Sie den Tag im Kalender aus.
  - Dabei öffnet sich ein Eingabefenster, in dem Sie den Typ des Sondertags auswählen können.



► Die Sondertage sind standardmäßig für den ganzen Tag gültig. Indem eine Beginn- und Endzeit bei den Feldern "Von" und "Bis" eingegeben wird, kann der Sondertag auf ein Zeitfenster (z. B. für eine Veranstaltung an einem Tag) begrenzt werden, so dass vor und nach diesem Zeitfenster die normalen Zutrittsrechte gelten.

► Mit der Schaltfläche "Löschen" können Sie einen einzelnen Sondertag löschen.

► Mit der Schaltfläche "Schließen“ verlassen Sie das Eingabefenster.
  - Die Daten werden erst für den GAT DC 7200 wirksam, wenn diese mit "Änderungen speichern“ auf der Seite "Berechtigungen" gespeichert werden.

8.4 Einschränkungen des Standalone Modus

Im Standalone Modus des GAT DC 7200 sind die meisten Funktionen des GAT DC 7200 verfügbar. Es gibt jedoch auch einige Einschränkungen:

- Die Sonderberechtigungen von Personen können nicht so fein gesteuert werden, wie dies in der vernetzen Variante über die Software möglich ist.
- Die Einbindung von batteriebetriebenen Schlössern ist nur im WiNET Mode möglich. CardNET oder Read Only Modes werden in der Standalone Variante nicht unterstützt.
- Lift- oder Schließfachsteuerungen sind in der Standalone Variante nicht möglich.
- Im Standalone Mode ist keine Kommunikation mit GAT Matrix oder GAT ACE 7000 möglich. Die Berechtigungen können in diesem Fall nur am GAT DC 7200 verwaltet werden!

9 FRAGEN UND ANTWORTEN

9.1 Ein- und Austritt

Für die Steuerung einer Türe mit Ein- und Austritt werden beim GAT DC 7200 zwei Türen verwendet. Dadurch ist eine genaue Einstellung der Berechtigungen inklusive der erforderlichen Kriterien für Identifikation und Verifikation möglich. Die Berechtigungen für Ein- und Austritt können auch unterschiedlich vergeben werden.

Die Kopplung der Türen erfolgt am Controller automatisch, wenn für zwei Türen die gleichen Ein- und Ausgänge für die Türe verwendet werden. So wird die Signalisierung an der Türe richtig dargestellt und es wird beim Öffnen der Türe in der anderen Richtung kein Alarm ausgelöst.

Beachten Sie dass für eine Türe mit Ein- und Austritt am GAT DC 7200 und in der Matrix zwei Türlizenzen vorhanden sein müssen!

9.2 Funksender

GAT Active Tag 552 oder GAT Active Tag 554 und der GAT Reader 550 AA können am GAT DC 7200 unter Verwendung eines GAT SR 7000 Wiegand angeschlossen werden.

Pro Controller kann nur ein GAT Reader 550 AA verwendet werden!

9.3 WiNET Access Points

An einem GAT DC 7200 können bis zu vier GAT DL 091 für maximal 16 Türen betrieben werden.

9.4 Türlizenzen

Der GAT DC 7200 ist für die Steuerung von vier Türen ausgelegt.
Durch den Erwerb einer GAT DC 7200 PLUS License kann die Funktion für 16 Türen erweitert werden. Die Lizenz wird nach Bekanntgabe der MAC Adresse per E-Mail an den Kunden gesendet (Art. Nr. 732222) oder bei Bestellung der Art. Nr. 753023 in Form einer Karte mit den aufgedruckten Lizenzdaten an den Kunden geliefert.

Die Lizenz kann über die Web-Oberfläche des Controllers eingegeben werden.

9.5 Proxy Ausweise

Proxy Ausweise werden vom GAT DC 7200 ohne die bisher verwendeten Proxy Customer Codes verwaltet. Dadurch ist eine Umstellung der Ausweisnummern erforderlich!

Die bisher typischen Proxy Customer Codes waren 001 = 0, 004 = 1, 015 = 2. Daraus ergeben sich das z. B. die bisherige Ausweisnummer 12345678901 des FLEX Systems wird im neuen System 0042345678901 lauten.

9.6 Proxy Leser

Proxy Leser wie der GAT Reader 405 AP und GAT Reader 500 UP können unter Verwendung eines GAT SR 7000 Wiegand an den GAT DC 7200 angeschlossen werden.

Vom GAT SR 7000 Wiegand wird keine Richtungsunterscheidung über die Card-in-Reader Leitung oder über die Sub-Brücke unterstützt.

Es müssen für Ein- und Austritt zwei GAT SR 7000 Wiegand verwendet werden. Es können bis zu max. 16 GAT SR 7000 Wiegand an einem Controller betrieben werden.

