



Security Tech Germany

TECTIQ

SYSTEMHANDBUCH

Vielen Dank, dass Sie sich für ein Zutrittssystem von ABUS Security Center entschieden haben. ABUS TECTIQ leistet einen wichtigen Beitrag zur Sicherung Ihres Eigentums und stellt sicher, dass ausschließlich autorisierte Personen Ihre gesicherten Bereiche betreten können.

Über dieses Handbuch

Dieses Handbuch enthält alle Informationen zum Umgang mit ABUS TECTIQ. Der erste Teil richtet sich an die einzelnen Nutzergruppen des Systems und fasst alle relevanten Anwendungsfälle übersichtlich zusammen. Im zweiten Teil werden die Funktionen der Schließsoftware TECTIQ Access Manager detailliert beschrieben.

An wen richtet sich dieses Handbuch

Nutzer – Sie sind zum Zutritt eines Gebäudes mit einer TECTIQ Zutrittskontrollanlage berechtigt. Sie haben ein TECTIQ Schließmedium erhalten und sind vom Betreiber der TECTIQ Zutrittskontrollanlage mit den Funktionen der Schließmedien vertraut gemacht worden. Sie sind darüber informiert, wann und zu welchen Zugängen Ihnen der Zutritt zum Objekt gewährt wird. Im Kapitel **TECTIQ – Für Nutzer** erhalten Sie alle Informationen zu Ihren Schließmedien und zu den Schritten, die Sie zu ihrer Nutzung an den Türkomponenten benötigen. Bei weiteren Fragen wenden Sie sich an den Administrator der TECTIQ Zutrittskontrollanlage oder an Ihren Vorgesetzten.

Administratoren – Sie sind Betreiber einer TECTIQ Zutrittskontrollanlage oder für die Verwaltung der Türkomponenten und Schließmedien in einer TECTIQ Zutrittskontrollanlage verantwortlich. Dieses Handbuch unterstützt Sie mit detaillierten Informationen zum Aufbau des Zutrittskontrollsystems, zur TECTIQ Zutrittskontrollzentrale, zu Schließmedien und Türkomponenten sowie zu weiteren Systemmedien, die Sie bei der Einrichtung, Verwaltung und Anpassung der Zutrittsberechtigungen unterstützen. Lesen Sie im Kapitel **TECTIQ – Für Administratoren**, wie Sie mit dem TECTIQ Access Manager neue Personengruppen und Personen hinzufügen, Schließberechtigungen erteilen oder ändern und Schließmedien verwalten. Es erleichtert Ihnen den Einstieg in den täglichen Umgang mit dem TECTIQ Access Manager.

Facherrichter – Als Service-Techniker, Planer oder ABUS Fachhandelspartner sind Sie mit der Errichtung von ABUS Zutrittskontrollsystemen vertraut. Unsere Montageanleitungen für die Komponenten der TECTIQ Zutrittskontrollanlage sind Ihnen bekannt. In diesem Handbuch sind alle Schritte zur Errichtung der TECTIQ Zutrittskontrollanlage sowie der Bedienung des TECTIQ Access Managers zusammengefasst. Informieren Sie sich im Kapitel **TECTIQ für Facherrichter** über alle Schritte zur Inbetriebnahme, Ersteinrichtung und Übergabe des TECTIQ Zutrittskontrollsystems an den Betreiber sowie zur Wartung und Betreuung des Systems.

Im **Referenzhandbuch** werden der Systemaufbau, alle Funktionen sowie technische Details, Leistungsdaten und Signalisierungen erläutert. Ebenso erhalten Sie Informationen zur Erweiterung und zur Skalierbarkeit des Systems.

Weiterführende Informationen finden Sie auf abus.com oder – für Fachhändler und Installateure – im Partnerportal auf www.partner-asc.abus.com

Rechtliches

Die Angaben in diesem Handbuch wurden nach bestem Wissen zusammengestellt und werden regelmäßig überprüft und aktualisiert. Bewahren Sie das Handbuch und die Bedienungsanleitungen der verwendeten Produkte während der Gebrauchsdauer des Systems auf.

Beachten Sie die Angaben und Hinweise in den TECTIQ Dokumentationen. Für Schäden, die in Folge fehlerhafter Montage, Inbetriebnahme oder anderer Fehlanwendung entstehen, übernimmt ABUS keine Haftung. Die Verantwortung für den Betrieb der Schließanlage nach Montage und Inbetriebnahme liegt beim Anlagenbetreiber, Hauptnutzer oder Eigentümer des Gebäudes. Beachten Sie unsere Gewährleistungsbedingungen – online oder in den TECTIQ Produktanleitungen.

Warenzeichen und Schutzrechte Dritter sind Eigentum der jeweiligen Inhaber und werden anerkannt.

Kundendienst / Customer Support

Fachhändler / Errichter: Bei auftretenden Fragen wenden Sie sich bitte an unsere Support-Hotline.

Endverbraucher: Wenden Sie sich bitte mit allen Fragen an Ihren Fachhändler oder Errichter. Ein geschulter ABUS Fachhandelspartner in Ihrer Nähe berät Sie gern. Eine Liste der ABUS Fachhandelspartner in Ihrer Region finden Sie hier: www.abus.com/ger/Haendlersuche

TECTIQ In Kürze.	8
1. Einführung	9
2. TECTIQ – Für Nutzer	14
3. TECTIQ – Für Administratoren	17
4. TECTIQ – Für Fachrichter	33
TECTIQ Referenzhandbuch.	52
5. Das System	53
6. TECTIQ Access Manager – Oberfläche	65
7. Hauptmenü Dashboard	68
8. Sicht Schließplan Keylockplan	75
9. Sicht Personen Persons	80
10. Sicht Türen Doors	91
11. Sicht Zeitpläne Schedules	98
12. Sicht Systemkomponenten Components	103
13. Sicht Systemeinstellungen Settings	107
14. LED-Signale	119
ANHANG	122
15. Protokolle	123
16. Übersicht – TECTIQ Türkomponenten	125
17. Wer macht was und wann?	126
18. TECTIQ Dokumentation – Hinweise und Symbole	127
19. Sicherheitshinweise	129
20. Glossar	131
21. Stichwortverzeichnis	136

TECTIQ In Kürze.	8
1. Einführung	9
1.1. Über ABUS TECTIQ	9
1.2. Merkmale und Funktion	10
1.3. Zutrittsberechtigungen	10
1.4. TECTIQ Systemkomponenten	11
1.5. Skalierbar – Standortübergreifende Zutrittsverwaltung, Fernzugriff und Online-Service	12
1.6. Protokolle	12
1.7. Verlust des Schließmediums	12
1.8. Datensicherheit	13
2. TECTIQ – Für Nutzer	14
2.1. Einweisung in die Schließanlage – Was Sie wissen müssen	14
2.2. Gesicherten Bereich betreten	15
2.3. Zutrittsberechtigung aktualisieren	15
2.4. Zutrittsberechtigung ändern	15
2.5. Zutrittsberechtigung sperren lassen	16
2.6. LED-Signale	16
3. TECTIQ – Für Administratoren	17
3.1. Umgang mit Schließmedien und Systemmedien	18
3.2. Zutrittskontrollzentrale mit TECTIQ Access Manager verbinden	18
3.3. Person hinzufügen	19
3.4. Person bearbeiten	20
3.5. Person löschen	24
3.6. Personengruppe hinzufügen	25
3.7. Personengruppe bearbeiten	26
3.8. Personengruppe sperren	27
3.9. Personengruppe löschen	28
3.10. Schließmedien und Systemmedien verwalten	28
3.11. Schließmedium oder Systemmedium sperren	29
3.12. Schließmedium Transponder bearbeiten	30
3.13. Schließmedium löschen	31
3.14. Zeitplan erstellen	32
3.15. Zeitplan bearbeiten	32
3.16. Zeitplan löschen	32
4. TECTIQ – Für Fachrichter	33
4.1. Realisieren einer TECTIQ Zutrittskontrollanlage – Erste Schritte	33
4.1.1. Montageort der Zutrittskontrollzentrale	33
4.1.2. Leitungsführung	34
4.1.3. Montageort des Update Terminals	34
4.1.4. Aufstellen des PC	35
4.1.5. Tischleser anschließen	35
4.1.6. Zutrittskontrollzentrale starten	35
4.1.7. Update Terminal mit Zutrittskontrollzentrale verbinden	41

4.1.8. Systemmedien einrichten	42
4.2. Projektierung und Inbetriebnahme	44
4.2.1. Türen und Türgruppen projektieren	45
4.2.2. Türkomponenten zuordnen und einstellen	45
4.2.3. Türkomponenten programmieren	48
4.2.4. Zeitpläne definieren	48
4.2.5. Personengruppen und Personen anlegen	49
4.2.6. Zutrittsberechtigungen vergeben	50
4.2.7. Schließmedien programmieren	51
4.3. TECTIQ Schließmedien ausgeben	51
4.4. TECTIQ System an den Betreiber übergeben	51
TECTIQ Referenzhandbuch.	52
5. Das System	53
5.1. Bestimmungsgemäße Verwendung	53
5.2. Komponenten	53
5.2.1. TECTIQ Zutrittskontrollzentrale	53
5.2.2. TECTIQ Access Manager	54
5.2.3. TECTIQ Tischleser	55
5.2.4. TECTIQ Online Update Terminal	55
5.2.5. TECTIQ Offline Türkomponenten	56
5.2.6. TECTIQ Schließmedien	57
5.2.7. TECTIQ Systemmedien	57
5.2.8. Admin App	59
5.3. Systemaufbau	60
5.4. Technische Daten	63
5.5. Wo sind welche Daten gespeichert?	64
6. TECTIQ Access Manager – Oberfläche	65
6.1. TECTIQ Access Manager – Oberfläche	65
6.2. Menüstruktur	67
7. Hauptmenü Dashboard	68
7.1. Übersicht Hauptmenü	68
7.2. Sammelmeldung Anlagenstatus	69
7.3. Schnelltasten Shortcuts	69
7.4. Listen & Schnelltasten	70
7.5. Verlust eines Schließmediums	71
7.6. Systemwarnungen	72
7.7. Batteriewarnungen	73
7.8. Offene Aufgaben – Aufgabenliste	73
7.9. Störungsmeldungen	74
7.10. Ereignisse	74
8. Sicht Schließplan Keylockplan	75
8.1. Übersicht	75

8.2. Darstellung	77
8.3. Individuelle Zutrittsberechtigungen	78
8.4. Gruppenberechtigungen	78
8.5. Zutrittsberechtigung erteilen	79
8.6. Zutrittsberechtigung entziehen	79
9. Sicht Personen Persons	80
9.1. Übersicht	80
9.2. Personengruppen	81
9.3. Eigenschaften von Personengruppen	82
9.4. Personen	85
9.5. Eigenschaften von Personen	86
9.6. Schließmedium hinzufügen	89
10. Sicht Türen Doors	91
10.1. Übersicht	91
10.2. Türgruppen	92
10.3. Türen	93
10.4. Eigenschaften von Türen	94
10.5. Daten in Türkomponente herunterladen	96
11. Sicht Zeitpläne Schedules	98
11.1. Übersicht	98
11.2. Zeitplan hinzufügen	99
11.3. Zeitplan bearbeiten	101
11.4. Zeitplan löschen	101
11.5. Zeitplan verwenden	101
12. Sicht Systemkomponenten Components	103
12.1. Übersicht	103
12.2. Online Update Terminal hinzufügen	104
12.3. Online Terminal mit Türansteuerung	105
12.4. USB-Tischleser	106
13. Sicht Systemeinstellungen Settings	107
13.1. Übersicht Systemeinstellungen	107
13.2. Systemkonfiguration	108
13.2.1. Systeminformationen	109
13.2.2. Netzwerkeinstellungen	110
13.2.3. Zeiteinstellungen	111
13.2.4. Firmware-Update	112
13.2.5. Datensicherung und Wiederherstellung	113
13.2.6. Gültigkeit der Schließmedien	115
13.2.7. Datenschutz und rechtliche Themen	116
13.3. Schließmedien	116
13.4. Systemmedien	117
13.5. Rollenverwaltung	118

14. LED-Signale	119
14.1. LED-Signale an Türkomponenten	119
14.2. LED-Signale am Update Terminal	120
14.3. LED-Signale am Tischleser	121
ANHANG	122
15. Protokolle	123
15.1. Schlüsselausgabeprotokoll (Muster)	123
15.2. Sperrliste (Muster)	124
16. Übersicht – TECTIQ Türkomponenten	125
17. Wer macht was und wann?	126
18. TECTIQ Dokumentation – Hinweise und Symbole	127
19. Sicherheitshinweise	129
19.1. Allgemeine Sicherheitshinweise	129
19.2. Sicherheitshinweise für Flucht- und Rettungswege	129
19.3. Sicherer Umgang mit Batterien	130
19.4. Fachgerechte Installation	130
20. Glossar	131
21. Stichwortverzeichnis	136

ABUS TECTIQ

TECTIQ In Kürze.

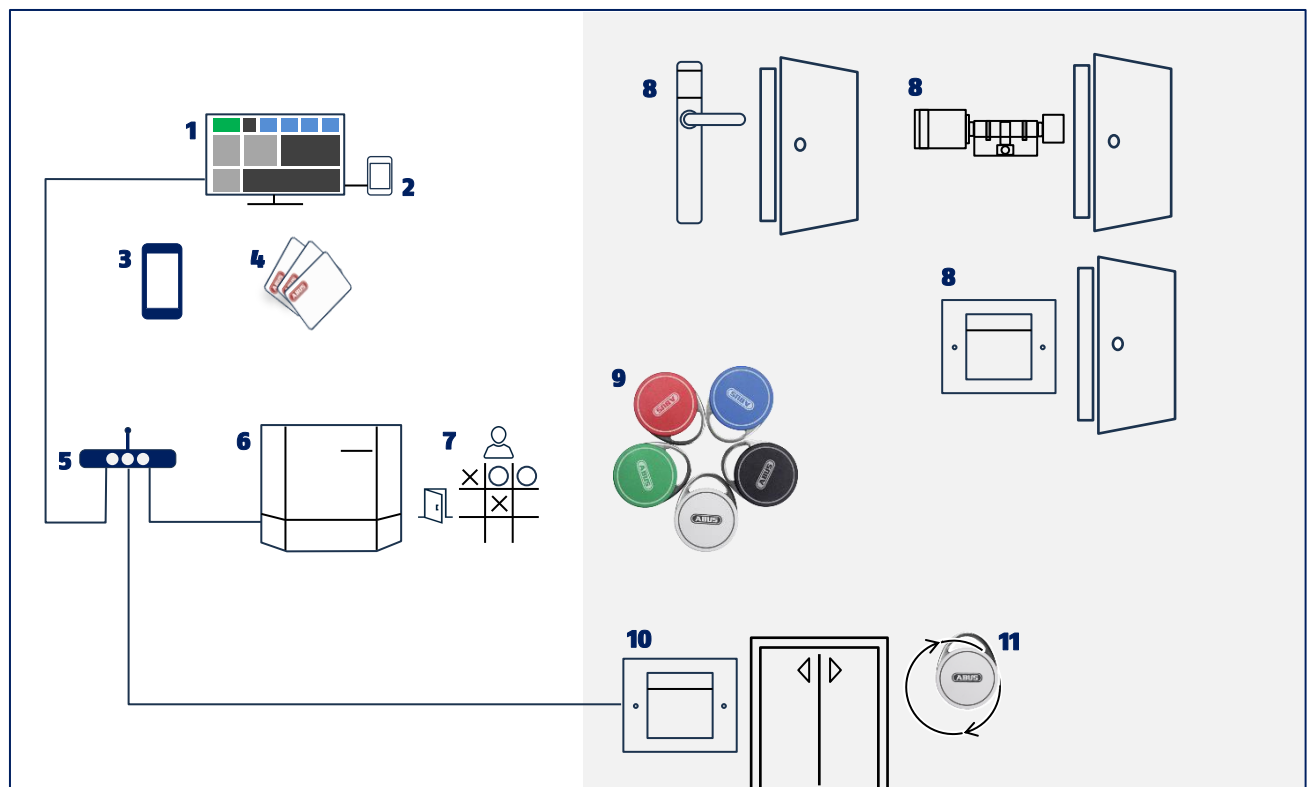
1. Einführung

Inhalt

- 1.1. Über ABUS TECTIQ
- 1.2. Merkmale und Funktion
- 1.3. Zutrittsberechtigungen
- 1.4. TECTIQ Systemkomponenten
- 1.5. Skalierbar – Standortübergreifende Zutrittsverwaltung, Fernzugriff und Online-Service
- 1.6. Protokolle
- 1.7. Verlust des Schließmediums
- 1.8. Datensicherheit

1.1. Über ABUS TECTIQ

ABUS TECTIQ ist der neue Standard unter den ABUS-Zutrittskontrollsystemen. Entwickelt und hergestellt in Deutschland, bietet TECTIQ hochwertige Türkomponenten für eine umfassende, leistungsfähige Zutrittskontroll- und Sicherheitslösung. TECTIQ ist flexibel, intuitiv und leicht handhabbar und erweiterbar. TECTIQ ist das elektronische Schließ- und Zutrittskontrollsystem für gewerbliche und öffentliche Gebäude nahezu jeder Größe.



- 1 Schließensoftware TECTIQ Access Manager
- 2 USB Tischleser
- 3 Admin App
- 4 Systemmedien
- 5 IP Router
- 6 TECTIQ Zutrittskontrollzentrale

- 7 Schließplan, Zeitpläne
- 8 TECTIQ Beschlag, Schließzylinder, Wandleser
- 9 Schließmedien
- 10 TECTIQ Update Terminal
- 11 Validierung und Aktualisierung

1.2. Merkmale und Funktion

ABUS TECTIQ gewährt berechtigten Personen den Zutritt zum gesicherten Bereich mit Hilfe elektronischer Schließmedien.

- ABUS TECTIQ funktioniert nach dem Prinzip **Data-on-Card**. Die Zutrittsberechtigungen sind auf den Schließmedien gespeichert. Bei Änderungen der Zutrittsberechtigungen werden die Schließmedien aktualisiert. Das Aktualisieren der Türkomponente ist nicht erforderlich.
- Die Türkomponenten **TECTIQ Zylinder** und **TECTIQ Beschlag** arbeiten offline und benötigen keine Verkabelung und keine Netzwerk- oder Funkverbindung. Sie können damit mit geringem Aufwand flexibel an jedem Einsatzort verwendet werden.
- Der Zeitraum der Gültigkeit der Zutrittsberechtigung auf dem Schließmedium ist im **TECTIQ Access Manager** einstellbar. Der Zutrittsberechtigte kann die Gültigkeit seines Schließmediums am nächsten **TECTIQ Update Terminal** selbstständig mit den in der **TECTIQ Zutrittskontrollzentrale** gespeicherten Einstellungen aktualisieren.
- In Anlagen ohne **TECTIQ Update Terminal** erfolgt die Aktualisierung mithilfe des **TECTIQ Tischlesers** und einem PC auf dem der **TECTIQ Access Manager** installiert ist.
- Das **TECTIQ Update Terminal** kann ohne Schließfunktion eingesetzt werden. Es kann aber selbst auch zur Ansteuerung von Aktoren eingerichtet werden (elektrische Türöffner, Türantriebe, Vereinzelungsanlagen etc.).
- Zutrittsberechtigungen werden mit der **TECTIQ Zutrittskontrollzentrale** und der Software **TECTIQ Access Manager** verwaltet und aktualisiert. Der Betreiber behält immer die Übersicht und kann seine Anlage flexibel verwalten. Die Synchronisation der Daten zwischen dem TECTIQ Access Manager, der Zentrale und den angeschlossenen Update Terminals erfolgt in Echtzeit.

1.3. Zutrittsberechtigungen

Die Erteilung von Zutrittsberechtigungen erfolgt in nachfolgenden Schritten:



Die **Anlage der Person im TECTIQ Access Manager**: Sobald eine Person im System erfasst ist, können ihr Berechtigungen für den Zutritt zu gesicherten Bereichen erteilt werden. Die Personengültigkeit kann über die Eingabe eines Gültigkeitszeitraums begrenzt werden. Die Zutrittsberechtigungen werden Personengruppen oder individuell einzelnen Personen zugewiesen. Der Nutzer erhält ein persönliches Schließmedium, auf das die aktuell gültigen Berechtigungen übertragen werden. Die Gültigkeit der persönlichen Schließmedien wird in den Systemeinstellungen voreingestellt und kann individuell angepasst werden.



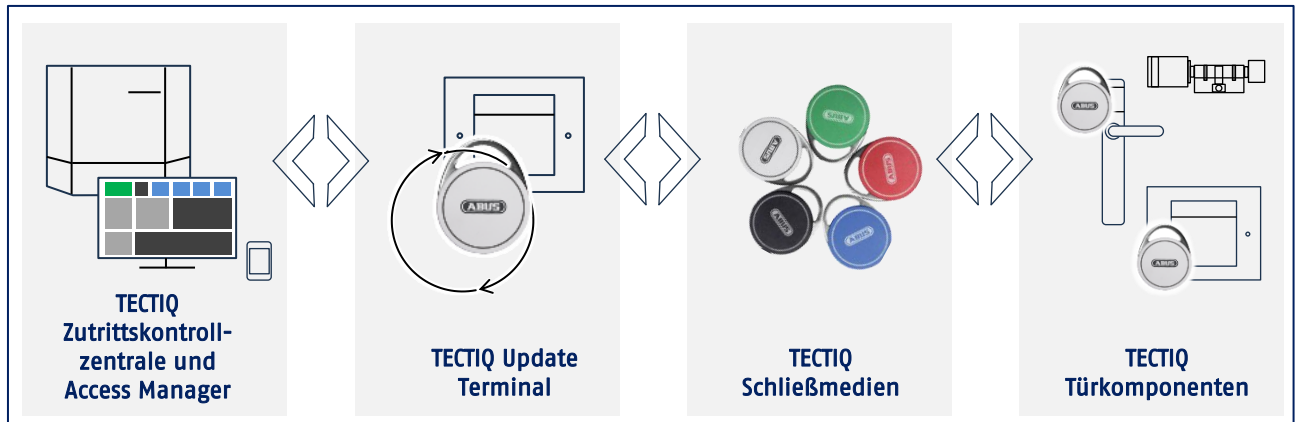
Validierung: Persönliche Schließmedien müssen regelmäßig aktualisiert werden. Mit der Validierung an einem **TECTIQ Update Terminal** wird die Gültigkeit des Schließmediums verlängert und zentral eingegebene Änderungen der Berechtigungen werden auf das Schließmedium übertragen. Schließmedien werden ohne Aktualisieren der Gültigkeit einfach ungültig. Kurze Gültigkeiten erhöhen die Sicherheit.



Zeitpläne organisieren den Zutritt zusätzlich zeitlich, z. B. entsprechend der individuellen Arbeitszeit, bei Schichtplänen oder mit Rücksicht auf Feiertage oder Urlaubszeiten.

In Anlagen ohne **TECTIQ Update Terminal** erfolgt die Aktualisierung und Validierung mit dem **TECTIQ-Tischleser** und dem **TECTIQ Access Manager**.

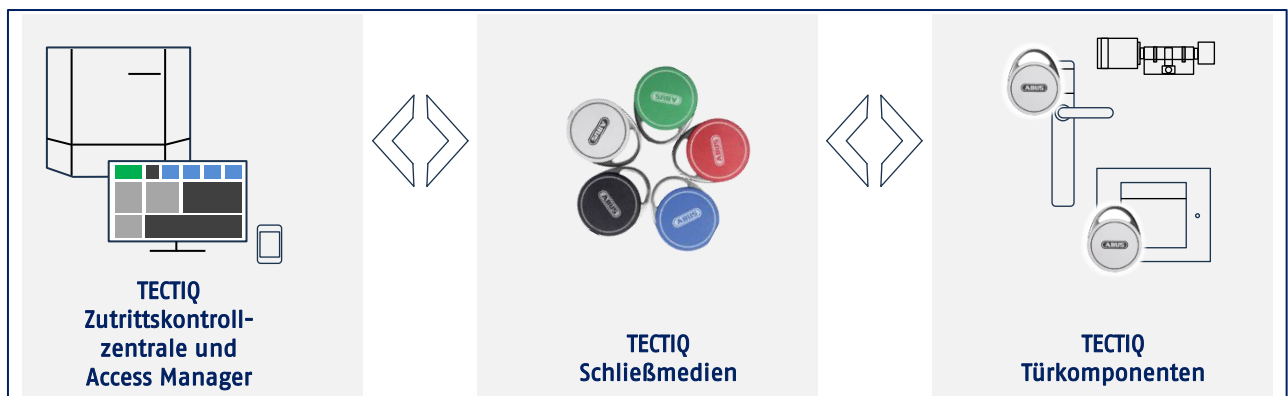
1.4. TECTIQ Systemkomponenten



In einer voll ausgestatteten TECTIQ Anlage sind die Komponenten fein aufeinander abgestimmt.

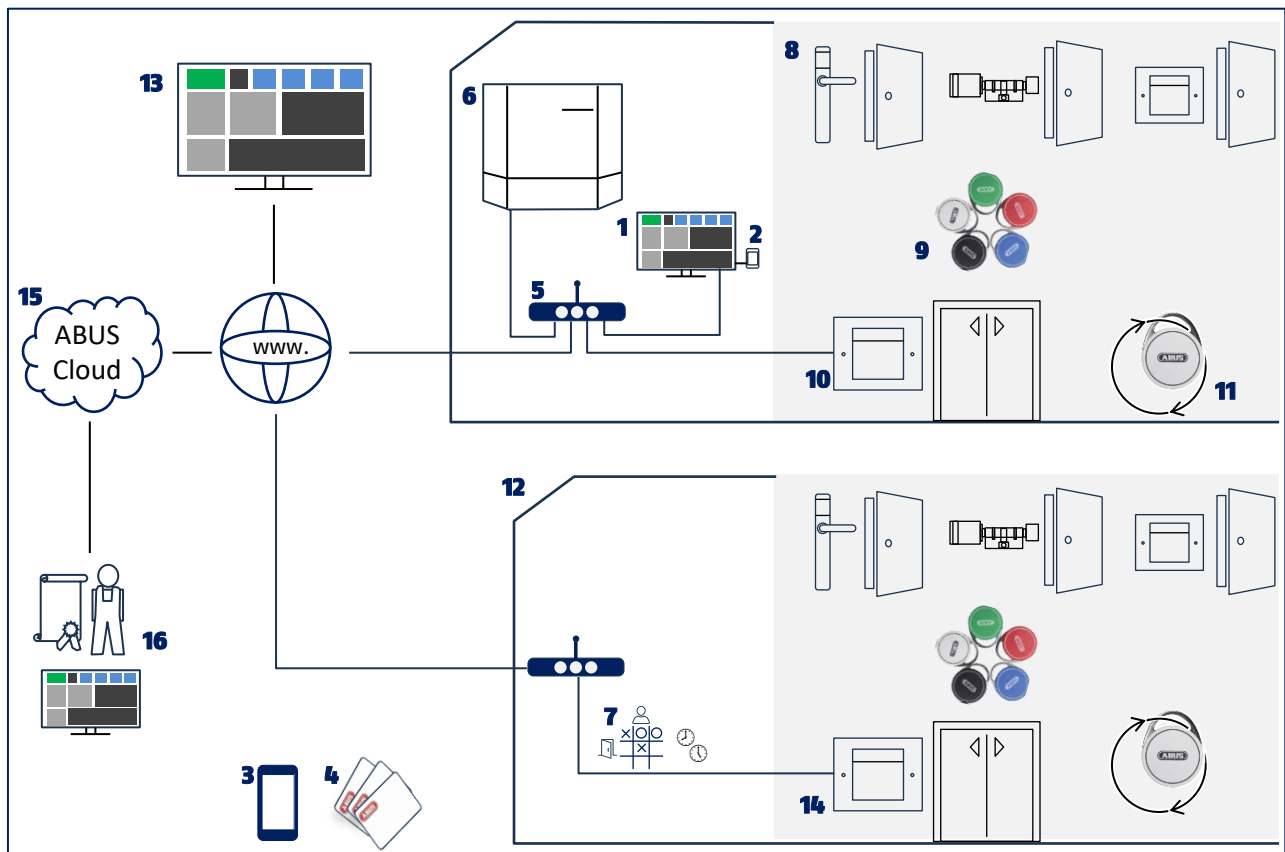
- Die Eigenschaften der Zutrittskontrollanlage werden in der Zutrittskontrollzentrale – mit Hilfe des **TECTIQ Access Managers** – eingestellt: Das beinhaltet den Schließplan mit den Zutrittsberechtigungen, die Personendaten und Schließmedien sowie die Daten für Türen und Türkomponenten.
- Die Zutrittskontrollzentrale synchronisiert sich in Echtzeit mit den Update Terminals in der Anlage.
- Die Update Terminals übertragen die Berechtigungen an die Schließmedien und aktualisieren diese. Im gleichen Zuge spielen die Schließmedien Protokolldaten aus der Anlage zurück zur Zentrale.
- Die Schließmedien speichern die Zutrittsberechtigungen. Das beinhaltet die individuellen Berechtigungen für jede einzelne Tür im System, hinterlegte Zeitpläne und Sperrtage sowie die Gültigkeit für das Schließmedium. Im Betrieb schreiben die Türkomponenten ihre Protokolldaten auf das Schließmedium zurück.
- Die Türkomponenten lesen die Schließmedien beim Präsentieren und prüfen, ob die für diese Tür erforderlichen Zutrittsberechtigungen vorhanden und gültig sind. Fällt die Prüfung positiv aus, erhalten berechtigte Personen den Zutritt zum gesicherten Bereich.

Ein Betrieb ohne **TECTIQ Update Terminal** ist auf Kundenwunsch bei reduziertem Funktionsumfang möglich. In diesem Fall werden die Zutrittsberechtigungen zeitlich unbegrenzt erteilt oder die Aktualisierung und Validierung erfolgen mittels **TECTIQ Tischleser** am Arbeitsplatz eines Administrators. Beachten Sie bitte hierzu auch unsere Hinweise in Kap. 1.7.



1.5. Skalierbar – Standortübergreifende Zutrittsverwaltung, Fernzugriff und Online-Service

TECTIQ bietet sowohl für kleinste, mittlere als auch für große bis sehr große Zutrittskontrollanlagen eine geeignete Lösung. Über Netzwerk- und Internetverbindung können Schließanlagen auch gebäudeübergreifend und sogar standortübergreifend verwaltet werden. Auch hier werden beim Betreten der Liegenschaft die Zutrittsberechtigungen aktualisiert. Der Betreiber hat über alle relevanten Türen den Überblick. Über den Fernzugriff kann Sie der ABUS Fachhandelspartner oder Werkservice bei Bedarf unterstützen.



1 bis 11 siehe oben, Kap. 1.1

12 Zutrittskontrolle für weitere Standorte

13 Online-Fernzugriff mit TECTIQ Access Manager (P2P)

14 Update Terminal mit Online-Verbindung zum

Hauptsystem (P2P)

15 Zugriffsrechte-Überwachung über die ABUS Cloud

16 Online-Service durch ABUS Fachhandelspartner

1.6. Protokolle

Die TECTIQ Türkomponenten protokollieren ihre Ereignisse und Statusmeldungen, wie z. B. erfolgte und verweigerte Zutrittsversuche, Systemmeldungen und Batteriewarnungen und übertragen diese bei jedem Nutzungsvorgang auf die Schließmedien bzw. beim Validierungsvorgang vom Schließmedium in die Zutrittskontrollzentrale. Alle Ereignisse und hieraus entstehende Aufgaben (z. B. Batteriewechsel erforderlich) werden im **TECTIQ Access Manager** übersichtlich angezeigt. Damit kann zeitnah auf Status- und Systemmeldungen, Batteriewarnungen reagiert werden.

1.7. Verlust des Schließmediums

Bitte achten Sie auf Ihr Schließmedium! Es gewährt auch unbefugten Personen während der Gültigkeit Zutritt zu den gesicherten Bereichen. Bei Verlust oder Diebstahl melden Sie den Vorfall sofort Ihrem Vorgesetzten und Ihrem

Administrator, um unverzüglich die Sperrung des Mediums zu veranlassen.

Das TECTIQ Zutrittskontrollsystem bietet höchstmöglichen Schutz, um einen möglichen Schaden gering zu halten. Nach Ablauf der Gültigkeit und Sperrung des Schließmediums in der Zutrittskontrollzentrale wird der Zutritt zu den gesicherten Bereichen nicht mehr gewährt. Unbefugte Zutrittsversuche werden in der Ereignisliste protokolliert.

Eine kurze Gültigkeit reduziert die Gefahr einer unbefugten Nutzung. Sollte das Schließmedium wieder aufgefunden werden, muss die Berechtigung in jedem Fall erneuert werden.

Für zusätzliche Sicherheit wird das Schließmedium in der Anlage gesperrt, indem es mittels Blacklistkarte auf die Sperrliste gesetzt wird. Die Sperrliste wird lokal in jeder Türkomponente gespeichert. Ist ein Schließmedium auf der Sperrliste der Türkomponente, wird die Türkomponente das Schließmedium auch bei unbegrenzter Gültigkeit ablehnen. Ein nicht autorisierter Zutritt durch Missbrauch fremder Schließmedien ist damit ausgeschlossen.

1.8. Datensicherheit

Eine gut geplante und umgesetzte TECTIQ Schließanlage lässt keine unbefugten Personen in Ihr Eigentum und überlässt auch keine sensiblen Daten dem Zufall. Hierfür sorgen:

- verschlüsselte Daten auf den Schließ- und Transpondermedien
TECTIQ nutzt das hochsichere Verschlüsselungsverfahren MIFARE® DESFIRE®. Es gewährleistet höchsten Schutz vor Manipulations- oder Kopierversuchen.
- geschützte Daten ausschließlich in der Zutrittskontrollzentrale
Alle sensiblen Daten sind in der Zutrittskontrollzentrale gespeichert. Mit dem **TECTIQ Access Manager** können Sie die Daten anzeigen und bearbeiten. Die notwendigen Daten zur Zutrittsberechtigung werden in Echtzeit an die Update Terminals übertragen. Gespeicherte Backups sind verschlüsselt und nur in Verbindung mit der konkreten Anlage zugänglich.
- hochsichere Peer-to-Peer-Verbindungen (P2P)
Verbindungen zwischen der Zutrittskontrollzentrale und dem PC mit dem **TECTIQ Access Manager** verzichten auf VPN- oder Webserver-Dienste und kommunizieren über ein verschlüsseltes Protokoll untereinander. Das Risiko für Manipulationsversuche ist hiermit gering.
- ein starker Passwortschutz im Netzwerk und in der **TECTIQ Zutrittskontrollzentrale**
Aktuelle Netzwerktechnologien mit sicheren Passwörtern fordern möglichen Angreifern ein hohes Maß an Rechenleistung ab. Ein gutes Passwort ist erst nach vielen Jahren überwindbar – wenn Sie Ihre Passwörter regelmäßig ändern, ist Ihr Schutz so gut wie perfekt.
- die korrekte Netzwerkkonfiguration in Ihrem Internet-Router
Aktivieren Sie in Ihrem Netzwerk-Router den höchst möglichen Schutz und beachten Sie die üblichen Sicherheitsmaßnahmen, wie sie z. B. durch das Bundesamt für Sicherheit in der Informationstechnik – bsi.bund.de – empfohlen werden.

2. TECTIQ – Für Nutzer

Sie sind Nutzer eines Gebäudes mit einem ABUS TECTIQ Zutrittskontrollsystem. Sie haben Ihr elektronisches Schließmedium erhalten und wurden von Ihrem Vorgesetzten oder dem Administrator in die Schließanlage eingewiesen. Sie kennen Ihre Zutrittsberechtigungen und wissen, wann Ihnen der Zutritt zum gesicherten Bereich gewährt wird.

Sobald Sie Ihr Schließmedium vor einer Türkomponente präsentieren, wird die Türkomponente für Sie freigegeben. Falls nicht, erhalten Sie eine optische Rückmeldung. Lesen Sie alles über die für Sie wichtigen Bedienschritte.

Verwahren Sie das Schließmedium sorgfältig.



Inhalt

- 2.1. Einweisung in die Schließanlage – Was Sie wissen müssen
- 2.2. Gesicherten Bereich betreten
- 2.3. Zutrittsberechtigung aktualisieren
- 2.4. Zutrittsberechtigung ändern
- 2.5. Zutrittsberechtigung sperren lassen
- 2.6. LED-Signale

2.1. Einweisung in die Schließanlage – Was Sie wissen müssen

Von Ihrem Vorgesetzten oder dem verantwortlichen Mitarbeiter sind Sie über die folgenden Punkte informiert worden:

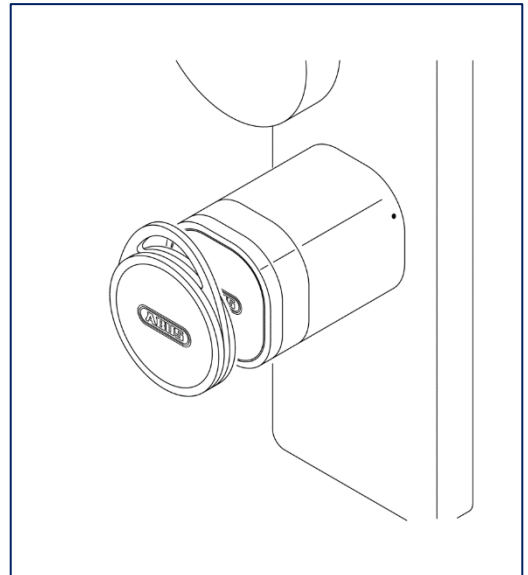
- Für welche Türen – und ggf. in welche Richtung – haben Sie Zutrittsberechtigungen?
- An welchen Tagen haben Sie Zutritt und zu welchen Zeiten?
- Wann haben Sie keinen Zutritt?
- Welche Funktionen können Sie mit Ihrem Schließmedium benutzen?
- Wie benutzen Sie Ihr Schließmedium an welcher Tür?
- Wie und wie oft aktualisieren Sie Ihr Schließmedium?
- Wo befinden sich Update Terminals, an denen Sie Ihr Schließmedium aktualisieren können?
- Wo können Sie Ihr Schließmedium aktualisieren, wenn keine Update Terminals vorhanden sind?
- An wen wenden Sie sich, wenn Sie ein Problem haben?

2.2. Gesicherten Bereich betreten

- ▶ Präsentieren Sie Ihr Schließmedium am Zylinderknopf, am Beschlag oder am Wandleser.
- Die Türfunktion wird freigegeben:
Der Schließzylinder koppelt die Schließfunktion ein, sodass Sie durch Drehen des Zylinders die Tür öffnen oder verriegeln können. Der Beschlag gibt den Türdrücker frei.
Der Wandleser öffnet die Tür oder gibt Ihre Öffnung frei.

Wenn:

- die Türfunktion nicht freigegeben wird und die LED rot blinkt
→ Aktualisieren Sie Ihre Zutrittsberechtigung.
- eine Tür sich auch nach Aktualisieren nicht öffnet
→ Informieren Sie Ihren Vorgesetzten oder Administrator.
- der Beschlag oder Zylinder verzögert reagiert
→ Batterie ist schwach. Informieren Sie Ihren Administrator, dass die Batterie möglichst bald gewechselt wird.



2.3. Zutrittsberechtigung aktualisieren

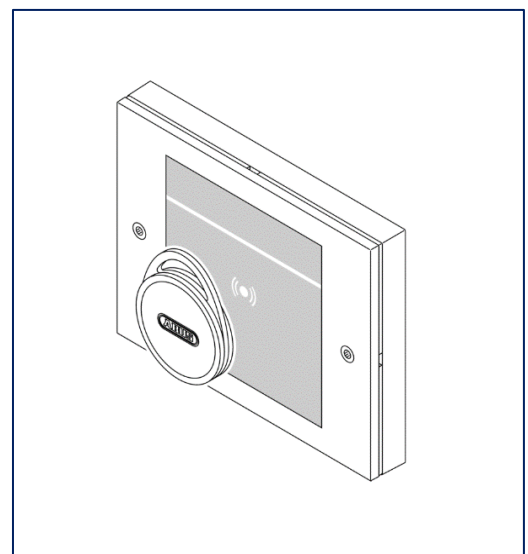
Die auf Ihrem Schließmedium gespeicherten Zutrittsberechtigungen können sich ändern und haben zum Schutz vor unbefugter Nutzung nur eine kurze Gültigkeit. Sie können aktuelle Zutrittsberechtigungen jederzeit auf Ihr Schließmedium übertragen.

- ▶ Präsentieren Sie Ihr Schließmedium am Update Terminal.
- Sie erhalten bei erfolgreicher Übertragung die Rückmeldung:
LED leuchtet grün, Terminal piept (1 s)

Ist das Update Terminal gleichzeitig als Türkomponente eingerichtet, wird die angeschlossene Tür geöffnet oder freigegeben.

Wenn:

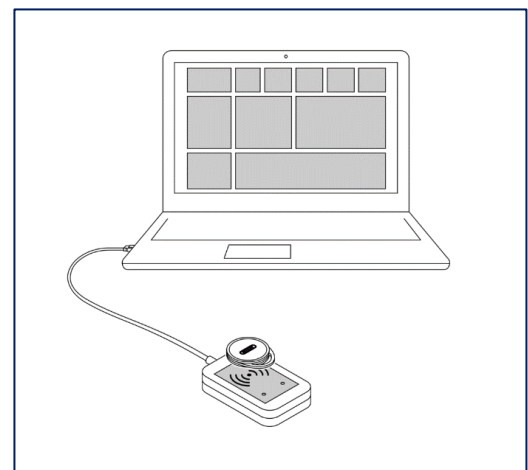
- die LED rot blinkt und das Terminal 2× kurz piept
→ Aktualisierung ist fehlgeschlagen
- Informieren Sie Ihren Administrator und lassen Sie Ihre Berechtigung ändern.



2.4. Zutrittsberechtigung ändern

Ihr Arbeitsplatz ist umgezogen oder Sie haben neue Verantwortungen oder der Zeitraum Ihrer Zutrittsberechtigung stimmt mit Ihren Aufgaben nicht überein.

- ▶ Wenden Sie sich an Ihren Vorgesetzten oder Administrator, um neue Berechtigungen im System zu erhalten.
- ▶ Aktualisieren Sie anschließend Ihr persönliches Schließmedium am Update Terminal oder über den TECTIQ Tischleser.



2.5. Zutrittsberechtigung sperren lassen




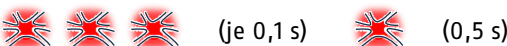








Wichtig! Verlorene Schließmedien, deren Verbleib nicht sicher geklärt ist, sind ein Risiko für Ihr Unternehmen. Veranlassen Sie die Sperrung des Schließmediums.

- ▶ Melden Sie den Verlust unverzüglich Ihrem Vorgesetzten oder Ihrem Administrator. Er setzt das Schließmedium auf die Sperrliste (Blacklist) und sperrt das Schließmedium dauerhaft. Es kann nicht mehr aktualisiert werden.
- ▶ Lassen Sie sich ein neues Schließmedium aushändigen.

2.6. LED-Signale

TECTIQ Türkomponenten signalisieren nach Betätigung ihren Zustand mittels LED-Signal:

	An Tür: Zutritt gewährt An Update Terminal: Zutrittsrechte wurden aktualisiert
 (je 0,1 s)	Zutritt verweigert Schließmedium abgelaufen oder keine Berechtigung für die Tür
 (0,1 s) (0,5 s)	Zutritt gewährt, Aktualisierung des Schließmediums am Update Terminal fehlgeschlagen
 (je 0,1 s) (0,5 s)	Zutritt verweigert, keine Berechtigung, Aktualisierung des Schließmediums am Update Terminal fehlgeschlagen
	Batteriewarnung, Zutritt gewährt
	Falsches oder fremdes Schließmedium / Lesefehler
	Allgemeiner Fehler
 (je 0,3 s)	Hardware-Fehler
 ...	Terminal ist offline; keine Verbindung zur Zentrale
	Anlagenstörung; kein Zutritt

3. TECTIQ – Für Administratoren

Sie sind Betreiber einer TECTIQ Zutrittskontrollanlage oder für den sicheren Betrieb einer TECTIQ Zutrittskontrollanlage verantwortlich.

Mit dem **TECTIQ Access Manager** verwalten Sie Zutrittsberechtigungen, Zeitpläne, Schließmedien und Systemmedien und bereiten die Programmierung der Türkomponenten vor. Die **TECTIQ Zutrittskontrollzentrale** sorgt für die Echtzeitbereitstellung notwendiger Daten an den Updateterminals und speichert alle eingegebenen Daten, Systemdaten und Systemzustände zentral. Auf dem Dashboard finden Sie eine Ereignisliste und eine Aufgabenliste, die aus den vorhandenen Daten generiert werden.

In diesem Abschnitt erhalten Sie eine Schritt-für-Schritt Anleitung für die regelmäßig anfallenden Aufgaben, wie z.B.

- die Anlage von Personengruppen und Personen,
- die Erstellung von Schließplänen zur Verwaltung der Zutrittsberechtigungen,
- die Einrichtung und Verwaltung der persönlichen Schließmedien für die Nutzer,
- die Einrichtung und Verwaltung von Systemmedien,
- die Programmierung der Türkomponenten und
- die Anlage von Zeitplänen.

Darüber hinaus erfahren Sie, welche Schritte notwendig sind

- wenn ein Schließmedium verloren gegangen ist oder gestohlen wurde,
- wenn sich Aufgaben eines Nutzers ändern und neue Zutrittsberechtigungen zugeteilt werden müssen,
- wenn sich persönliche Arbeitszeiten geändert haben und Zeitpläne aktualisiert werden müssen,
- wenn Personen aus dem Unternehmen ausscheiden,
- wenn Batterien in Türkomponenten zu erneuern sind oder
- eine Türkomponente oder ein Terminal einen Fehler meldet.



Wichtig! Halten Sie Zugangsdaten zum **TECTIQ Access Manager** unter Verschluss. Stimmen Sie sich bei Neuanlage von Berechtigungen mit den Verantwortlichen ab. Informieren Sie Ihre Vorgesetzten, wenn Sie sich unsicher sind. Bei technischen Fragen wenden Sie sich an Ihren ABUS Facherrichter.

Inhalt

- 3.1. Umgang mit Schließmedien und Systemmedien
- 3.2. Zutrittskontrollzentrale mit TECTIQ Access Manager verbinden
- 3.3. Person hinzufügen
- 3.4. Person bearbeiten
- 3.5. Person löschen
- 3.6. Personengruppe hinzufügen
- 3.7. Personengruppe bearbeiten
- 3.8. Personengruppe sperren
- 3.9. Personengruppe löschen
- 3.10. Schließmedien und Systemmedien verwalten
- 3.11. Schließmedium oder Systemmedium sperren
- 3.12. Schließmedium | Transponder bearbeiten
- 3.13. Schließmedium löschen
- 3.14. Zeitplan erstellen
- 3.15. Zeitplan bearbeiten
- 3.16. Zeitplan löschen

3.1. Umgang mit Schließmedien und Systemmedien

Bitte verwahren Sie Schließ- und Systemmedien an einem gesicherten Ort auf! Wenn Sie in falsche Hände geraten, gewähren Sie auch unbefugten Nutzern während ihrer Gültigkeit Zutritt zu den gesicherten Bereichen.

Beachten Sie die folgenden Grundregeln:

<ul style="list-style-type: none"> • Halten Sie Systemmedien (z. B. Parameterkarte) immer unter Verschluss! Benutzen Sie sie nur bei ausdrücklichem Bedarf!
<ul style="list-style-type: none"> • Tragen Sie Schließmedien mit aktiven Zutrittsrechten nur dann in die Schließanlage ein, wenn Sie sie Personen zuweisen und diesen aushändigen!
<ul style="list-style-type: none"> • Halten Sie insbesondere einen programmierten Notöffnungstransponder unter Verschluss, z. B. im Schlüsseldepot!
<ul style="list-style-type: none"> • Legen Sie keine Schließmedien mit aktiven Zutrittsberechtigungen „auf Vorrat“ an!
<ul style="list-style-type: none"> • Sperren Sie ein Schließmedium oder Systemmedium bei Verlust oder der Möglichkeit eines unbefugten Zugriffs! Zutrittsversuche mit gesperrten Schließmedien werden protokolliert.
<ul style="list-style-type: none"> • Soll ein Schließmedium gelöscht werden, müssen Sie es am Lesegerät präsentieren!

Besondere Anwendungen können Ausnahmen von diesen Regeln erfordern. Dokumentieren Sie in diesem Fall die Verwendung der Schließ- und Systemmedien. Ihr ABUS Fachhandelspartner steht für Fragen gerne zur Verfügung.

3.2. Zutrittskontrollzentrale mit TECTIQ Access Manager verbinden

Voraussetzungen:

- **TECTIQ Access Manager** ist installiert und eingerichtet.
 - **TECTIQ Zutrittskontrollzentrale** ist vorhanden, eingerichtet und verbunden.
- ▷ Starten Sie das Programm.
 - ▷ Loggen Sie sich mit Ihrem ABUS Account ein.
Nach dem Einloggen öffnet sich das Verbindungsfenster.

Falls für die Anlage kein ABUS Account besteht, registrieren Sie sich mit einem neuen ABUS Konto. Ihr ABUS Account muss von Ihrem ABUS Fachhändler in der Zutrittskontrollzentrale hinterlegt werden.

Die verfügbaren TECTIQ Zutrittskontrollzentralen werden automatisch angezeigt. Wird Ihre Zentrale nicht angezeigt, fügen Sie sie manuell über die IP-Adresse oder Connect-ID hinzu. Die IP-Adresse erhalten Sie über Ihren IT-Verantwortlichen, die Connect-ID über Ihren ABUS Fachhändler.



- ▷ Wählen Sie die gewünschte Zutrittskontrollzentrale mit einem Mausklick aus. Es öffnet sich das Fenster „Sicherheit und Datenschutz“.
- ▷ Lesen Sie die Nutzungsbedingungen und stimmen Sie zu.
- ▷ Lesen Sie die Datenschutzbestimmungen und stimmen Sie zu.
- ▷ Klicken Sie auf die Schaltfläche „Anwenden“.
Das Arbeitsfenster des TECTIQ Access Managers öffnet sich.

TECTIQ In Kürze.

3 TECTIQ – Für Administratoren

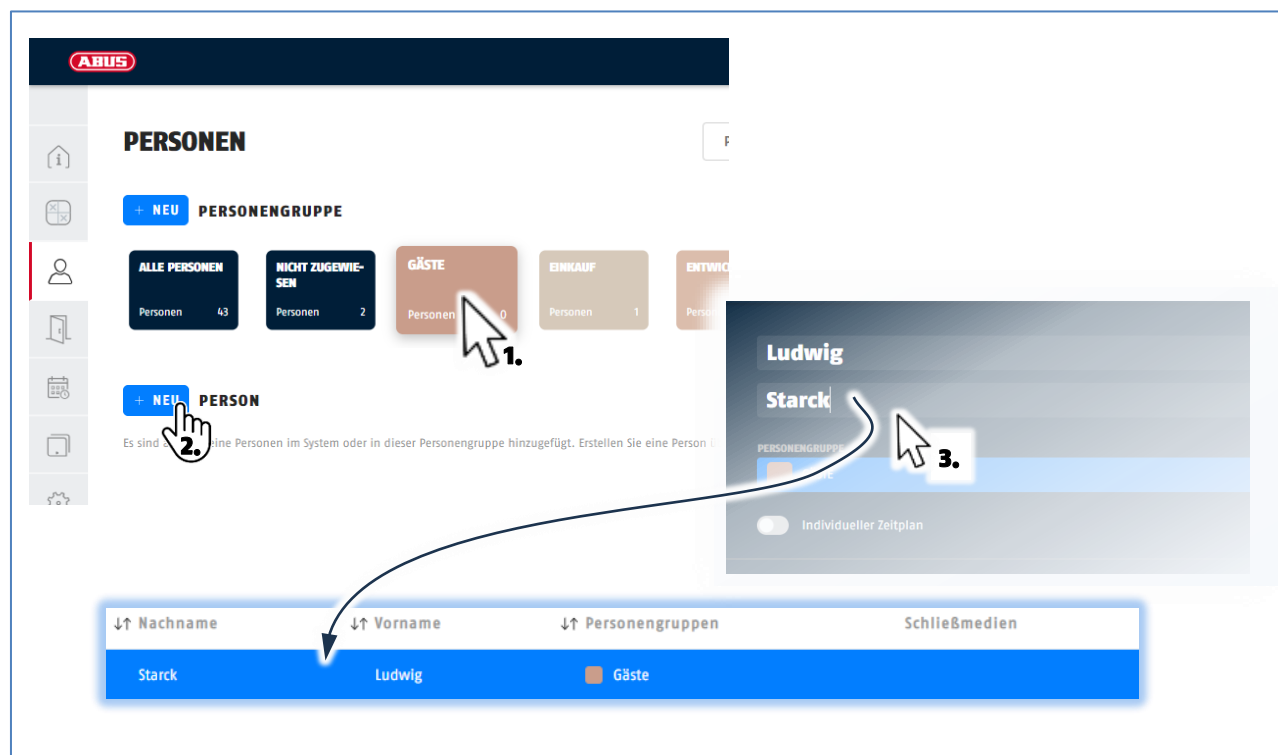
In den nachfolgenden Abschnitten erfahren Sie in Kürze

- wie Sie Personen und Personengruppen anlegen und verwalten,
- wie Sie Zutrittsberechtigungen verwalten,
- wie Sie persönliche Schließmedien für die Nutzer und Systemmedien verwalten,
- wie sie Zeitpläne anlegen und verwalten.

Für eine ausführliche Beschreibung zum Aufbau des TECTIQ Access Managers, seiner Funktionalitäten und Bedienung gehen Sie bitte zu Kap. 6 ff im Referenzhandbuch.

3.3. Person hinzufügen

- ▷ Öffnen Sie die Sicht „Personen“.
- ▷ Wählen Sie die Personengruppe, in die Ihr neuer Nutzer aufgenommen werden soll (1.).
- ▷ Betätigen Sie über der Personenliste die Schaltfläche „+ NEU“ (2.).
- ▷ Tragen Sie die Personendaten ein (3.).



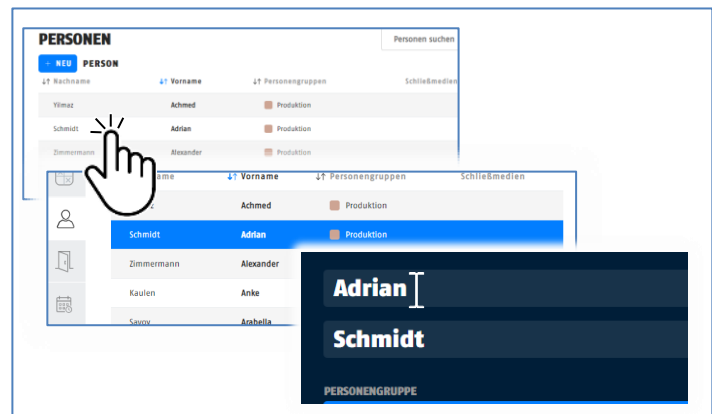
Dem neuen Nutzer werden alle Zugangsberechtigungen der ausgewählten Personengruppe automatisch zugeordnet. Sie können individuelle Berechtigungen für die Person hinzufügen oder abwählen.

- ▷ Wechseln Sie in die Sicht Schließplan und passen Sie die Berechtigungen zu Türen oder Türgruppen individuell an.
- ▷ Für individuelle Zutrittszeiten: Wählen Sie einen bestehenden Zeitplan aus oder erstellen Sie einen Neuen.
- ▷ Setzen Sie die Gültigkeit des Schließmediums. Voreingestellt ist die Gültigkeit aus der Systemkonfiguration.
- ▷ Weisen Sie der Person ein Schließmedium zu und programmieren es. Nach der Programmierung steht Ihnen unter dem Menüpunkt „Mehr Informationen“ eine Empfangsquittung mit allen relevanten Daten zum Ausdruck zur Verfügung. Siehe Muster im Anhang.
- ▷ Händigen Sie der Person ihr Schließmedium aus und lassen Sie sich den Empfang quittieren.
- ▷ Weisen Sie die Person in die Anlage ein und informieren Sie sie über ihre Berechtigungen, Zeiten und die Validierung und Aktualisierung des persönlichen Schließmediums.

3.4. Person bearbeiten

Personennamen bearbeiten

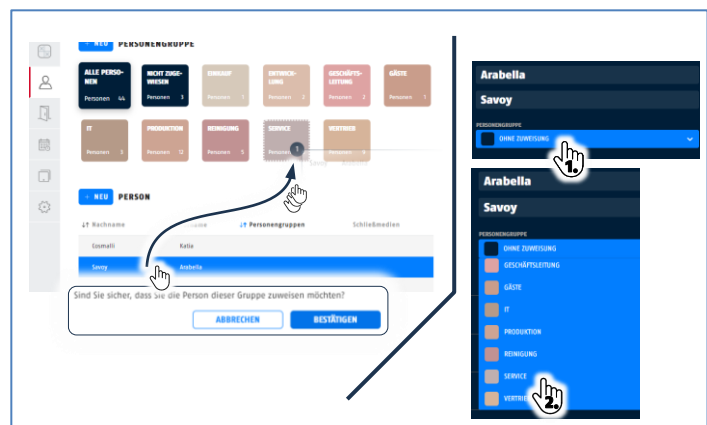
- Öffnen Sie die Sicht „Personen“.
- Wählen Sie die Person in der Personenliste aus.
Wenn die Person in der Liste markiert ist, wechselt der Editierbereich in den Bearbeitungsmodus.
- Setzen Sie den Mauszeiger in die Eingabefelder und nehmen Sie Ihre Eingaben vor.



Personengruppe ändern

Fügen Sie eine Person zu einer (anderen) Personengruppe hinzu, um ihr die Zutrittsrechte dieser Gruppe zuzuweisen.

- Öffnen Sie die Sicht „Personen“.
 - Wählen Sie die Person in der Personenliste aus.
 - Schieben Sie die Person aus der Liste auf die gewünschte Personengruppe.
- oder -
- Öffnen Sie das Listenfeld Personengruppe und wählen Sie die gewünschte Gruppe aus.
-
- Schließen Sie den Vorgang ab, indem Sie das Schließmedium programmieren.



Zutrittsberechtigung ändern

Wenn Sie einem Nutzer die Zutrittsberechtigung einer Personengruppe zuweisen wollen, fügen Sie sie zu dieser Gruppe hinzu (siehe → Personengruppe ändern).

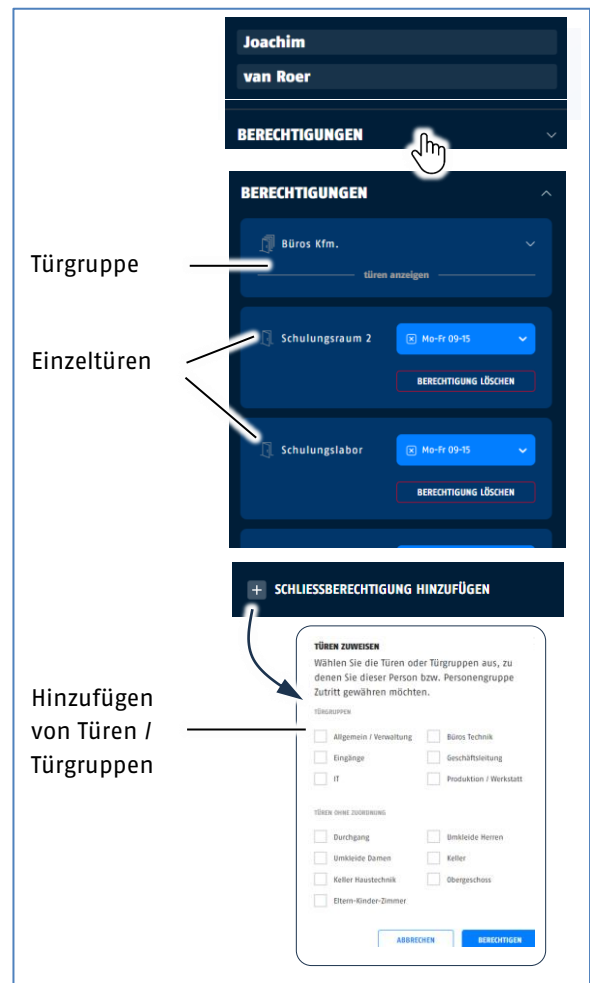
Erteilen Sie Zutrittsberechtigungen zu weiteren Türen oder Türgruppen in der Sicht Personen oder in der Sicht Schließplan.

In der Sicht Personen:

- ▶ Öffnen Sie die Sicht „Personen“.
- ▶ Wählen Sie die Person in der Personenliste aus.
- ▶ Klappen Sie das Listenfeld „Berechtigungen“ aus.

Beachten Sie: Änderungen werden sofort übernommen.

- ▶ Entziehen Sie eine Berechtigung, indem Sie für die betreffende Tür die Schaltfläche „Berechtigung löschen“ betätigen.
- ▶ Schließen Sie den Vorgang ab, indem Sie das Schließmedium programmieren.

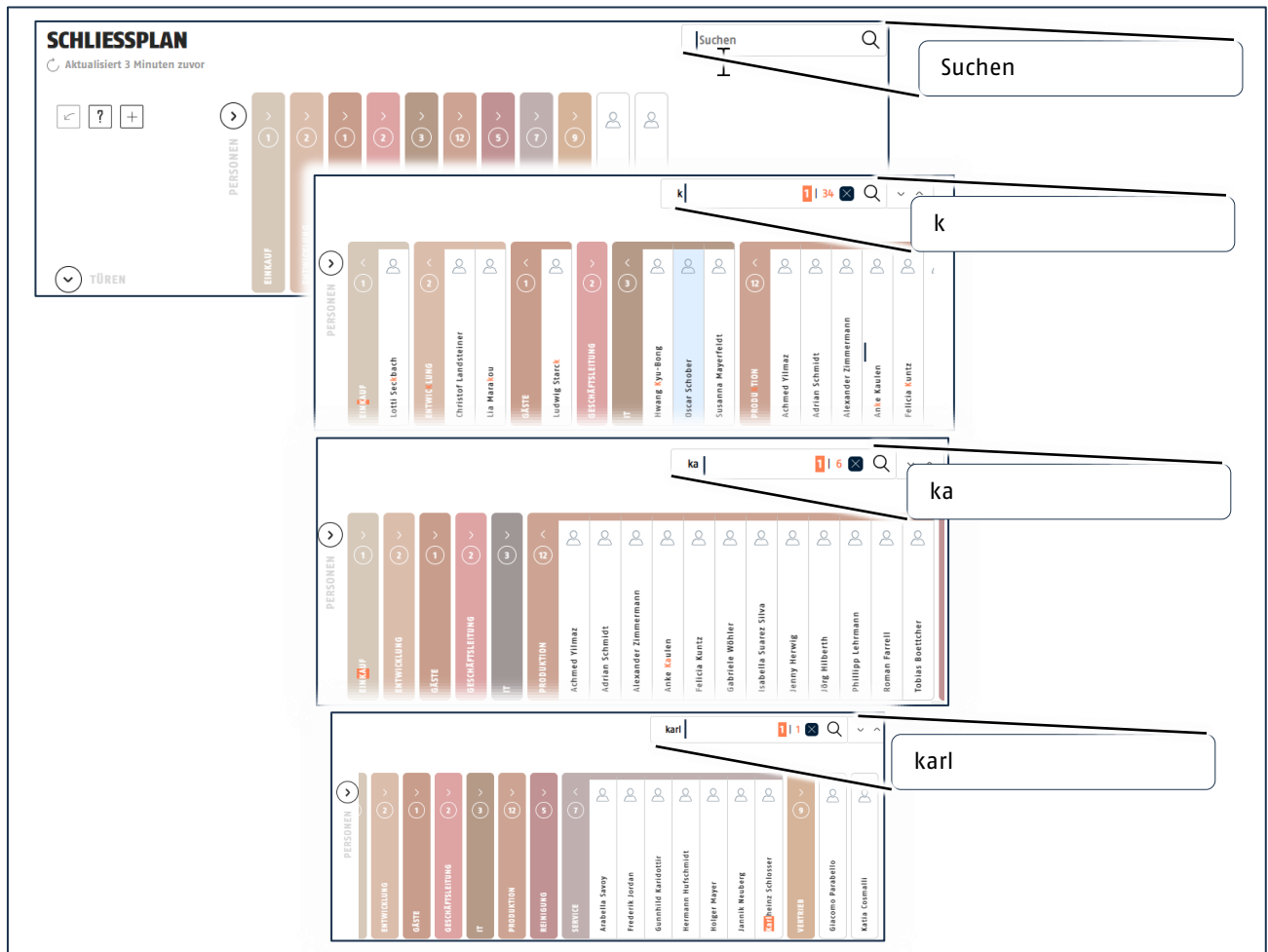


TECTIQ In Kürze.

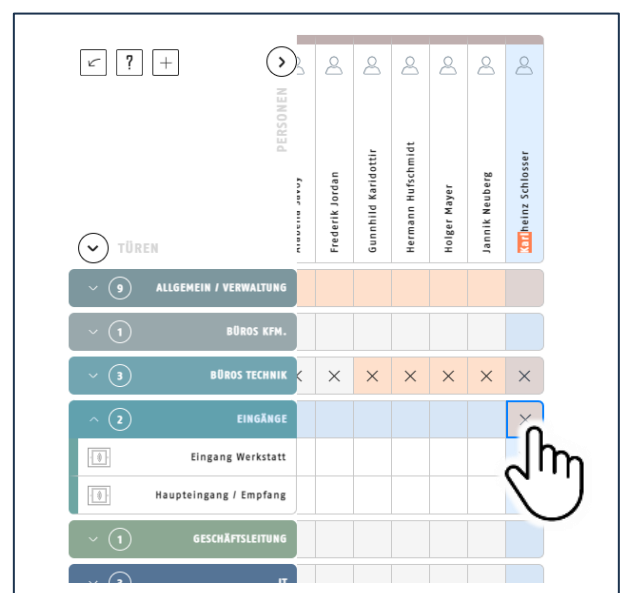
3 TECTIQ – Für Administratoren

In der Sicht Schließplan:

- Öffnen Sie die Sicht Schließplan.
- Finden Sie die Person, indem Sie ihren Namen in das Suchfeld eintragen. Der Schließplan bietet bereits während der Eingabe passende Suchergebnisse an.



- Weisen Sie der Person die gewünschten Berechtigungen zu Türen oder Türgruppen zu, indem Sie an der passenden Stelle im Schließplan ein **×** setzen.
- Entziehen Sie Zutrittsberechtigungen indem Sie an der entsprechenden Stelle das **×** löschen.
- Schließen Sie den Vorgang ab, indem Sie das Schließmedium programmieren.



TECTIQ In Kürze.

3 TECTIQ – Für Administratoren

Zeitplan zuweisen

Ein Zeitplan schränkt die Zutrittszeiten der Person ein. Voreingestellt ist der Zeitplan der Personengruppe.

Sie können der Person einen anderen Zeitplan zuweisen. Zusätzlich können Sie für einzelne Türen die Berechtigung permanent erteilen oder komplett entfernen.

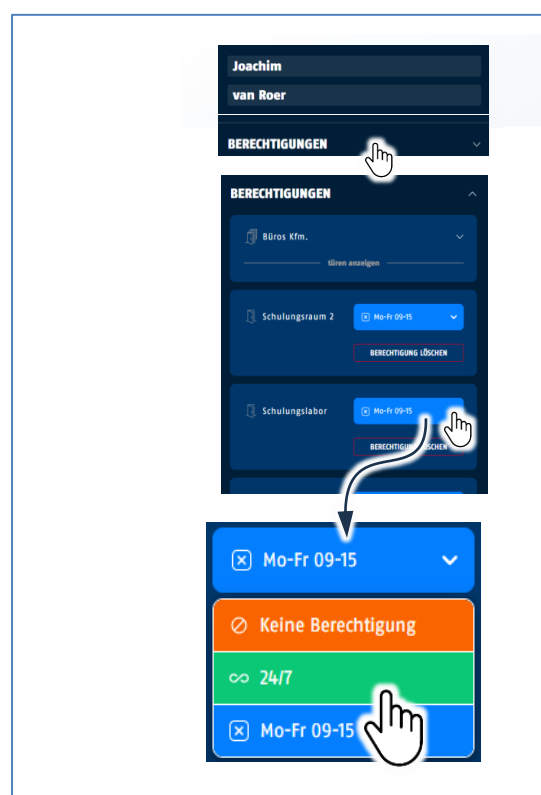
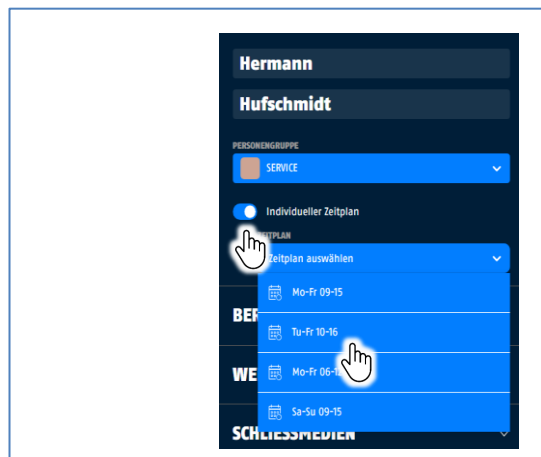
- ▶ Öffnen Sie die Sicht „Personen“.
- ▶ Wählen Sie die Person in der Personenliste aus.

Weisen Sie der Person einen anderen Zeitplan zu:

- ▶ Klicken Sie auf den Schalter „Individueller Zeitplan“.
- ▶ Klappen Sie die Liste mit Zeitplänen aus.
- ▶ Wählen Sie aus der Liste einen Zeitplan aus.

Weisen Sie der Person für einzelne Türen einen anderen Zeitplan zu:

- ▶ Klappen Sie das Listenfeld „Berechtigungen“ aus.
- ▶ Wählen Sie in der Liste die zu ändernde Tür oder Türgruppe aus.
- ▶ Klappen Sie die Liste mit Zeitplänen aus.
- ▶ Vergeben Sie die permanente Zutrittsberechtigung, indem Sie den Eintrag „24/7“ auswählen.
- ▶ Schränken Sie die Zutrittsberechtigung zeitlich ein, indem Sie einen Zeitplan auswählen.
Falls kein Zeitplan auswählbar ist, erstellen Sie einen Zeitplan in der Sicht Zeitpläne und weisen sie ihn der Personengruppe oder der Person zu.
- ▶ Entziehen Sie Berechtigung, indem Sie „Keine Berechtigung“ auswählen.
Bei Einzeltüren ist diese Einstellung gleichbedeutend mit der Schaltfläche „Berechtigung löschen“.
- ▶ Schließen Sie den Vorgang ab, indem Sie das Schließmedium programmieren.



TECTIQ In Kürze.

3 TECTIQ – Für Administratoren

Zutrittsberechtigung zeitlich begrenzen

Für einen zeitlich begrenzten Zugang – z. B. für Besucher, Praktikanten oder Handwerker, denen nur für einen begrenzten Zeitraum der Zutritt gewährt wird - setzen Sie Beginn und Ende für die Gültigkeit des Schließmediums.

- ▷ Öffnen Sie die Sicht „Personen“.
- ▷ Wählen Sie die Person in der Personenliste aus.
- ▷ Klappen Sie das Listenfeld „Weitere Einstellungen“ aus.
- ▷ Klicken Sie auf den Schalter „Gültigkeit der Zutrittsrechte (von...bis)“.
- ▷ Wählen Sie ein Startdatum und ein Enddatum aus.
Ohne Startdatum sind die Zutrittsberechtigungen sofort gültig.
Ohne Enddatum sind die Zutrittsberechtigungen unbegrenzt gültig.

Wenn der Zutritt auch auf bestimmte Uhrzeiten eingeschränkt werden soll, weisen Sie der Person (oder Personengruppe) zusätzlich einen Zeitplan zu.

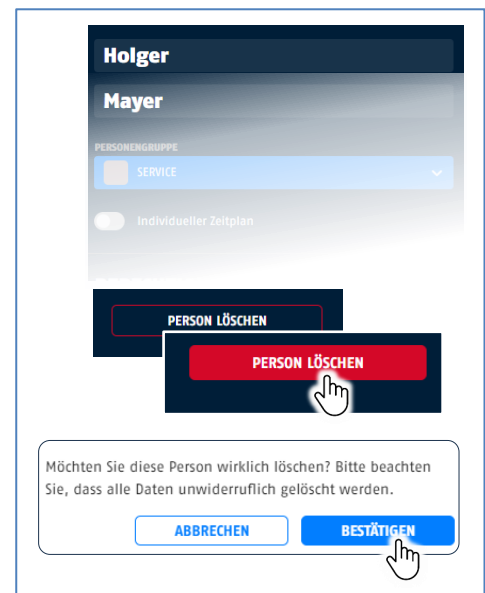
- ▷ Schließen Sie den Vorgang ab, indem Sie das Schließmedium programmieren.

3.5. Person löschen

Das Löschen eines Nutzers bewirkt, dass sämtliche Daten der Person gelöscht werden.

Beachten Sie: Personen können nur gelöscht werden, wenn alle Schließmedien zurückgegeben wurden und die Zuweisungen der Medien zur Person entfernt wurden. So wird sichergestellt, dass Zutrittsversuche mit gesperrten Schließmedien zurückgewiesen und protokolliert werden. Eine Änderung des Personennamens ist möglich.

- ▷ Öffnen Sie die Sicht „Personen“.
- ▷ Wählen Sie die Person in der Personenliste aus.
- ▷ Betätigen Sie die Schaltfläche „Person löschen“.
- ▷ Wenn Sie sicher sind, die Person aus der Anlage zu entfernen, beantworten Sie die Sicherheitsabfrage mit „Bestätigen“.



3.6. Personengruppe hinzufügen

Zur besseren Orientierung fassen Sie Personen mit ähnlichen Berechtigungen in Personengruppen zusammen. Personengruppen erleichtern die Verwaltung einer Schließanlage. Einer Personengruppe können gesammelt Zutrittsrechte erteilt oder entzogen werden, Zeitpläne können vorgegeben werden und anderes mehr.

Eine Person kann maximal einer Personengruppe zugewiesen sein.

- Öffnen Sie die Sicht Personen.
- Betätigen Sie im oberen Teil des Fensters „Personen“ die Schaltfläche „+ NEU“ (1).
- Tragen Sie im Editierbereich eine Bezeichnung für die Gruppe (2) ein.
Sobald das Programm eine Bezeichnung erkennt, wird für die neue Gruppe eine Kachel (3) erzeugt und der Name angezeigt.

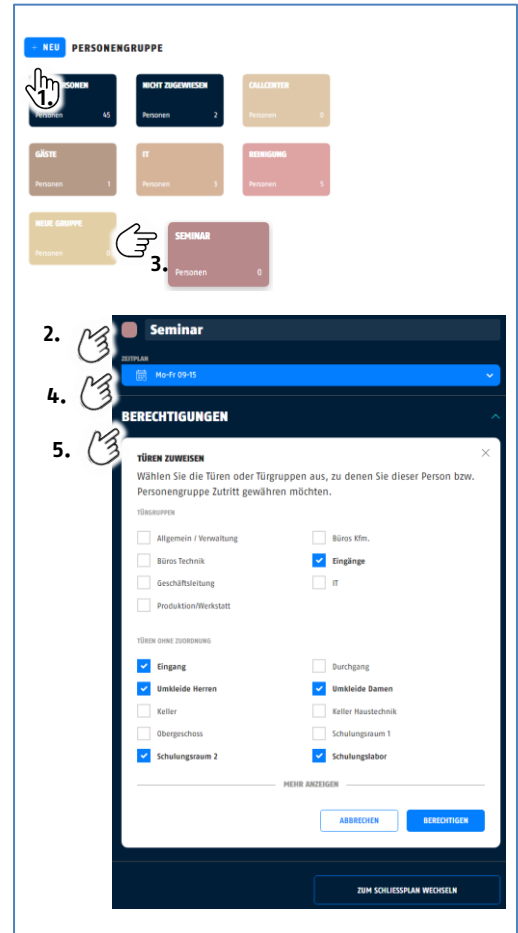
Wenn zutreffend:

- Wählen Sie für die neue Gruppe einen Zeitplan (4).
- Wählen Sie für die Personengruppe Zutrittsberechtigungen für Türen oder Türgruppen aus (5).

Gruppenberechtigungen werden für alle Personen, die der Gruppe angehören, vererbt.

Gruppenberechtigungen können in der Sicht Personen oder in der Sicht Schließplan erteilt werden.

Es ist nicht möglich, für eine Personengruppe ein Schließmedium zu erzeugen und zu programmieren. Schließmedien können nur Personen zugewiesen werden.



3.7. Personengruppe bearbeiten

Gruppennamen ändern

- Öffnen Sie die Sicht Personen.
- Wählen Sie die Kachel für die Gruppe aus.
- Setzen Sie den Mauszeiger auf das Namensfeld mit dem Gruppennamen.
- Ändern Sie den Gruppennamen wie gewünscht.



Zeitplan für Personengruppe zuweisen

- Falls noch nicht vorhanden, erstellen Sie einen passenden Zeitplan in der Sicht Zeitpläne.
- Öffnen Sie die Sicht „Personen“.
- Wählen Sie die Kachel für die Gruppe aus.

Wenn ein Zeitplan für alle Türen und Türgruppen gültig sein soll:

- Klappen Sie das Listenfeld „Zeitplan“ aus und wählen Sie aus der Liste den gewünschten Zeitplan.

Wenn ein Zeitplan nur für einzelne Türen oder Türgruppen gültig sein soll:

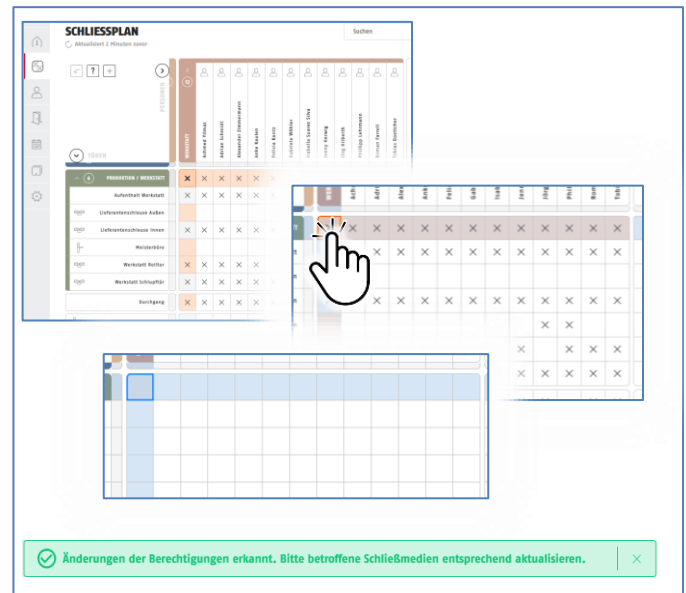
- Klappen Sie das Listenfeld „Berechtigungen“ aus.
- Wählen Sie aus der Liste die gewünschte Tür oder Türgruppe aus.
- Klappen Sie die Liste mit Zeitplänen aus.
- Vergeben Sie die permanente Zutrittsberechtigung, indem Sie den Eintrag „24/7“ auswählen.
- Schränken Sie die Zutrittsberechtigung zeitlich ein, indem Sie einen Zeitplan auswählen.
- Wenn Sie anstelle eines Zeitplans „Keine Berechtigung“ auswählen, entziehen Sie die entsprechende Berechtigung. Diese Einstellung ist gleichbedeutend mit der Schaltfläche „Berechtigung löschen“.



3.8. Personengruppe sperren

Entziehen Sie allen Personen einer Personengruppe die Zutrittsberechtigungen.
 Beim Entziehen der Zutrittsberechtigungen bleiben die Daten noch in der Anlage gespeichert und der Zutritt kann aktiv unterbunden werden. Verweigerte Zutrittsversuche – z. B. mit Hilfe nicht zurückgegebener Schließmedien – werden zusätzlich protokolliert.

- ▷ Öffnen Sie die Sicht „Schließplan“.
- ▷ Wählen Sie die Gruppenspalte aus.
- ▷ Entfernen Sie in der kompletten Gruppenspalte alle Berechtigungen, indem Sie das × entfernen.



Alternativ können Sie Berechtigungen in der Sicht Personengruppe entziehen:

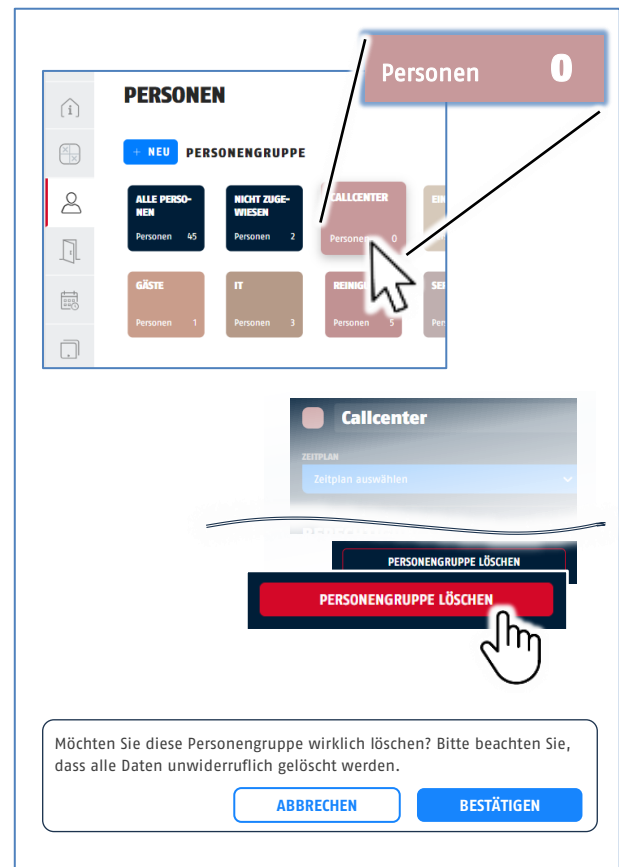
- ▷ Öffnen Sie die Sicht „Personen“ und wählen Sie die Kachel für die Gruppe aus.
- ▷ Klappen Sie das Listenfeld „Berechtigungen“ aus.
- ▷ Wählen Sie aus der Liste die gewünschte Tür oder Türgruppe aus.
- ▷ Entziehen Sie die Berechtigung, indem Sie die Schaltfläche „Berechtigung löschen“ betätigen. Diese Einstellung ist gleichbedeutend mit dem Eintrag „Keine Berechtigung“ in der Liste der Zeitpläne.



3.9. Personengruppe löschen

Sie können leere Personengruppen löschen.

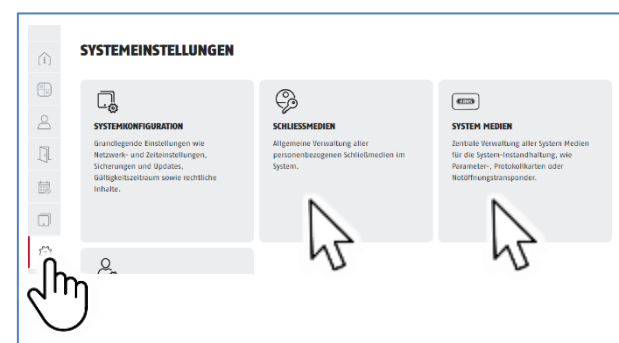
- ▷ Öffnen Sie die Sicht Personen.
- ▷ Wählen Sie die zu löschende Personengruppe aus.
- ▷ Weisen Sie die enthaltenen Personen anderen Personengruppen zu, indem Sie die Personen in der Liste auswählen und in die betreffende Gruppe verschieben.
Für eine Mehrfachauswahl drücken Sie die Umschalttaste und klicken die gewünschten Personen an.
Alternativ verschieben Sie die Personen in die Gruppe „Nicht zugewiesen“ oder löschen Sie sie.
- ▷ Wenn die Personengruppe keine Personen mehr enthält, betätigen Sie die Schaltfläche „Personengruppe löschen“.



3.10. Schließmedien und Systemmedien verwalten

Unter den Systemeinstellungen können Sie sich alle im System vorhandenen Schließmedien und Systemmedien übersichtlich anzeigen lassen. Sie haben hierdurch einen schnellen Überblick über noch verfügbare Medien.

Informationen zu den Schließmedien können hier angepasst werden. Die Zuweisung der Schließmedien erfolgt während der Neuanlage und Bearbeitung von Personen.



Unter Systemmedien erfolgt die Anzeige von Karteninformationen sowie zentrale Verwaltung aller für die Systembetreuung und Instandhaltung notwendigen Systemkarten, wie Parameterkarten, Protokollkarten, Resetkarten, Blacklistkarten und Notöffnungstransponder.

Sie können Systemmedien einen Namen geben, eine Beschreibung hinzufügen und die Gültigkeit des Systemmediums festlegen. Für Notöffnungstransponder ist eine unbegrenzte Gültigkeit systemseitig eingestellt. Sie kann nicht geändert werden. Alle Systemmedien können gelöscht werden. Beachten Sie jedoch, dass Sie auf wichtige Funktionen ohne Systemkarte nicht zugreifen können.

TECTIQ In Kürze.

3 TECTIQ – Für Administratoren

3.11. Schließmedium oder Systemmedium sperren

Sperren Sie ein Schließmedium oder Systemmedium, wenn es verlorengegangen ist oder gestohlen wurde.

Voraussetzungen für die Sperrung eines Schließmediums:

- Sie benötigen eine Blacklistkarte für Ihre Schließanlage, um die Sperrung des Schließmediums in allen Türkomponenten zu aktivieren.
- Öffnen Sie die Sicht Dashboard.
- Wählen Sie die Kachel „Schließmedium verloren oder gestohlen“.
- Geben Sie in das Suchfeld den Namen der Person deren Schließmedium gesperrt werden soll oder den Namen des Systemmediums ein.
- Die gefundenen Schließ- und Systemmedien werden als Ergebnisliste angezeigt.

Wenn Sie den Namen nicht genau kennen, zeigt Ihnen die Suchfunktion bereits nach der Eingabe von 2 Buchstaben übereinstimmende Einträge an.

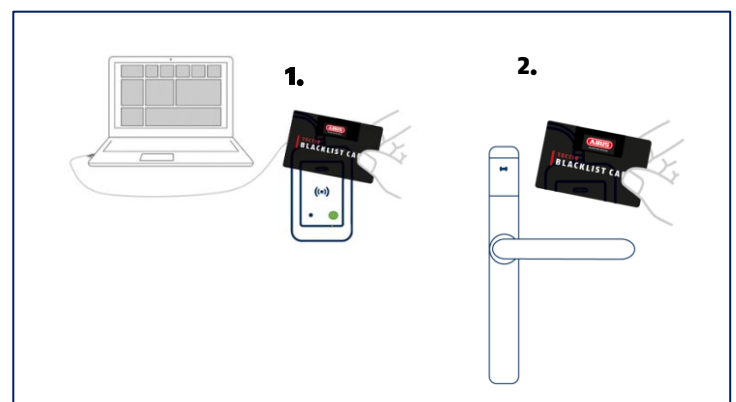
- Betätigen Sie in der gewünschten Zeile den Schalter „Medium blockieren“.
- Die Sperrung wird bestätigt und eine Liste mit allen betroffenen Türen wird zum Download bereitgestellt.
- Laden Sie die Liste durch Klicken auf den blauen Download-Button auf Ihren PC.