9.7 Liftsteuerung

Die Lift- oder Schließfachsteuerung können am GAT DC 7200 mit Relaisexpandern (einem oder zwei GAT IO 055 oder mit bis zu 8 GAT IO 7054 und/oder GAT IO 7055) realisiert werden. Dadurch stehen bis je nach Expander eine unterschiedliche Anzahl weiterer Relaisausgänge und Optokopplereingänge zur Verfügung. Die Relais können einer oder mehreren Türen zugewiesen werden. Die Relaisexpander werden an der SUB bzw. Reader Schnittstelle des GAT DC 7200 angeschlossen.

Für die Lift- oder Schließfachsteuerung ist die GAT DC 7200 Elevator License erforderlich. Ohne diese Lizenz können die Relais der Relaisexpander nur als allgemeine Ausgänge verwendet werden.

Mit GAT DIRECT.Connect ist die Liftsteuerung nicht möglich.

9.8 Anti-Pass-Back

Die Anti-Pass-Back Funktion ist in der Version 1.0 des GAT DC 7200 noch nicht enthalten. Diese Funktion wird zu einem späteren Zeitpunkt realisiert. Der erste Entwicklungsschritt wird ein „lokales Anti-Pass-Back“ auf dem Controller sein. Ein „Controller übergreifendes Anti-Pass-Back“ wird in einem weiteren Schritt realisiert.

Für die Anti-Pass-Back Funktion ist die GAT DC 7200 Anti-Pass-Back License erforderlich.

9.9 Longrange Leser

Longrange Leser wie der GAT SR 861 können unter Verwendung eines GAT SR 7000 Wiegand am Controller angeschlossen werden.

9.10 Netzwerksicherheit

Die GAT DC 7200 bieten die Möglichkeit, für die Kommunikation TLS (früher SSL) zu aktivieren. Damit ist die Verbindung über eine gesicherte HTTPS Verbindung möglich. Das Zertifikat für diese Verbindung kann von einem GAT DC 7200 selbst erzeugt werden oder mittels Zertifikatsignierungsanforderung (CSR) von einer Zertifizierungsstelle für X.509-Zertifikate (CA) angefordert werden.

9.11 Konfiguration speichern

Bei Verwendung des GAT DC 7200 mit der GAT ACE 7000 wird eine Änderung der Konfiguration des Controllers automatisch von der GAT ACE 7000 bemerkt und ein Backup erstellt. Somit sind die Einstellungen jedes Controllers in der Datenbank der GAT ACE 7000 abgelegt und gesichert.

9.12 Konfigurationen verteilen

Bei Verwendung des GAT DC 7200 mit der GAT ACE 7000 können systemweite Einstellungen (z. B. Karteneinstellungen) an einem Controller gemacht werden. Diese Einstellungen werden über die GAT ACE 7000 vom Controller kopiert und an alle anderen Controller gesendet.

Die Auswahl welche Einstellungen kopiert werden sollen, kann vom Anwender in der GAT ACE 7000 bestimmt werden.

9.13 Ausgänge erweitern

Der GAT DC 7200 bietet sechs Relais Ausgänge. Diese können wesentlich flexibler verwendet werden als dies beim bisherigen System. Als weitere Ausgänge können die Relais auf den GR7 verwendet werden.

Werden weitere Ausgänge im sicheren Bereich benötigt, so können ein oder mehrere GAT SR 7000 Wiegand (1 Ausgang pro Modul) angeschlossen werden. Jedes GAT SR 7000 Wiegand benötigt eine Türlizenz am Controller.

Es besteht auch die Möglichkeit, Relaisexpander anzuschließen und somit die Anzahl Ausgängen zu erweitern. Es können dabei bis zu 2 GAT IO 055 oder bis zu 8 GAT IO 7054 und/oder GAT IO 7055 an einem GAT DC 7200 angeschlossen werden. Die Anzahl an Eingängen und Ausgängen wird pro Relaisexpander um folgende Werte erweitert:

- GAT IO 055: 32 zusätzliche Ausgänge
- GAT IO 7054: 4 zusätzliche Ausgänge
- GAT IO 7055: 8 zusätzliche Ausgänge

9.14 Eingänge erweitern

Der GAT DC 7200 bietet sechs Optokoppler Eingänge. Diese können wesentlich flexibler verwendet werden, als dies beim bisherigen System. Als weitere Eingänge können die Optokoppler auf den GR7 verwendet werden.

Werden weitere Eingänge im sicheren Bereich benötigt, so können ein oder mehrere GAT SR 7000 Wiegand (2 Eingänge pro Modul) angeschlossen werden. Jedes GAT SR 7000 Wiegand benötigt eine Türlizenz am Controller.

Außerdem kann die Anzahl an Eingängen auch mittels Relaisexpandern um folgende Werte erweitert werden:

- GAT IO 7054: 12 zusätzliche Eingänge
- GAT IO 7055: 16 zusätzliche Eingänge

9.15 Video Integration

Im Live View des GAT DC 7200 kann pro Türe ein Videosignal eingebunden werden. Es können Video Streams von verschiedenen Kameras angezeigt werden. Die Video Streams müssen von der Kamera direkt geliefert werden und müssen ohne weitere Plug-Ins in einem Browser angezeigt werden können, damit sie für den GAT DC 7200 verwendbar sind.