- Sie finden die Download-Liste in Ihrem Download-Verzeichnis

ID	NAME
2	Besprechung 1
4	Büro 1: Verwaltung
11	Büro 2: Entwicklung
19	Büro 1 Notausgang
21	Haupteingang / Empfang
26	Schulungsraum 1

- Nehmen Sie die Blacklistkarte zur Hand.
- Präsentieren Sie die Blacklistkarte am Tischleser (1).
- Gehen Sie zu allen Türkomponenten aus der Download-Liste und präsentieren Sie dort die Blacklistkarte (2).



Beachten Sie:

Sperrlisten werden nur über die Blacklistkarte auf die Türkomponenten übertragen!

3.12. Schließmedium | Transponder bearbeiten

Sie können den Schließmedien im Editierbereich der Person Informationen hinzufügen.

Name des Schließmediums ändern

- ▶ Geben Sie dem Schließmedium einen prägnanten Namen.
- Wählen Sie z.B. die auf dem Schließmedium aufgedruckte Transpondernummer „KDExxxxx“.
- Hinweis: Eine sorgfältige Datenpflege erleichtert Ihnen die Zuordnung ausgegebener Schließmedien zu Personen.

Schließmedium sperren und entsperren

Der aktuelle Sperrstatus wird angezeigt. Sie können eine Sperre setzen und wieder aufheben, z.B. wenn das Schließmedium wiedergefunden wurde.

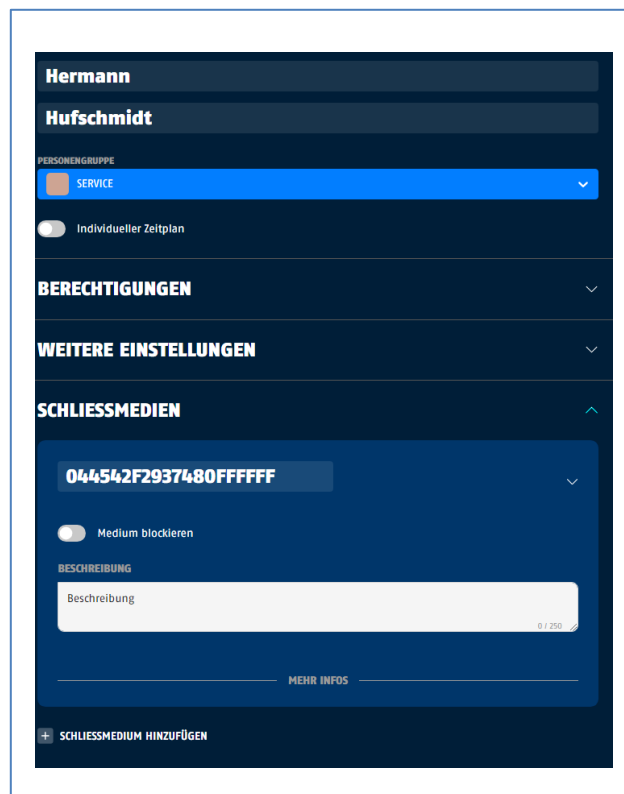
Beachten Sie: Jede Änderung des Sperrstatus muss anhand der Sperrliste mit der Sperrkarte (Blacklistkarte) auf jede Türkomponente übertragen werden.

Beschreibung zum Schließmediums ergänzen

- ▶ Sie können jedem Schließmedium eine Beschreibung hinzufügen, z.B. „Ersatzmedium ausgegeben am “.

Weiteres Schließmedium hinzufügen

- ▶ Sie können einer Person ein weiteres Schließmedium erstellen und aushändigen.



3.13. Schließmedium löschen

Schließmedien können durch Löschung von einer Person getrennt werden.

- ▶ Klappen Sie dazu in der Sicht Personen unter Schließmedien die Bearbeitungssicht „Mehr Infos“ auf.
- ▶ Klicken Sie „Schließmedium löschen“ an.
- ▶ Wenn Sie die Schaltfläche „Löschen bestätigen“ anklicken, wird die Zuweisung des Schließmediums zur Person aufgehoben.

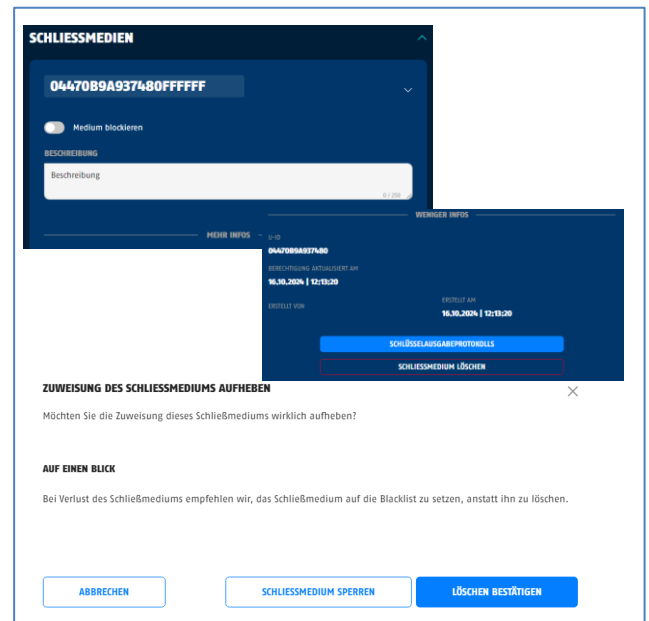
Das Schließmedium wird dem Pool nicht zugewiesener Schließmedien zugeordnet und kann hier gelöscht und danach einer anderen Person zugewiesen werden

Beachten Sie:

Der Versuch, Zutritt mit nicht zugewiesenen Schlüsseln zu erlangen, wird nicht protokolliert. Daher wird in den meisten Fällen eine Sperrung eines Schließmediums empfohlen!

Um ein Schließmedium zu löschen, darf es nicht blockiert sein.

Während des Löschvorgangs muss das Schließmedium am Tischleser präsentiert werden. Verlorene Schließmedien können nicht gelöscht werden und müssen blockiert werden.

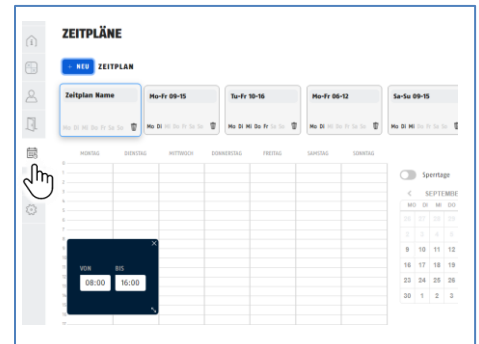


3.14. Zeitplan erstellen

- ▶ Erstellen Sie einen neuen Zeitplan in der Sicht Zeitpläne.
- ▶ Im Referenzhandbuch Kap. 11 erfahren Sie alles über die Anlage und Bearbeitung von Zeitplänen.

In der TECTIQ Zutrittskontrollanlage können bis zu 300 Zeitpläne mit jeweils bis zu 15 Zeitintervallen gespeichert werden.

Pro Person ist immer nur ein Zeitplan gültig. Bei der erstmaligen Anlage erbt der neue Nutzer den Zeitplan der Personengruppe, der er zugeordnet ist. Der Zeitplan kann individuell angepasst oder ein neuer individueller Zeitplan erstellt werden.



Jeder Zeitplan kann von allen Personengruppen und/oder Personen im System genutzt werden. Es wird daher empfohlen, Zeitpläne einfach, neutral und einheitlich zu benennen (z.B. nach eingestelltem Zeitintervall „Mo-Fr 08-18 Uhr“).

Jedem Zeitplan können Sperrtage hinzugefügt werden, an denen die Nutzer keinen Zutritt zum gesicherten Bereich haben (z.B. Betriebsferien).

- ▶ Beachten Sie: Ein Zeitplan wird nur angewendet, wenn er einer Personengruppe oder einer Person zugewiesen wurde und die zugehörigen Schließmedien aktualisiert wurden.

3.15. Zeitplan bearbeiten

Ein Zeitplan kann in der Sicht Zeitpläne bearbeitet/geändert werden. Siehe hierzu Referenzhandbuch Kap. 11.

- ▶ Beachten Sie: Ein Zeitplan wird erst nach Aktualisierung des Schließmediums wirksam.
- ▶ Beachten Sie: Jede Änderung eines Zeitplans hat Einfluss auf alle Personengruppe und Personen, deren Berechtigung mit dem Zeitplan verknüpft ist.

3.16. Zeitplan löschen

Ein Zeitplan kann in der Sicht Zeitpläne gelöscht werden. Voraussetzung ist, dass er keiner Personengruppe oder Person mehr zugewiesen ist.

4. TECTIQ – Für Fachrichter

Sie sind Service-Techniker oder ABUS Fachhandelspartner. Sie planen Zutrittskontrollanlagen mit ABUS TECTIQ. Sie projektieren die Anlage, stellen die Bedarfe fest, bestellen die Komponenten. Sie planen Türen und Systemkomponenten. Sie sind der Ansprechpartner für Ihre Kunden oder haben Service- und Wartungsverträge abgeschlossen.

Inhalt

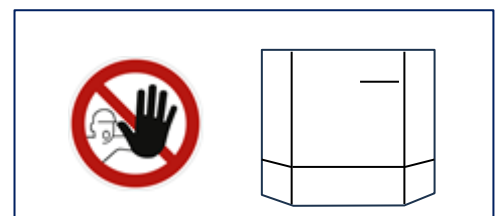
- 4.1. Realisieren einer TECTIQ Zutrittskontrollanlage – Erste Schritte
 - 4.1.1. Montageort der Zutrittskontrollzentrale
 - 4.1.2. Leitungsführung
 - 4.1.3. Montageort des Update Terminals
 - 4.1.4. Aufstellen des PC
 - 4.1.5. Tischleser anschließen
 - 4.1.6. Zutrittskontrollzentrale starten
 - 4.1.7. Update Terminal mit Zutrittskontrollzentrale verbinden
 - 4.1.8. Systemmedien einrichten
- 4.2. Projektierung und Inbetriebnahme
 - 4.2.1. Türen und Türgruppen projektieren
 - 4.2.2. Türkomponenten zuordnen und einstellen
 - 4.2.3. Türkomponenten programmieren
 - 4.2.4. Zeitpläne definieren
 - 4.2.5. Personengruppen und Personen anlegen
 - 4.2.6. Zutrittsberechtigungen vergeben
 - 4.2.7. Schließmedien programmieren
- 4.3. TECTIQ Schließmedien ausgeben
- 4.4. TECTIQ System an den Betreiber übergeben

4.1. Realisieren einer TECTIQ Zutrittskontrollanlage – Erste Schritte

Die ersten Schritte in der Umsetzung einer TECTIQ Zutrittskontrollanlage beziehen sich auf die Systemkomponenten Zentrale, Update Terminal, PC und Tischleser sowie die Systemmedien (Parameterkarte).

4.1.1. Montageort der Zutrittskontrollzentrale

- Vor unbefugtem Zugriff geschützt – z. B. Serverraum
Im Bedarfsfall muss das Gerät für Wartungspersonal erreichbar sein, z. B. zum Ablesen der LED.
- Versorgung mit Netzspannung
- Empfehlung: USV-gepuffert
- Netzwerkanschluss
- Empfehlung: eigener Netzwerkstrang
- ausreichende Belüftung in geschlossenen Umgebungen (z. B. Verteilerschrank)





Wichtig! Bei längerem Ausfall der Stromversorgung an der Zentrale werden die Zutrittsberechtigungen in Update Terminals nicht mehr aktualisiert.

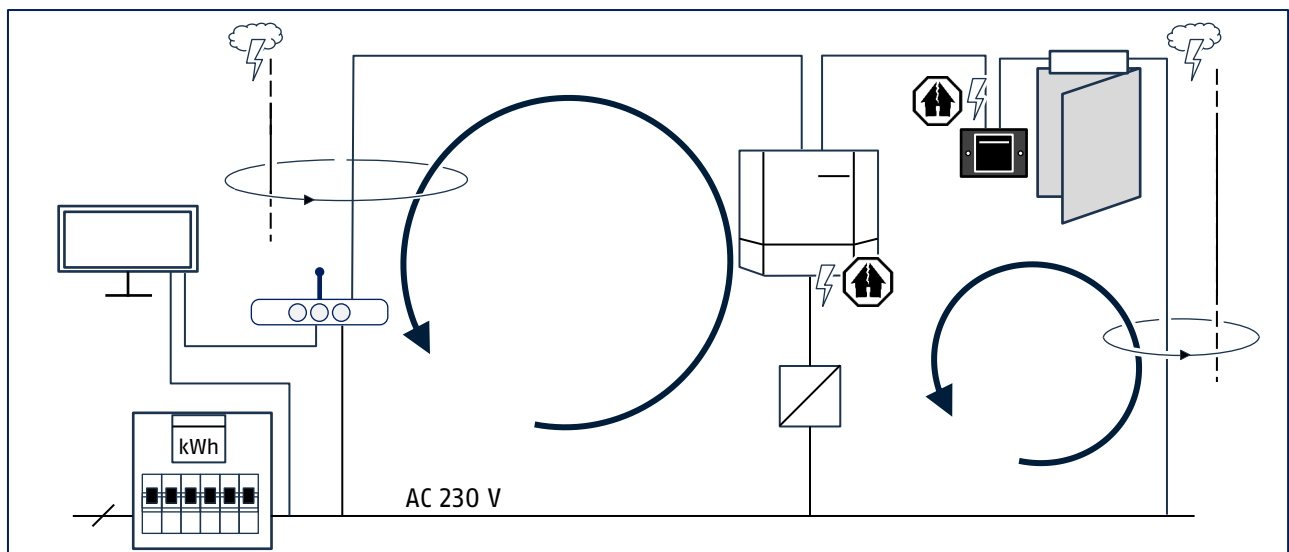
- Stellen Sie sicher, dass das Netzteil nicht aus der Steckdose gezogen werden kann!
- Sichern Sie die Versorgung der Zutrittskontrollzentrale separat ab.

4.1.2. Leitungsführung



HINWEIS Energiereiche Ereignisse im Leitungsnetz, z. B. in Folge eines Blitzeinschlags, können elektronische Geräte durch Überspannungen zerstören.

- Vermeiden Sie Leiterschleifen bei der Elektro- und Netzwerkinstallation (siehe Bild).
- Installieren Sie einen Blitz- und Überspannungsschutz.



- ▶ Achten Sie auf Manipulationsmöglichkeiten, besonders bei Versorgungs- und Netzwerkleitungen. Wenn sinnvoll, verlegen Sie separate Leitungen und sichern Sie diese separat ab.

4.1.3. Montageort des Update Terminals

Das Update Terminal besteht aus der Wandleseinheit und der Steuereinheit. Hier gelten die gleichen Kriterien und Maßnahmen wie bei der Zentrale.

Die Kompaktmontage (Wandleser- und Steuereinheit in einer gemeinsamen Unterputzdose) sollte nur im geschützten Innenbereich erfolgen, wo keine unbefugten Eingriffe zu erwarten sind. In allen anderen Fällen montieren Sie Wandleser- und Steuereinheit voneinander getrennt, z. B.:

- im Außenbereich,
- in öffentlich zugänglichen Bereichen (Flure, Treppenhäuser),
- wenn am Montageort der Leseinheit keine sensiblen Anschlussleitungen liegen sollen (Netzwerk, Türansteuerung),

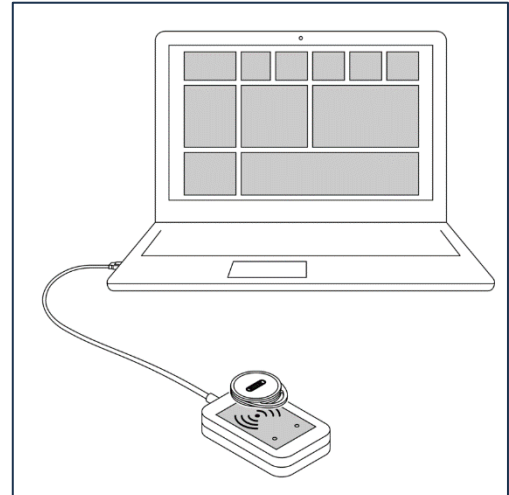
TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

4.1.4. Aufstellen des PC

Der PC wird für das Arbeiten mit der Zutrittskontrollsoftware TECTIQ Access Manager und das Beschreiben der Schließmedien und Systemmedien benötigt. Für den Betrieb der Anlage und das Aktualisieren der Schließmedien ist der PC grundsätzlich nicht erforderlich. Sie benötigen:

- **Netzwerkanschluss**
Der PC kann auch über WLAN mit dem Netzwerk-Router verbunden sein.
- **IT-Administrator-Rechte** zum Installieren der Software.



4.1.5. Tischleser anschließen

- ▶ Schließen Sie den Tischleser an einen freien USB-Anschluss des PC an.

4.1.6. Zutrittskontrollzentrale starten

Voraussetzungen:

- TECTIQ Zutrittskontrollzentrale an Netzwerk und Versorgung angeschlossen.
- Im Netzwerk oder im Router ist ein DHCP-Server oder ein DNS-Server vorhanden.
- TECTIQ Zutrittskontrollzentrale und PC sind im gleichen Netzwerk erreichbar.
- PC an Netzwerk und Versorgung angeschlossen.
- Zutrittskontrollsoftware TECTIQ Access Manager ist auf PC installiert.
- TECTIQ Tischleser ist an PC angeschlossen.

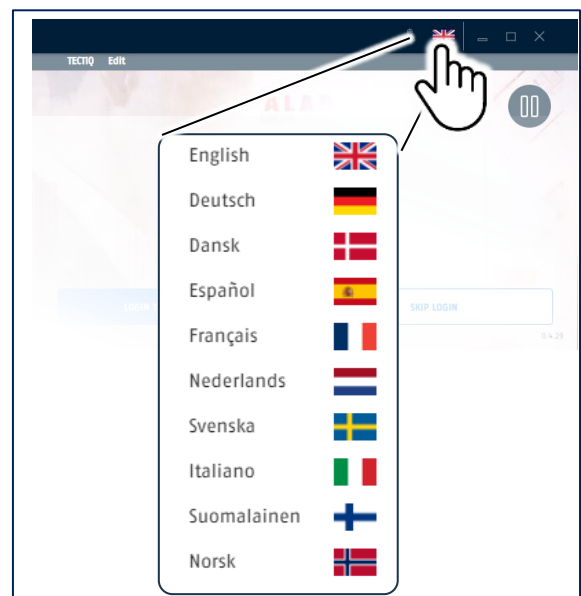
TECTIQ Access Manager starten

- ▶ PC einschalten.
- ▶ TECTIQ Access Manager starten.

Sprache wählen

Wählen Sie die Sprache für die Nutzeroberfläche der Software TECTIQ Access Manager.

- ▶ Klicken Sie auf die Flagge in der Kopfzeile.
- ▶ Wählen Sie in dem Listenfeld die gewünschte Sprache. Die ausgewählte Sprache wird als Flagge in der Kopfzeile angezeigt.

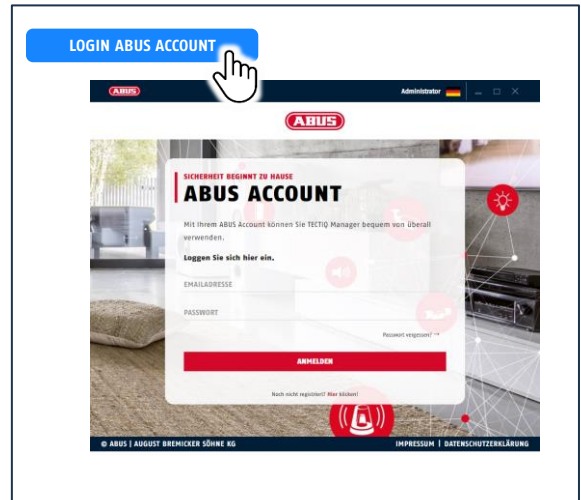


Einloggen mit ABUS Account

Zum Einrichten einer neuen Zutrittskontrollzentrale benötigen Sie einen ABUS Online Account als Fachrichter.

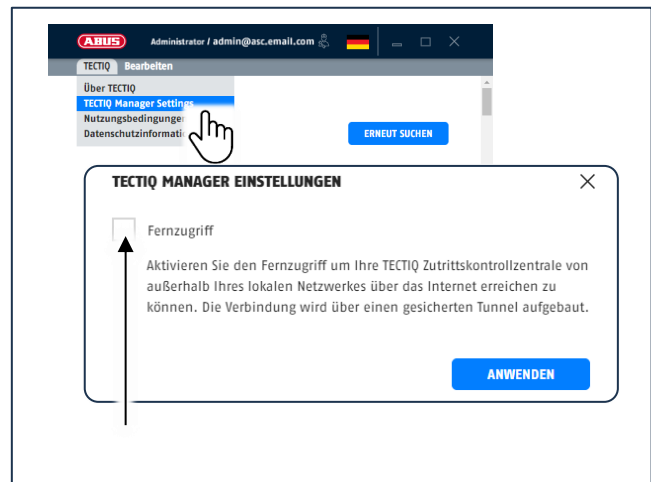
Wenn noch kein ABUS Account vorliegt, registrieren Sie sich und legen Sie einen neuen ABUS Account an. Die Registrierung als Fachrichter ist autorisierten Fachhandelspartnern vorbehalten.

- Anmeldedaten eingeben.
- „Schaltfläche „Anmelden“ betätigen.



Einstellungen für erstmaliges Verbinden

- Menü TECTIQ öffnen.
- TECTIQ Manager Settings öffnen.
- Fernzugriff aktivieren.



TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

Zutrittskontrollzentrale einschalten und verbinden

Im Auslieferungszustand ist die TECTIQ Zutrittskontrollzentrale für den Anschluss über einen Router und die Adressierung über DHCP konfiguriert. In der Regel sollte der Router die Zentrale beim Einschalten finden.

i Stimmen Sie die Adressierung der TECTIQ Geräte im Netzwerk mit dem Administrator der IT-Anlage ab.

- ▶ Versorgung für TECTIQ Zutrittskontrollzentrale einschalten.

Die Zentrale fährt hoch. Dieser Vorgang kann einige Minuten dauern.

Sobald die LED und grün leuchten, ist die Zentrale betriebsbereit und hat Verbindung zum Netzwerk.

Eine gefundene Zutrittskontrollzentrale sollte automatisch auf der Oberfläche erscheinen.

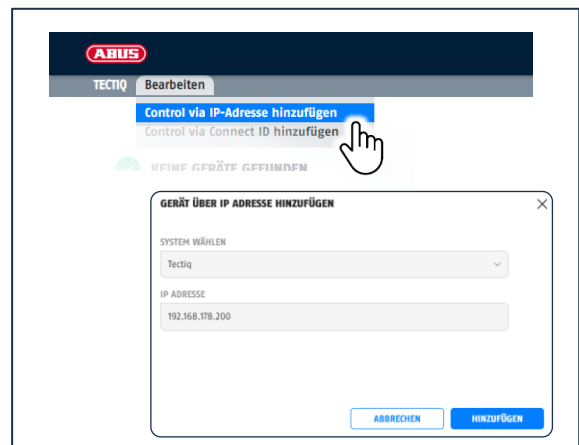
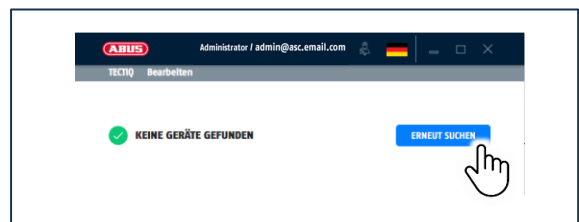
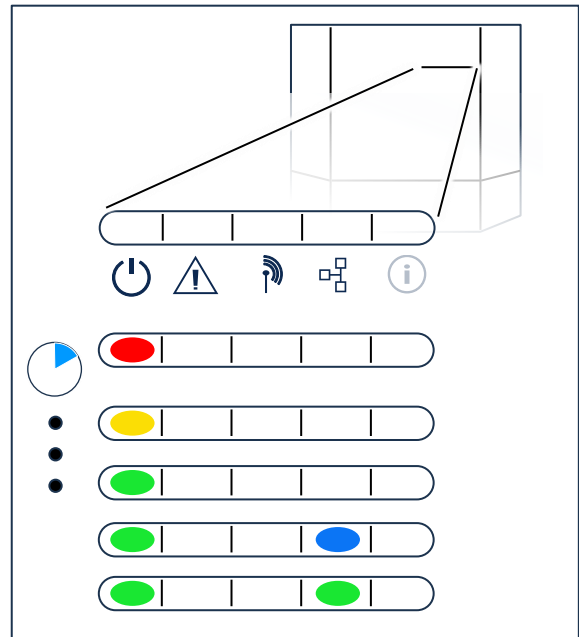
Wenn die Zentrale nicht automatisch auf der Oberfläche erscheint:

- ▶ Schaltfläche „Erneut suchen“ betätigen.

- oder -

Verbinden via IP-Adresse:

- ▶ IP-Adresse im Netzwerk-Router ablesen.
- ▶ Menü „Bearbeiten“ öffnen.
- ▶ „Control via IP-Adresse hinzufügen“ auswählen.
- ▶ Die IP-Adresse der Zentrale eingeben.
- ▶ „Hinzufügen“ anklicken.



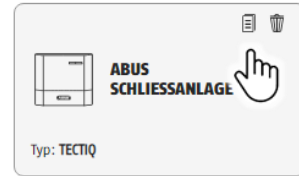
TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

Wenn an einer Zentrale bereits der Vorgang zum erstmaligen Erkennen ausgeführt wurde, verfügt sie über eine Connect ID und kann auch mit dieser hinzugefügt werden. Die Connect ID kann aus einem Access Manager, dem die Zutrittskontrollzentrale bekannt ist, kopiert werden.

Wenn Sie Zugriff auf den Access Manager haben, in dem die Zugriffskontrollzentrale angemeldet ist:

- ▶ Zutrittskontrollzentrale in ursprünglichem Access Manager auswählen.
 - ▶ Symbol neben Papierkorb anklicken.
- Connect-ID wird in Zwischenablage kopiert.



- ▶ Aktuellen Access Manager öffnen.
- ▶ Menü „Bearbeiten“ öffnen.
- ▶ „Control via Connect ID hinzufügen“ auswählen.
- ▶ Die Connect-ID aus Zwischenablage einfügen.
- ▶ „Hinzufügen“ anklicken.



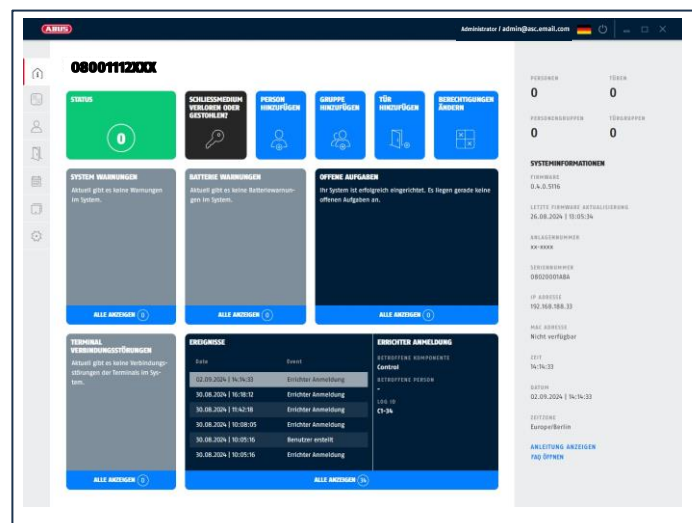
Sie identifizieren die gefundene Zutrittskontrollzentrale anhand ihrer Seriennummer.

Mit gefundener Zentrale verbinden:

- ▶ Mausklick auf die gewünschte Kachel.






Die Zentrale wird in einem neuen Fenster angezeigt.



Datum und Uhrzeit einstellen

Überprüfen Sie die Uhrzeit in der Zutrittskontrollzentrale und aktualisieren Sie bei Bedarf die Einstellungen.

i Die Systemzeit ist für eine zuverlässige Funktion des Zutrittskontrollsystems von zentraler Bedeutung. Ist die Systemzeit nicht richtig eingestellt, ist es möglich, dass kein Zutritt zum gesicherten Bereich gewährt wird.

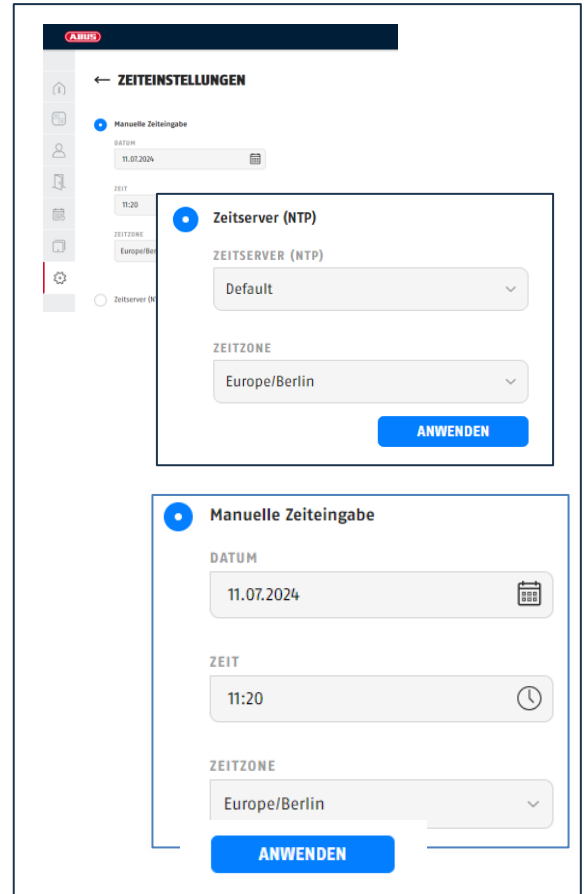
- ▶ Starten Sie den Access Manager und verbinden Sie sich mit der Zutrittskontrollzentrale.
- ▶ Wählen Sie die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Zeiteinstellungen.

i Empfohlen wird die Zeiteinstellung über Zeitserver (NTP)!

- ▶ Wählen Sie „Zeitserver (NTP)“, damit die Anlage Datum und Uhrzeit regelmäßig automatisch synchronisieren kann.
- ▶ Wählen Sie im Feld „Zeitserver (NTP)“ „Default“ oder die Option für eine manuelle Eingabe. Geben Sie im letzten Fall eine Internet-Adresse für einen Zeitserver an – z. B. für die gesetzliche Zeit in Deutschland: ptbtime1.ptb.de
- ▶ Beenden Sie die Eingabe mit „Anwenden“.




- um die Uhrzeit manuelle einzustellen:

- ▶ Wählen Sie „Manuelle Zeiteingabe“
- ▶ Geben Sie aktuelle Werte für „Datum“ und „Zeit“ ein. Geben Sie die dem Anlagenstandort entsprechende Zeitzone an, z. B. für die Zeit in Mitteleuropa „Europe/Berlin“.



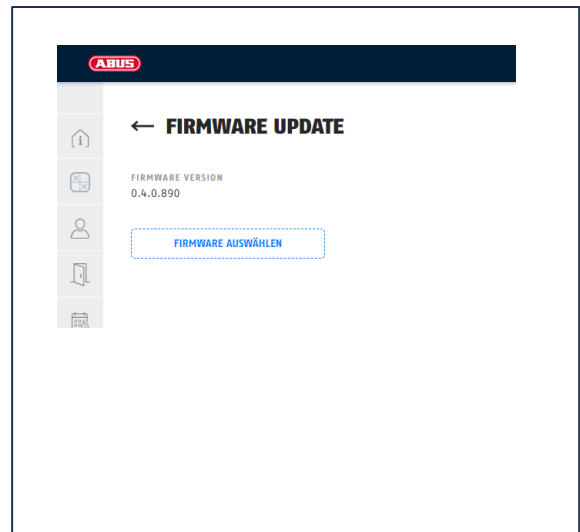
Firmware aktualisieren

Vor dem Arbeiten in der Software stellen Sie sicher, dass die Firmware in der Zutrittskontrollzentrale aktuell ist.

- ▶ Starten Sie den Access Manager und verbinden Sie sich mit der Zutrittskontrollzentrale.
- ▶ Wählen Sie die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Firmware Update.

Die aktuell vorhandene Firmware-Version wird angezeigt.

- ▶ Laden Sie eine aktualisierte Firmware herunter auf die lokale Festplatte.
- ▶ Wählen Sie die Schaltfläche „Firmware Update“ und wählen Sie auf Ihrem lokalen PC die heruntergeladene Software aus.
- ▶ Folgen Sie den weiteren Anweisungen.

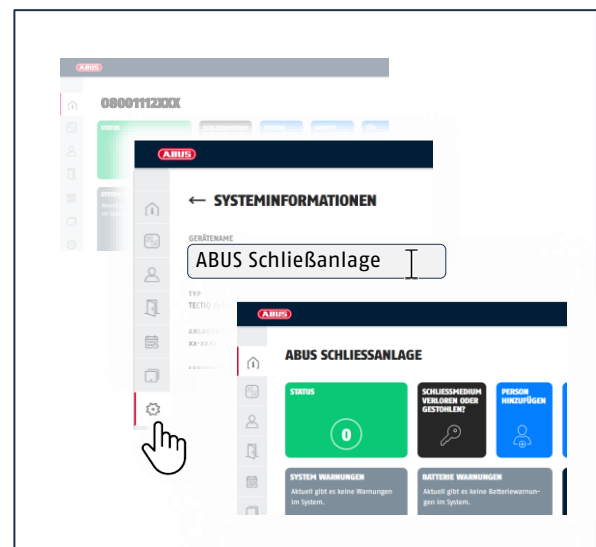


Projektdaten eingeben

Der Anlagenname wird oben im Dashboard angezeigt. In der Werksauslieferung ist hier die Seriennummer der Zutrittskontrollzentrale voreingestellt.

Tragen Sie den mit dem Betreiber abgestimmten Anlagennamen ein.

- ▶ Sicht Systemeinstellungen → Systemkonfiguration → Systeminformationen
- ▶ Gerätenamen eingeben.

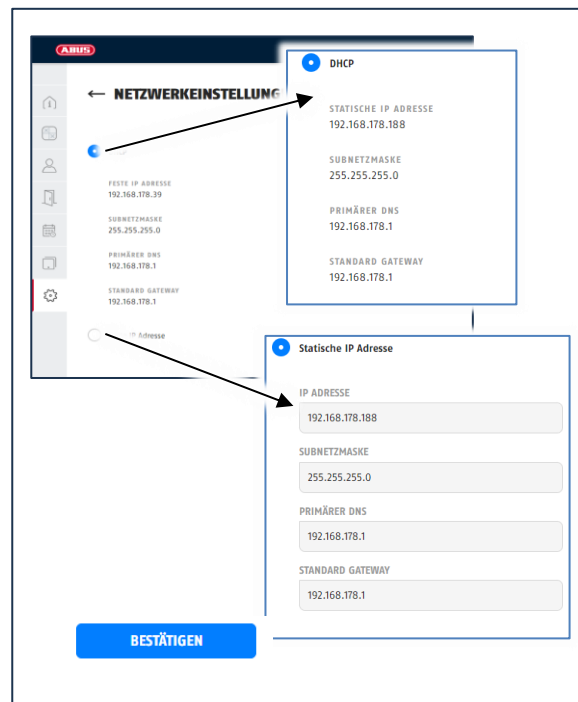


Netzwerkeinstellungen

Wenn Ihre Netzwerkeinstellungen eine feste (statische) IP-Adresse erfordern, konfigurieren Sie den Netzzugang der Zutrittskontrollzentrale.

- ▶ Wählen Sie die Sicht Systemeinstellungen und die Schaltflächen Systemkonfiguration und Netzwerkeinstellungen.
- ▶ Wählen Sie Ihre Einstellungen entsprechend der Netzwerkkonfiguration am endgültigen Einbauort.
- ▶ Wählen Sie „DHCP“ für die automatische Adressvergabe.
- ▶ Wählen Sie „Statische IP Adresse“ für die manuelle Einstellung der Internet-Adresse. Die erforderlichen Daten erhalten Sie vom Netzwerkadministrator.
- ▶ Beenden Sie die Eingabe mit „Bestätigen“.

Nach dem Ändern der Netzwerkeinstellungen startet die Zentrale neu und trennt die Verbindung. Die Verbindung zur Zentrale muss dann neu wiederhergestellt werden.



Falls Sie die Netzwerkeinstellungen versehentlich verstellt und keinen Zugriff auf die Zentrale mehr haben, können Sie die Netzwerkeinstellungen zurücksetzen.

4.1.7. Update Terminal mit Zutrittskontrollzentrale verbinden

Voraussetzungen:

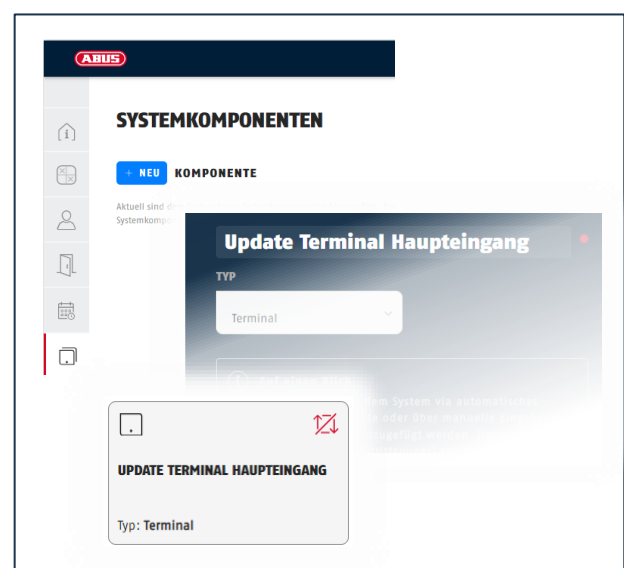
- TECTIQ Zutrittskontrollzentrale angeschlossen und betriebsbereit.
 - Update Terminal an Versorgung und Netzwerk angeschlossen.
 - Update Terminal und Zutrittskontrollzentrale im gleichen Netzwerk erreichbar.
- ▶ Stimmen Sie die Adressierung der TECTIQ Geräte im Netzwerk mit dem Administrator der IT-Anlage ab.

Update Terminal hinzufügen

- ▶ Wählen Sie die Sicht Systemkomponenten .
- ▶ Drücken Sie die Schaltfläche „+ NEU“.
- ▶ Tragen Sie im Editierbereich eine Bezeichnung für das Update Terminal ein.

Das Update Terminal wird als Kachel auf der Oberfläche angezeigt.

- ▶ Wählen Sie Ihre Einstellungen entsprechend der Netzwerkkonfiguration am endgültigen Einbauort.



TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

Mit Update Terminal verbinden

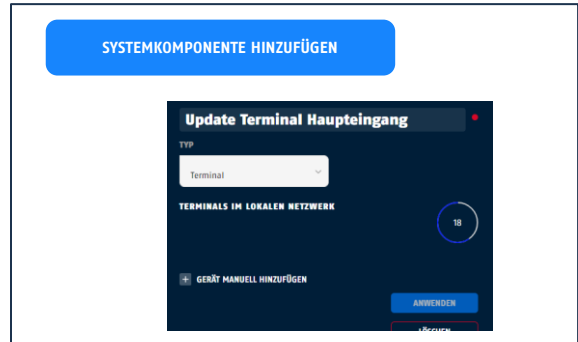
- Klicken Sie mit dem Mauszeiger das gewünschte Update Terminal an.

Update Terminal automatisch hinzufügen:

- Wählen Sie „Systemkomponente hinzufügen“.

Die Zentrale startet einen Suchvorgang im Netzwerk.

Wenn kein Update Terminal gefunden wurde, kann die Suche später erneut gestartet werden („Aktualisieren“).

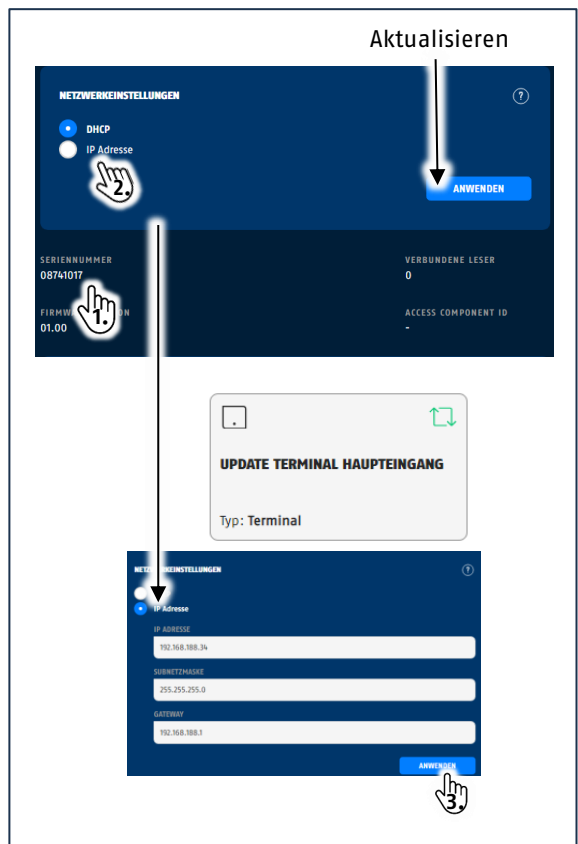


Im Netzwerk gefundene Update Terminals werden mit ihrer Seriennummer angezeigt (1.).

- Betätigen Sie die Schaltfläche „Anwenden“.

Die Zentrale verbindet sich mit dem Terminal.

Das verbundene Update Terminal wird im Arbeitsbereich mit dem Zustand „Grün“ (= „Verbunden“) angezeigt.



Alternativ geben Sie die IP-Adresse für das Update Terminal manuell ein (2.):



- Wählen Sie IP-Adresse.
- Geben Sie die Verbindungsdaten aus Ihrem Router ein.
- Wählen Sie „Anwenden“.

4.1.8. Systemmedien einrichten

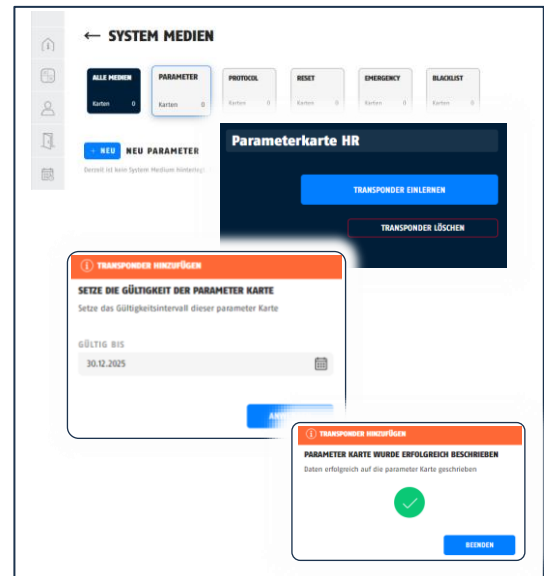
Legen Sie für die Anlage die benötigten Systemmedien an. Sie benötigen hierzu den Tischleser.

- Parameterkarte – erforderlich
- Blacklistkarte – erforderlich
- Notöffnungstransponder – je nach Gebäude möglicherweise erforderlich
- Protokollkarte – optional
- Resetkarte – erforderlich



- ▶ Wählen Sie die Sicht Systemeinstellungen  und Systemmedien .
- ▶ Wählen Sie den zu beschreibenden Medientyp, indem Sie die betreffende Schaltfläche betätigen.
- ▶ Betätigen Sie die Schaltfläche „+ NEU“.
- ▶ Geben Sie eine Bezeichnung für das Systemmedium ein.
- ▶ Geben Sie ein Datum ein, bis zu dem das Medium gültig sein soll.
- ▶ Betätigen Sie die Schaltfläche „Anwenden“.
- ▶ Legen Sie das Medium auf den Tischleser und warten, bis der Schreibvorgang beendet wurde.

Das Systemmedium auf dem Tischleser muss mit dem gewählten Medientyp übereinstimmen.



4.2. Projektierung und Inbetriebnahme

Beim **Projektieren** geben Sie die Anlagendaten – Türen, Türgruppen, Systemgeräte – in den TECTIQ Access Manager ein. Anschließend geben Sie die Personendaten ein und weisen die Zutrittsberechtigungen im Schließplan zu.

Bei der **Inbetriebnahme** der Anlage werden die projektierten Daten in die Türkomponenten geschrieben. Grundsätzlich sind zwei verschiedene Vorgehensweisen sinnvoll, die sich je nach Kunde oder konkreter Anforderung ändern können.

- Bei der Inbetriebnahme vor Ort sind die Türkomponenten bereits beim Kunden installiert und Sie laden die Daten an der Tür in die Türkomponenten ein.
- Bei der Werkstatt-Inbetriebnahme programmieren Sie die Komponenten zuerst, bevor Sie sie anschließend beim Kunden montieren.
Beachten Sie bei diesem Vorgehen, dass Türkomponenten nach dem Programmieren immer ausgekoppelt sind. Ohne funktionierendes Schließmedium oder geeignete andere Maßnahmen können Sie sich aus dem gesicherten Bereich aussperren!

Generell empfiehlt sich für Projektierung und Inbetriebnahme von TECTIQ Zutrittskontrollanlagen die folgende Reihenfolge.

1.	Türen und Türgruppen anlegen.
2.	Türkomponenten den Türen zuordnen.
3.	Türkomponenten programmieren.
4.	Zeitpläne definieren (optional).
5.	Personen und Personengruppen anlegen.
6.	Zutrittsberechtigungen im Schließplan erteilen.
7.	Schließmedien projektieren.
8.	Schließmedien programmieren.
9.	Funktion der Türkomponenten und Schließmedien testen.
10.	Schließmedien an Nutzer ausgeben.
11.	Anlage an Betreiber übergeben.

TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

4.2.1. Türen und Türgruppen projektieren

Geben Sie die geplanten Türen und Türgruppen in den Access Manager ein.

Sie können hierfür zwei Wege benutzen:

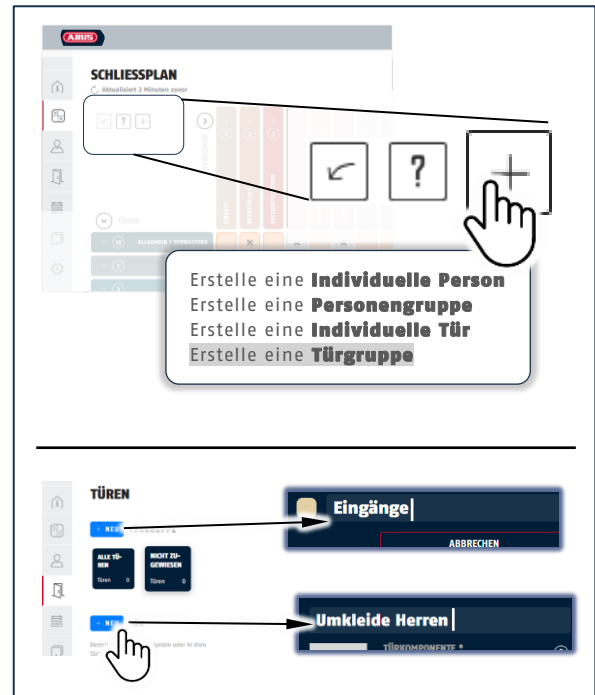
In der Sicht Schließplan:

- ▶ Betätigen Sie die Schnelltaste und wählen Sie im Listenfeld den Befehl „Erstelle eine Türgruppe [individuelle Tür]“.
- ▶ Tragen Sie die Bezeichnung für die Tür bzw. Türgruppe ein.

In der Sicht Türen:

- ▶ Betätigen Sie eine der beiden Schaltflächen „+ NEU“.
- ▶ Tragen Sie die Bezeichnung für die Tür bzw. Türgruppe ein.

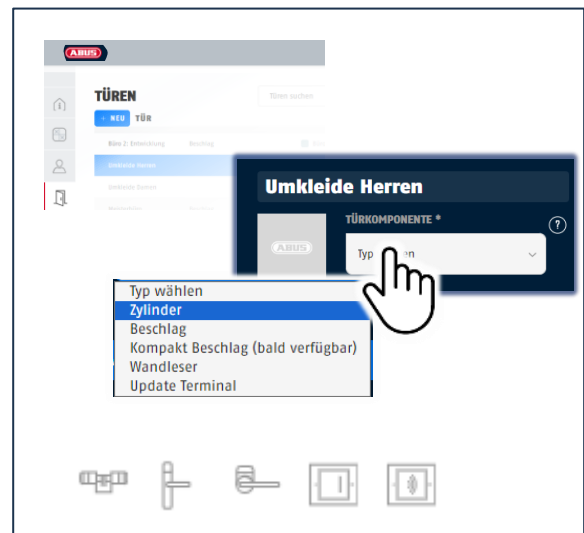
In der Sicht Türen können Sie anschließend fortfahren mit dem Auswählen der Türkomponenten (Zylinder, Beschlag oder Wandler).



4.2.2. Türkomponenten zuordnen und einstellen

Ordnen Sie den Türen die richtige Türkomponente zu.

- ▶ Wählen Sie die Sicht Türen.
- ▶ Wählen Sie aus der Türliste die gewünschte Tür aus. Bei großen Listen können Sie die Türliste einschränken, indem Sie die passende Türgruppe vorwählen.
- ▶ Klicken Sie auf das Listenfeld „Türkomponenten“.
- ▶ Wählen Sie die gewünschte Türkomponente aus – Zylinder, Beschlag, Wandler oder Update Terminal. Wenn ein Update Terminal zusätzlich eine Tür ansteuert, projektieren Sie es als Systemgerät und zusätzlich als Türkomponente.

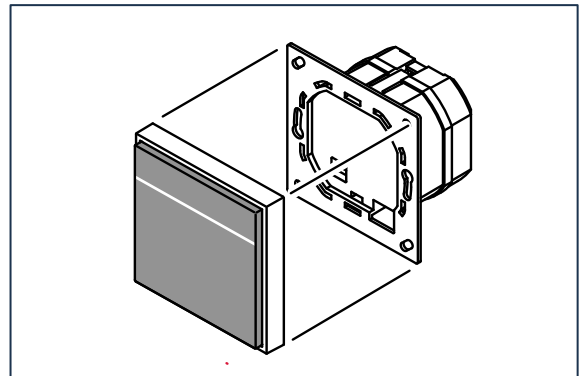


Stellen Sie die korrekten Betriebsparameter für die Türkomponenten ein. Tragen Sie bei Bedarf weitere Informationen für die Türen ein.

Update Terminal als Türkomponente / Wandleser

Wählen Sie die Charakteristik für die Relaiskonfiguration entsprechend dem Aktor an der angesteuerten Tür.

Beachten Sie hierbei die Stromstärke, die beim Öffnen fließt. Bauteile wie Türöffner dürfen möglicherweise nur für eine bestimmte Einschaltdauer (ED) bestromt werden. Motorische Türantriebe oder elektronische Türansteuerungen haben in der Regel hochohmige Eingänge, die dauerhaft bestromt werden dürfen.



- ▶ Stimmen Sie die Einstellungen mit dem Einsatzzweck ab, insbesondere auch für Türen, die dauerhaft geöffnet werden.

Für Türöffner oder einfache Türantriebe:

- Schließer-Impuls: „NO impulse“

Für Türöffner oder Türantriebe mit Ruhestromüberwachung:

- Öffner-Impuls: „NC impulse“

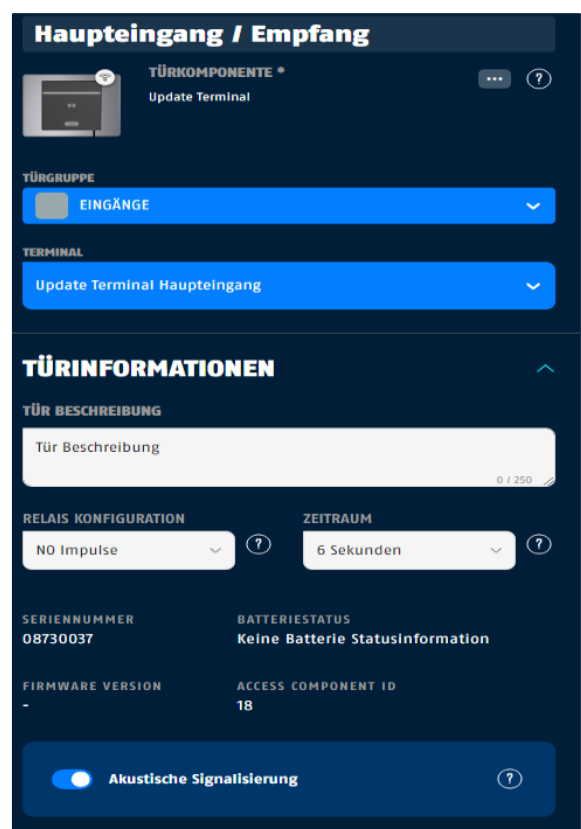
Für Drehkreuze, Eingangsbereiche

- Schließer-Impuls: „NO impulse“

Türantrieb mit Ruhestromüberwachung:

- Schließer-Impuls: „NO impulse“

- ▶ Stellen Sie unter Zeitraum die Freigabedauer für das Relais ein.
- ▶ Wählen Sie aus, ob ein akustisches Signal beim Präsentieren eines Mediums am Wandleser ertönt.



TECTIQ In Kürze.

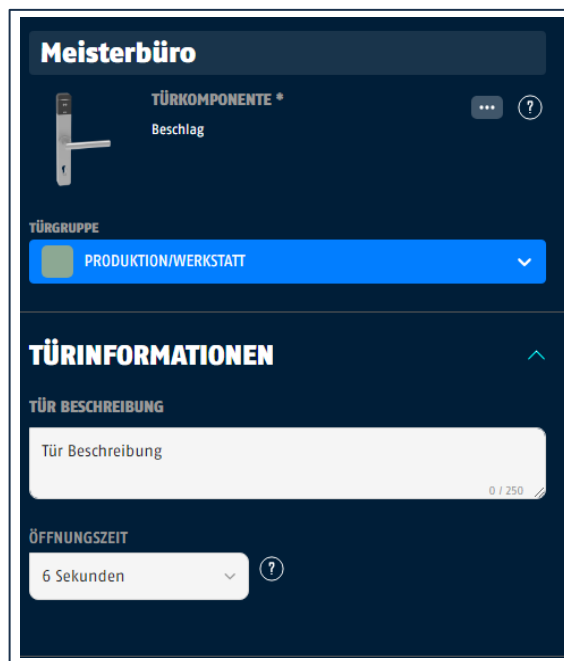
4 TECTIQ – Für Fachrichter

Beschlag

- Vergeben Sie einen Namen für die Türkomponente.
- Ordnen Sie die Tür einer Türgruppe zu.
- Stellen Sie unter Öffnungszeit die Freigabedauer der Tür ein.

Bei Lieferung ist der elektronische Beschlag eingekoppelt, d.h. für die Montage ist der Zutritt von beiden Seiten gewährleistet.

- ❗ Nach der Programmierung befindet sich der Beschlag im ausgekoppelten Zustand. Der Zutritt ist dann von dieser Seite gesperrt.
 - Wenn Sie den Beschlag vorab programmieren und anschließend montieren, stellen Sie sicher, dass Sie sich nicht aussperren.
 - Halten Sie die Tür geöffnet oder verteilen Sie zeitnah gültige Schließmedien.

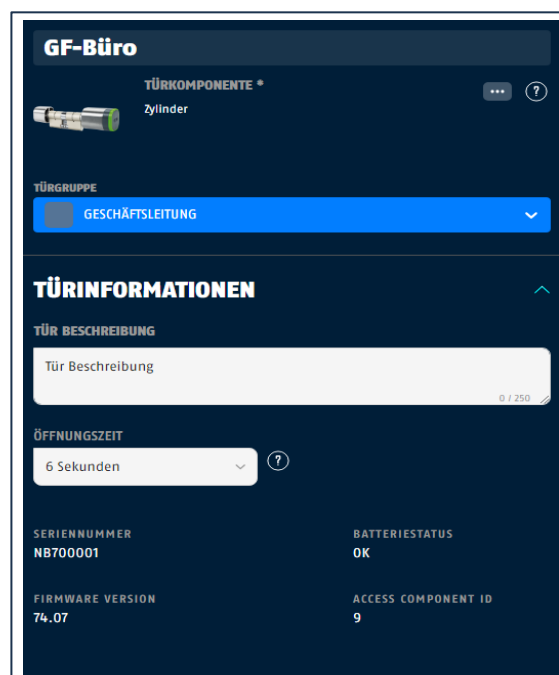


Zylinder

- Vergeben Sie einen Namen für die Türkomponente.
- Ordnen Sie die Tür einer Türgruppe zu.
- Stellen Sie unter Öffnungszeit die Freigabedauer der Tür ein.

Bei Lieferung ist der elektronische Schließzylinder eingekoppelt, d.h. für die Montage ist der Zutritt von beiden Seiten gewährleistet.

- ❗ Nach der Programmierung befindet sich der Lesekopf im ausgekoppelten Zustand. Der Zutritt ist dann von dieser Seite gesperrt.
 - Wenn Sie den Schließzylinder vorab programmieren und anschließend montieren, stellen Sie sicher, dass Sie sich nicht aussperren.
 - Halten Sie die Tür geöffnet oder verteilen Sie zeitnah gültige Schließmedien.



4.2.3. Türkomponenten programmieren

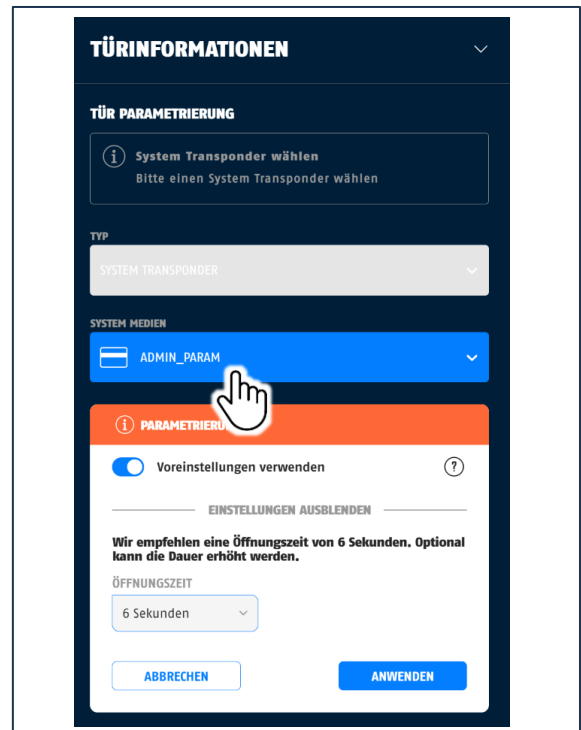
Die Programmierung der Türkomponente erfolgt nach der Zuordnung und Einstellung der Türkomponente im Editierbereich der Türkomponente oder später in der Aufgabenliste.

Um eine Türkomponente zu programmieren benötigen Sie den TECTIQ Access Manager, das TECTIQ Lesegerät und eine Parameterkarte (Systemmedium). Beachten Sie: Die Parameterkarte kann nach der Programmierung nur 15 min zur Parametrisierung der Türkomponente verwendet werden.

Wählen Sie eine Parameterkarte aus.

- Wählen Sie den Button „Anwenden“
- Legen Sie die ausgewählte Parameterkarte auf das Tischlesegerät und warten Sie, bis die grüne LED leuchtet.
- Präsentieren Sie innerhalb von 15 min die Parameterkarte an der Türkomponente. Warten Sie, bis die LED an der Türkomponente grün leuchtet.

Beachten Sie: Der Vorgang ist erst abgeschlossen, wenn Sie die Parameterkarte erneut am Tischleser präsentieren und die LED am Tischleser grün leuchtet.



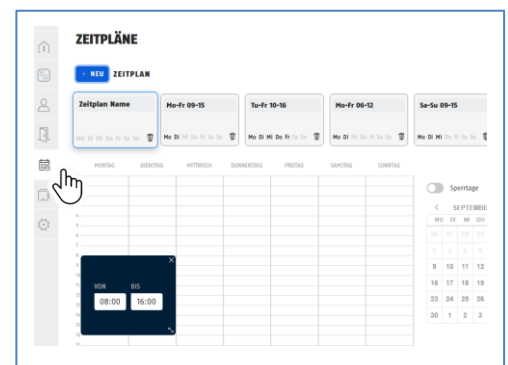
4.2.4. Zeitpläne definieren

Zeitpläne dienen dazu, Zutrittsberechtigungen zeitlich einzuschränken. Zeitpläne können für einzelne Personen oder für ganze Personengruppen verwendet werden. Um beim Anlegen von Personen auf Zeitpläne zuzugreifen, müssen sie vorher definiert sein. Die Anlage von Zeitplänen ist optional.

- Sie erstellen einen neuen Zeitplan in der Sicht Zeitpläne.
- Im Referenzhandbuch Kap. 11 erfahren Sie alles über die Anlage und Bearbeitung von Zeitplänen.

In der TECTIQ Zutrittskontrollanlage können bis zu 300 Zeitpläne mit jeweils bis zu 15 Zeitintervallen gespeichert werden.

Pro Person ist immer nur ein Zeitplan gültig. Bei der erstmaligen Anlage erbt der neue Nutzer den Zeitplan der Personengruppe, der er zugeordnet ist. Der Zeitplan kann individuell angepasst oder ein neuer individueller Zeitplan erstellt werden.



TECTIQ In Kürze.

4 TECTIQ – Für Fachrichter

4.2.5. Personengruppen und Personen anlegen

Zur einfachen Verwaltung von Berechtigungen legen Sie Personengruppen an. Einer Personengruppe können gesammelt Zutrittsrechte erteilt oder entzogen werden, Zeitpläne können vorgegeben werden und anderes mehr.

Eine Person kann maximal einer Personengruppe zugewiesen sein.

- ▶ Öffnen Sie die Sicht Personen.
- ▶ Betätigen Sie im oberen Teil des Fensters „Personen“ die Schaltfläche „+ NEU“ (1).
- ▶ Tragen Sie im Editierbereich eine Bezeichnung für die Gruppe (2) ein.
- Sobald das Programm eine Bezeichnung erkennt, wird für die neue Gruppe eine Kachel (3) erzeugt und der Name angezeigt.

Wenn zutreffend:

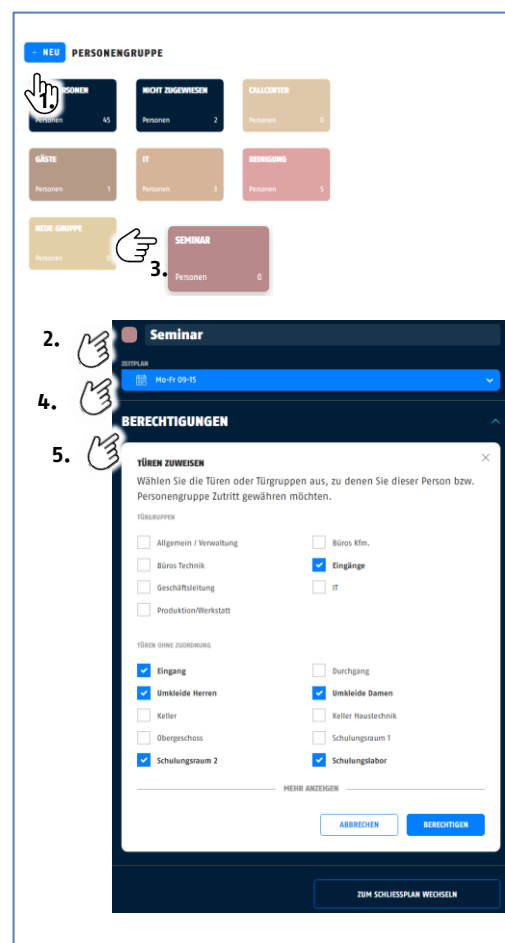
- ▶ Wählen Sie für die neue Gruppe einen Zeitplan (4).
- ▶ Wählen Sie für die Personengruppe Zutrittsberechtigungen für Türen oder Türgruppen aus (5).

Gruppenberechtigungen werden für alle Personen, die der Gruppe angehören, vererbt.

Gruppenberechtigungen können in der Sicht Personen oder in der Sicht Schließplan erteilt werden.

Es ist nicht möglich, für eine Personengruppe ein Schließmedium zu erzeugen und zu programmieren. Schließmedien können nur Personen zugewiesen werden.

Weitere Informationen zu Bearbeitung von Personengruppen finden Sie im Kapitel 3 und im Referenzhandbuch.



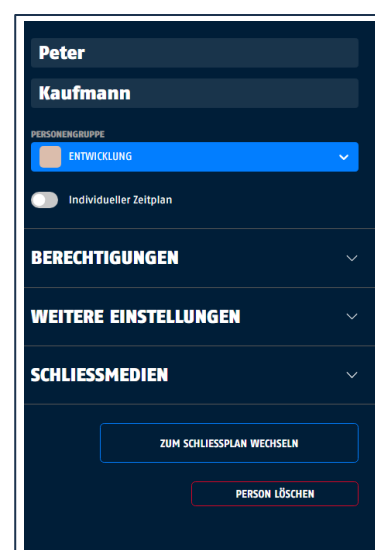
Person der Personengruppe hinzufügen

Bleiben Sie in der Sicht Personen.

- ▶ Betätigen Sie über der Personenliste die Schaltfläche „+ NEU“.
- ▶ Tragen Sie die Personendaten ein.

Nach Eingabe des Namens im Bearbeitungsbereich und Auswahl der Personengruppe werden dem neuen Nutzer alle Zugangsberechtigungen der ausgewählten Personengruppe automatisch zugeordnet.

Der Editierbereich bietet Ihnen erweiterte Einstellungsmöglichkeiten.



4.2.6. Zutrittsberechtigungen vergeben

In der Sicht Schließplan ordnen Sie Personengruppen und Personen die Berechtigung für Türgruppen und Türen in einer graphischen Übersicht zu.

- ▶ Weisen Sie Personengruppen und Personen die gewünschten Berechtigungen zu Türen oder Türgruppen im Schließplan zu, indem Sie an der passenden Stelle ein **x** setzen.
- ▶ Erteilen Sie zunächst Berechtigungen auf Gruppenebene.
- ▶ Fügen Sie individuelle Zutrittsberechtigungen durch setzen eines **x** hinzu oder entfernen sie Berechtigungen, indem Sie an der entsprechenden Stelle das **x** löschen.

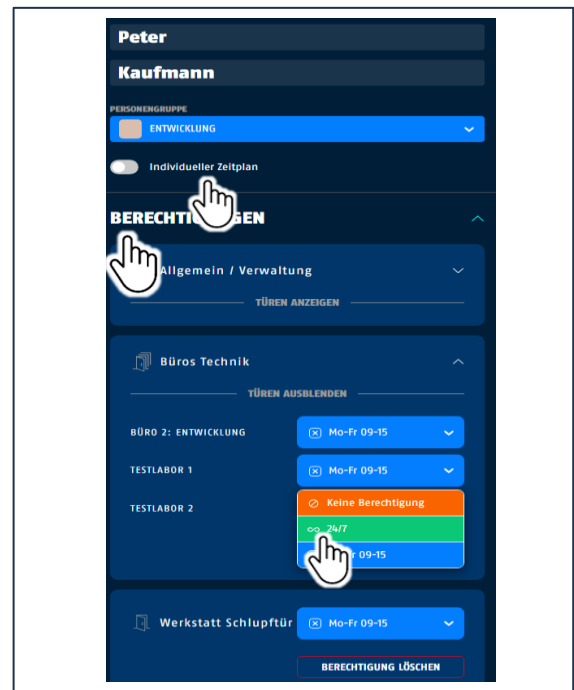


In der Sicht Personen ordnen Sie Personengruppen oder Personen einen Zeitplan zu. Der Zeitplan einer Personengruppe wird bei der Aufnahme einer Person in die Personengruppe voreingestellt. Er wird durch die Auswahl eines individuellen Zeitplans ersetzt.

Statt eines Zeitplans kann unter Berechtigungen für jede Tür die Einstellung „keine Berechtigung“ oder „24/7“ für eine durchgängige Berechtigung gewählt werden.

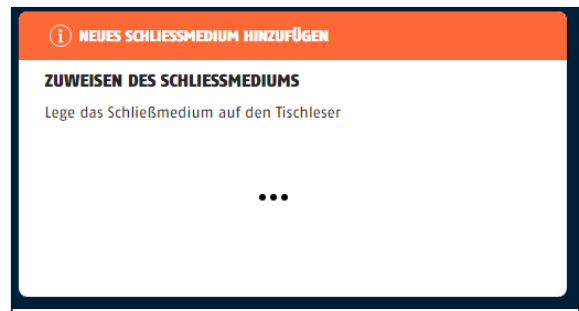
- ▶ Legen Sie unter weitere Einstellungen die Gültigkeit der Zugriffsberechtigung fest.

Beachten Sie: Schließberechtigungen und Zeitpläne müssen auf ein gültiges Schließmedium übertragen werden, bevor sie wirksam werden.



4.2.7. Schließmedien programmieren

- ▶ Setzen Sie die Gültigkeit des Schließmediums. Voreingestellt ist die Gültigkeit aus der Systemkonfiguration.
- ▶ Weisen Sie das Schließmedium einer Person zu.
- ▶ Präsentieren Sie das Schließmedium am Lesegerät.



Nach erfolgreicher Programmierung meldet das System „Schliessmedium zugewiesen“.

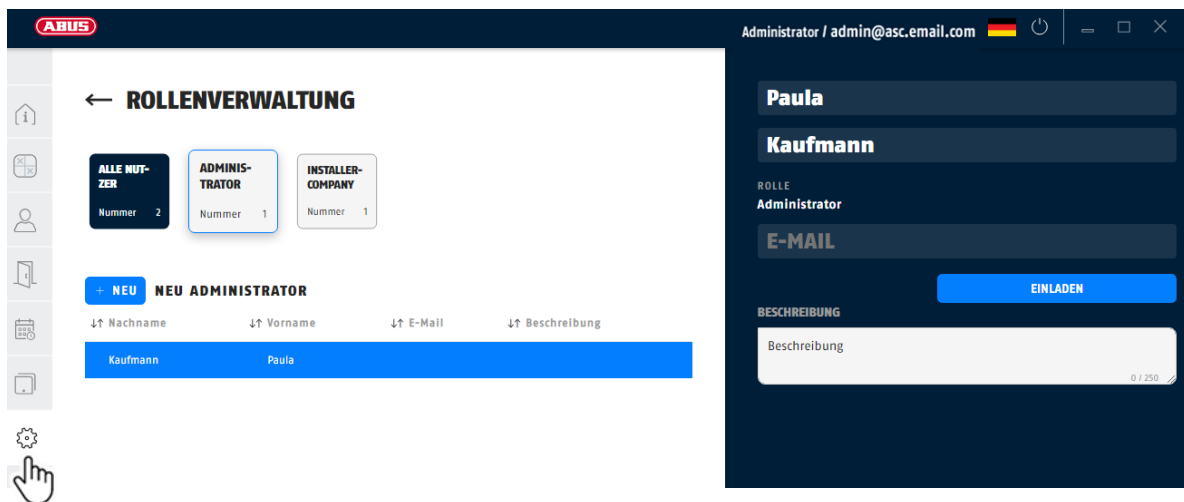
- ▶ Schließen Sie den Vorgang ab.

4.3. TECTIQ Schließmedien ausgeben

- ▶ Nach der Programmierung steht unter dem Menüpunkt „Mehr Informationen“ eine Empfangsquittung mit allen relevanten Daten des Schließmediums zum Ausdruck zur Verfügung. Siehe Muster im Anhang.
- ▶ Händigen Sie die für den Betreiber angelegten Schließmedien an den Betreiber aus.
- ▶ Informieren Sie den Betreiber, dass Empfangsquittungen für die Schließmedien im System verfügbar sind.

4.4. TECTIQ System an den Betreiber übergeben

- ▶ Wählen sie in den Systemeinstellungen die Rollenverwaltung aus.



- ▶ Legen Sie den Betreiber oder seinen Bevollmächtigten als Administrator an oder vervollständigen Sie die Daten.
- ▶ Legen Sie einen ABUS Online Account für den Betreiber ein.
- ▶ Loggen Sie sich mit den Daten des Betreibers ein.
- ▶ Vervollständigen Sie unter Installer Company die Daten Ihres Unternehmens.
- ▶ Falls der Kunde es wünscht, deaktivieren Sie Ihren Zugriff (optional).

ABUS TECTIQ

TECTIQ Referenzhandbuch.

5. Das System

Inhalt

- 5.1. Bestimmungsgemäße Verwendung
- 5.2. Komponenten
 - 5.2.1. TECTIQ Zutrittskontrollzentrale
 - 5.2.2. TECTIQ Access Manager
 - 5.2.3. TECTIQ Tischleser
 - 5.2.4. TECTIQ Online Update Terminal
 - 5.2.5. TECTIQ Offline Türkomponenten
 - 5.2.6. TECTIQ Schließmedien
 - 5.2.7. TECTIQ Systemmedien
 - 5.2.8. Admin App
- 5.3. Systemaufbau
- 5.4. Technische Daten
- 5.5. Wo sind welche Daten gespeichert?

5.1. Bestimmungsgemäße Verwendung

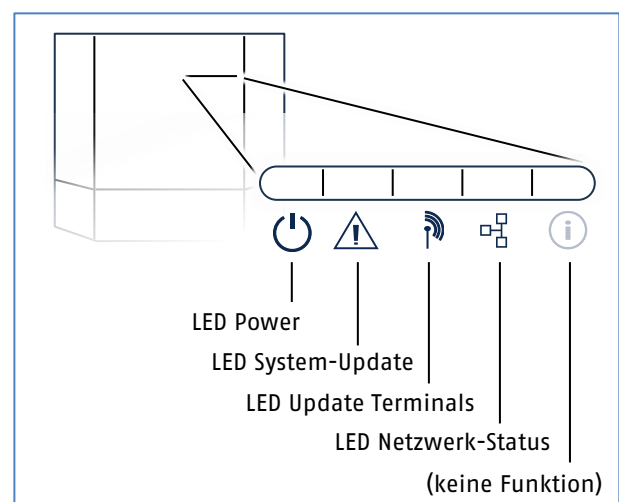
- Schließmediengesteuerte Zutrittskontrolle für private und öffentliche Gebäude
- Verwaltung und Ansteuerung elektronischer Türkomponenten wie Türbeschläge, Türzylinder und Wandleser-Terminals für elektrische Türöffner, Türantriebe, Drehkreuze in Eingangsbereichen und andere – für Gebäudetüren im Innen- und Außenbereich
- Verwalten von Zutrittsberechtigungen

Nicht bestimmungsgemäße Verwendung, nicht ausdrücklich von ABUS zugelassene Reparaturarbeiten oder Modifikationen sowie nicht fachgemäßer Service können zu Funktionsstörungen führen und führen zu Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.

5.2. Komponenten

5.2.1. TECTIQ Zutrittskontrollzentrale

Die TECTIQ Zutrittskontrollzentrale steuert das System. Sie ist in einem geschützten Raum, z. B. im Büro des verantwortlichen Managers oder in einem separaten Technikraum, untergebracht und speichert alle Systemdaten über alle Standorte, die zu steuernden Türen, die Nutzer der Anlage und deren Zutrittsrechte. Die Zutrittskontrollzentrale wird mit Hilfe eines externen Computers – z. B. PC oder Notebook – und der Zutrittskontrollsoftware TECTIQ Access Manager konfiguriert. Die Zutrittskontrollzentrale ist in das lokale Netzwerk eingebunden.

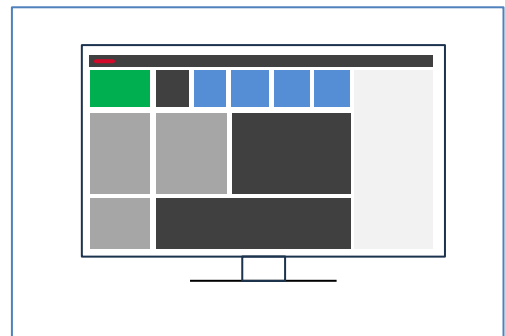


Der aktuelle Status der Zutrittskontrollzentrale wird mit Hilfe von Status-LEDs angezeigt:

	LED Power	rot	Systemstart wird vorbereitet
		gelb	System fährt hoch
		grün	System bereit
	LED System-Update	blau	Systemsoftware wird aktualisiert
	LED Update Terminals	grün	Verbindung zu allen Update Terminals OK
		gelb	Verbindung zu mindestens einem Update Terminal gestört
	LED Netzwerk-Status	grün	Online-Verbindung zum Internet
		blau	Verbindung zum lokalen Netzwerk-Router
		aus	Keine Netzwerkverbindung

5.2.2. TECTIQ Access Manager

Der TECTIQ Access Manager ist die Konfigurationssoftware für das System und läuft auf einem Standard-PC. Die TECTIQ Zutrittskontrollzentrale stellt ihre Daten über Netzwerk der Schließsoftware TECTIQ Access Manager zur Verfügung. Mit einer Internet-Verbindung und der Einstellung Fernzugriff kann die TECTIQ Zutrittskontrollzentrale auch von einem entfernten Standort aus bedient werden.



Anforderungen PC / Netzwerk

Prozessor	min. 2,0 GHz
Arbeitsspeicher	min. 2 GB
Speicherplatz	min. 2 GB
Bildschirmauflösung	min. 1440 × 1080
Netzwerkanschluss	Ethernet 10/100/1000 (opt. WLAN)
Schnittstellen	3×USB (für Tischleser, Maus und Tastatur)
Betriebssystem	Microsoft Windows 10, Windows 11 (64-Bit-Versionen)
Internet-/Netzwerk Router	ja



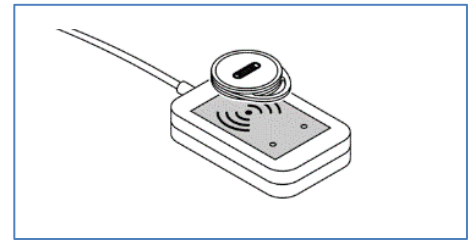
HINWEIS

Computersysteme können ausgespäht und sabotiert werden! Unbefugte können Zutrittsberechtigungen manipulieren und Ihr Eigentum bedrohen.

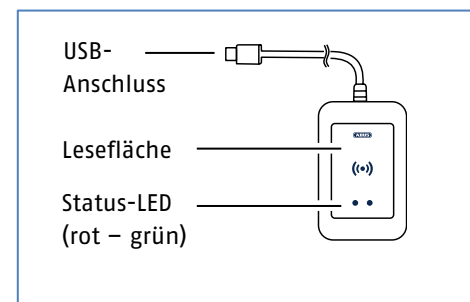
- Verwenden Sie kein Betriebssystem, welches nicht mehr vom Hersteller aktualisiert wird.
- Ersetzen Sie abgekündigte Betriebssysteme so bald wie möglich durch ein aktuelles Betriebssystem.
- Nutzen Sie ein Virenschutzprogramm und installieren Sie die aktuellen Updates.
- Informieren Sie sich über Warnungen und Sicherheitsmaßnahmen und befolgen Sie diese.
- Nutzen Sie den PC nur mit zuverlässiger Software.
- Zuverlässige Informationen über Sicherheitsrisiken und Maßnahmen erhalten Sie z. B. vom Bundesamt für Sicherheit in der Informationstechnik – [bsi.bund.de](https://www.bsi.bund.de).

5.2.3. TECTIQ Tischleser

Der TECTIQ Tischleser dient zum Lesen und Beschreiben von Schließmedien und Systemmedien. Sie benötigen den Tischleser zur Inbetriebnahme des Systems, bei Änderungen und zum Erteilen von Zugriffsrechten. Er wird an den Computer angeschlossen, auf dem die Schließsoftware TECTIQ Access Manager läuft. Über zwei Status-LEDs zeigt der TECTIQ Tischleser seinen Betriebszustand sowie den Status aktueller Vorgänge an.



Die zu beschreibenden Medien werden vom TECTIQ Access Manager angefordert. In diesem Fall präsentieren Sie bitte das betreffende Schließ- oder Systemmedium solange auf der Lesefläche des Tischlesers, bis das Ende des Vorgangs signalisiert wird.



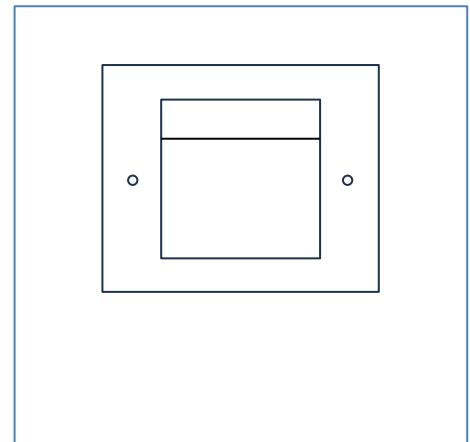
5.2.4. TECTIQ Online Update Terminal

Das TECTIQ Online Update Terminal steht über Netzwerk mit der Zutrittskontrollzentrale in Verbindung. Die Verbindung ist verschlüsselt und damit sicher gegen Abhören oder sonstige Manipulation.

Das TECTIQ Online Update Terminal besteht aus einem Wandlerleser, kombiniert mit dem zugehörigen Steuergerät. Es dient zum

- Lesen und Beschreiben von Schließmedien und Systemmedien,
- Aktualisieren von Zutrittsrechten und
- Weiterleiten von Informationen, Ereignissen und Rückmeldungen der Offline Türkomponenten (erfolgte Zutritte, Batteriewarnungen etc.).

Zusätzlich kann das Online Update Terminal einen Türöffner oder eine Türsteuerung ansteuern. Hiermit ist es z. B. möglich, dass bei erstmaligem Zutritt zum gesicherten Bereich bei Arbeitsbeginn gleichzeitig die Zutrittsberechtigungen auf dem persönlichen Schließmedium aktualisiert werden.



HINWEIS Datenbanksynchronisation zwischen Terminal und Zutrittskontrollzentrale.

- Beim initialen Aufsetzen der Anlage wird eine Datensynchronisation zwischen den Update Terminals und der Zutrittskontrollzentrale durchgeführt. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.
- Nach einem längeren Verbindungsausfall, einem Firmware-Update und bei substantiellen Berechtigungsänderungen im System kann es notwendig sein, dass die Datenbank unter Laufzeit synchronisiert werden muss. Während dieser Datenbanksynchronisation ist ein Zutritt am Update Terminal als Türkomponente vorübergehend nicht möglich.

5.2.5. TECTIQ Offline Türkomponenten

Offline Türkomponenten ermöglichen dem berechtigten Nutzer den Zutritt zum gesicherten Bereich. Sie geben je nach Funktion den Zutritt frei, steuern einen Türöffner oder schalten einen Türantrieb ein. Darüber hinaus speichern sie Ereignisse und Daten die zur Zutrittskontrolle benötigt werden.

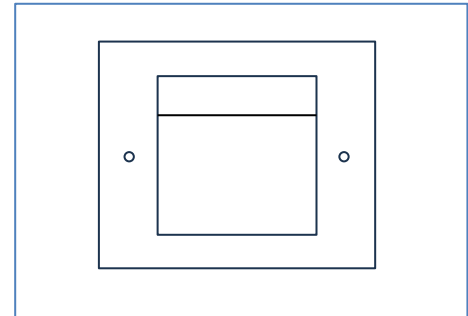
Wandleser

Mit Wandleser werden Aktoren zum Betätigen von

- elektrischen Türöffnern, Schranken oder Toren oder
- motorisch angetriebene Türen, z. B. für Drehtüren, Schiebetüren, Karuselltüren, Drehkreuze

nach Kontrolle der Zutrittsberechtigung angesteuert.

Über eine LED-Anzeige wird der Freigabestatus signalisiert, zusätzlich kann ein akustisches Signal, das bei Betätigung ertönt, eingestellt werden.

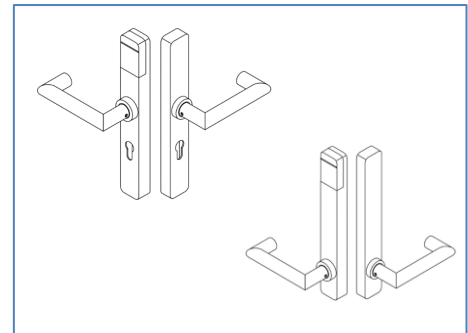


Elektronischer Beschlag

Elektronischen Beschläge geben nach der Kontrolle der Zutrittsberechtigung die Bedienung der Drücker frei. Sie sind in verschiedenen Ausführungen verfügbar.

Elektronische Beschläge können in Kombination mit einem Schließzylinder (Euro-, Rund- oder Ovalprofil) betrieben werden, wobei die Funktion der elektronischen Zutrittskontrolle mechanisch übersteuert wird.

Über eine LED-Anzeige wird der Freigabestatus signalisiert.



Elektronischer Schließzylinder

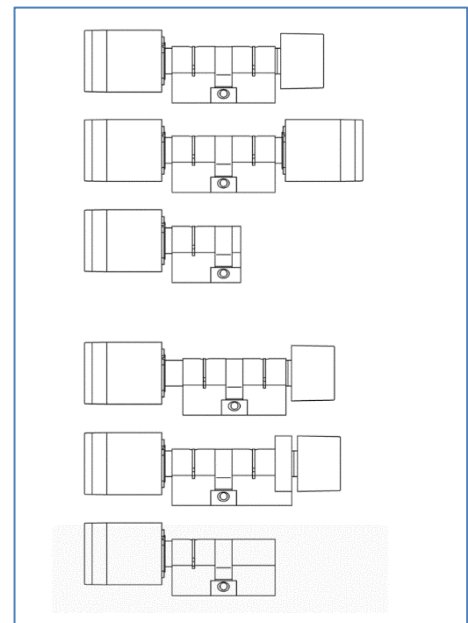
Elektronischen Schließzylinder koppeln nach der Kontrolle der Zutrittsberechtigung die Schließfunktion ein. Hierdurch kann der Zutrittsberechtigte die Tür Öffnen und Verriegeln.

Elektronische Schließzylinder sind in verschiedenen Ausführungen verfügbar.

- Euro-Profilzylinder
- Schweizer Rundprofil
- Skandinavischer Oval-Zylinder und Rokoko-Zylinder

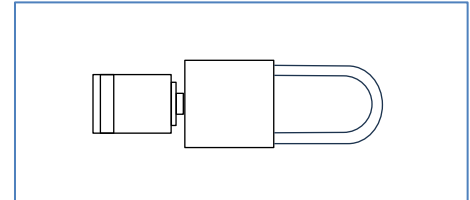
Mit den elektronischen Schließzylindern ist eine einseitige oder doppelseitige Zutrittskontrolle möglich.

Über eine LED-Anzeige wird der Freigabestatus signalisiert.



Elektronisches Vorhangschloss

- Für Schaltschränke, Maschinenbereiche, Depots, Garagen, EMV-Außenplätze, Grillhütten, Schuppen, Fahrradketten u.v.a.m.
- Projektieren und in Betrieb nehmen wie einen elektronischen Zylinder.



5.2.6. TECTIQ Schließmedien

TECTIQ Schließmedien sind kontaktlose Transpondersysteme mit dem besonders sicheren MIFARE® DESFIRE® System. Schließmedien sind in unterschiedlichen Formen verfügbar, z. B. als Schlüsselanhänger oder als Transponderkarte.

Der Nutzer präsentiert sein Schließmedium an der Türkomponente oder dem Terminal. Bei entsprechender Berechtigung kann der Nutzer einen Bereich auch dauerhaft öffnen. Dieser Modus eignet sich besonders z. B. für Ladengeschäfte oder andere Gebäude mit Öffnungszeiten für Kunden oder Publikum.