9.16 Plug&Play PLUS

Die Plug&Play PLUS Funktion des GAT DC 7200 ermöglicht es, dass angeschlossene Geräte die die Plug&Play PLUS Funktion ebenfalls unterstützen automatisch erkannt, konfiguriert und einer Türe zugewiesen werden.

Diese Funktion ist nur dann möglich, wenn pro Reader Port ein Gerät angeschlossen ist. Wird an einen Reader Port mehr als ein Gerät angeschlossen, so ist die automatische Türzuordnung nicht möglich.

Geräte die die Plug&Play PLUS Funktion nicht unterstützen (z. B GAT SR 3xx oder GAT SLR 3xx) müssen manuell gesucht und konfiguriert werden.

9.17 CardNET

CardNET ist mit dem GAT DC 7200 nur unter Verwendung von GR7 und GAT S(L)R.73xx Lesern möglich. Die GAT SR 3xx werden für das Schreiben von CardNET Daten nicht unterstützt!

CardNET ist an jedem GAT DC 7200 möglich (sofern es konfiguriert wird) und kann an allen Türen aktiv sein. Damit es an der Türe aktiv ist, muss der verwendete Leser entsprechend autorisiert sein.

CardNET ist in der Standalone Version des GAT DC 7200 nicht verfügbar.

9.18 GANTNER SVN

GANTNER SVN ist eine Kombination aus der Salto Virtual Network (SVN) Technologie und MIFARE DESFire Datenträgern mit einer GANTNER Codierung.

Nähere Informationen bezüglich Voraussetzungen für GANTNER SVN siehe Kapitel "7. BERECHTIGUNGSVERGABE".

9.19 Kurzschlussfeste Anschlüsse

Die Reader Ports und der Sub Port sind kurzschlussfest. Wird an einem der Ports ein Strom vom mehr als ca. 1 A benötigt, wird die Spannung an diesem Port automatisch abgeschaltet. Die anderen Ports können weiterhin normal verwendet werden.

Sollte im Fall eines Kurzschlusses der Controller neu starten, ist das Netzgerät zu schwach dimensioniert und der Neustart wird durch eine Unterspannung in der Controller Versorgung verursacht.

Die Spannung an einem Reader Port kann auch über die Konfiguration ausgeschaltet werden. Der Status der Spannungsversorgung (ein/aus) wird an der gelben LED des Reader Ports und über das Web Interface angezeigt.

9.20 Kommunikation am Reader Port

Die grüne LED an einem Reader Port zeigt für Geräte mit Plug&Play PLUS Unterstützung an, wenn mit dem angeschlossenen Gerät (oder den angeschlossenen Geräten) eine aktive Kommunikation stattfindet.

Für Geräte ohne Plug&Play PLUS Funktion wird die Kommunikation am Reader Port nicht signalisiert.

9.21 Factory Reset

Über einen Taster kann der GAT DC 7200 auf Werkseinstellungen zurückgesetzt werden. Dies ist z. B. notwendig, wenn die Zugangsdaten (siehe Netzwerksicherheit) verstellt wurden und nicht mehr bekannt sind. Die Factory Reset Funktion ist mehrstufig (siehe 5.5 Neustart und Rücksetzen auf Werkseinstellungen).

9.22 Netzwerkverbindung

Es ist aus Sicherheitsgründen pro Controller nur eine Netzwerkverbindung möglich. Ob eine solche Verbindung besteht ist an der LED 1 ersichtlich (siehe 5.6 Signalisierungsübersicht).

9.23 Leser der Generation SR 3xx verwenden

Der GAT DC 7200 unterstützt auch Leser der GAT SR 3xx Generation, jedoch nicht den GAT SR 380. Bei den unterstützen Lesern ist die Plug&Play PLUS Funktion und CardNET jedoch nicht möglich. Es werden von den Lesern dieser Generation LEGIC prime und advant Datenträger (ISO 14443 und ISO 15693) unterstützt.

9.24 MIFARE Classic

Die Unikatsnummer von Mifare Classic oder anderen ISO 14443A Datenträgern können am GAT DC 7200 verwendet werden. Dabei ist es nicht relevant, ob es sich um 4- oder 7-Byte Unikatsnummern handelt.

Auf Grund der unsicheren Technologie werden vom GAT DC 7200 jedoch keine Ausweisnummern aus Sektoren von Mifare Classic Datenträgern gelesen.

9.25 MIFARE DESFire

Neben der Unikatsnummer können von Mifare DESFire Datenträgern auch codierte Daten gelesen und auch CardNET Daten geschrieben werden. Dafür wird auf Datenträger eine GANTNER Applikation mit entsprechenden Files codiert.