TECTIQ Schließmedien übernehmen bei der Nutzung einer Türkomponente Informationen zum Batteriestatus und andere Ereignisse auf und übertragen diese beim nächsten Aktualisierungsvorgang am TECTIQ Update Terminal an die TECTIQ Zutrittskontrollzentrale zurück. Hiermit ist sichergestellt, dass die Zutrittskontrollanlage zu allen Türkomponenten aktuell gehalten wird.



5.2.7. TECTIQ Systemmedien

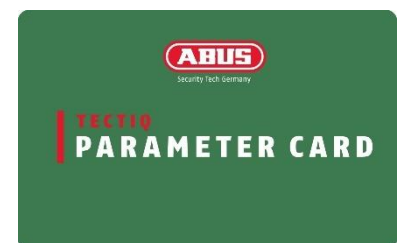
TECTIQ Systemmedien werden für die Systembetreuung und -instandhaltung eingesetzt. Sie werden u.a. für Einrichtungsvorgänge, zur Verhinderung unbefugter Zutritte und zum Einlernen oder Auslernen von Türkomponenten genutzt. Sie sollen an einem sicheren Ort verwahrt werden und nur von wenigen, autorisierten Personen genutzt werden.

Parameterkarte

Die Parameterkarte speichert Konfigurationsdaten und transportiert diese zu der Türkomponente vor Ort. Sowohl bei der Erstprogrammierung als auch bei Änderungen wird die Parameterkarte mit dem Tischleser beschrieben und vor Ort von der jeweiligen Komponente ausgelesen.

Die Parameterkarte dient auch zur Übertragung der aktuellen Zeit (Datum und Uhrzeit) auf die Türkomponente.

- ▶ Präsentieren Sie hierzu die Parameterkarte an den Tischleser oder an ein Update Terminal, wenn keine aktive Programmieraufgabe zugewiesen ist.
- ▶ Präsentieren Sie die Parameterkarte im Anschluss an der Türkomponente.



Die Parameterkarte ist maximal 15 Minuten nach Beschreiben gültig.

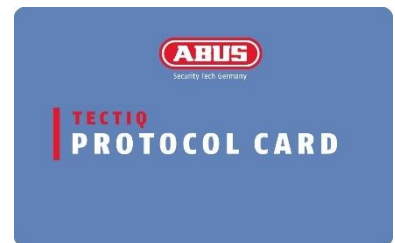
Resetkarte

Die Resetkarte dient dem Rücksetzen von Türkomponenten, um sie aus dem TECTIQ System zu entfernen. Um eine versehentliche Rücksetzung zu vermeiden, ist eine gestufte Präsentation an der Türkomponente in einer vorgegeben zeitlichen Sequenz notwendig.



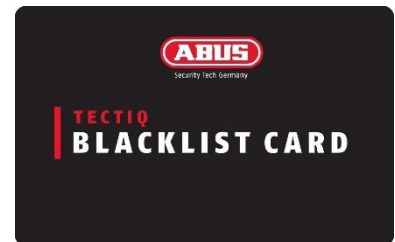
Protokollkarte

Die Protokollkarte liest Protokolldaten aus den Türkomponenten. Jede TECTIQ Türkomponente – Beschlag, Zylinder oder Wandleser-Terminal – speichert bis zu 900 Einträge. Diese Einträge beinhalten z. B. erteilten oder verweigerten Zutritt, Batteriewarnungen oder Batteriewechsel.



Blacklistkarte

Sollte ein TECTIQ Schließmedium verloren gegangen oder gestohlen worden, kann es gegen unbefugte Nutzung gesperrt werden. Die Blacklistkarte dient dazu, das betreffende Schließmedium in den Offline Türkomponenten aktiv zu sperren. Jede Türkomponente speichert ihre Sperrliste mit Einträgen über gesperrte Schließmedien.



Die Blacklistkarte wird bei Bedarf vom Administrator mit den notwendigen Daten geladen und an jeder betroffenen Türkomponente präsentiert. Die TECTIQ Türkomponenten lesen die Blacklistkarte aus und aktualisieren ihre interne Sperrliste. Damit ist der Zutritt mit dem gesperrten Schließmedium nicht mehr möglich. Eine Sperrung muss mit der Blacklistkarte aufgehoben werden, um ein wiedergefundenes Schließmedium wieder nutzen zu können.

Ein versuchter Zutritt mit einem gesperrten Schließmedium wird in der Ereignisliste der Türkomponente gespeichert und über die Nutzung von Schließmedien an die TECTIQ Zutrittskontrollzentrale übermittelt. Die Ereignisliste wird auch über die Protokollkarte an die TECTIQ Zutrittskontrollzentrale übertragen.

Notöffnungstransponder

Der Notöffnungstransponder ermöglicht Einsatzkräften den Zutritt zum gesicherten Gebäude oder Bereich. Der Notöffnungstransponder wird in der Regel in einem Feuerwehr-Schlüsseldepot am Objekt verwahrt. Der einfachen Handhabbarkeit halber ist dieses Medium als Transponder ausgeführt.



Im Notfall – das ist in der Regel der Notruf bei der Feuerwehr – schaltet die Einsatzzentrale den Zugang zum Schlüsseldepot für die Einsatzkräfte frei. Mit dem TECTIQ Notöffnungstransponder versetzen die Einsatzkräfte beim Präsentieren die jeweiligen Türen dauerhaft in den Geöffnet-Zustand. Dieser Zustand muss nach Abschluss des Einsatzes wieder zurückgesetzt werden.

Der Notöffnungstransponder kann im Auslieferungszustand von allen Türkomponenten gelesen werden und aktiviert bzw. deaktiviert den Zustand „Dauer-offen“.

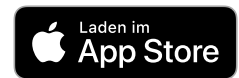
5.2.8. Admin App

Mit der TECTIQ Admin App nutzen Sie ein Smartphone zur Wartung der Türkomponenten. Die TECTIQ Admin App überträgt Daten drahtlos via Bluetooth auf die Türkomponenten. Sie dient z.B.

- zum Synchronisieren von Uhrzeit und Datum nach einem Batteriewechsel.
- zum Aktualisieren der Firmware.

Der Funktionsumfang der Admin App wird stetig erweitert. Aktuelle Details erfahren Sie unter [Abus.com](https://abus.com).

Sie erhalten die Admin App für iOS oder Android im App Store bzw. Google Play Store.



5.3. Systemaufbau

Je nach Kundenanforderung sind verschiedene Ausbaustufen eines TECTIQ Zutrittskontrollsystems möglich, z. B.

- Einfache TECTIQ Anlage ohne Update Terminal
- TECTIQ Anlage mit Update Terminal – an einem Standort
- TECTIQ Anlage mit Update Terminals an mehreren Standorten

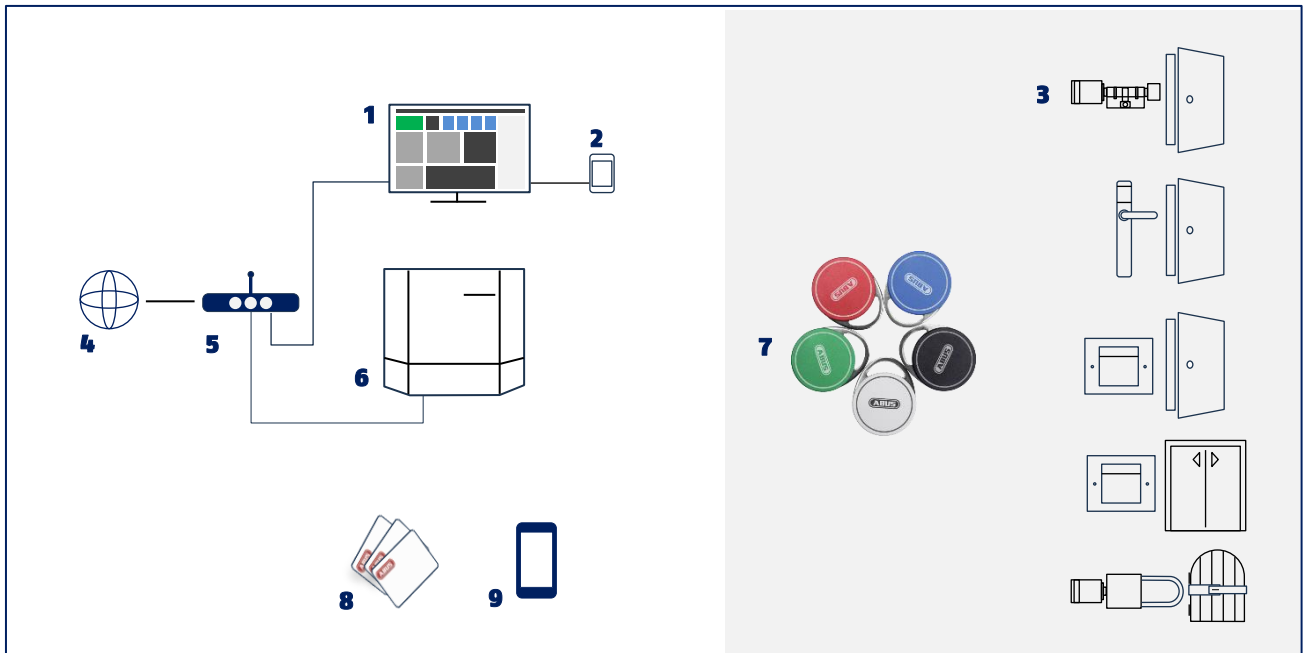
	ohne Update Terminal	mit Update Terminal
Anzahl Schließmedien	10 Schließmedien pro Person	10 Schließmedien pro Person
Anzahl Systemmedien	25 Systemmedien pro Typ	25 Systemmedien pro Typ
Gebäudeübergreifend	Ja	Ja
Standortübergreifend	Ja	Ja
Batteriestatusmeldung Türkomponenten	Nur über LED oder Protokollkarte	Über LED, Schließmedien oder Protokollkarte
Protokolle Türkomponenten	Nur über Protokollkarte	Über Schließmedien oder Protokollkarte
Zeitliche Begrenzung von Zutrittsberechtigungen	Ja, über Gültigkeit des Schließmediums	Ja
Automatische Verlängerung von Zutrittsberechtigungen	Nein	Ja
Ändern von Zutrittsberechtigungen (zeitlich, räumlich)	Nur über Admin am Tischleser	An Update Terminal oder Tischleser
Sperren von Zutrittsberechtigungen	Über Sperrliste (in Türkomponenten)	Automatisch (bei Ablauf der Berechtigung) oder über Sperrliste (in Türkomponenten)
Fernzugriff	Nur auf Zentrale, Aktualisieren von Berechtigungen lokal am Tischleser erforderlich.	Ja

Elemente einer TECTIQ Anlage

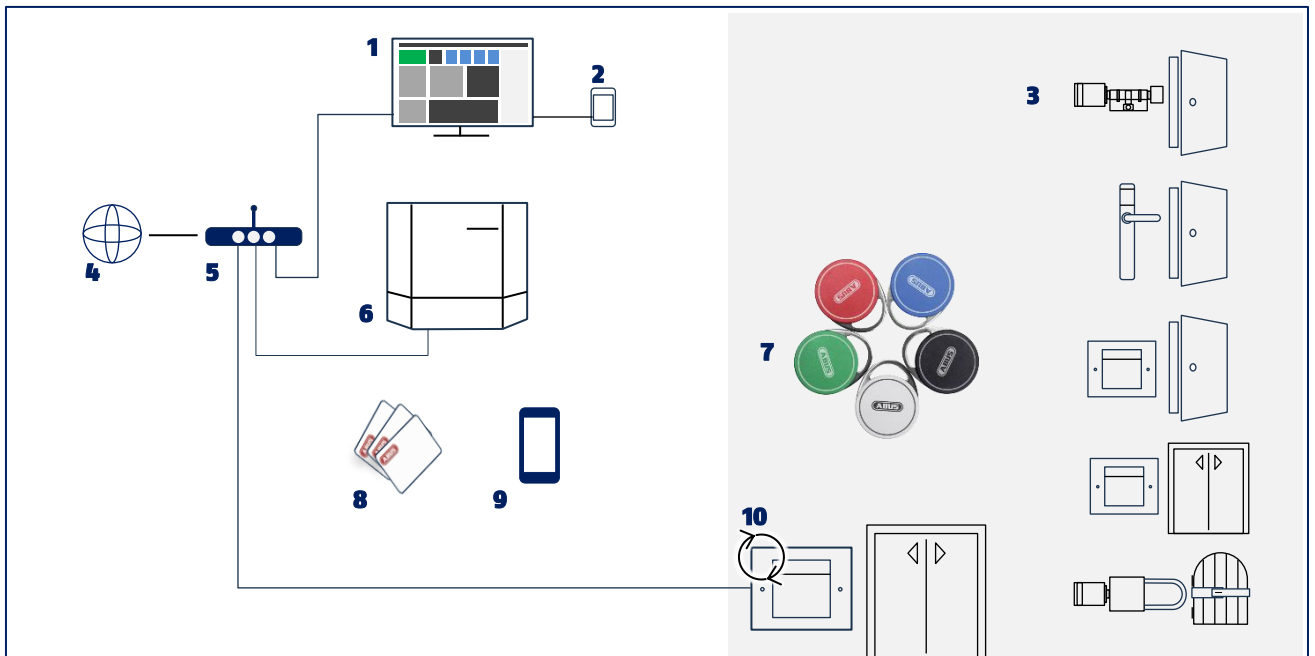
(Legende für folgende Abbildungen)

- | | |
|---|---|
| <ul style="list-style-type: none"> 1 TECTIQ Access Manager 2 USB-Tischleser 3 TECTIQ Türkomponenten, z. B. Schließzylinder, Beschlag, Wandleser mit Türöffner, Wandleser mit Türantrieb, Vorhangschloss 4 Anbindung an Internet (optional) 5 IP-Router 6 TECTIQ Zutrittskontrollzentrale 7 Schließmedien 8 Systemmedien | <ul style="list-style-type: none"> 9 Admin App 10 Update Terminal
Validieren von Zutrittsberechtigungen,
Aktualisieren von Zutrittsberechtigungen,
Lesen von Statusinformationen (Türkomponenten) 11 Hauptgebäude 12 Externes Gebäude 13 Update Terminal
mit Online-Verbindung zum Hauptsystem (P2P-Dienst) 14 Fernzugriff durch Admin oder Facherrichter |
|---|---|

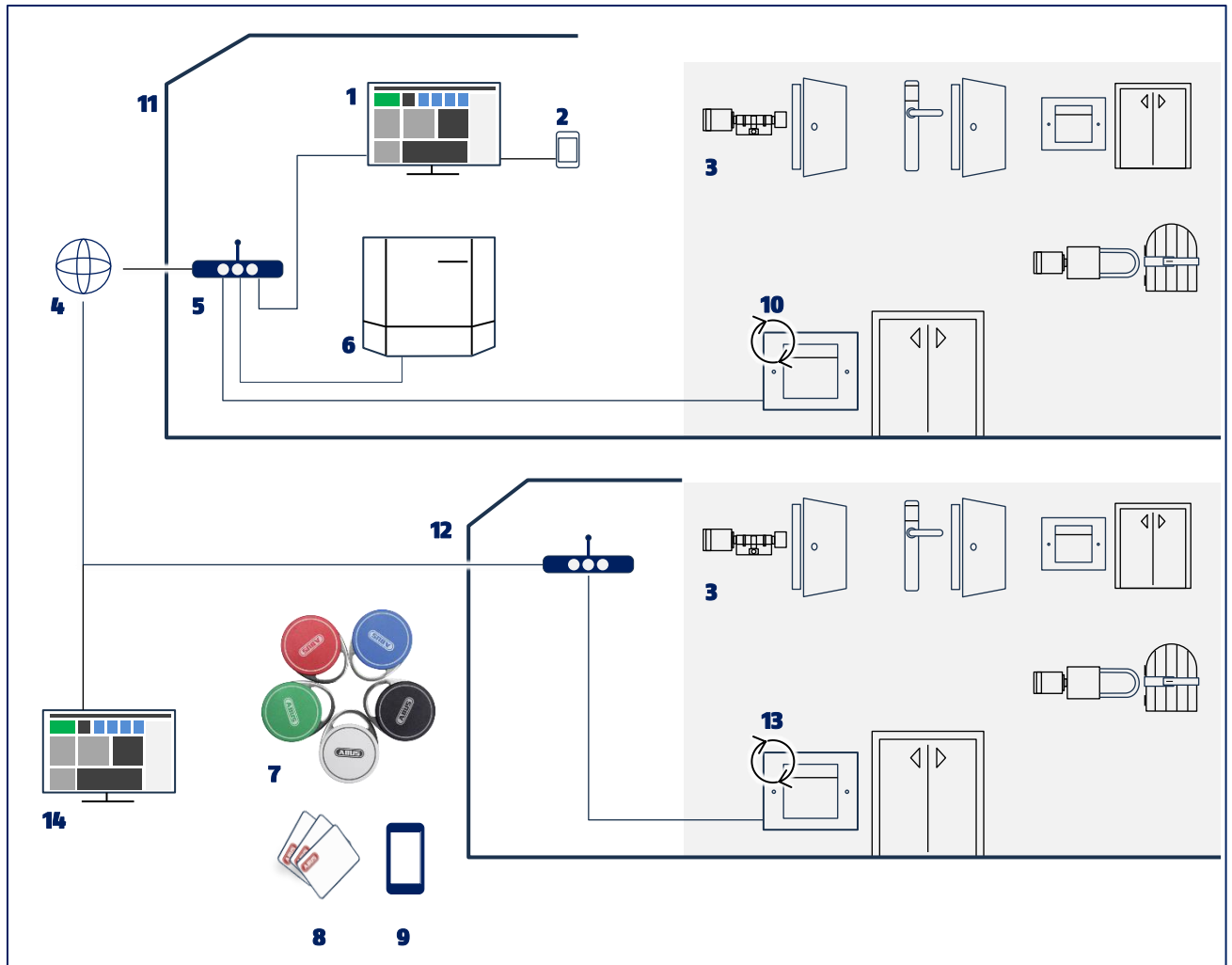
TECTIQ Anlage ohne Update Terminal



TECTIQ Anlage mit Update Terminal – 1 Standort



TECTIQ Anlage mit Update Terminal – mehrere Gebäude oder Standorte



5.4. Technische Daten

Systemdaten

Anzahl Türen	3004 (Türen mit beidseitiger Zutrittskontrolle zählen als 2 Türen)
Anzahl Türen/Türgruppen	1004
Anzahl Türkomponenten	max. 3004 (entspricht der Anzahl der im Access Manager projektierten Türen)
Anzahl Personen	2000
Anzahl Personengruppen	200
Anzahl Terminals	100
Anzahl Zeitpläne	300
Zeitintervalle pro Zeitplan	15
Anzahl Sperrtage	30 je Zeitplan
Anzahl Systemtransponder	25 je Typ / max. 125
Anzahl Administratoren	5
Anzahl Schließmedien pro Person	10
Anzahl Systemprotokolleinträge	100.000

Türkomponenten

Protokolleinträge	Max. 900
Blacklist-Einträge	Max. 120

Schließmedien

Art	ABUS MIFARE® DESFire® (3DES, AES128)
-----	--------------------------------------

5.5. Wo sind welche Daten gespeichert?

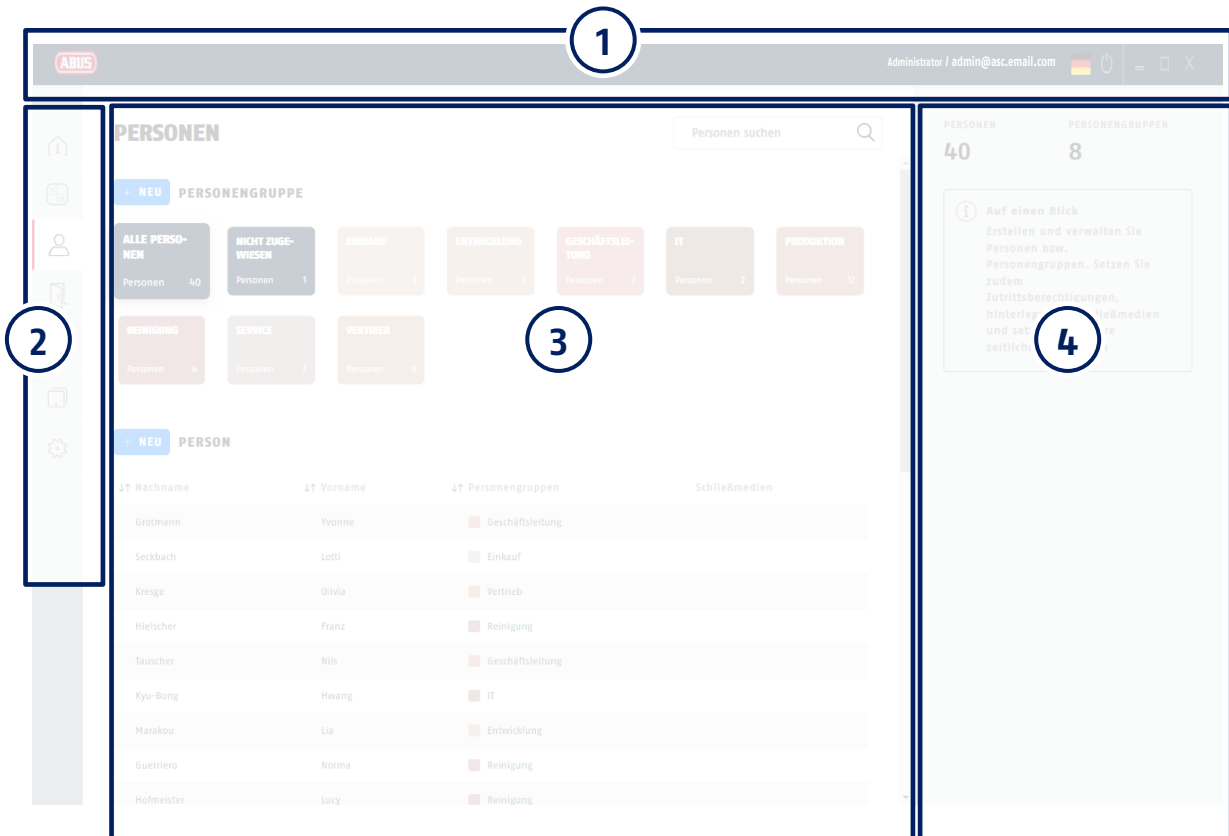
<p>Türkomponenten</p> <ul style="list-style-type: none"> • Firmware – System- und Anwendungssoftware • Konfigurationsdaten – Anlagen-ID, Tür, Türgruppe • Betriebsdaten – erteilte oder verweigerete Zutritte, Datum/Uhrzeit • Sperrliste 	<p>Zutrittskontrollzentrale</p> <ul style="list-style-type: none"> • Firmware – Systemsoftware • Projektdaten – Anlagen-ID, Netzwerkverwaltung, Türen, Türgruppen, Türkomponenten, Personen, Personengruppen, Schließmedien, Systemkomponenten, Schließplan, Sperrliste, Zeitpläne • Protokolldaten • Firmware für Türkomponenten
<p>Schließmedien</p> <ul style="list-style-type: none"> • Türberechtigungen • Gültigkeit der Berechtigungen • Gültigkeit des Schließmediums • Zeitpläne • Berechtigungen für Dauer-Öffnung • Übertragene Protokolldaten (temporär) 	<p>Systemmedien</p> <ul style="list-style-type: none"> • Alle Karten: Anlagen-ID, Gültigkeit (15 Minuten) • Blacklist-Karte: Sperrliste • Parameterkarte: Programmierdaten für Schließmedium • Protokoll-Karte: Protokolldaten einer Türkomponente • Resetkarte: Berechtigung zum Zurücksetzen einer bestimmten Türkomponente
<p>Update Terminal</p> <ul style="list-style-type: none"> • Aktualisierte Zutrittsberechtigungen • Gültigkeitsdauer bei Verbindungsstörung • Übertragene Protokolldaten (temporär) 	<p>Admin App</p> <ul style="list-style-type: none"> • Firmware-Aktualisierungen für Türkomponenten • Funktionalität wird zukünftig erweitert, z.B. Berechtigung zum Parametrieren durch Administratoren und ABUS Fachhändler
<p>TECTIQ Access Manager</p> <ul style="list-style-type: none"> • Anwendungssoftware • Datensicherungsdateien (Backups, verschlüsselt) 	<p>ABUS Online-Account</p> <ul style="list-style-type: none"> • ABUS Fachpartner / Email-Kontakt • Betreiber / Email-Kontakt

6. TECTIQ Access Manager – Oberfläche

Inhalt

- 6.1. TECTIQ Access Manager – Oberfläche
- 6.2. Menüstruktur

6.1. TECTIQ Access Manager – Oberfläche



1 Titelzeile 2 Menüleiste 3 Arbeitsbereich 4 Editierbereich

Titelzeile (1)

Die Titelzeile zeigt als grundlegende Elemente die Sprachauswahl sowie einen Button zum Abmelden aus der Anlage.

Menüleiste (2)

In der Menüleiste wählen Sie die Sicht für Ihre Aktivitäten. Die ausgewählte Sicht wird im Arbeitsbereich angezeigt.

- | | | | | | |
|--|------------------------|--|--------------------------|--|---------------------|
| | Titelseite / Dashboard | | Sicht Türen | | Sicht Einstellungen |
| | Sicht Schließplan | | Sicht Zeitpläne | | |
| | Sicht Personen | | Sicht System-Komponenten | | |

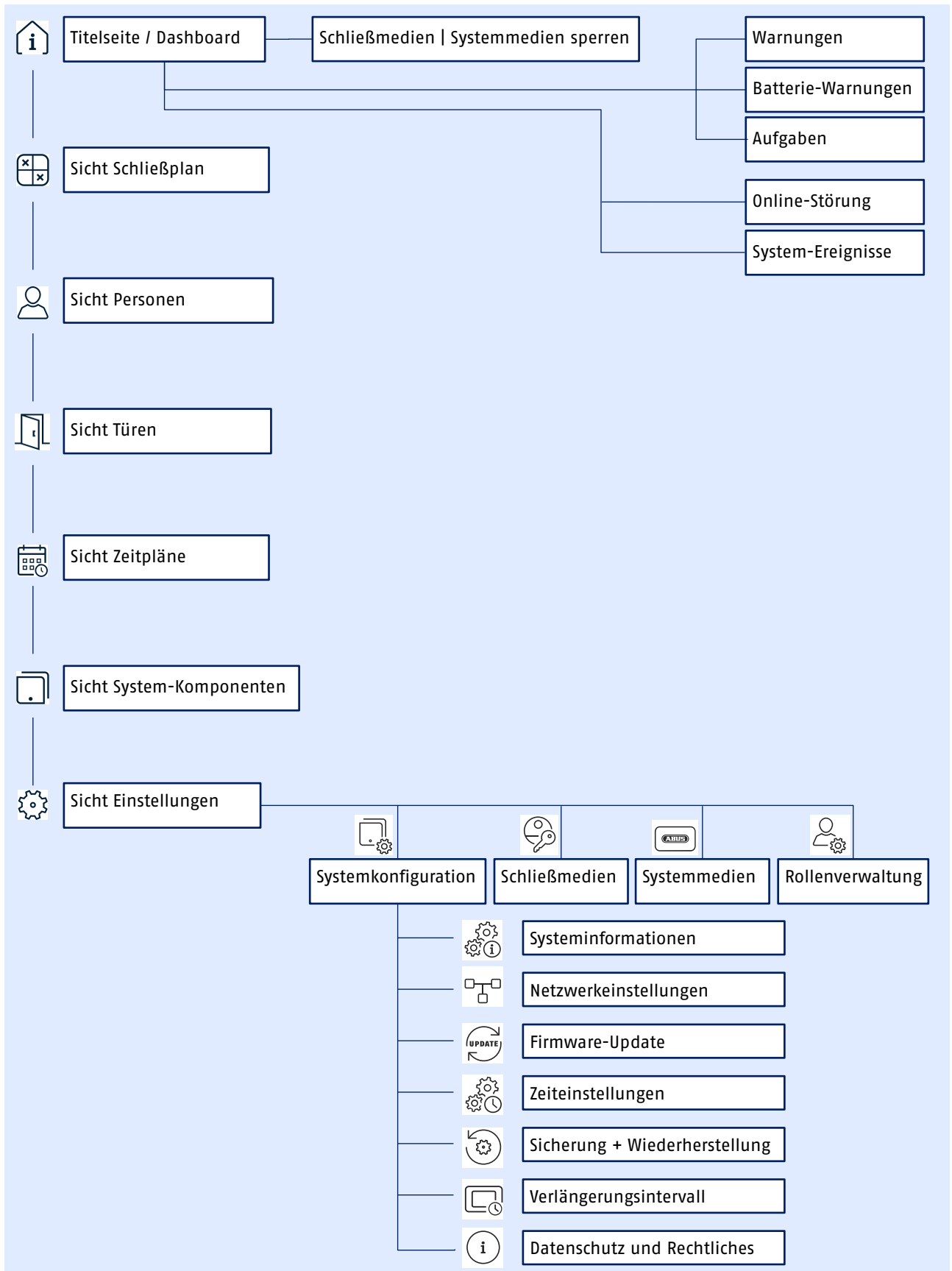
Arbeitsbereich (3)

Im Arbeitsbereich findet der Großteil Ihrer Aktivitäten statt. Je nach aktivierter Sicht finden Sie hier Ihre Werkzeuge zum Verwalten von Türen, TECTIQ Türkomponenten, Personen, Schließplänen und Einstellungen.

Editierbereich (4)

Der Inhalt des Editierbereichs hängt von der gewählten Sicht und der jeweiligen Aktivität im Arbeitsbereich ab. Sie finden hier Hinweistexte über Programmfunktionen und geben hier die Daten über Ihre Schließanlage und ihre Nutzer ein.

6.2. Menüstruktur



7. Hauptmenü | Dashboard

Inhalt

- 7.1. Übersicht Hauptmenü
- 7.2. Sammelmeldung Anlagenstatus
- 7.3. Schnelltasten | Shortcuts
- 7.4. Listen & Schnelltasten
- 7.5. Verlust eines Schließmediums
- 7.6. Systemwarnungen
- 7.7. Batteriewarnungen
- 7.8. Offene Aufgaben – Aufgabenliste
- 7.9. Störungsmeldungen
- 7.10. Ereignisse

7.1. Übersicht Hauptmenü

Das Hauptmenü – oder auch Dashboard – wird nach dem Programmstart und Einloggen in die Anlage angezeigt. Von anderen Sichten erreichen Sie das Hauptmenü über die Schaltfläche (1). Hier haben Sie die Übersicht über

- den aktuellen Systemstatus,
- wichtige Systemereignisse,
- offene Aufgaben (z. B. notwendige Batteriewechsel),

Im Hauptmenü/Dashboard haben Sie den schnellen Zugriff auf die wichtigsten Funktionen und werden direkt zu den jeweiligen Untermenüs weitergeleitet.

The screenshot shows the ABUS TECTIQ dashboard interface. It features a top navigation bar with the ABUS logo and user information. The main content area is divided into several sections: a status overview, quick actions for keys, groups, and permissions, system and battery warnings, a list of open tasks, terminal connection issues, a detailed event log, and a door management section. On the right, there are summary statistics for persons and doors, and system information including firmware version and IP address. A sidebar on the left contains navigation icons. Numbered callouts (1-8) point to specific elements: 1 (Anlagenname), 2 (Sammelmeldung), 3 (Schnelltasten), 4 (Listen & Schnelltasten), 5 (Aktuelle Anlagennutzung), 6 (Systemübersicht), 7 (Links, FAQ), and 8 (Status overview).

- | | | | |
|-----------------|--------------------------|---------------------------|---------------|
| 1 Anlagenname | 3 Schnelltasten | 5 Aktuelle Anlagennutzung | 7 Links , FAQ |
| 2 Sammelmeldung | 4 Listen & Schnelltasten | 6 Systemübersicht | |

7.2. Sammelmeldung Anlagenstatus

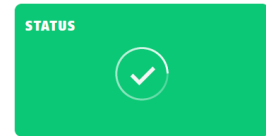
Die Sammelmeldung über den Anlagenstatus gibt eine schnelle Orientierung über den Anlagenstatus und signalisiert unmittelbar erforderliche Tätigkeiten durch den Betreiber der Anlage.

Grün: Keine akute Meldung.

Orange: System-Meldung

- Software-Aktualisierungen
- Batteriewarnungen

Rot: Verbindungsstörung zu einem Online-Terminal

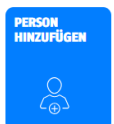


7.3. Schnellkasten | Shortcuts

Die Schnellkasten in der obersten Reihe führen Sie unmittelbar zur ausgewählten Funktion:



„Schließmedium verloren oder gestohlen?“
Weiter zum Menü „Schließmedium sperren“



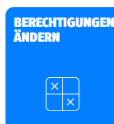
„Person hinzufügen“: Weiter zum Menü „Personen“ | Neue Person hinzufügen



„Gruppe hinzufügen“: Weiter zum Menü „Personen“ | Neue Gruppe hinzufügen

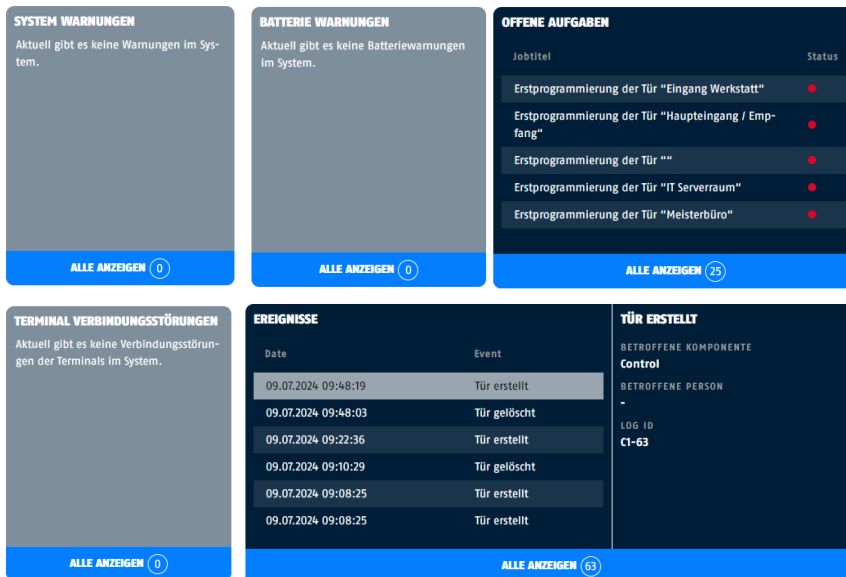


„Tür hinzufügen“: Weiter zum Menü „Türen“ | Tür hinzufügen



„Berechtigungen ändern“: Weiter zum Menü „Schließplan“

7.4. Listen & Schnellasten



SYSTEM WARNUNGEN
Aktuell gibt es keine Warnungen im System.
ALLE ANZEIGEN 0

BATTERIE WARNUNGEN
Aktuell gibt es keine Batteriewarnungen im System.
ALLE ANZEIGEN 0

OFFENE AUFGABEN

Jobtitel	Status
Erstprogrammierung der Tür "Eingang Werkstatt"	●
Erstprogrammierung der Tür "Haupteingang / Empfang"	●
Erstprogrammierung der Tür ""	●
Erstprogrammierung der Tür "IT Serverraum"	●
Erstprogrammierung der Tür "Meisterbüro"	●

ALLE ANZEIGEN 25

TERMINAL VERBINDUNGSSTÖRUNGEN
Aktuell gibt es keine Verbindungsstörungen der Terminals im System.
ALLE ANZEIGEN 0

EREIGNISSE

Date	Event
09.07.2024 09:48:19	Tür erstellt
09.07.2024 09:48:03	Tür gelöscht
09.07.2024 09:22:36	Tür erstellt
09.07.2024 09:10:29	Tür gelöscht
09.07.2024 09:08:25	Tür erstellt
09.07.2024 09:08:25	Tür erstellt

TÜR ERSTELLT

BETROFFENE KOMPONENTE
Control

BETROFFENE PERSON
-

LOG ID
C1-63

ALLE ANZEIGEN 63

Die Listenfelder zeigen die letzten Zustandsmeldungen an. Mit einem Mausklick in das blaue Feld gelangen Sie in die Bearbeitungssicht der ausgewählten Liste, in der Meldungen ausgewählt, angezeigt und bearbeitet werden können. Das Dashboard zeigt

- **Systemwarnungen:**
Meldungen mit systemrelevantem Bezug, z. B. Firmware-Update für Türkomponenten oder gestörte Internet-Verbindung.
- **Batteriewarnungen:**
Meldungen über Türkomponenten, deren Batteriestand die erste Warnmeldung unterschritten hat.
- **Offene Aufgaben:**
Meldungen über zu erledigende Aufgaben in der Anlage, z. B. erforderliche Einstellungen, Parametrierungen, oder Aktualisierungen.
- **Terminal Verbindungsstörungen:**
Meldungen über gestörte Verbindungen zu Online-Terminals. Die betreffende Türfunktion ist in diesem Fall nicht beeinträchtigt; Zutrittsberechtigungen in TECTIQ Schließmedien werden vor Ort bis zu 72 Stunden weiterhin aktualisiert.
- **Ereignisse:**
Informationen zu personen- und systembezogenen Ereignissen

7.5. Verlust eines Schließmediums

Das TECTIQ Zutrittskontrollsystem bietet höchstmöglichen Schutz vor unbefugtem Zutritt zum gesicherten Bereich. Durch die Einstellung einer kurzen Gültigkeit der Zutrittsberechtigung auf dem TECTIQ Schließmedium wird die Dauer, in der eine unbefugte Nutzung möglich ist, auf ein Minimum reduziert.

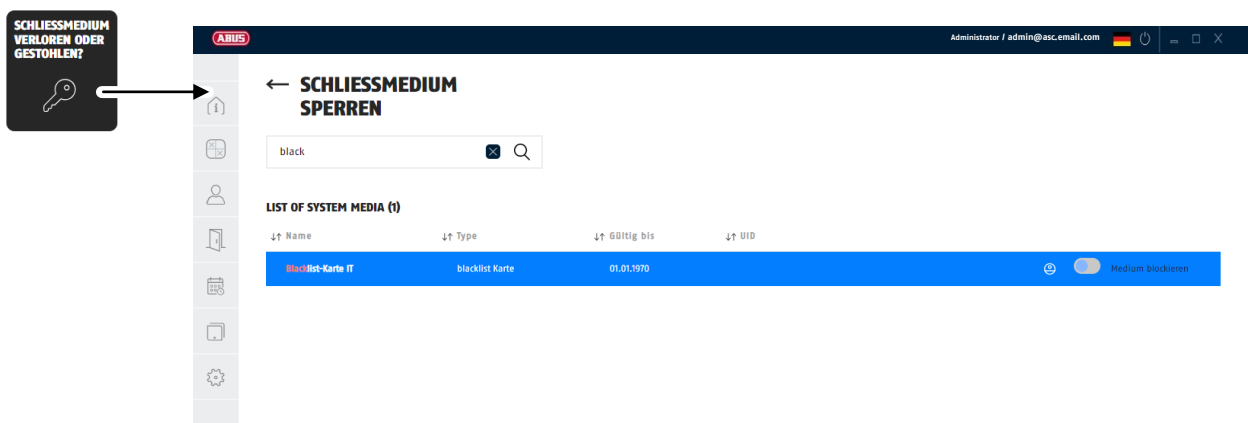
Ist jedoch ein Schließmedium abhandengekommen, sind sofort Maßnahmen einzuleiten, um die Gefahr einer unbefugten Nutzung zu verhindern. Geben Sie daher Anweisungen, dass der Administrator unverzüglich über den Verlust eines Schließmediums informiert wird.

Das Schließmedium ist vom Administrator unverzüglich im TECTIQ Accessmanager zu sperren. Eine Löschung des Schließmediums ist aus Sicherheitsgründen nicht möglich. Nach Ablauf der Gültigkeit und Sperrung des Schließmediums in der Zutrittskontrollzentrale wird der Zutritt zu den gesicherten Bereichen nicht mehr gewährt. Unbefugte Zutrittsversuche werden in der Ereignisliste protokolliert.

Das Sperren eines Schließmediums hat mehrere Auswirkungen:

- Das regelmäßige Aktualisieren der Zutrittsberechtigung für dieses Schließmedium wird verhindert. Somit ist gewährleistet, dass – spätestens nach Ablauf der Gültigkeit – mit diesem Schließmedium kein Missbrauch erfolgen kann.
- Die geänderte Zutrittsberechtigung ist in den vorhandenen Online-Terminals sofort vorhanden. Das bedeutet: Sobald das Schließmedium an einer dieser Komponenten präsentiert wird, wird die Gültigkeit auf dem Medium gelöscht.
- Die Sperrliste in der TECTIQ Zutrittskontrollzentrale wird aktualisiert und muss schnellstmöglich in allen betroffenen Offline Türkomponenten gespeichert werden. Für die Übertragung der Sperrliste in die Türkomponenten ist eine Blacklistkarte erforderlich.

Gleiches gilt für das Sperren eines Systemmediums: Das betreffende Systemmedium wird aktiv aus der Anlage ausgeschlossen und hat keine Funktion mehr.



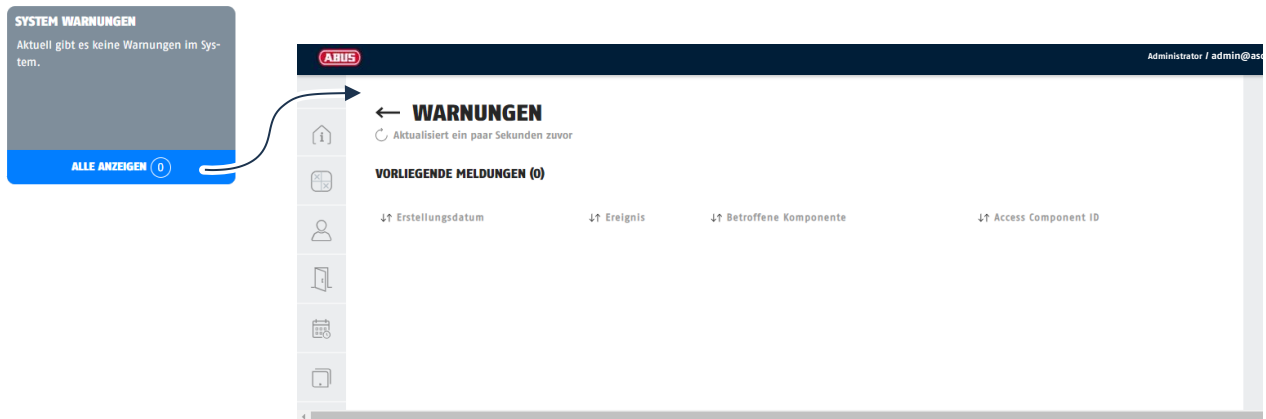
Auswahl der Schaltfläche „Schließmedium verloren oder gestohlen?“ führt ins Fenster „Schließmedium sperren“. Hier geben Sie in das Eingabefeld die Bezeichnung für das betreffende Schließ- oder Systemmedium ein. Das Programm zeigt Übereinstimmungen unmittelbar an.

- ▶ Betätigen Sie den Schieber mit dem Mauszeiger um das Medium zu sperren oder zu entsperren.

Beachten Sie: Eine Sperrung oder Entsperrung wird in den Offline Türkomponenten erst wirksam, wenn die Sperrliste mittels Blacklistkarte in die Türkomponenten übertragen wurde!

7.6. Systemwarnungen

Anklicken der blauen Fläche im Listenfeld „Systemwarnungen“ führt ins Untermenü „Warnungen“. Hier werden im System gespeicherte aktuelle Warnmeldungen angezeigt. Die Liste kann nach Spalten auf- oder absteigend sortiert werden.



Die folgenden Warnmeldungen werden im Fenster „Warnungen angezeigt“:

Warnmeldung	Bedeutung	Was ist zu tun:
Firmware Update verfügbar	Für das angegebene Gerät ist eine aktualisierte Software verfügbar.	Installieren Sie die aktualisierte Software für das angegebene Gerät.
Internet-Verbindung verloren	Die Zutrittskontrollzentrale hat keine Verbindung mehr zum Internet. Verbindungen zu anderen Standorten können unterbrochen sein (siehe hierzu auch die separate Meldung)	Melden Sie sich aus dem Accessmanager ab. Prüfen Sie den korrekten Sitz von Netzwerkkabeln. Starten Sie die Zutrittskontrollzentrale ggf. neu. Falls weiterhin keine IT-Verbindung besteht, informieren Sie Ihre IT-Abteilung oder wenden sich an Ihren ABUS-Fachhändler.

Warnmeldungen werden nach Behebung bzw. Installation der Firmware in der Ereignis-Liste abgelegt.

7.7. Batteriewarnungen

Anklicken der blauen Fläche im Listenfeld „Batteriewarnungen“ führt ins Untermenü „Batteriewarnungen“. Hier werden Türkomponenten angezeigt, die einen niedrigen Batteriestand gemeldet haben. Die Liste kann nach Spalten auf- oder absteigend sortiert werden.



Anklicken einer Batteriewarnung zeigt im Editierbereich Details sowie die jeweilige Türkomponente an.

- Wechseln Sie die Batterien der Türkomponenten so bald wie möglich!

Batteriewarnungen werden nach Erneuerung der Batterie in die Ereignis-Liste verschoben. Beachten Sie, dass der neue Status erst nach Nutzung eines Schließmediums und anschließender Validierung in die Zutrittskontrollanlage übertragen wird. Eine eventuelle zeitliche Verzögerung hat keinen Einfluss auf die Funktion der Anlage.

7.8. Offene Aufgaben – Aufgabenliste

Anklicken der blauen Fläche im Listenfeld „Offene Aufgaben“ führt ins Untermenü „Aufgabenliste“. Hier werden Aufgaben angezeigt, die einen Eingriff durch den Anlagenbetreiber erfordern, z. B. neue Türkomponenten parametrieren. Die Liste kann nach Spalten auf- oder absteigend sortiert werden.



7.9. Störungsmeldungen

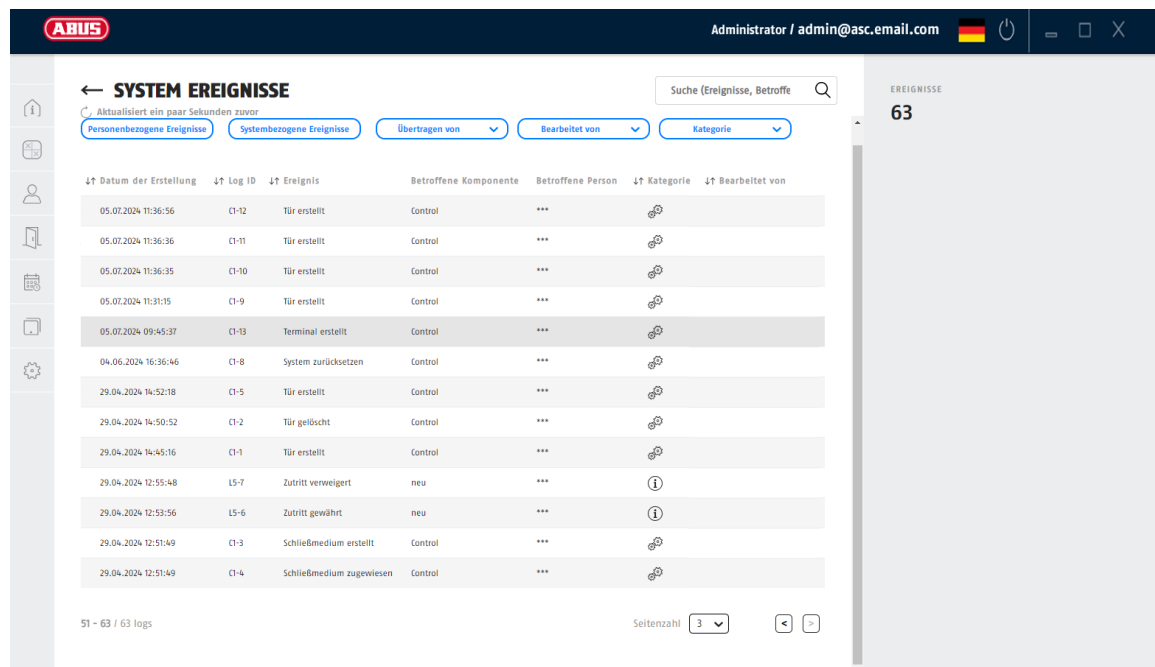
Im Listenfeld „Terminal Verbindungsstörungen“ werden gestörte Verbindungen zu Online-Terminals angezeigt. Die betreffende Türfunktion ist hierdurch nicht betroffen. Zutrittsberechtigungen in TECTIQ Schließmedien werden weiterhin – bis max. 72 Stunden nach Auftreten der Störung – auf Basis der lokal gespeicherten Daten aktualisiert.



7.10. Ereignisse

Die Ereignisliste zeigt Ihnen übersichtlich Informationen zur Nutzung und Anlagenbetreuung an. Angezeigt werden Meldungen über Ereignisse wie erteilte oder verweigerte Zutrittsversuche, erfolgte Software-Aktualisierungen, Beschreiben von Schließmedien, Hinzufügen oder Löschen von Türkomponenten. Damit erhalten Sie schnell eine Übersicht darüber, ob ungewöhnliche Vorgänge in der Anlage erkannt wurden.

Ereignisse werden standardmäßig in der Reihenfolge des Auftretens angezeigt und können nach verschiedenen Kriterien sortiert werden.



8. Sicht Schließplan | Keylockplan

Inhalt


- 8.1. Übersicht
- 8.2. Darstellung
- 8.3. Individuelle Zutrittsberechtigungen
- 8.4. Gruppenberechtigungen
- 8.5. Zutrittsberechtigung erteilen
- 8.6. Zutrittsberechtigung entziehen

8.1. Übersicht

Der Schließplan zeigt die aktuellen Berechtigungen für Personen und die zugelassenen Türen übersichtlich an.

Hier können Sie

- Personen und Personengruppen die Zutrittsberechtigung zu Türen oder Türgruppen erteilen
- Zutrittsberechtigungen ändern
- Zutrittsberechtigungen entziehen

Sie erreichen den Schließplan über die Schaltfläche  Schließplan. Hier sind die Personen und Personengruppen horizontal und die Türen und Türgruppen senkrecht angeordnet. Personengruppen und Türgruppen werden zunächst eingeklappt angezeigt, können jederzeit einzeln oder gesammelt ausgeklappt werden.

Personengruppen (eingeklappt) Personen (ohne Gruppe)

Schaltfläche Schließplan

Türgruppen (eingeklappt)

Türen (ohne Gruppe)

Letzte Aktion rückgängig

Hilfe

Schnelltaste

Gruppen ausklappen

Gruppen einklappen

Gruppen ein-/ausklappen

Innerhalb des Schließplans klappen Sie die Tür- oder Personengruppen auf, indem Sie auf das Symbol bzw. der jeweiligen Gruppe klicken.

Wenn einer Tür bereits eine Türkomponente zugeordnet ist, wird diese als Symbol neben der Türbezeichnung dargestellt.

Funktionstasten

Drei Funktionstasten erlauben den schnellen Zugriff für komfortables und sicheres Arbeiten:



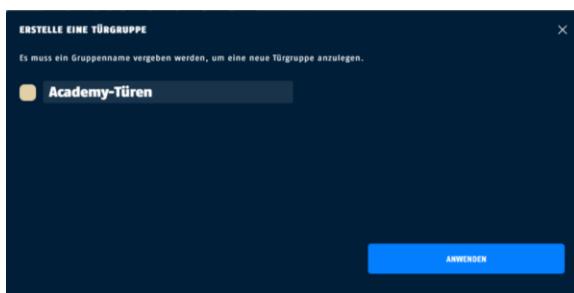
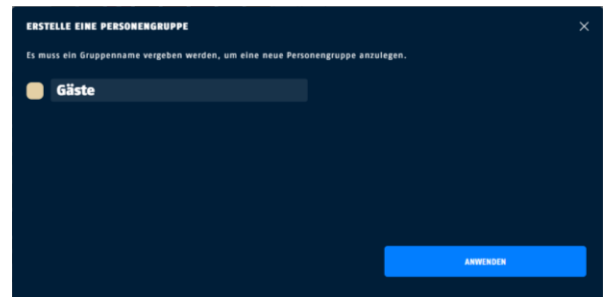
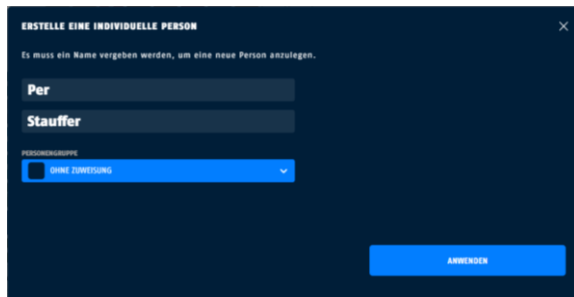
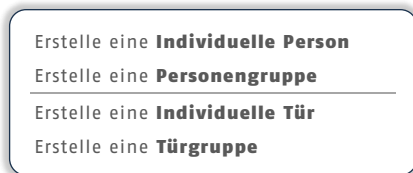
Macht die letzte veränderte Zutrittsberechtigung rückgängig (bis zu 5 Schritte).



Zeigt einen Hilfetext an.

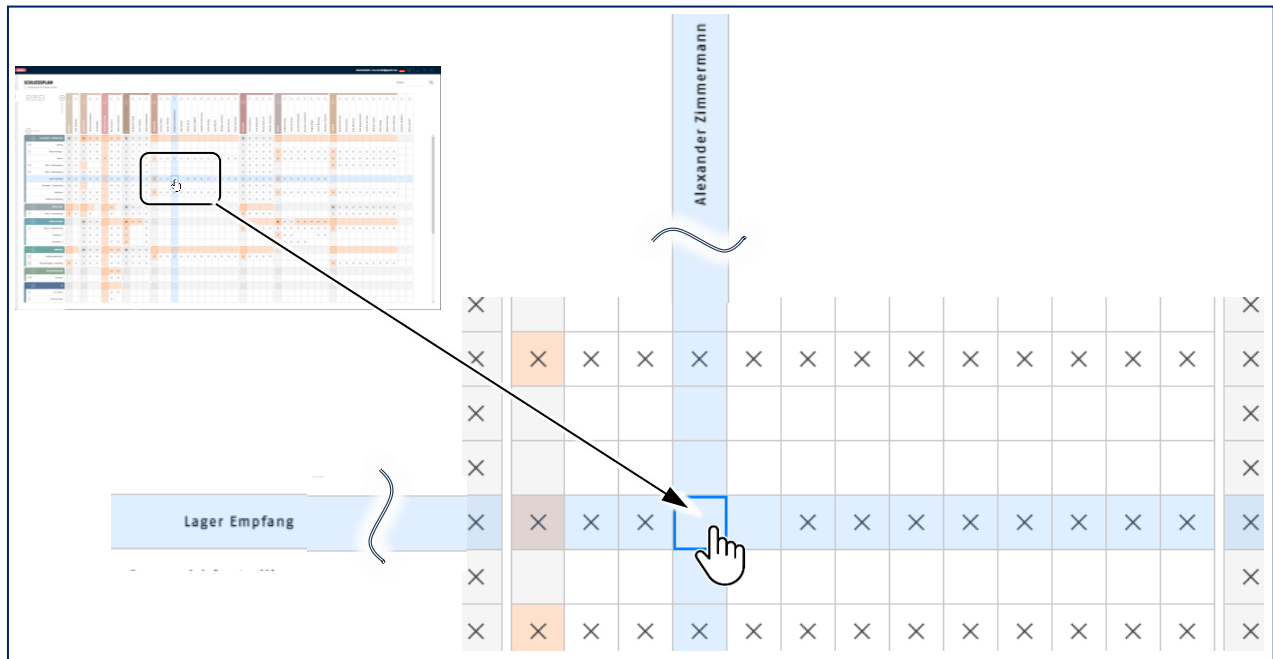


Schnellaste: Hiermit können **Personen**, Personengruppen, Türen oder Türgruppen schnell angelegt werden, ohne den Schließplan zu verlassen.



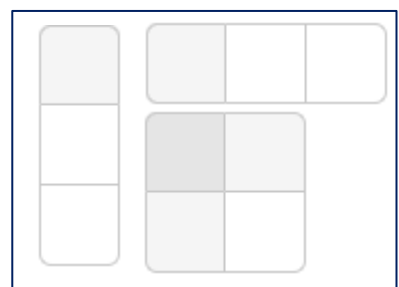
8.2. Darstellung

Personen und Türen sind im Schließplan in Form einer Matrix dargestellt. Personengruppen und Türgruppen sind in Blöcken zusammengefasst, die unter dem jeweiligen Gruppennamen aus- oder eingeklappt werden können. Die jeweils erste Zeile bzw. Spalte enthält den Gruppennamen und ist von den übrigen Zellen farblich abgesetzt. Die jeweils erste Zeile bzw. Spalte enthält den Gruppennamen und ist von den übrigen Zellen farblich abgesetzt. Die aktuelle Mausposition innerhalb des Schließplans und die Zuordnung hinsichtlich Person und Tür ist blau hinterlegt.



Berechtigungen im Schließplan

- Weiße Felder im Schließplan symbolisieren eine individuelle Tür / Person.
- Graue Felder kennzeichnen die Kopfzeilen-/spalten von Türgruppen bzw. Personengruppen.
- Ein × kennzeichnet eine aktive Zutrittsberechtigung einer Person zu einer Tür.
- Ein × innerhalb eines grauen Feldes kennzeichnet eine Gruppenberechtigung.



- Ein fettes * bedeutet, dass die Gruppenberechtigung für den kompletten Block (sowohl für die Türgruppe als auch für die Personengruppe) gilt. Neue Türen oder Personen zu einer Gruppe erben die voreingestellten Berechtigungen der Gruppe.

*	×	×	×
×	×	×	×
×	×	×	×

- Orange Felder tauchen nur in den Kopfzeilen-/spalten auf. Sie kennzeichnen, ob in einer Tür-/Personengruppe Berechtigungen individuell geändert – erteilt oder entzogen – sind.

	×
×	×

- Ein oranges Feld mit einem fetten * in der Schließplanmatrix zeigt an, dass für den kompletten Block aus Tür- und Personengruppe Gruppenberechtigungen voreingestellt sind, aber bei einzelnen Elementen individuelle Abweichungen eingestellt sind.
Neue Türen oder Personen, die zur Gruppe hinzugefügt werden, erhalten zunächst alle Gruppenberechtigungen. Die Berechtigungen können danach individuell angepasst werden.

*	×	×	×	×
×	×	×	×	×
×	×	×		×
×	×	×	×	

8.3. Individuelle Zutrittsberechtigungen

Individuelle Zutrittsberechtigungen gelten grundsätzlich für die ausgewählte Person bzw. Tür. Berechtigungen können für eine Person – bzw. eine Tür – individuell erteilt und auch individuell entzogen werden.

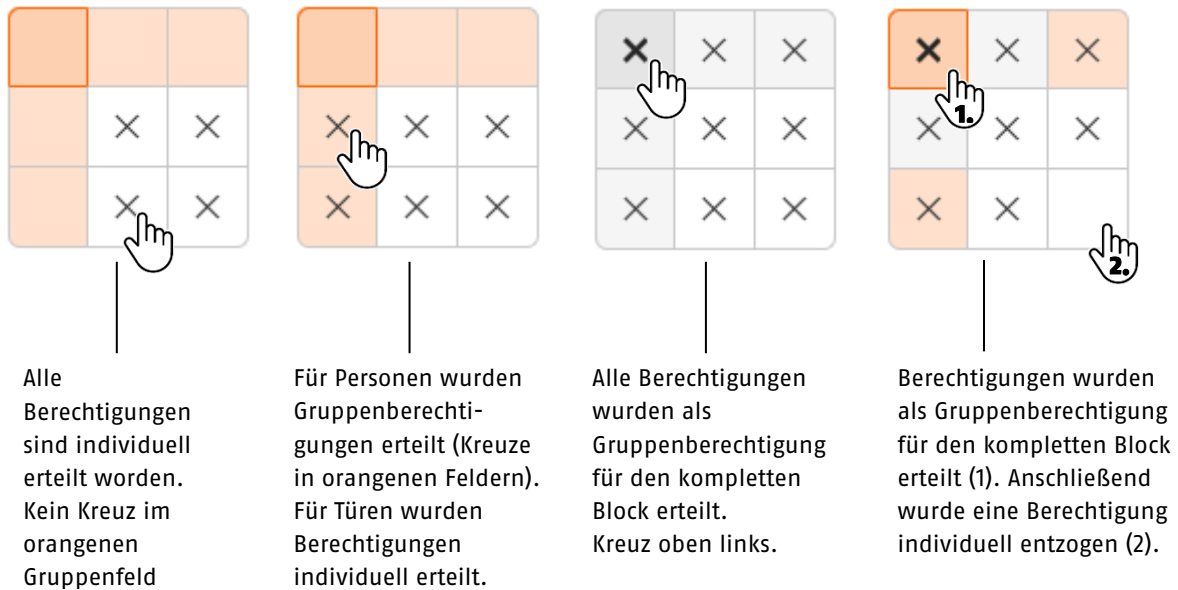
8.4. Gruppenberechtigungen

Gruppenberechtigungen gelten für alle Türen bzw. Personen innerhalb dieser Gruppe. Eine Gruppenberechtigung wird für alle enthaltenen Türen/Personen erteilt oder entzogen.

Gruppenberechtigungen werden bei Hinzufügen neuer Elemente zur Gruppe vererbt.

Nach dem Erteilen einer Gruppenberechtigung können bei einzelnen Türen/Personen die Berechtigungen individuell geändert werden. Diese Änderungen wirken sich grundsätzlich nicht auf die Voreinstellung der Gruppe – und auch nicht auf die anderen Elemente der Gruppe – aus.

Nachfolgend werden die möglichen Eingabevarianten nochmal zusammengefasst:



In den ersten 3 Fällen sind die aktuell erteilten Schließberechtigungen gleich. Bei Hinzufügen einer neuen Tür bzw. Person unterscheiden sich jedoch die Voreinstellungen.

8.5. Zutrittsberechtigung erteilen

- ▶ Erteilen Sie eine Zutrittsberechtigung, indem Sie für die betreffende Person und die Tür ein Kreuz setzen.

Zutrittsberechtigungen können auch für komplette Personen- und Türgruppen erteilt werden. Bereits bestehende Gruppenberechtigungen werden dabei an die enthaltenen Personen und Türen vererbt.

8.6. Zutrittsberechtigung entziehen

- ▶ Entziehen Sie eine individuelle Zutrittsberechtigung, indem Sie für die Person und die Tür im Schließplan das Kreuz × entfernen.
- ▶ Entziehen Sie die Zutrittsberechtigungen für komplette Personengruppen und Türgruppen, indem Sie für die komplette Gruppe im Schließplan das Kreuz *|× entfernen.


9. Sicht Personen | Persons

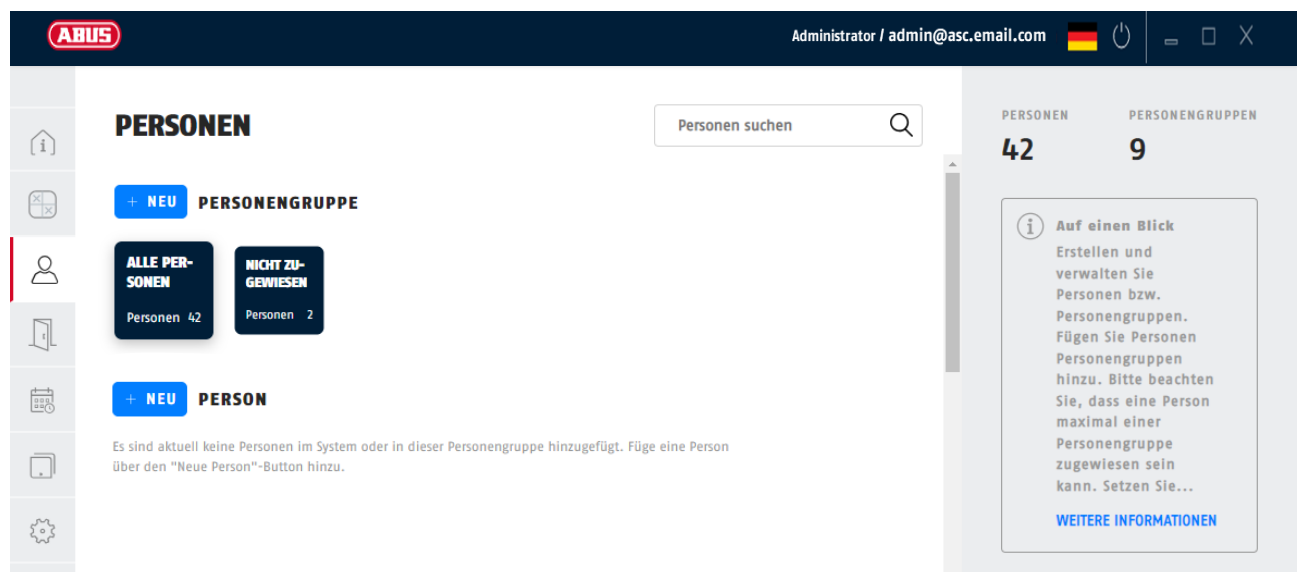
Inhalt

- 9.1. Übersicht
- 9.2. Personengruppen
- 9.3. Eigenschaften von Personengruppen
- 9.4. Personen
- 9.5. Eigenschaften von Personen
- 9.6. Schließmedium hinzufügen

9.1. Übersicht

In der Sicht Personen erstellen und verwalten Sie Personen und ordnen ihnen Schließmedien zu. Zur besseren Orientierung fassen Sie Personen mit ähnlichen Berechtigungen in Personengruppen zusammen. Eine Person kann dabei maximal einer Personengruppe zugewiesen sein.

Sie erreichen die Sicht Personen über die Schaltfläche .



Schaltfläche Personen

Verwalten von Personengruppen

Personen-Liste

Übersicht

Listen-Navigation bei vielen Personen

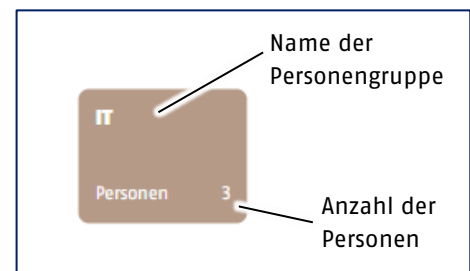
Eingeben von Personen

+ NEU Neue Person oder Neue Personengruppe hinzufügen

9.2. Personengruppen

Personengruppen erleichtern die Verwaltung einer Schließanlage. Einer Personengruppe können gesammelt Zutrittsrechte erteilt oder entzogen werden und Zeitpläne können vorgegeben werden. Die Einstellungen der Personengruppe werden an Personen vererbt, können aber für einzelne Personen immer individuell angepasst werden.

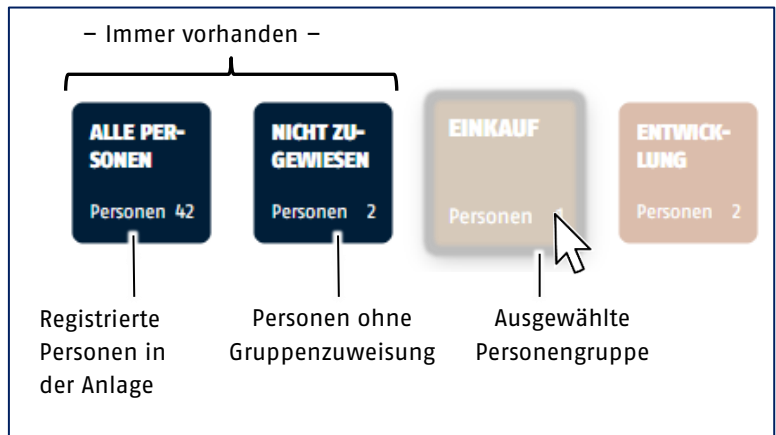
Im oberen Teil der Sicht Personen sind die Personengruppen als Kacheln mit dem Namen und der Anzahl der zugeordneten Personen dargestellt.



Immer vorhanden sind die Kacheln „Alle Personen“ und „Nicht zugewiesen“.

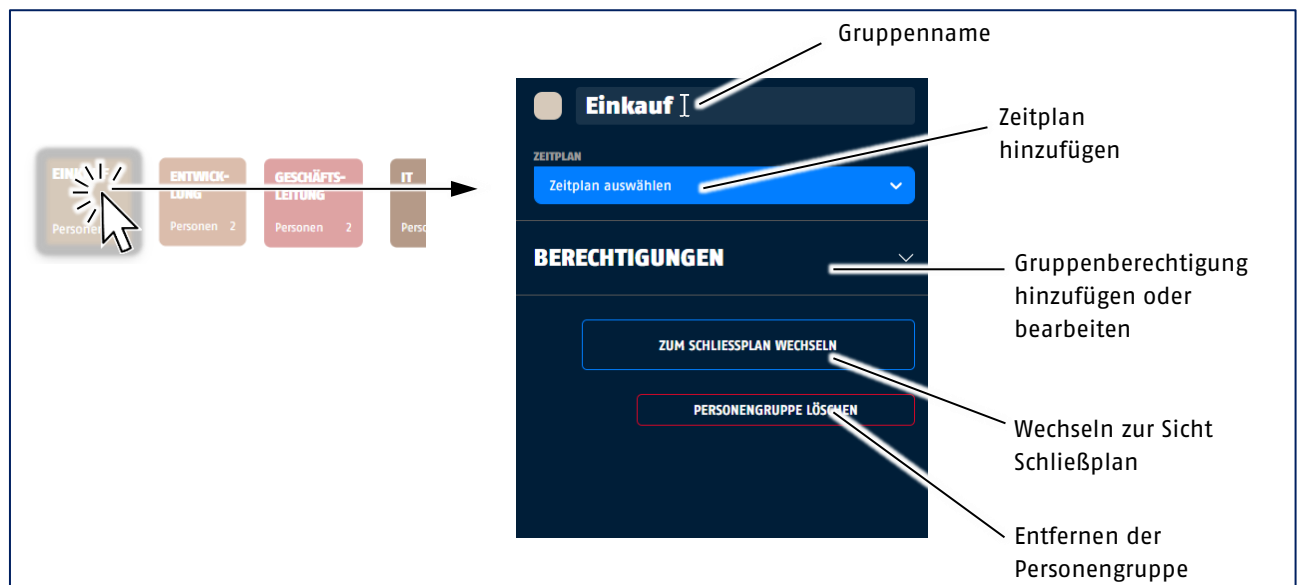
Eine Personengruppe wird durch Anklicken ausgewählt. Die ausgewählte Personengruppe wird hervorgehoben dargestellt.

Nach Auswahl einer Personengruppe werden in der Personenliste die enthaltenen Personen angezeigt.



9.3. Eigenschaften von Personengruppen

Weisen Sie Personengruppen weitere Eigenschaften zu.



Gruppenname bearbeiten

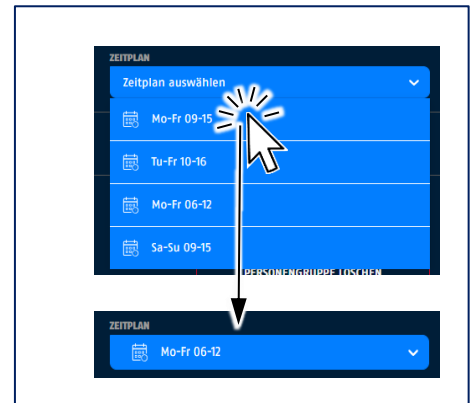
Sie bearbeiten den Gruppennamen, indem Sie die Einfügemarke mit dem Mauszeiger in das Fenster setzen und Ihre Änderungen vornehmen.



Zeitplan hinzufügen

Weisen Sie der Personengruppe einen vorher definierten Zeitplan zu, indem Sie die Liste unter „Zeitpläne“ aufklappen und den gewünschten Zeitplan anklicken.

Zeitpläne erstellen Sie in der Sicht Zeitpläne.

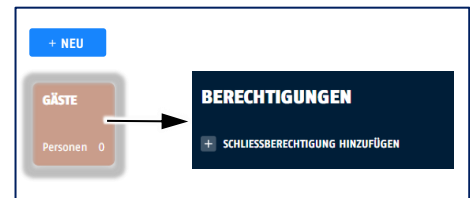


Gruppenberechtigung bearbeiten

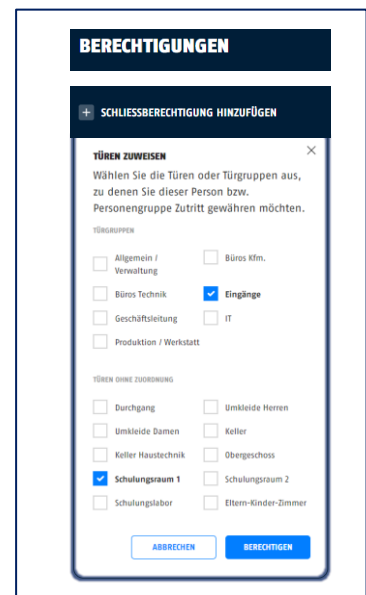
Zum Bearbeiten der Gruppenberechtigung klappen Sie das Menü Berechtigungen auf.

Hier sehen Sie die aktuell erteilten Zutrittsberechtigungen für Türgruppen, einzelne Türen – mit oder ohne Zeitpläne.

Die Ansicht variiert, je nachdem, ob der Gruppe schon Berechtigungen erteilt wurden oder nicht.

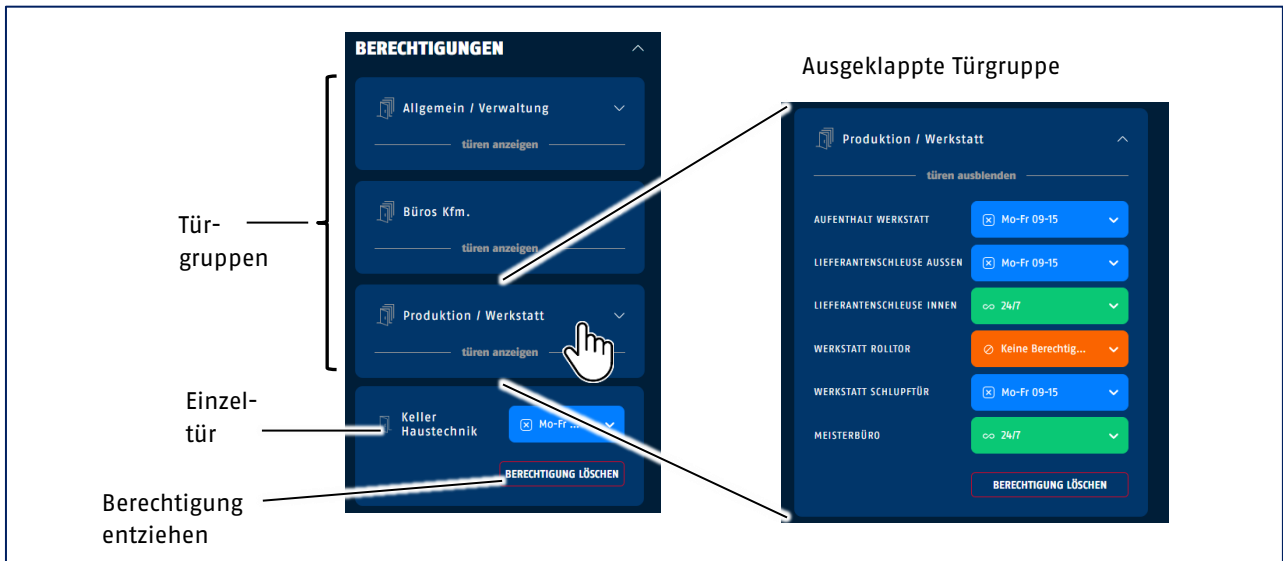


Sie können Zutrittsberechtigungen hinzufügen, ohne in die Sicht Schließplan zu wechseln.

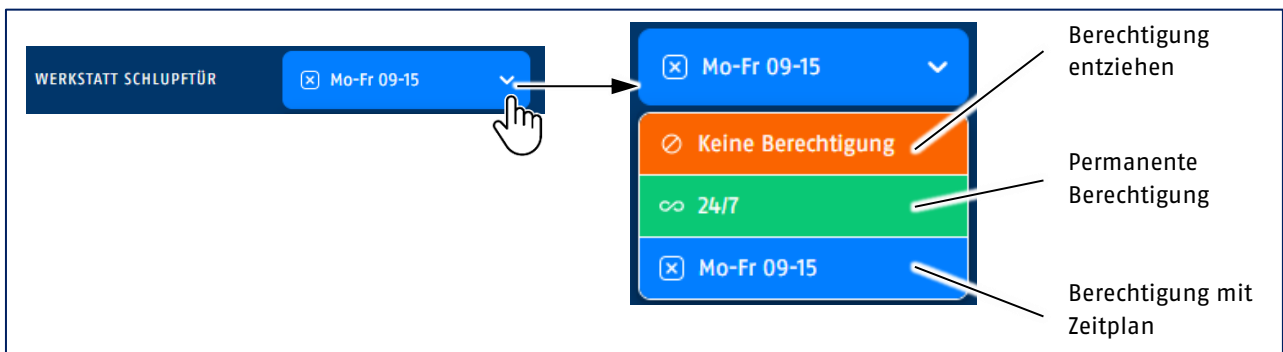


Wenn der Personengruppe bereits Berechtigungen erteilt wurden, erscheint beim Ausklappen eine Liste mit den zugewiesenen Türgruppen und Einzeltüren.

Türgruppen klappen beim Anklicken aus und die Berechtigungen der Einzeltüren werden sichtbar.



Sie können für jede Tür die Berechtigung permanent oder innerhalb eines Zeitplans zuweisen oder eine erteilte Berechtigung wieder entziehen.



9.4. Personen

Personen werden in der Personenliste angezeigt.

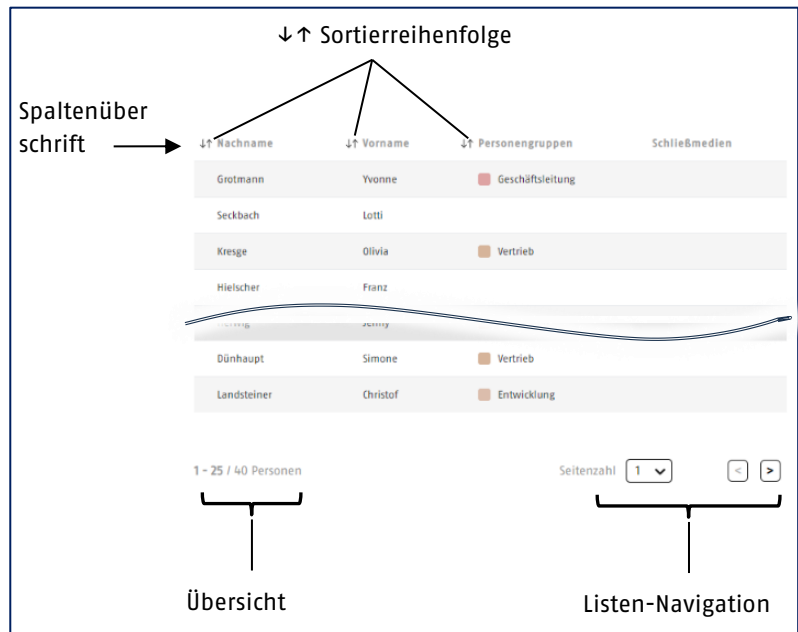
In der Liste enthalten sind

- Nachname,
- Vorname,
- die zugeordnete Personengruppe und
- die zugewiesenen Schließmedien.

Personen sortieren

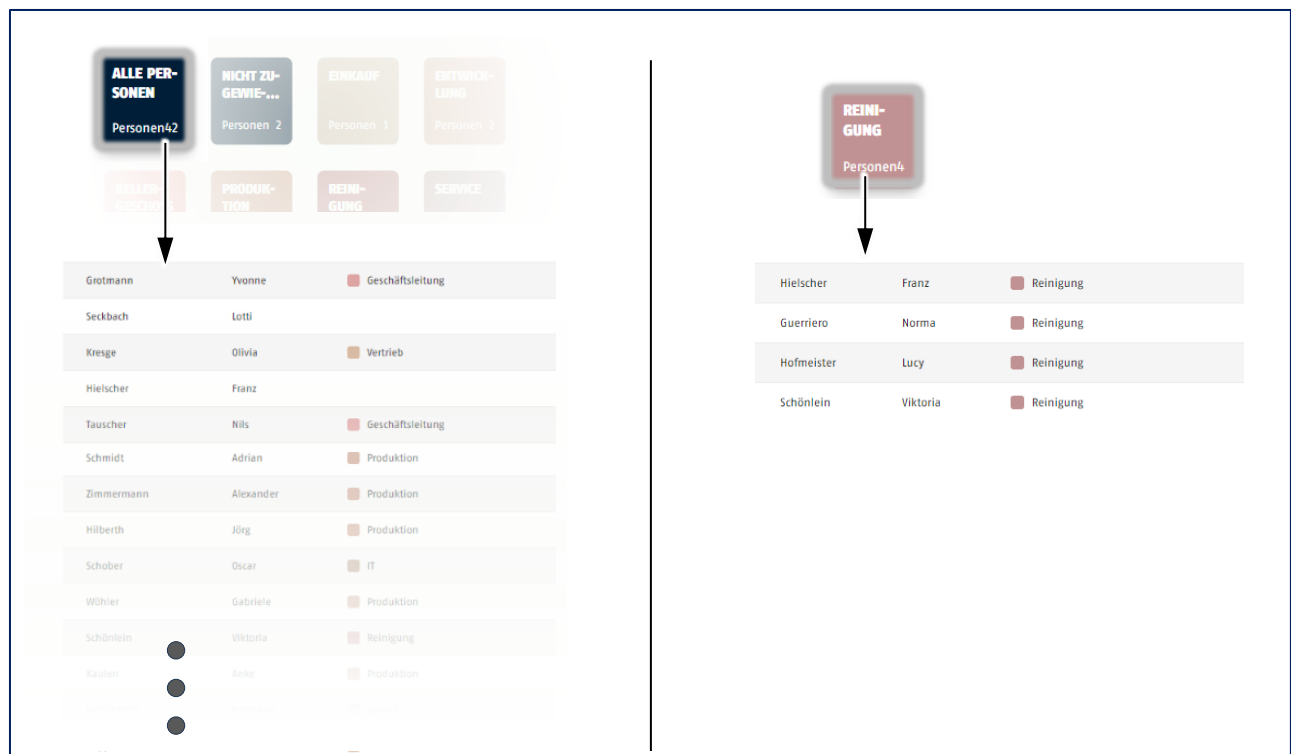
Sortieren Sie Personen, indem Sie auf die entsprechende Spaltenüberschrift klicken. Die Sortierung wird angezeigt und wechselt bei jedem Mausklick.

- ↓↑ in der Reihenfolge der Eingabe
- ↓↑ alphabetisch aufsteigend sortiert 0...9 / A...Z
- ↓↑ alphabetisch absteigend sortiert Z...A / 9...0



Angezeigte Personen einschränken

Schränken Sie die Anzeige auf eine Personengruppe ein, indem Sie die entsprechende Kachel anklicken.



9.5. Eigenschaften von Personen

Neue Person hinzufügen

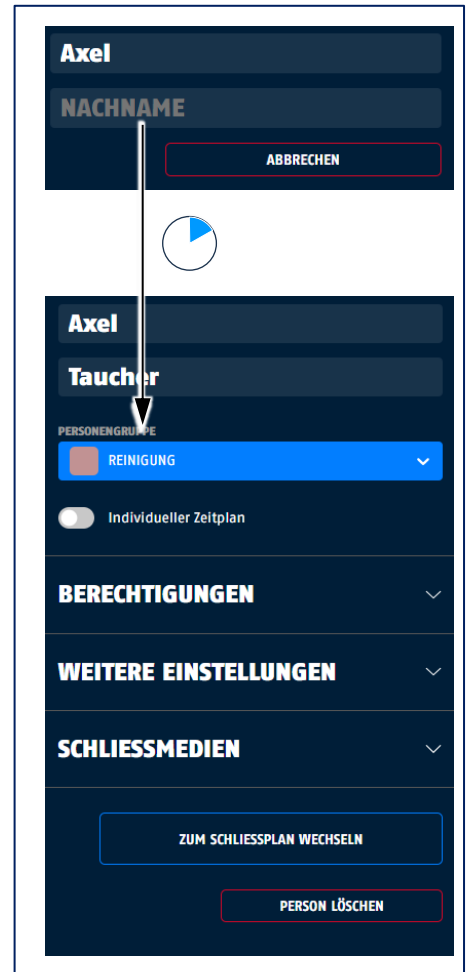
Fügen Sie eine neue Person hinzu, indem Sie über der Personenliste auf die Schaltfläche „+ NEU“ klicken.

Im Editierbereich können Sie einen Vornamen und einen Nachnamen eingeben. Die Eingabe wird automatisch übernommen, wenn die Zutrittskontrollzentrale einen Nachnamen erkannt hat. Sobald die Eingabe übernommen wurde, werden weitere Eingabemöglichkeiten zur Verfügung gestellt.

Sie können die Eigenschaften von Personen jederzeit bearbeiten.

Personenname bearbeiten

Sie bearbeiten Personennamen, indem Sie die Einfügemarke in das Fenster setzen und Ihre Änderungen vornehmen.

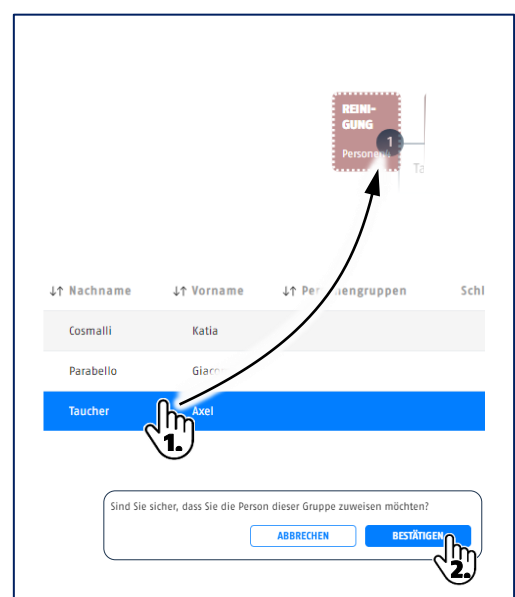


Personengruppe zuweisen

Beim Zuweisen einer Personengruppe erhält die Person die Zutrittsberechtigungen, die für die Gruppe eingestellt sind. Bereits vorhandene individuelle Berechtigungen müssen ggf. neu gesetzt werden.

Personengruppen können auf unterschiedliche Weise zugewiesen werden.

- Wählen Sie vor dem Anlegen der neuen Person eine Personengruppe aus
- oder
- Klappen Sie im Editierbereich die Liste „Personengruppe“ aus und weisen Sie die gewünschte Personengruppe zu
- oder
- Ziehen Sie die Person aus der Personenliste via Drag'n'Drop auf die gewünschte Personengruppe.



Individuellen Zeitplan hinzufügen

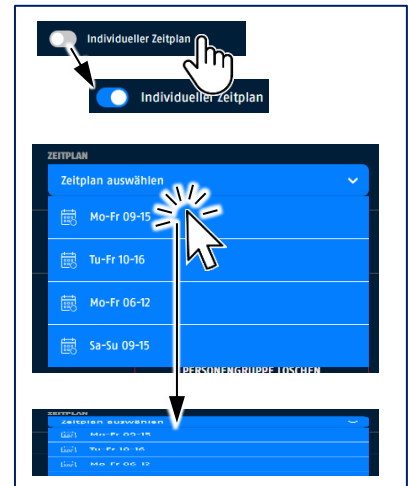
Weisen Sie der Person einen vorher definierten Zeitplan zu:

- ▶ Betätigen Sie den Schalter „Individueller Zeitplan“.