Unterstützt werden DESFire EV1 und DESFire EV2 Datenträger.

Hinweis: Für die GANTNER SVN Funktion müssen immer MIFARE DESFire Datenträger verwendet werden.

9.26 LEGIC prime und advant

GANTNER spezifische Segmente, KGH Segmente, LEGIC advant Access Standard Segmente und zahlreiche Kundensegmente werden vom GAT DC 7200 unterstützt.

9.27 HID iClass

Die Unikatsnummer von HID iCass Datenträgern kann am GAT DC 7200 verwendet werden. Lesen von Datenbereichen ist mit diesen Datenträgern nicht möglich.

9.28 Buchungen

Der GAT DC 7200 hat zwei unabhängige Ringspeicher für Buchungen. Im einen werden personenbezogene Buchungen und Zutrittsereignisse gespeichert. Im anderen werden systembezogene Ereignisse gespeichert. Beide Ringspeicher können von der Größe frei konfiguriert werden, so dass der Zeitraum der ausgewertet wird unterschiedlich lang sein kann.

Für die personenbezogenen Buchungen kann auch eine Anonymisierung aktiviert werden, so dass Buchungen der Zutritte zwar gespeichert werden, jedoch kein Rückschluss auf die Person erfolgen kann.

9.29 Datenträger Typen

Der GAT DC 7200 kann bis zu neun verschieden Datenträgertypen gleichzeitig behandeln. Dabei kann es sich um verschiedene Technologien (z. B. LEGIC prime und advant) oder verschiedene Codierungen (Segmente oder Kundencodes) handeln. Die verschiedenen Kartentypen können in der Zutrittskontrollsoftware als ein oder mehrere unterschiedlichen Typen verwaltet werden (sofern dies von der Software unterstützt wird).

Sollen als ein Datenträgertyp die Unikatsnummer eines Datenträgers verwendet werden, muss berücksichtigt werden, dass dies zu unerwünschten Auswirkungen führen kann. Wenden Sie sich für weitere Infos an Ihren Lieferanten oder an unsere Spezialisten beim Support.

9.30 Alarm System

Am GAT DC 7200 können bis zu vier Alarmanlagenbereich gesteuert und für eine Blockschlossfunktion definiert werden. Die Scharf- und Unscharf-Schaltung ist von mehreren Türen möglich. Die Beeinflussung als Blockschloss kann für einzelne oder alle Türen verwendet werden.

Durch die Bereichssteuerung für mehrere Türen ist weniger Verkabelungsaufwand erforderlich und es werden weniger Ein- und Ausgänge am Controller benötigt.

Pro Türe kann definiert werden, ob der Status des Alarmsystems am Leser angezeigt werden soll oder nicht.

Für die Scharf- und Unscharf-Schaltung kann pro Alarmanlagenbereich definiert werden, ob eine Verifikation für den Vorgang erforderlich ist oder nicht und was als Verifikation verwendet wird (PIN oder Biometrie). Die Berechtigung wird zusätzlich über eine Sonderberechtigung für Personen verwaltet.

9.31 Zustand der Ein-/Ausgänge

Der Zustand der Ein- und Ausgänge kann komfortabel über das Web Interface angezeigt. Es ist somit nicht mehr erforderlich, dass man dafür den Einbauort des Controllers aufsuchen muss, um die Signale zu prüfen.

9.32 Zeitserver

Die Zeitsynchronisierung des GAT DC 7200 erfolgt über einen frei einstellbaren Zeitserver (NTP Server). Der Controller holt sich in einstellbaren Abständen die aktuelle Zeit von diesem Server. Die Konfiguration des Zeitservers kann manuell oder über die Option des DHCP Servers (DHCP Option 42) erfolgen.

9.33 Zeitzone

Die Zeitzone in der der GAT DC 7200 betrieben wird kann frei eingestellt werden.

9.34 Sommer-/Winterzeitumschaltung

Die Sommer-/Winterzeitumschaltung wird vom Controller selbständig durchgeführt.

9.35 Backup Einstellungen

Konfigurationen, die am GAT DC 7200 eingestellt wurden, werden von der GAT ACE 7000 automatisch in Form eines Backups gespeichert. Sollte die GAT ACE 7000 noch nicht installiert sein, kann ein Backup auch manuell über das Webinterface erstellt und auch wieder eingespielt werden.

9.36 Update Controller und Leser

Updates vom GAT DC 7200 und angeschlossenen Peripheriegeräten können komfortabel über die GAT ACE 7000 gemacht werden. Sollte die GAT ACE 7000 noch nicht installiert sein, kann das Update auch über die Weboberfläche gemacht werden.

Das Update von Peripheriegeräten ist nur dann möglich, wenn dieses von den Peripheriegeräten unterstützt wird (z. B. GAT DL 091 wird derzeit nicht unterstützt).