Das Listenfeld „Zeitplan“ erscheint.

- ▶ Klappen Sie die Liste „Zeitpläne“ auf und klicken den gewünschten Zeitplan an.

Wenn der benötigte Zeitplan noch nicht existiert, erstellen Sie ihn in der Sicht Zeitpläne.

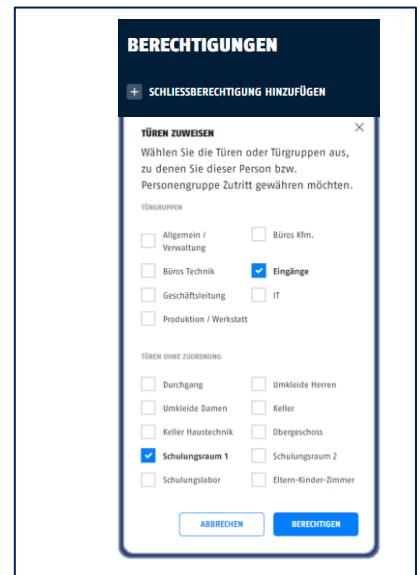


Individuelle Berechtigungen ändern

Zum Bearbeiten der Zutrittsberechtigungen für eine individuelle Person klappen Sie das Menü Berechtigungen aus.

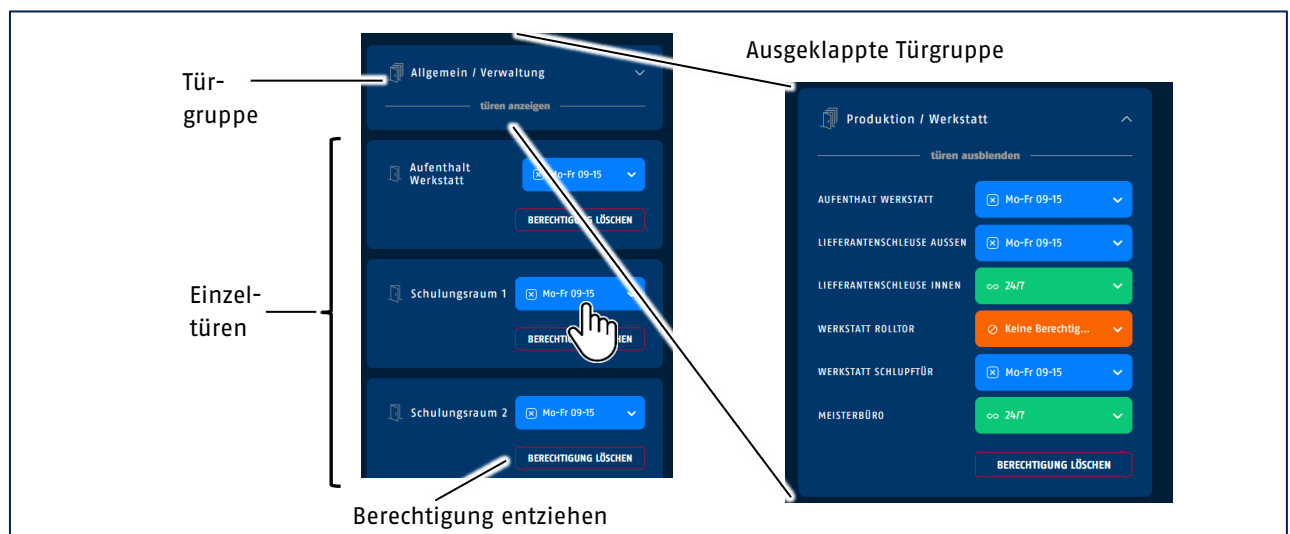
Hier sehen Sie die aktuell erteilten Zutrittsberechtigungen und einen eventuell ausgewählten Zeitplan für die Person. Die Ansicht variiert, je nachdem, ob der Person bereits Berechtigungen erteilt wurden oder nicht. Ist die Person einer Personengruppe zugewiesen, so sind die Gruppenberechtigungen hier schon vererbt worden.

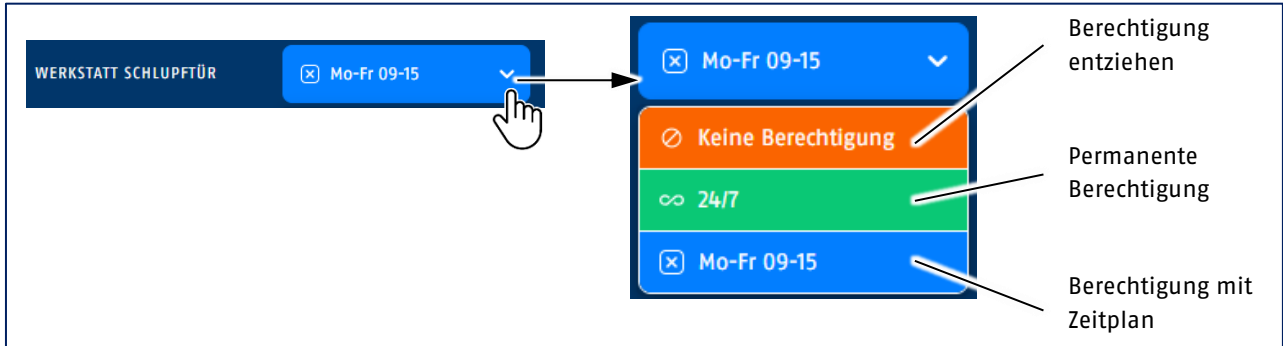
Mit dem Befehl „+ Schließberechtigung hinzufügen“ können Sie unmittelbar Zutrittsberechtigungen hinzufügen, ohne in die Sicht Schließplan zu wechseln.



Wenn der Person bereits Berechtigungen erteilt wurden, erscheint eine Liste mit den zugewiesenen Türgruppen und Einzeltüren.

Türgruppen klappen beim Anklicken aus und die Berechtigungen der Einzeltüren werden sichtbar.





Bemerkungen zur Person notieren

Für Notizen zur Person steht das Feld „Beschreibung“ zur Verfügung.

- ▶ Klappen Sie das Menü „Weitere Einstellungen“ auf.
- ▶ Tragen Sie Ihre Notizen im Feld „Beschreibung“ ein (max. 250 Zeichen).



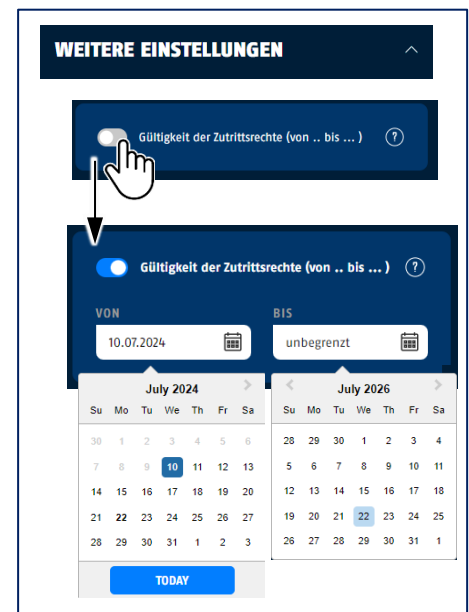
Gültigkeit der Zutrittsrechte begrenzen

Die Gültigkeit der Zutrittsrechte kann den Zeitraum, in dem Zutrittsberechtigung für eine Person auf dem Schließmedium erteilt werden, begrenzen.

Wird kein Enddatum gesetzt, ist die Gültigkeit für die Person nicht eingeschränkt, z. B. für festangestellte Mitarbeiter.

Bei vorübergehender Gültigkeit, z. B. bei Besuchern oder Praktikanten können Beginn und Ende der Gültigkeit eingestellt werden.

- ▶ Klappen Sie das Menü „Weitere Einstellungen“ auf.
- ▶ Betätigen Sie den Schalter „Gültigkeit der Zutrittsrechte“.
- ▶ Tragen Sie Beginn und – falls zutreffend – Ende der Gültigkeit ein.



Gültigkeitsintervall des Schließmediums festlegen

Legen Sie die Gültigkeit des Schließmediums abweichend von der globalen Einstellung (siehe → Kapitel Systemkonfiguration) fest.

Die Gültigkeit des TECTIQ Schließmediums ist in der Regel zeitlich begrenzt und muss spätestens nach Ablauf des Gültigkeitsintervalls an einem Update Terminal verlängert werden.

- ▶ Klappen Sie das Menü „Weitere Einstellungen“ auf.
- ▶ Klappen Sie das Listenfeld „Gültigkeit des Schließmediums“ auf und wählen Sie das gewünschte Zeitintervall.



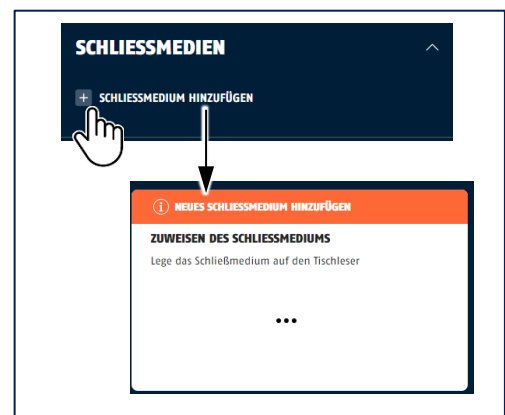
In der Regel sollte die Gültigkeit eines Schließmediums auf einen möglichst kurzen Zeitraum begrenzt werden, z. B. um bei Verlust eines Schließmediums den unbefugten Zutritt zu unterbinden.

9.6. Schließmedium hinzufügen

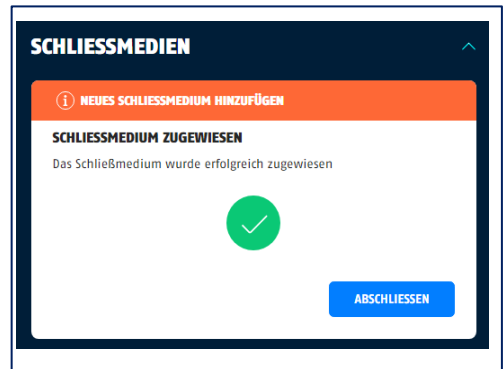
Wenn Anlagendaten und Personendaten feststehen, können den Personen Schließmedien hinzugefügt werden. Schließmedien werden immer physisch hinzugefügt. Sie benötigen hierzu

- den PC mit TECTIQ Access Manager,
- einen TECTIQ Tischleser und
- das Schließmedium.

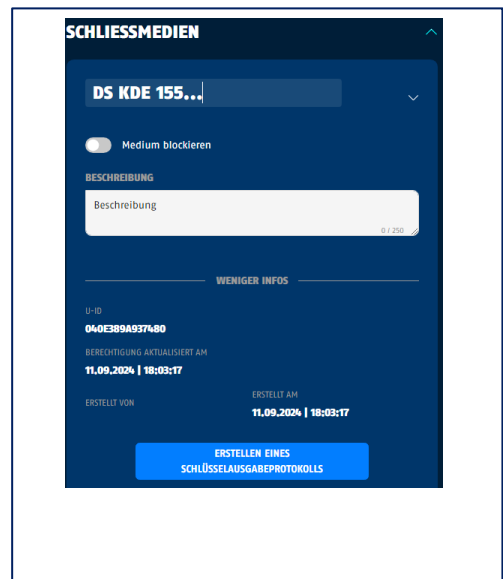
- ▶ Klappen Sie das Menü „Schließmedien“ auf.
- ▶ Klicken Sie auf den Befehl „Schließmedium hinzufügen“.
- ▶ Legen Sie das Schließmedium auf den Tischleser und warten Sie, bis alle Daten auf das Schließmedium geschrieben sind.



- ▶ Nach erfolgreicher Zuweisung schließen Sie den Vorgang mit einem Klick auf den Button „Abschliessen“ ab.



- ▶ Geben Sie dem Schließmedium einen Namen.
- ▶ Erstellen Sie unter dem Menüpunkt „Mehr Infos / Weniger Infos“ das Schlüsselausgabeprotokoll.




10. Sicht Türen | Doors

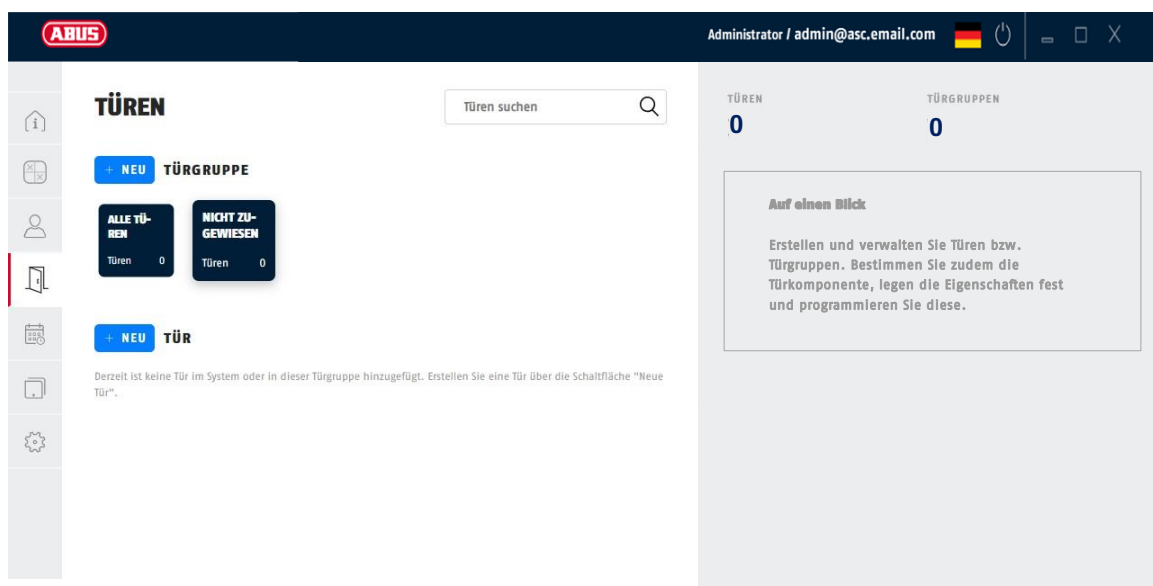
Inhalt

- 10.1. Übersicht
- 10.2. Türgruppen
- 10.3. Türen
- 10.4. Eigenschaften von Türen
- 10.5. Daten in Türkomponente herunterladen

10.1. Übersicht

In der Sicht Türen erstellen und verwalten Sie Türen und Türkomponenten in der TECTIQ Schließanlage. Türen werden einfach und komfortabel Bezeichnungen zugewiesen. Zur besseren Orientierung fassen Sie Türen in Türgruppen zusammen. Wählen Sie nach dem Anlegen einer Tür die Türkomponente aus, die an der Tür installiert ist – Schließzylinder, Beschlag oder Wandleser.

Sie erreichen die Sicht Türen über die Schaltfläche  .



TÜREN

Administrator / admin@asc.email.com

Türen suchen

TÜREN 34 TÜRGRUPPEN 7

+ NEU TÜRGRUPPE

- ALLE TÜREN: Türen 34
- NICHT ZUGEWIESEN: Türen 10
- ALLGEMEIN / VERWALT...: Türen 9
- BÜROS KFM...: Türen 1
- BÜROS TECHNIK: Türen 3
- EINGÄNGE: Türen 2
- GESCHÄFTSLEITUNG: Türen 1
- IT: Türen 2
- PRODUKTION / WER...: Türen 6

+ NEU TÜR

Name	Typ	Türgruppen
Besprechung 1	Beschlag	Allgemein / Verwaltung
Teeküche	Beschlag	Allgemein / Verwaltung
Büro 1: Verwaltung	Beschlag	Büros Kfm.
Durchgang		
Aufzug	Zylinder	Allgemein / Verwaltung
GF-Büro	Zylinder	Geschäftsleitung
Lager Empfang	Beschlag	Allgemein / Verwaltung

+ NEU Neue Tür oder Neue Türgruppe hinzufügen

Anzahl Türen + Türgruppen

10.2. Türgruppen

Türgruppen erleichtern die Verwaltung und den Umgang mit einer Schließanlage. Personen können gesammelt die Zutrittsberechtigungen für komplette Türgruppen erteilt oder entzogen werden.

Im oberen Teil der Sicht Türen sind die Türgruppen als Kacheln mit ihrem Namen und der Anzahl der zugeordneten Türen dargestellt.

Name der Türgruppe

Anzahl der Türen

Immer vorhanden sind die Kacheln „Alle Türen“ und „Nicht zugewiesen“.

Eine Türgruppe wird durch Anklicken ausgewählt. Die ausgewählte Türgruppe wird hervorgehoben dargestellt.

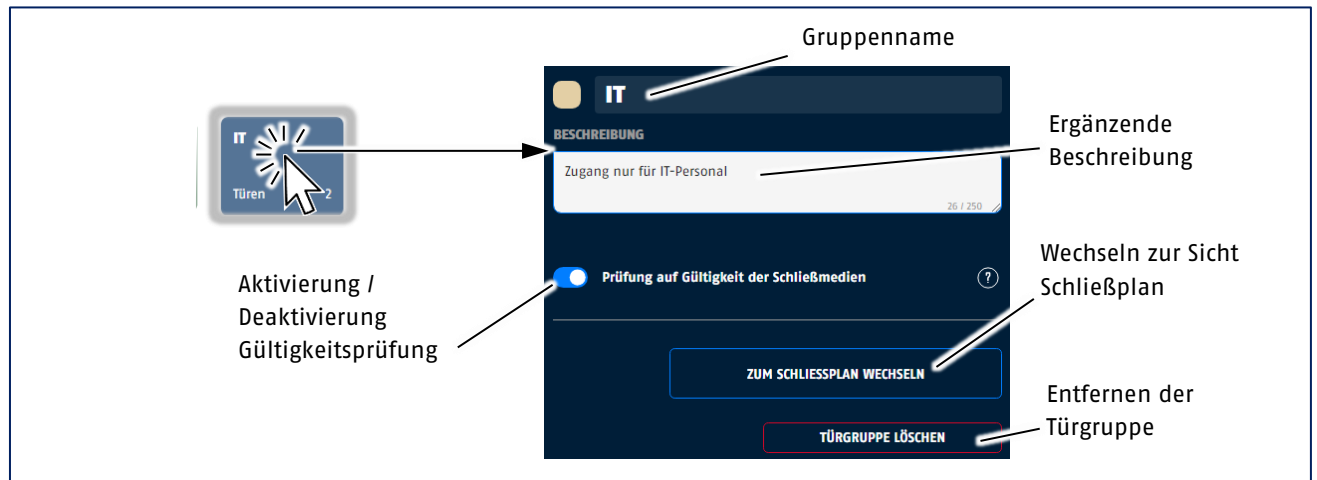
Nach Auswahl einer Türgruppe werden in der Türenliste die enthaltenen Türen angezeigt.

– Immer vorhanden –

- ALLE TÜREN: Türen 34 (Registrierte Türen in der Anlage)
- NICHT ZUGEWIESEN: Türen 10 (Türen ohne Gruppenzuweisung)
- ALLGEMEIN / VERWALTUNG: Türen 9 (Ausgewählte Türgruppe)
- BÜROS KFM.: Türen 1

Gruppenname bearbeiten

Sie bearbeiten Namen für die Türgruppe, indem Sie die Einfügemarke in das Fenster setzen und Ihre Änderungen vornehmen. Eingaben werden automatisch übernommen, wenn die Zutrittskontrollzentrale eine plausible Bezeichnung erkannt hat. Die Einstellungen können jederzeit bearbeitet werden.



Gültigkeitsprüfung deaktivieren

Sie können für eine Türgruppe die Gültigkeitsprüfung für Schließmedien deaktivieren. Hiermit können Sie Bereiche für den Zutritt für alle Personen, die über ein Schließmedium verfügen, ohne vorherige Validierung der Gültigkeit freigeben. Dies kann z.B. an Schranken zum Parkplatz oder für Türen zu einem Raum mit Updateterminal sinnvoll sein.

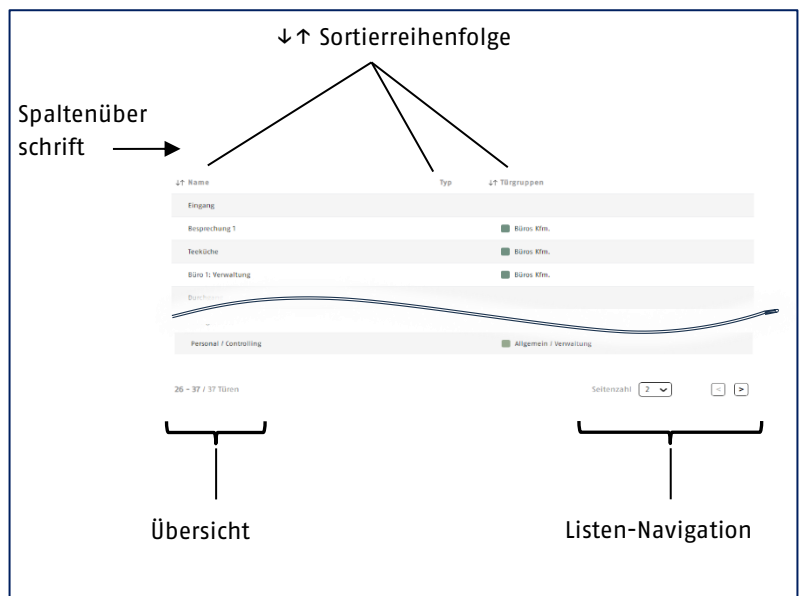
10.3. Türen

Türen werden in der Türliste angezeigt. In der Liste enthalten sind

- Bezeichnung der Tür
- die an der Tür montierte Türkomponente
- die zugeordnete Türgruppe.

Türen sortieren

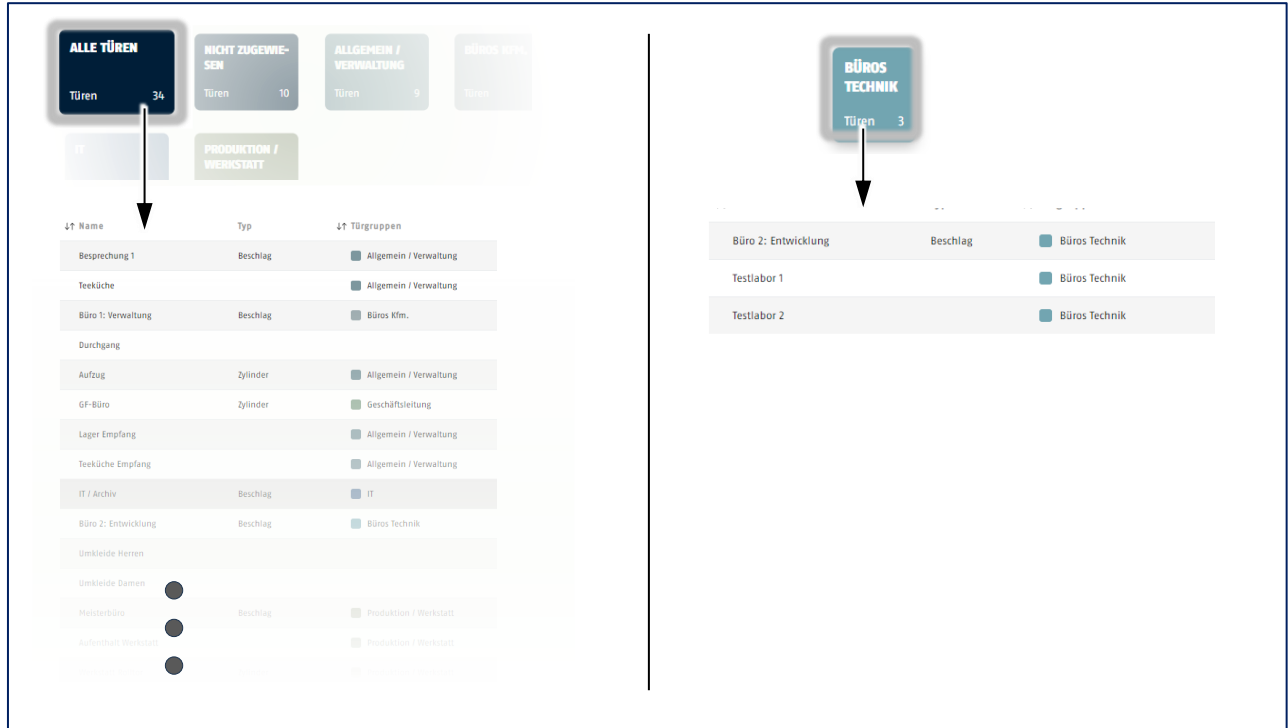
Sortieren Sie Türen, indem Sie auf die entsprechende Spaltenüberschrift klicken. Die Sortierung wird angezeigt und wechselt bei jedem Mausklick.



- ↓↑ in der Reihenfolge der Eingabe
- ↓↑ alphabetisch aufsteigend sortiert 0...9 / A...Z
- ↓↑ alphabetisch absteigend sortiert Z...A / 9...0

Angezeigte Türen einschränken

Schränken Sie die Anzeige auf eine Türgruppe ein, indem Sie die entsprechende Kachel anklicken.



10.4. Eigenschaften von Türen

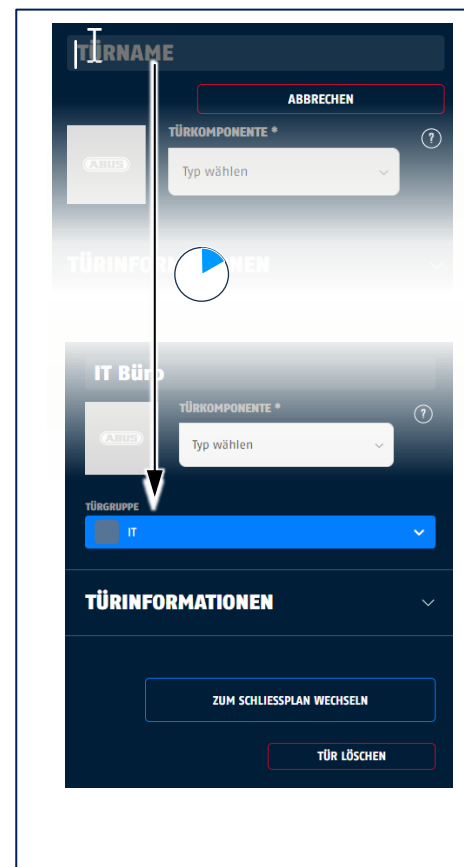
Neue Tür hinzufügen

Fügen Sie eine Tür hinzu, indem Sie über der Türliste auf die Schaltfläche „+ NEU“ klicken.

Im Editierbereich können Sie eine Türbezeichnung angeben. Die Eingabe wird automatisch übernommen, wenn die Zutrittskontrollzentrale eine plausible Bezeichnung erkannt hat. Sobald die Eingabe übernommen wurde, werden weitere Eingabemöglichkeiten zur Verfügung gestellt. Sie können die Türeigenschaften jederzeit bearbeiten.

Türname bearbeiten

Sie bearbeiten den Türnamen, indem Sie die Einfügemarke in das Fenster setzen und Ihre Änderungen vornehmen.

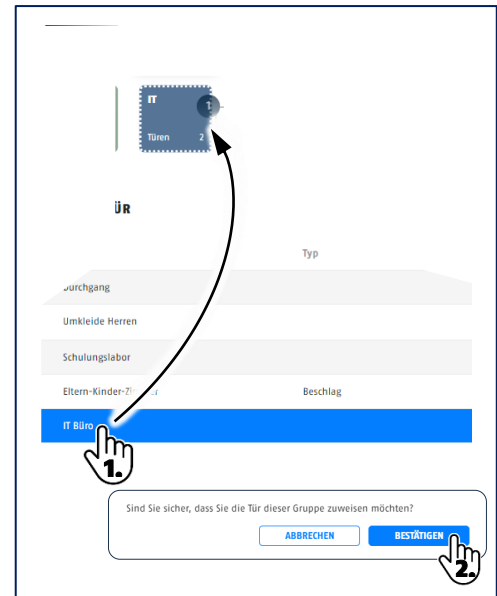


Türgruppe zuweisen

Türgruppen können auf unterschiedliche Weise zugewiesen werden:

- Wählen Sie vor dem Anlegen der neuen Tür eine Türgruppe aus oder
- klappen Sie im Editierbereich die Liste „Türgruppe“ aus und weisen Sie die gewünschte Türgruppe zu oder
- ziehen Sie die Tür aus der Türliste via Drag'n'Drop auf die gewünschte Türgruppe.

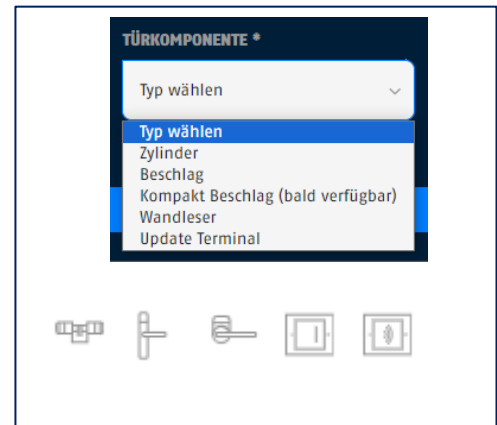
Nach Zuweisen zu einer Türgruppe muss die Türkomponente neu programmiert werden.



Türkomponente wählen

Wählen Sie die Türkomponente, die an der Tür montiert wird.

- ▶ Für einen elektronischen Schließzylinder wählen Sie den Eintrag: „Zylinder“.
- ▶ Für einen elektronischen Beschlag wählen Sie den Eintrag: „Beschlag“.
- ▶ Für einen elektronischen Kompaktbeschlag (nur für Innentüren) wählen Sie den Eintrag: „Kompakt Beschlag“.
- ▶ Für einen Offline Wandler wählen Sie den Eintrag: „Wandler“.
- ▶ Für ein Online Update Terminal wählen Sie den Eintrag: „Update Terminal“.

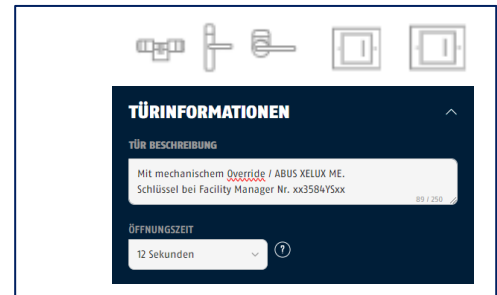


Beachten Sie:

- Für einen elektronischen Schließzylinder mit beidseitigem Leser planen Sie zwei Schließzylinder – für die Innenseite und die Außenseite der Tür.
- Für einen zweiseitigen Wandler – das ist ein offline-Steuergerät, welches eine Tür (Türschließer oder Türantrieb) mit zwei angeschlossenen Wandlern ansteuert – planen Sie zwei Wandler.
- Ein Online Update Terminal mit angeschlossener Tür planen Sie zunächst als Systemkomponente. Anschließend planen Sie das Gerät für die Zutrittskontrolle zusätzlich als „Tür“ (bei zwei angeschlossenen Wandlern ebenfalls zweimal).
- Bei Zurücksetzen des Wandlers (online oder offline) wird die Relaiskonfiguration auf die Default Einstellung „NO“ zurückgestellt.

Eigenschaften für Türkomponenten einstellen

Je nach Art der Türkomponente stehen unterschiedliche Eigenschaften zur Verfügung.



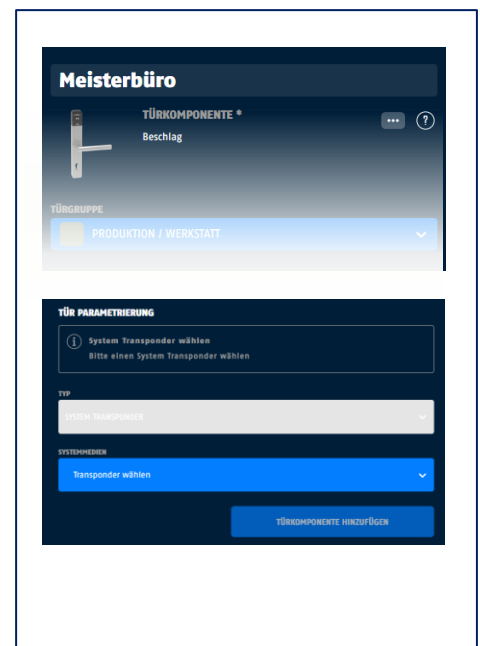
Zylinder, Vorhangschloss	Beschlag	Wandleser	Update Terminal
Türbeschreibung max. 250 Zeichen	Türbeschreibung max. 250 Zeichen	Türbeschreibung max. 250 Zeichen	Türbeschreibung max. 250 Zeichen
Öffnungszeit 6 Sekunden 12 Sekunden	Öffnungszeit 6 Sekunden 12 Sekunden	–	–
–	–	Relais-Konfiguration NO-imp: Schließer-Impuls NC-imp: Öffner-Impuls NO: Schließer (permanent) NC: Öffner (permanent)	Relais-Konfiguration NO-imp: Schließer-Impuls NC-imp: Öffner-Impuls NO: Schließer (permanent) NC: Öffner (permanent)
–	–	Zeitraum 1, 2, 4, 6, 8, 12 Sekunden	Zeitraum 1, 2, 4, 6, 8, 12 Sekunden
–	–	–	Akustische Signalisierung Ein / aus

10.5. Daten in Türkomponente herunterladen

Geänderte Konfigurationsdaten müssen in die Türkomponente geladen werden.

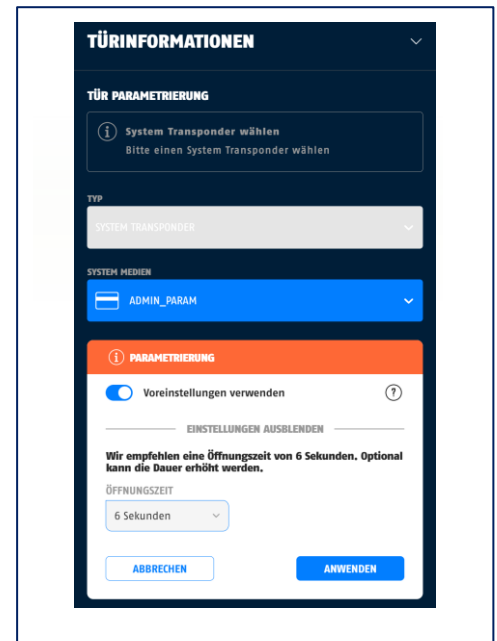
Sie benötigen hierzu:

- eine Parameterkarte, die mit den Anlagendaten initialisiert ist, siehe → Kapitel Systemmedien.
 - einen USB-Tischleser, der an den lokalen PC angeschlossen ist.
- ▷ Wählen Sie in der Sicht Türen die Tür aus.
 - ▷ Wählen Sie im Editierbereich den Systemtransponder-Typ „Parameterkarte“.
 - ▷ Wählen Sie aus der Liste „Systemmedien“ Ihre Parameterkarte aus.
 - ▷ Betätigen Sie die Schaltfläche „Türkomponente hinzufügen“.



- Sie können jetzt die Öffnungszeit der Türkomponente einstellen oder die Voreinstellung wählen.
- ▷ Betätigen Sie die Schaltfläche „Anwenden“
- ▷ Legen Sie die Parameterkarte nach Aufforderung auf den Tischleser. Der Schreibvorgang wird als blinkendes LED-Signal angezeigt. Warten Sie, bis die Tischleser-LED den Vorgang abgeschlossen meldet.
- ▷ Präsentieren Sie innerhalb von 15 min die Parameterkarte an der Türkomponente. Warten Sie, bis die LED an der Türkomponente grün leuchtet.

Beachten Sie: Der Vorgang ist erst abgeschlossen, wenn Sie die Parameterkarte erneut am Tischleser präsentieren und die LED am Tischleser grün leuchtet.



11. Sicht Zeitpläne | Schedules

Inhalt

- 11.1. Übersicht
- 11.2. Zeitplan hinzufügen
- 11.3. Zeitplan bearbeiten
- 11.4. Zeitplan löschen
- 11.5. Zeitplan verwenden

11.1. Übersicht

In der Sicht Zeitpläne organisieren Sie die Zutrittsrechte zusätzlich, z.B. entsprechend der individuellen Arbeitszeit oder der Öffnungszeiten von Objekten mit Kundenverkehr. Hier legen Sie auch Sperrtage fest für betriebsfreie Zeiten wie Feiertage oder Betriebsferien.

Sie erreichen die Sicht Zeitpläne über die Schaltfläche .

Verwalten mehrerer Zeitpläne

Administrator / admin@asc.email.com

ZEITPLÄNE

+ NEU ZEITPLAN

Zeitplan Name

Mo-Fr 09-15

Tu-Fr 10-16

Mo-Fr 06-12

Sa-Su 09-15

Mo Di Mi Do Fr Sa So

Mo Di Mi Do Fr Sa So

Mo Di Mi Do Fr Sa So

Mo Di Mi Do Fr Sa So

Mo Di Mi Do Fr Sa So

+ NEU

MONTAGDIENSTAGMITTWOCHDONNERSTAGFREITAGSAMSTAGSONNTAG

0						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						

Sperrtage

< JULI 2024 >

MO	DI	MI	DO	FR	SA	SO
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Verwalten von Sperrtagen

+ NEU

Neuen Zeitplan anlegen

Schaltfläche
Zeitpläne

Wochenkalender
für
Zeitpläne

11.2. Zeitplan hinzufügen

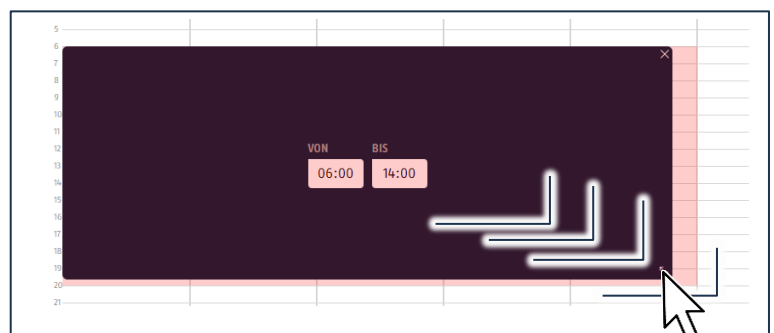
- ▶ Fügen Sie einen neuen Zeitplan hinzu, indem Sie die Schaltfläche „+ NEU“ betätigen. Für den neuen Zeitplan wird eine neue Kachel angezeigt und im Arbeitsbereich wird ein Block für ein Zeitintervall vorgeschlagen.
- ▶ Setzen Sie den Mauszeiger in das Namen-Feld und tragen Sie eine passende Bezeichnung für den Zeitplan ein. Diese Bezeichnung wird Ihnen beim Verwenden von Zeitplänen für Personen und Personengruppen angeboten. Gleiche Bezeichnungen sind dabei nicht zulässig.



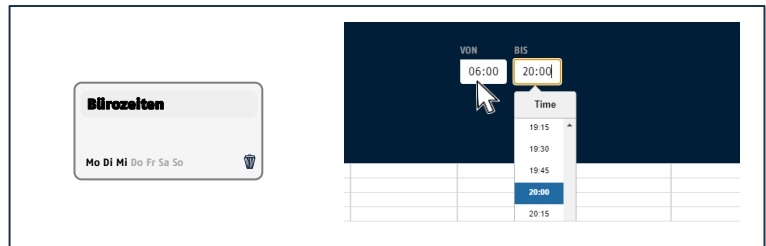
Zeitintervall einstellen

Ein Zeitintervall umfasst eine Anfangszeit und eine Endzeit und ist für mehrere aneinandergrenzende Wochentage gültig.

- ▶ Verschieben Sie den Block im Wochenplan, bis die linke obere Ecke mit dem gewünschten Wochentag und der Anfangszeit übereinstimmt.
- ▶ Ziehen Sie anschließend die rechte untere Ecke des Blocks, bis sie mit der gewünschten Endzeit und dem passenden Wochentag übereinstimmt.



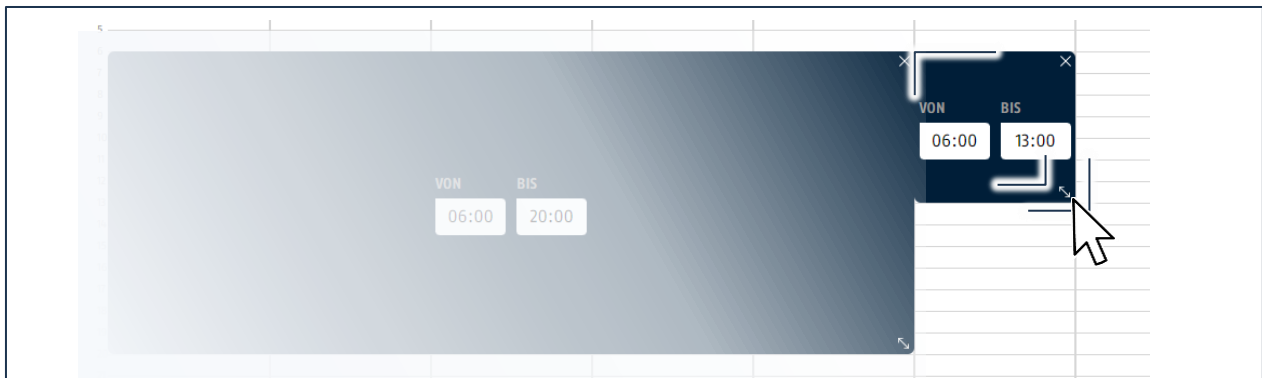
- ▶ Alternativ dazu setzen Sie den Mauszeiger in das Eingabefeld und tragen die Uhrzeit manuell ein.



Zeitintervall hinzufügen

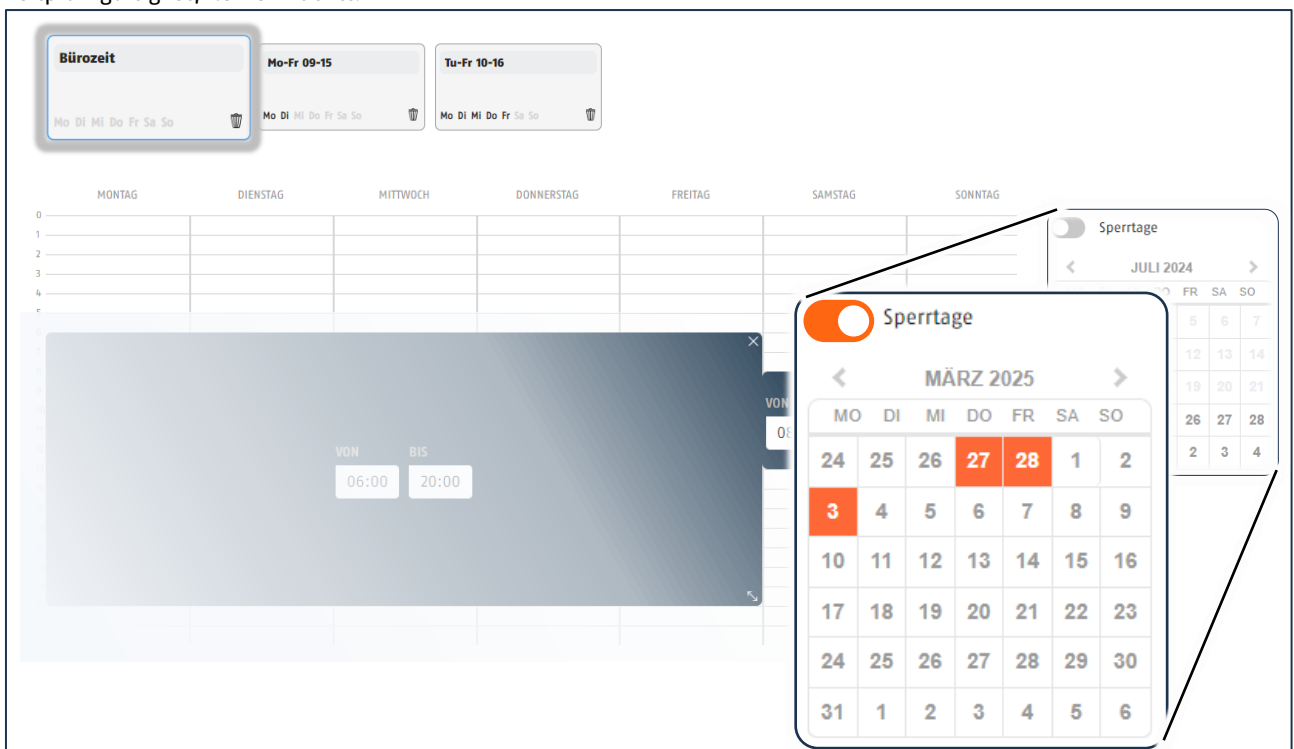
Jeder Zeitplan kann bis zu 15 einzelne Zeitintervalle enthalten.