9.37 Installation

Der GAT DC 7200 ist für den Einbau in Verteilerschränken ausgelegt und weist eine Schutzklasse von IP 30 auf. Soll der Controllerunter anderen Bedingungen eingesetzt werden, ist ein entsprechendes Gehäuse (z. B. Installation Box 9118 oder 9236) vorzusehen.

9.38 Reader Ports

Bei den Reader Anschlüssen, handelt es sich um RS-485 Schnittstellen, die über entsprechende Splitter auch auf mehrere RJ45 Anschlüsse aufgeteilt werden können. Damit ist eine einfache Verkabelung auch dann möglich, wenn mehr als vier Leser an einen Controller angeschlossen werden sollen.

Auf die maximale Leitungslänge des Systems ist zu achten (max. 200 m pro Leser, max. 1000 m für alle Peripheriegeräte zusammen).

9.39 Spannung für Schlösser

Der GAT DC 7200 und die Leser stellen potentialfreie Kontakte für die Ansteuerung von Schlössern oder Rückmeldekontakten zur Verfügung. Die Spannungsversorgung für die Schlösser muss über ein eigenes Netzgerät und eine Verkabelung mit einem passenden Leitungsquerschnitt vorgesehen werden.

9.40 Identifikation und Verifikation

Mit dem GAT DC 7200 ist eine noch feinere Festlegung von Identifikations- und Verifikationsmitteln möglich. So kann z. B. eine Identifikation über eine Nummerneingabe zeitlich gesteuert werden oder die Kriterien für die Verifikation können abhängig von der Tageszeit oder dem Wochentag verändert werden (z. B. PIN während des Tages, Biometrie während der Nachstunden).

9.41 Sonderberechtigungen

Sonderberechtigungen können mit dem GAT DC 7200 noch detaillierter verwaltet werden wie bisher. So ist es z. B. möglich, dass verschiedene Personen die Alarmanlage zwar scharf, aber nicht unscharf schalten können oder bestimmte Personen benötigen für die Verifikation den Finger und für andere ist ein PIN ausreichend.

9.42 Multicard-Handling

Der GAT DC 7200 unterstützt ein Multicard-Handling bei dem aus mehreren Ausweisen der für Zutritt relevante Datenträger selektiert und ausgewertet wird. Somit kann der Ausweis in der Geldbörse bleiben und EC- oder Kreditkarten beeinträchtigen den Zutritt nicht mehr.

Eine entsprechende Codierung der Ausweise ist dafür Voraussetzung. Für weitere Informationen wenden Sie sich bitte an Ihren Lieferanten oder an unsere Spezialisten beim Support.

9.43 Lesereichweite

Bei den Lesern der Serie GR7 sowie GAT SR 73xx und GAT SLR 73xx wurde die Lesereichweite deutlich verbessert und das Zentrum des Lesers ist der blau beleuchtete Punkt beim Lesersymbol.

Außerhalb des Zentrums sinkt die Lesereichweite deutlich ab.

9.44 ISO 15693 Standard

Ausweise die dem ISO 15693 Standard entsprechen, können an den GR7, GAT SR 73xx und GAT SLR 73xx Lesern zusammen mit dem GAT DC 7200 für die Identifikation verwendet werden. Für LEGIC advant Ausweise nach diesem Standard können codiert Informationen verwendet werden. Für andere Typen wird die Unikatsnummer als Ausweisnummer verwendet.

9.45 ISO 14443 Standard

Ausweise die dem ISO 14443 Standard entsprechen, können an den GR7, GAT SR 73xx und GAT SLR 73xx Lesern zusammen mit dem GAT DC 7200 für die Identifikation verwendet werden. Für LEGIC advant oder MIFARE DESFire Ausweise nach diesem Standard können codiert Informationen verwendet werden. Für andere Typen wird die Unikatsnummer als Ausweisnummer verwendet.

9.46 Leser Geschwindigkeit

Leser der GR7 Serie sind schneller als bisherige Leser. Dies ist bei der Behandlung von Datenträgern spürbar (abhängig von der Technologie und Codierung). Ein deutlicher Geschwindigkeitsunterschied ist auch bei der Verarbeitung und Speicherung von Fingerprint Templates zu bemerken.

9.47 Berechtigungsänderungen

Geänderte Berechtigungen können um ein Vielfaches schneller an den GAT DC 7200 gesendet werden wie dies im bisherigen FLEX System der Fall war. Es werden bei Berechtigungsänderungen immer alle Daten an den Controller gesendet. Dadurch kann es zu keinen Dateninkonsistenzen kommen.

Während dem Empfangen der Daten bleibt der GAT DC 7200 voll funktionsfähig. Nachdem alle Daten empfangen wurden, wird der aktive Speichergereich ohne merkbare Unterbrechung gewechselt und die neuen Berechtigungen sind ab diesem Zeitpunkt aktiv.

Über GAT DIRECT.Connect können keine Daten in den GAT DC 7200 geladen werden.

9.48 Ein- und Ausgänge

Beim GAT DC 7200 gibt es keine fixe vorgegebene Zuordnung von Ein- und Ausgängen zu Türen. Die Vorgaben bei Werkseinstellung können in der Konfiguration beliebig geändert werden. Dadurch ist deutlich mehr Flexibilität als beim Vorgängersystem vorhanden und mit der gleichen Anzahl an Ein- und Ausgängen könnte mehr Funktionalität umgesetzt werden.

Ungeachtet von dem, hat der GAT DC 7200 mehr Ein- und Ausgänge als das Vorgängersystem.

9.49 Montage

Durch die Hutschienenmontage kann der GAT DC 7200 schnell und einfach in einen Verteiler eingebaut werden. Sollte dennoch eine Wandmontage notwendig sein, kann der Controller mit zwei Schrauben auch ohne Hutschiene montiert werden.

9.50 WiNET

Der GAT DC 7200 bietet in der Grundfunktionalität bereits alle Voraussetzungen, dass WiNET Systeme einfach installiert und in Betrieb genommen werden. Durch die Anzeige von Signalstärken der einzelnen Schlösser ist auch die Positionierung der WiNET Access Points einfach machbar.

Über GAT DIRECT.Connect wird keine WiNET Funktion unterstützt.

9.51 Test Mode

Durch das Web-Interface des GAT DC 7200 kann eine Installation sehr einfach getestet werden, wenn noch keine Zutrittskontrollsoftware installiert oder keine Berechtigungen verteilt sind.

Die korrekte Ansteuerung und Rückmeldung der Türe kann durch die Fernsteuermöglichkeit geprüft werden. Sollte noch kein Schloss an den GAT DC 7200 angeschlossen sein, kann man den Zustand der Ein- und Ausgänge im Web Interface überprüfen, oder auch den eingebauten Piepser als „Signal“ für einen Zustand verwenden.

Datenträger Einstellungen können anhand der Buchungen überprüft werden.

Der eingebaute Piepser soll auch schon mal für die Suche des Einbau Ortes eines GAT DC 7200 verwendet worden sein.

9.52 Fernsteuerung von Türen

Türen können über das Web Interface nicht nur überwacht, sondern auch ferngesteuert werden. Hier sind Einzelentriegelungen, Dauerentriegelungen aber auch Sperren von Türen möglich. Dies kann auch ohne vorhandenen Sicherheitsleitstand genutzt werden.

9.53 GAT DIRECT.Connect Schnittstelle

Bei Verwendung dieser Schnittstelle muss die Online Management Lizenz installiert sein (enthalten in 1100190 - GAT DC 7200 APB license email oder 1100191 - GAT DC 7200 APB license). Mit dieser Software und dem entsprechenden Adapter ist die Anbindung des GAT DC 7200 in eine Zutrittskontrollsoftware möglich, ohne dass eine Anpassung der Software notwendig ist.

Es können bis zu 16 Türen und unterschiedliche Leser wie GR7, GAT SR 7xxx, GDL7m verwendet werden und es ist möglich, Steuerbefehle an den Controller zu senden.

Folgende Einschränkungen sind mit GAT DIRECT.Connect zu beachten:

- Es werden keine WiNET Geräte am GAT DC 7200 unterstützt.
- Es werden keine Lift- und Schließfachsteuerungen (z.B. GAT IO 705x) unterstützt.
- Es werden keine Daten in den GAT DC 7200 geladen.
- Es ist keine parallele Verbindung zu GAT ACE bzw. Matrix möglich.

9.54 Mobile Credential

Mit Mobile Credential können auf Mobilgeräten wie Smartphones oder Smartwatches gespeicherte Berechtigungen für die Identifikation von Benutzern an den Lesern, die am GAT DC 7200 angeschlossen sind, verwendet werden. Damit diese Funktion verwendet werden kann, muss eine Mobile Credential Lizenz im GAT DC 7200 aktiviert werden. Außerdem sind bestimmte Voraussetzungen (mind. Firmware Version 3.7, u.a.) und Konfigurationsschritte notwendig. Siehe dazu Abschnitt "6.5. Mobile Credential konfigurieren".

10 TECHNISCHE DATEN

10.1 Spannungsversorgung

Nennspannung:	DC 12 / 24 V
Zulässiger Spannungsbereich:	DC 10 - 28 V
Versorgung:	nur mit LPS (Limited Power Source) Netzgerät
Max. Stromaufnahme:	4 A bei 12 V 2 A bei 24 V

10.2 Serverschnittstelle

Schnittstellentyp:	Ethernet 10/100 MBit
Standard:	IEEE 802.3
Benötigte Ports:	- 20, 21 (für FTP, wird ab Version 2.0 der GAT ACE 7000 nicht mehr benötigt) - 443 (für Web-Schnittstelle über TLS/SSL), 80 ohne TLS/SSL (nicht empfohlen) - 8000 (Standard für Kommunikation zu GAT ACE 7000, kann auch geändert werden) - 123 UDP (NTP, für Zeitsynchronisation) - 8239 für GAT DIRECT.Connect Anbindung

10.3 Leser

Schnittstellentyp:	RS-485
Unterstützte Leser:	GANTNER Lesergeneration 7: GAT SR 7300 / 7305 / 7307 GAT SR 7310 / 7315 7317 GAT SR 7340 / 7345 / 7347 GAT SR 7350 / 7355 / 7357 GAT SR 7380 GAT SLR 7300 / 7307 GAT SLR 7310 / 7317 GAT SR 7000 Wiegand GR7.1300 / 1310 / 2300 / 2310 / 7380 GANTNER Lesergeneration 3xx (mit Einschränkungen): GAT SR 300 / 305 GAT SR 310 / 315 GAT SR 340 / 345 / 347 GAT SR 350 / 355 / 357 GAT SLR 300 GAT SLR 310 WiNET Leser: GAT DL 091

10.4 Peripherieschnittstelle "SUB"

Schnittstellentyp:	RS-485
Unterstützte Geräte:	- GAT IO 055 Relaisexpander - GAT IO 7054 / GAT IO 7055 - GAT DL 091 WiNET Access Point - GAT REX 118 RS485 - GAT SR 7000 Wiegand **Hinweis:** Wenn ein GAT DL 091 mit Firmware Version älter als V4.1 verwendet wird, kann der GAT DL 091 nicht gleichzeitig mit dem GAT IO 055 oder GAT REX 118 angeschlossen werden.

10.5 Relaisausgang

Anzahl:	6
Funktion:	NO/NC, Funktion und Zeitverhalten konfigurierbar
Schaltspannung:	max. 30 VAC/DC
Dauerstrom:	max. 2 A
Schaltleistung:	max. 60 VA

10.6 Optokopplereingang

Anzahl:	6
Funktion:	Funktion konfigurierbar
Eingangsspannung:	10 bis 30 VDC
Eingangsstrom:	4,5 mA

10.7 Speicher und Zeitmessung

Speichergrößen:	- 16 MB Flash - 8 GB Massenspeicher
speicherbare Datensätze:	Dynamische Speicheraufteilung, z. B.: 50.000* Personen + 100.000 Datenträger + 100.000 Berechtigungen + 100.000 Buchungen * … Bei Anlagen mit mehr als 5.000 Personen kontaktieren Sie bitte ihren Lieferanten oder den Support von GANTNER Electronic GmbH für eine Beratung zur bestmöglichen Systemkonfiguration
Interne Uhr:	- integrierte Echtzeituhr, Uhrzeit gegen Stromausfall geschützt - automatische Sommer-/Winterzeitumschaltung - Unterstützung für automatische Zeiteinstellung über SNTP Server

10.8 Anzeigeelemente

Leuchtanzeige:	LEDs für Ethernet, RS-485 Schnittstellen (Leser, Peripheriegeräte), Host-Verbindung
Akustischer Signalgeber:	Piepser

10.9 Gehäuse

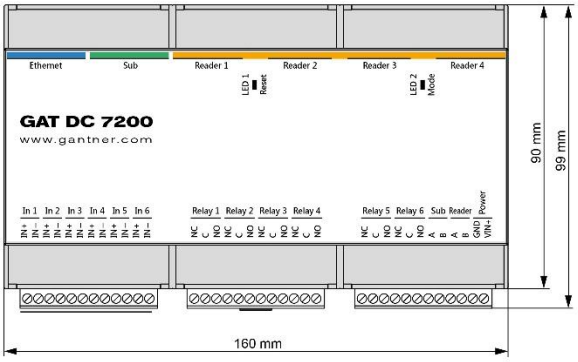
Gehäusematerial:	Stoßfestes, robustes Gehäuse aus Kunststoff
Abmessungen:	160 mm x 90 mm x 32 mm
Gewicht:	ca. 210 g

10.10 Umgebungsbedingungen

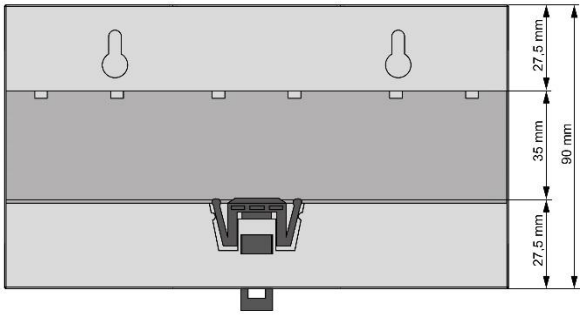
Zul. Umgebungstemperatur:	-10° C bis +55°C
Zul. Lagertemperatur:	-10° C bis +55°C
Schutzart:	IP 30
Umweltklasse in Anlehnung an VdS 2110:	II (Bedingungen in Innenräumen)

10.11 Abmessungen

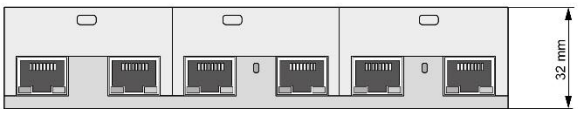
Vorderansicht



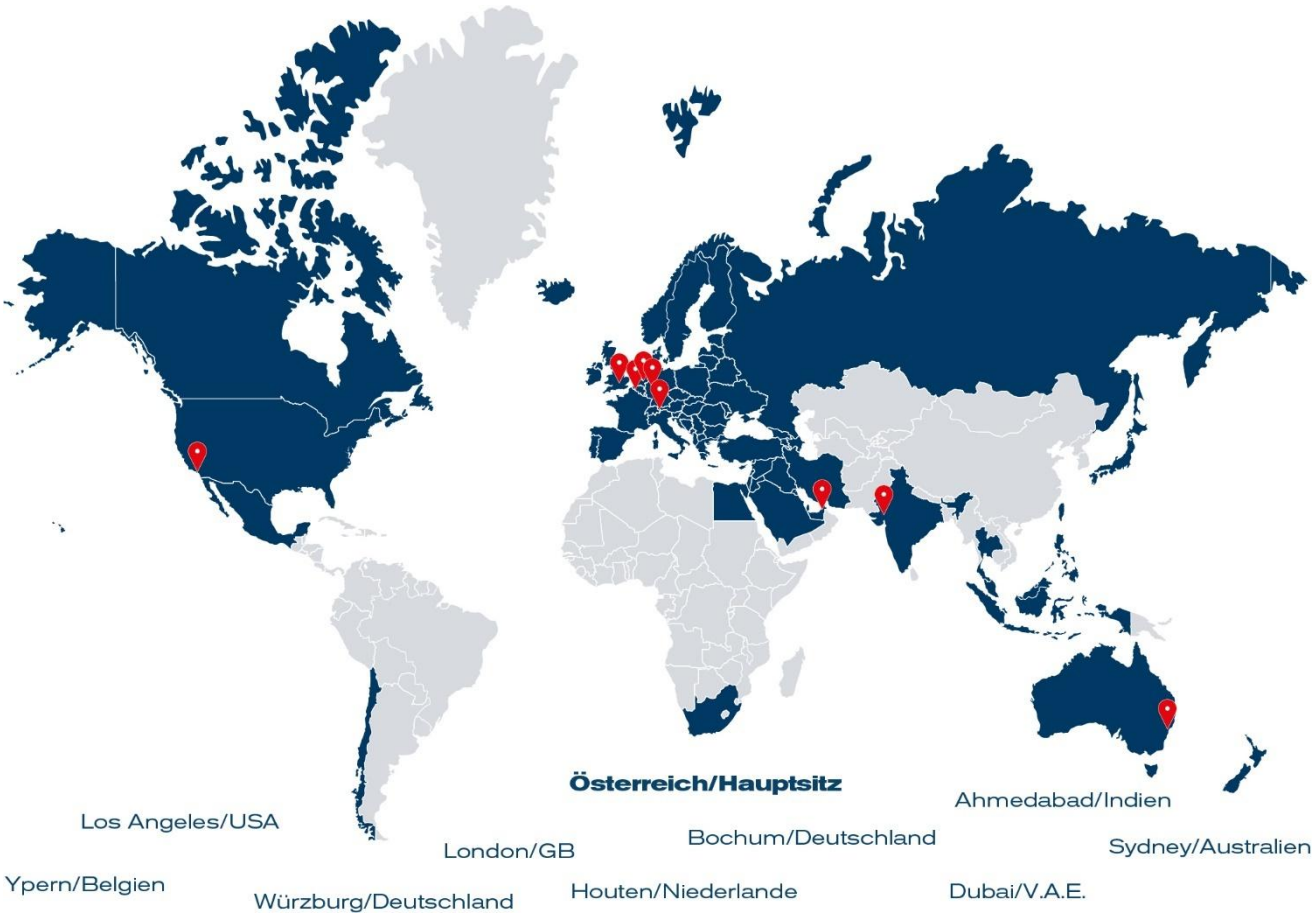
Untersicht



Aufsicht



Hinweis:
Dieses Handbuch ist gültig ab 5. März 2026. Änderungen und Ergänzungen dieses Handbuchs sind jederzeit ohne Vorankündigung möglich!



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

Nüziders, Österreich
info@gantner.com

Houten, Niederlande
info@gantner.nl

Sydney, Australien
info-aus@gantner.com

London, GB
info-uk@gantner.com

Bochum, Deutschland
info-de@gantner.com

Los Angeles, USA
info-us@gantner.com

Ypern, Belgien
info@gantner.be

Dubai, Mittlerer Osten
info-me@gantner.com

Ahmedabad, Indien
info@gantnerticketing.com

Aktuelle Kontaktdaten: www.gantner.com/locations

Artikel-Nr.: 831020