- ▶ Fügen Sie weitere Zeitintervalle hinzu, indem Sie in den Wochenplan klicken und einen Bereich in der gewünschten Größe aufziehen.



Sperrtage zu einem Zeitplan hinzufügen

Für jeden Zeitplan können Sie Sperrtage einrichten. An den eingetragenen Sperrtagen haben die Personen, für die der Zeitplan gültig ist, keinen Zutritt.



- ▷ Wählen Sie den gewünschten Zeitplan aus.
- ▷ Betätigen Sie den Schalter „Sperrtage“.
- ▷ Wählen Sie in der Kalenderansicht mit den Schaltflächen </> den gewünschten Monat aus.
- ▷ Klicken Sie auf das gewünschte Datum.

Die aktiven Sperrtage werden rot angezeigt. Je Zeitplan können bis zu 30 Sperrtage gesetzt werden.

11.3. Zeitplan bearbeiten

Alle Einstellungen eines Zeitplans können jederzeit verändert werden:

- Wochentag
- Anfangs- und Endzeit
- Name des Zeitplans

Zeitintervall löschen

- ▷ Löschen Sie ein Zeitintervall in einem Zeitplan, indem Sie auf die rechte obere Ecke klicken.



Beachten Sie: Änderungen in Zeitplänen, die bereits Personen oder Personengruppen zugewiesen wurden, werden erst nach der nächsten Validierung des Schließmediums am Update Terminal oder am Tischleser wirksam.

11.4. Zeitplan löschen

Ein Zeitplan kann gelöscht werden.

- ▷ Weisen Sie allen Personen und Personengruppen, die den Zeitplan, der gelöscht werden soll, verwenden einen anderen Zeitplan zu.
- ▷ Löschen Sie den Zeitplan, indem Sie auf das Löschen-Symbol in der entsprechenden Kachel klicken, und beantworten Sie die Sicherheitsabfrage.
- ▷ Ist einer Person oder einer Personengruppe kein Zeitplan zugeordnet, gilt die permanente Zutrittsberechtigung „24/7“.



11.5. Zeitplan verwenden

Sie können Zeitpläne auf verschiedene Weise verwenden:

- Uneingeschränkt für eine Personengruppe
- Für eine Personengruppe auf eine Türgruppe bezogen
- Für eine Personengruppe auf eine bestimmte Tür innerhalb einer Türgruppe bezogen

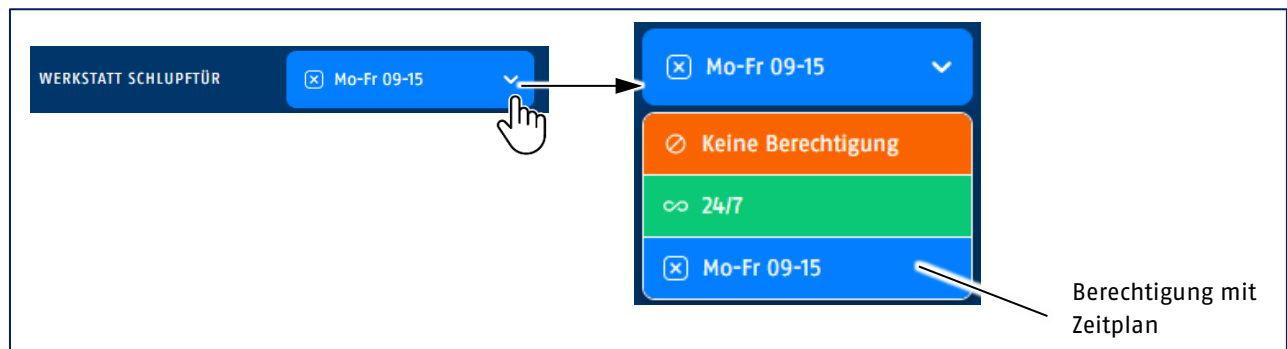
TECTIQ Referenzhandbuch.

11 Sicht Zeitpläne | Schedules

- Für eine Personengruppe auf eine einzelne Tür bezogen
- Uneingeschränkt für eine individuelle Person
- Für eine individuelle Person auf eine Türgruppe bezogen
- Für eine individuelle Person auf eine bestimmte Tür innerhalb einer Türgruppe bezogen
- Für eine individuelle Person auf eine einzelne Tür bezogen

Beachten Sie: Pro Person kann immer nur ein Zeitplan gültig sein.

► Verwenden Sie einen Zeitplan in der Sicht Personen und weisen den Zeitplan zu.



Nach Zuweisen eines Zeitplans muss das Schließmedium für die betroffenen Personen programmiert werden.


12. Sicht Systemkomponenten | Components

Inhalt

- 12.1. Übersicht
- 12.2. Online Update Terminal hinzufügen
- 12.3. Online Terminal mit Türsteuerung
- 12.4. USB-Tischleser

12.1. Übersicht

In der Sicht Systemkomponenten verwalten Sie die Online Update Terminals, an denen Personen ihre Zutrittsberechtigung aktualisieren. Die Systemkomponenten sind immer mit der TECTIQ Zutrittskontrollzentrale verbunden – entweder über das lokale Netzwerk oder über den Fernzugriff an einem anderen Standort.

Sie erreichen die Sicht Systemkomponenten über die Schaltfläche .

SYSTEMKOMPONENTEN

+ NEU KOMPONENTE

UPDATE TERMINAL HAUPTINGANG
Typ: Terminal

UPD VERWALTUNG
Typ: Terminal

UPD IT
Typ: Terminal

+ NEU Neue Systemkomponente anlegen

ÜBERSICHT

TERMINAL
3

Information: Auf einen Blick Systemkomponenten sind die Komponenten im System, die nicht direkt einem Zutritt an einer Tür zugeordnet werden. In erster Linie betrifft das Update Terminals, die Sie hier hinzufügen können. Standard...

[WEITERE INFORMATIONEN](#)



Anzahl Systemkomponenten

Die Systemkomponenten werden im Arbeitsbereich mit ihrem aktuellen Verbindungszustand angezeigt.

Bezeichnung — **HAUPTINGANG UPDT**

Art des Geräts — Typ: Terminal

Verbindungsstatus:

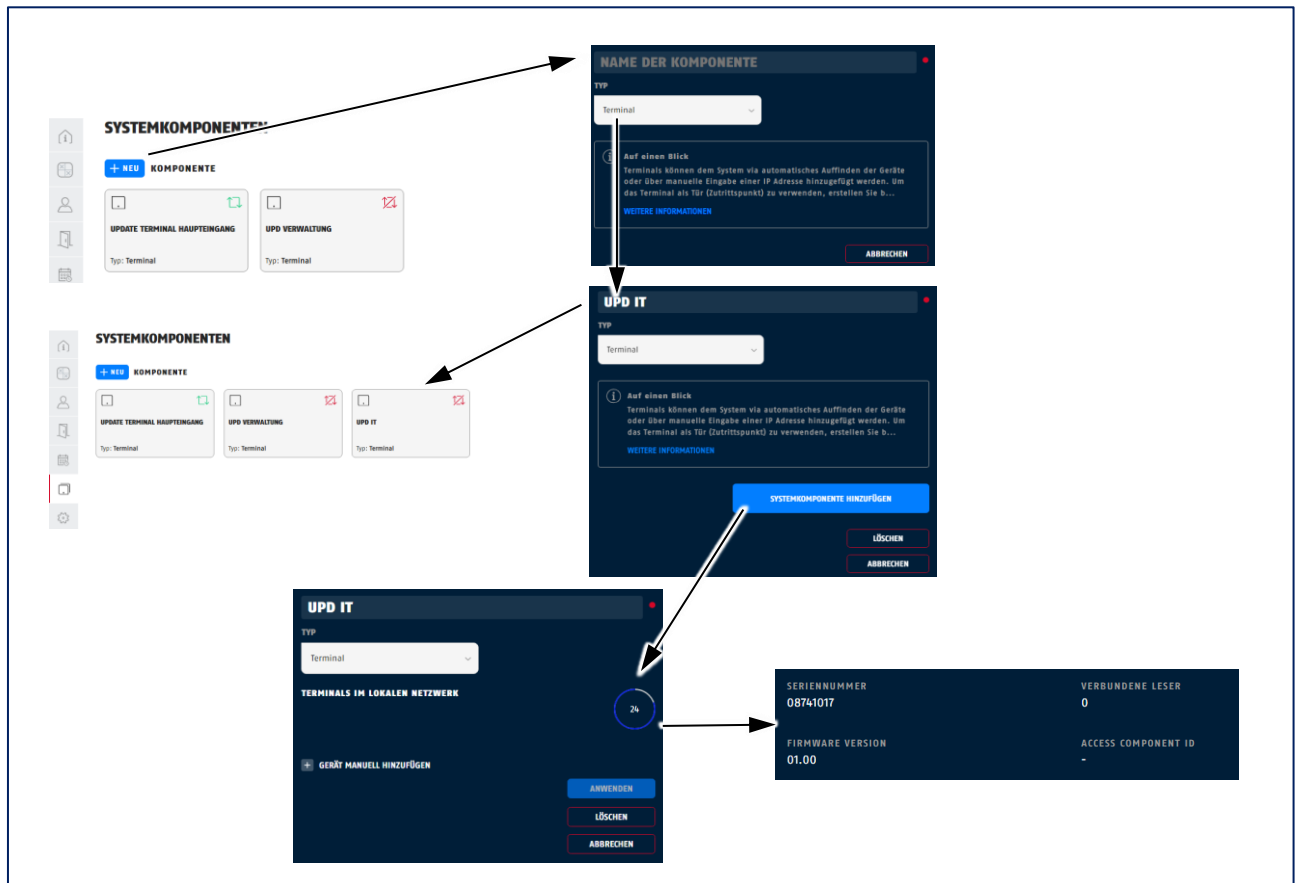
-  Verbunden
-  Nicht verbunden

12.2. Online Update Terminal hinzufügen

Fügen Sie für jedes in der Anlage installierte Terminal eine Systemkomponente hinzu:

- Betätigen Sie die Schaltfläche „+ NEU“.
- Geben Sie eine Bezeichnung für die Systemkomponente ein.

Die Eingabe wird automatisch übernommen. Die Systemkomponente wird in Form einer Kachel im Arbeitsbereich angezeigt.




Zur Ersteinrichtung des Online Terminals ist ein sogenannter Discovery-Service integriert, mit dem das Online Terminal automatisch erkannt wird. Voraussetzung ist, dass sich beide Komponenten innerhalb eines gemeinsamen lokalen Netzwerks befinden.

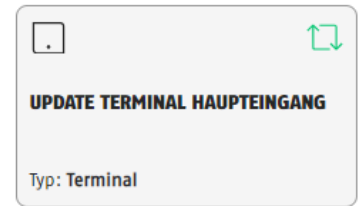
- Schließen Sie das Online-Terminal an das gleiche Netzwerk wie die Zutrittskontrollzentrale an.
- Starten Sie den Verbindungsvorgang mit der Zutrittskontrollzentrale. Betätigen Sie im Editierbereich die Schaltfläche „Systemkomponente hinzufügen“.

Die Zentrale startet einen Suchvorgang. Gefundene Terminals werden im Arbeitsbereich mit ihrer Seriennummer angezeigt.

- Betätigen Sie die Schaltfläche „Anwenden“ um das Online-Terminal zu verbinden. Das Online-Terminal erhält über DHCP automatisch eine Netzwerk-Adresse.

Die Zentrale verbindet sich mit dem Update Terminal und zeigt den Verbindungszustand „grün“ an.

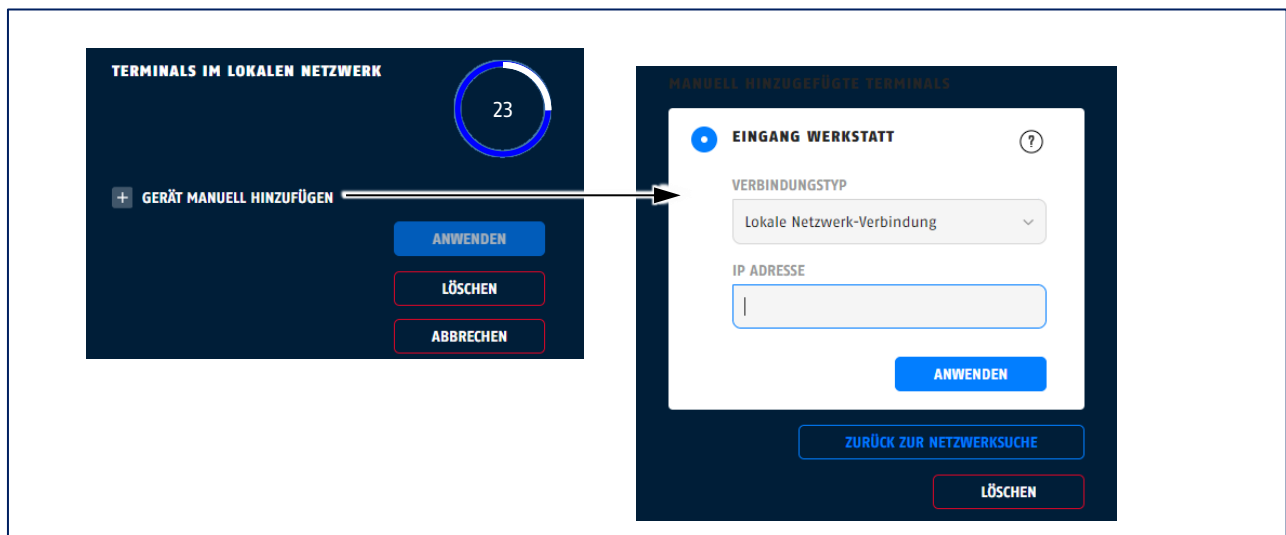
Wenn alle Update Terminals auf der Arbeitsfläche mit einem Gerät in der Anlage verbunden sind, zeigt an der Zentrale die LED  grünes Licht.



Wenn der Suchvorgang nicht erfolgreich ist, prüfen Sie im IP-Router, ob das Terminal im Netzwerk verfügbar ist. Stimmen Sie sich mit Ihrem IT-Administrator ab und vergeben Sie die IP-Adresse manuell.

- ▶ Wählen Sie den Befehl „Geräte manuell hinzufügen“.
- ▶ Wählen Sie im Listenfeld „Verbindungstyp“ den Eintrag „Lokale Netzwerk-Verbindung“.
- ▶ Tragen Sie im Feld „IP Adresse“ die IP-Adresse des Terminals ein und betätigen Sie die Schaltfläche „Anwenden“.

Sie können den Adressierungsvorgang mit der Schaltfläche „Zurück zur Netzwerksuche“ oder der Schaltfläche „Abbrechen“ beenden.



12.3. Online Terminal mit Türansteuerung

Ein Online Update Terminal kann alleine – als reines Update Terminal – verwendet werden, oder Sie können auch Türöffner, Türantriebe, Türkreuze und anderes mehr direkt ansteuern.

Im letzteren Fall erfüllt das Terminal zusätzlich die Aufgabe einer Offline Türkomponente und wird gesondert in der Sicht Türen angelegt.

- ▶ Legen Sie das Terminal als Systemkomponente an und nehmen Sie die Netzwerkverbindung in Betrieb.
- ▶ Planen Sie die an das Terminal angeschlossene Tür in der Sicht Türen.
- ▶ Wählen Sie als Türkomponente „Update Terminal“.
- ▶ Klappen Sie das Listenfeld „Terminal“ aus und wählen Sie das betreffende Update Terminal.

Vergeben Sie die Zutrittsberechtigungen in der Sicht Schließplan.

12.4. USB-Tischleser

Der TECTIQ Tischleser kann als Systemkomponente und Update Terminal verwendet werden.

- ▷ Schließen Sie den Tischleser an einen freien USB-Anschluss an dem PC, auf dem der TECTIQ Access Manager läuft, an.
- ▷ Starten Sie die Software TECTIQ Access Manager.
- ▷ Stellen Sie die Verbindung zwischen PC und der TECTIQ Zutrittskontrollzentrale her.
- ▷ Stellen Sie sicher, dass die Software in den Nutzungszeiten aktiv ist.

Bei der Nutzung des Tischlesers als Update Terminal sollten Sie sicherstellen, dass kein unbefugter Zugriff auf den PC und die Software erfolgen kann:

- Lassen Sie den PC nicht unbeaufsichtigt.
- oder
- Stellen Sie den Tischleser und den PC baulich getrennt auf, z. B. den Tischleser in einem Durchgangsbereich und den PC in einem separaten, angrenzenden Raum.

Der Tischleser wird nicht gesondert in der Anlage angezeigt.


13. Sicht Systemeinstellungen | Settings

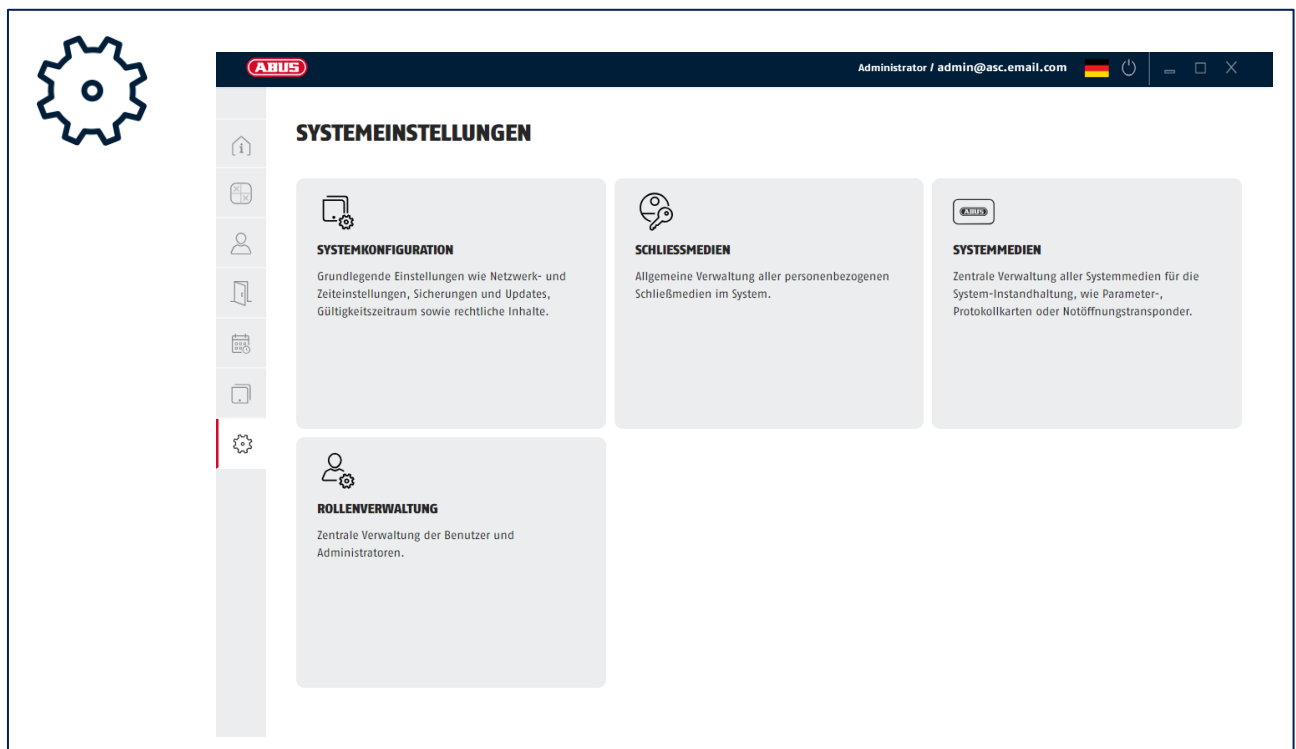
Inhalt

- 13.1. Übersicht Systemeinstellungen
- 13.2. Systemkonfiguration
 - 13.2.1. Systeminformationen
 - 13.2.2. Netzwerkeinstellungen
 - 13.2.3. Zeiteinstellungen
 - 13.2.4. Firmware-Update
 - 13.2.5. Datensicherung und Wiederherstellung
 - 13.2.6. Gültigkeit der Schließmedien
 - 13.2.7. Datenschutz und rechtliche Themen
- 13.3. Schließmedien
- 13.4. Systemmedien
- 13.5. Rollenverwaltung

13.1. Übersicht Systemeinstellungen



In der Sicht Systemeinstellungen finden Sie alle Einstellmöglichkeiten und Informationen über die Anlage und für das Programm Access Manager.

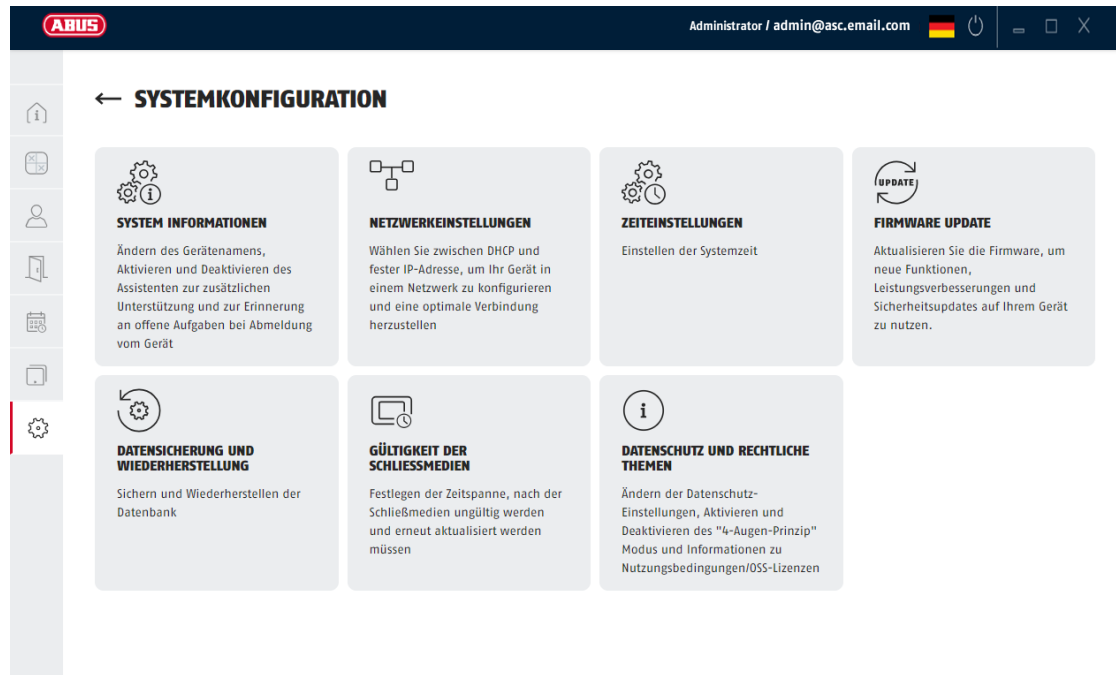
Sie erreichen die Systemeinstellungen über die Schaltfläche  .



13.2. Systemkonfiguration




Unter Systemkonfiguration finden Sie eine Übersicht über allgemeine Informationen zur Identifikation und Konfiguration Ihrer Schließanlage und Ihrer TECTIQ Zutrittskontrollzentrale. Sie können Standardeinstellungen für den Betrieb Ihrer Anlage einsehen und anpassen.

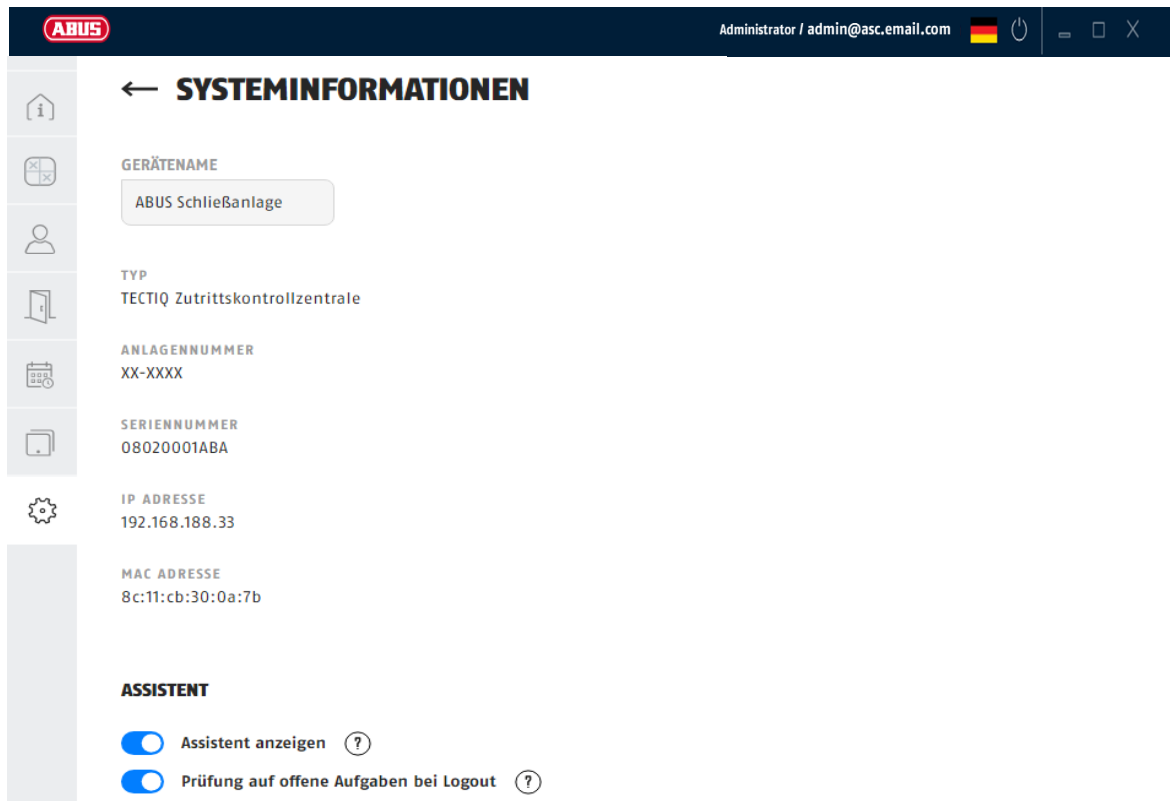
Sie erreichen die Systemkonfiguration über die Sicht Systemeinstellungen  und die Schaltfläche  Systemkonfiguration.



13.2.1. Systeminformationen

Unter Systeminformation finden Sie die wichtigsten Informationen zur Identifikation Ihrer Schließanlage und Ihrer TECTIQ Zutrittskontrollzentrale. Darüber hinaus haben Sie die Möglichkeit, Voreinstellungen für die programmseitige Unterstützung der Bedienung des Systems vorzunehmen.



Sie erreichen die Systeminformation über die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Systeminformationen.



The screenshot shows the 'SYSTEMINFORMATIONEN' page in the ABUS web interface. The top navigation bar includes the ABUS logo, the user role 'Administrator / admin@asc.email.com', a German flag, and system control icons. A left sidebar contains navigation icons for home, system, user, door, calendar, and settings. The main content area displays the following information:

- GERÄTENAME:** ABUS Schließanlage
- TYP:** TECTIQ Zutrittskontrollzentrale
- ANLAGENUMMER:** XX-XXXX
- SERIENNUMMER:** 08020001ABA
- IP ADRESSE:** 192.168.188.33
- MAC ADRESSE:** 8c:11:cb:30:0a:7b




Below this information is the 'ASSISTENT' section with two toggle switches:

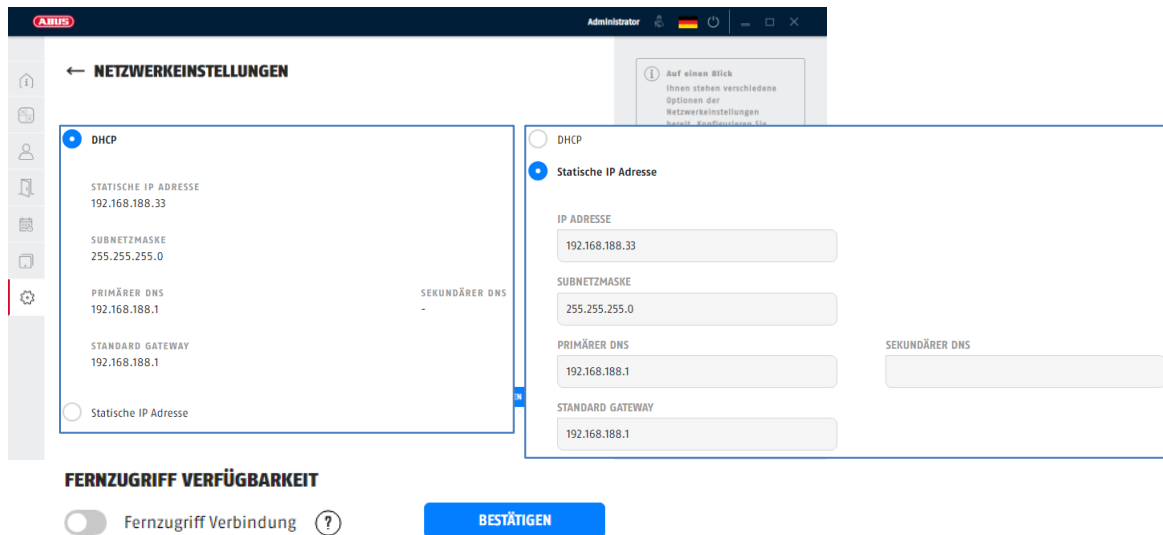
- Assistent anzeigen 
- Prüfung auf offene Aufgaben bei Logout 

Die folgenden Informationen werden angezeigt:

- **Gerätename:** Die Bezeichnung der Anlage, die im Dashboard angezeigt wird. Sie können den Gerätenamen ändern.
- **Typ:** Der Gerätetyp der TECTIQ Zutrittskontrollzentrale. Nicht veränderbar.
- **Anlagennummer:** Identifiziert die TECTIQ Schließanlage. Ist bei Auslieferung eingestellt und ist nicht änderbar.
- **Seriennummer:** Eindeutige Identifikation der TECTIQ Zutrittskontrollzentrale. Nicht änderbar.
- **IP Adresse:** Die aktuell eingestellte IP-Adresse der TECTIQ Zutrittskontrollzentrale, wie sie im Netzwerk manuell vorgegeben oder durch DHCP zugewiesen wurde.
- **MAC Adresse:** Die eindeutige Hardware-Adresse des Netzadapters der TECTIQ Zutrittskontrollzentrale. Nicht änderbar.
- **Anleitung anzeigen:** Internet-Link zur aktuellen Systemanleitung.
- **Assistent anzeigen:** Wenn die Einstellung aktiviert ist, erhalten Sie kurze Hilfetexte, wenn Sie Anlagendaten ändern, Personen hinzufügen o.ä.
- **Prüfung auf offene Aufgaben bei Logout:** Wenn diese Einstellung aktiviert ist, erhalten Sie beim Beenden des Programms eine Meldung, wenn noch nicht erledigte Aufgaben in der Aufgabenliste enthalten sind.

13.2.2. Netzwerkeinstellungen

In der Netzwerkeinstellungen konfigurieren Sie den Netzzugang der TECTIQ Zutrittskontrollzentrale.
Sie erreichen die Netzwerkeinstellungen über die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Netzwerkeinstellungen.






- ▶ Wählen Sie Ihre Einstellungen entsprechend der Netzwerkkonfiguration vor Ort.
 - ▶ Wählen Sie „DHCP“ für die automatische Adressvergabe.
 - ▶ Wählen Sie „Statische IP Adresse“ für die manuelle Einstellung der Internet-Adresse. Die erforderlichen Daten erhalten Sie vom Netzwerkadministrator.
 - ▶ Beenden Sie die Eingabe mit „Bestätigen“.
- ▶ Aktivieren Sie den Fernzugriff um Ihre TECTIQ Zutrittskontrollzentrale von außerhalb Ihres lokalen Netzwerkes über das Internet erreichen zu können. Die Verbindung wird über einen gesicherten Tunnel aufgebaut.

Nach dem Ändern der Netzwerkeinstellungen startet die Zentrale neu und trennt die Verbindung. Der Nutzer muss anschließend die Verbindung zur Zentrale neu wiederherstellen.

13.2.3. Zeiteinstellungen

Für eine sichere Funktion benötigt die TECTIQ Anlage die aktuelle Uhrzeit. Wenn die TECTIQ Zutrittskontrollzentrale mit dem Internet verbunden ist, kann sich die Anlage über einen Zeitserver automatisch mit der korrekten Uhrzeit synchronisieren. Alternativ können Sie Datum und Zeit manuell vorgeben.

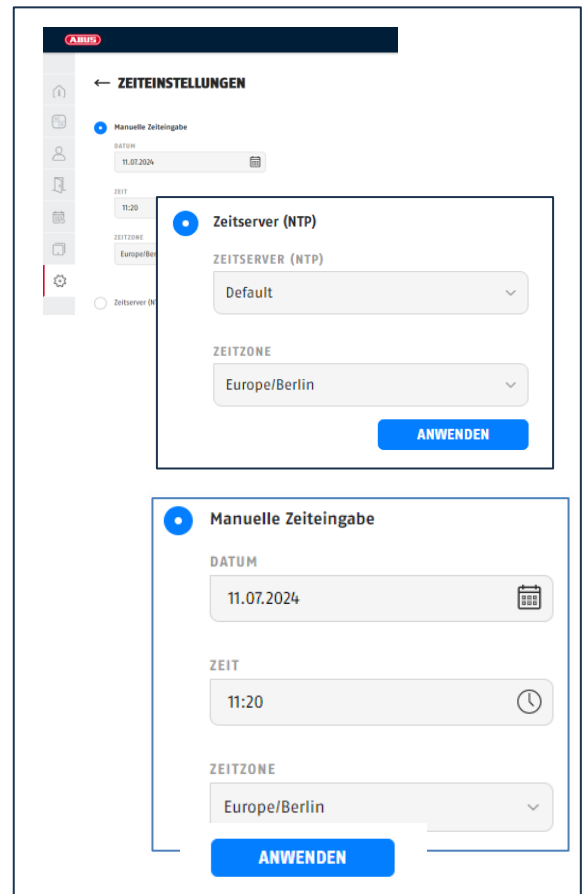
Sie erreichen die Zeiteinstellungen über die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Zeiteinstellungen.

 Empfohlen wird die Zeiteinstellung über Zeitserver (NTP)!

- ▶ Wählen Sie „Zeitserver (NTP)“, damit die Anlage Datum und Uhrzeit regelmäßig automatisch synchronisieren kann.
- ▶ Wählen Sie im Feld „Zeitserver (NTP)“ „Default“ oder die Option für eine manuelle Eingabe. Vorschläge für Ihren Standort finden Sie im Informationsfenster.
- ▶ Beenden Sie die Eingabe durch Betätigen der Schaltfläche „Anwenden“.

- um die Uhrzeit manuelle einzustellen:




- ▶ Wählen Sie „Manuelle Zeiteingabe“
- ▶ Geben Sie aktuelle Werte für „Datum“ und „Zeit“ ein. Geben Sie die dem Anlagenstandort entsprechende Zeitzone an, z. B. für die Zeit in Mitteleuropa „Europe/Berlin“.
- ▶ Beenden Sie die Eingabe durch Betätigen der Schaltfläche „Anwenden“.



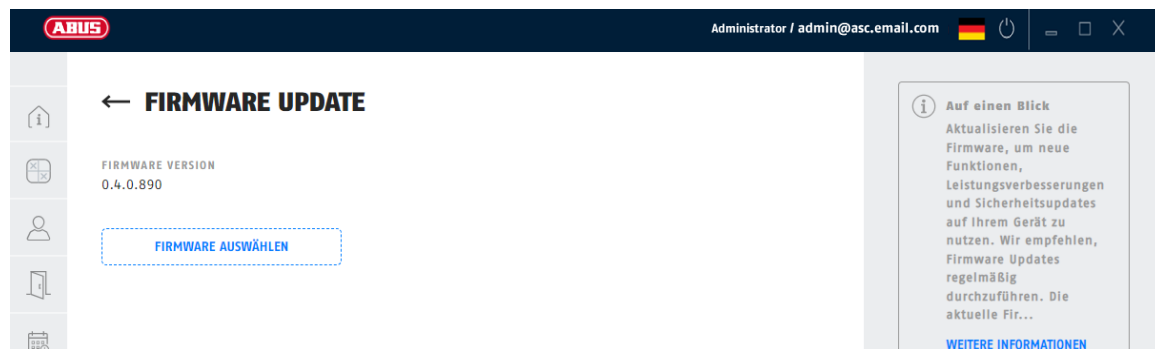
The screenshot displays the 'ZEITEINSTELLUNGEN' (Time Settings) screen. It features two main configuration panels. The top panel, 'Zeitserver (NTP)', is selected and shows a dropdown menu for 'ZEITSERVER (NTP)' with 'Default' selected, and another dropdown for 'ZEITZONE' with 'Europe/Berlin' selected. A blue 'ANWENDEN' button is at the bottom right. The bottom panel, 'Manuelle Zeiteingabe', is unselected and shows input fields for 'DATUM' (11.07.2024), 'ZEIT' (11:20), and 'ZEITZONE' (Europe/Berlin), with a blue 'ANWENDEN' button at the bottom. A sidebar on the left contains navigation icons, and the top header shows the ABUS logo.

13.2.4. Firmware-Update

Sobald für die TECTIQ Zutrittskontrollzentrale eine aktualisierte Systemsoftware (die sogenannte Firmware) zur Verfügung steht, erfolgt eine Meldung auf dem Dashboard. Eine aktualisierte Firmware umfasst z. B. neue Funktionen, Sicherheitsupdates oder Leistungsverbesserungen.

Sie erreichen die Funktion über die Sicht Systemeinstellungen  und die Schaltflächen  Systemkonfiguration und  Firmware Update.

Die aktuell vorhandene Firmware-Version wird angezeigt.



Achten Sie darauf, dass Sie ausschließlich von ABUS autorisierte sichere Quellen nutzen! Nähere Informationen erhalten Sie über www.ABUS.com oder über unseren Support.

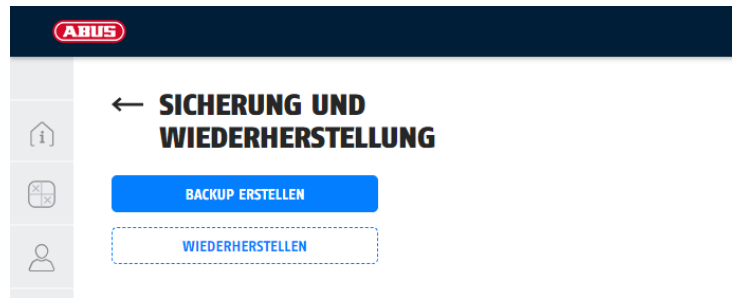
- ▶ Laden Sie eine aktualisierte Firmware herunter auf die lokale Festplatte.
- ▶ Wählen Sie die Schaltfläche „Firmware Update“ und wählen Sie auf Ihrem lokalen PC die heruntergeladene Software aus.
- ▶ Folgen Sie den weiteren Anweisungen.

13.2.5. Datensicherung und Wiederherstellung

Sichern Sie die Daten Ihrer Schließanlage mit den eingegebenen Personen, Türen und Schließplan spätestens nach Abschluss der Inbetriebnahme der Anlage.

Die gesicherten Daten werden auf Ihrem PC lokal hinterlegt und können bei Bedarf wieder geladen werden.

Sie erreichen die Datensicherung über die Sicht Systemeinstellungen und die Schaltflächen Systeminformationen und Datensicherung und Wiederherstellung.



TECTIQ Anlagendaten sichern

- ▶ Wählen Sie „Backup erstellen“, um die Daten der TECTIQ Zutrittskontrollzentrale zu sichern.
- ▶ Folgen Sie den Anweisungen und geben Sie ein Passwort ein.



Wichtig! Unsichere Passwörter können ausgespäht oder erraten werden – auch wenn sie die Kriterien formal erfüllen (siehe → Bild). Unberechtigte Personen können die Schließanlage überwinden und Ihrem Eigentum großen Schaden zufügen.

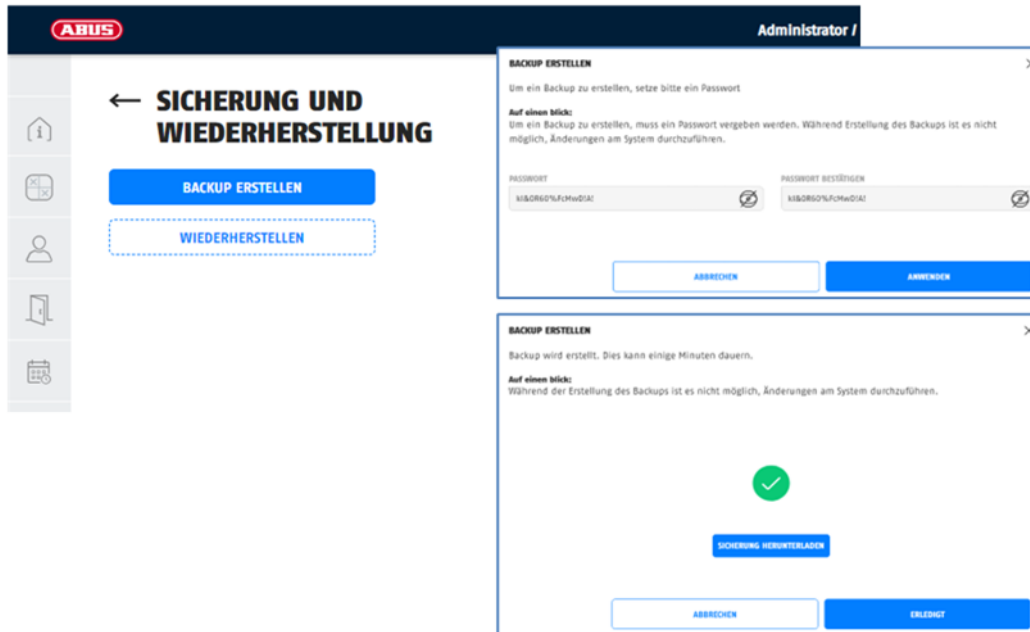
- Nutzen Sie nur sichere Passwörter.
- Beachten Sie Regeln und Ratgeber, wie ein sicheres Passwort beschaffen sein sollte, z. B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI).
- Wenn Sie einen Passwort-Generator verwenden, verändern Sie den erhaltenen Passwort-Vorschlag nochmals, z. B. durch Hinzufügen oder Ändern eines Zeichens.

Die TECTIQ Zutrittskontrollzentrale akzeptiert nur Passwörter, die

- aus mindestens 8 Zeichen bestehen,
- sowohl Groß- als auch Kleinbuchstaben enthalten,
- mindestens eine Ziffer enthalten,
- mindestens ein Sonderzeichen – z. B. \$!%) [%& – enthalten

- ▶ Geben Sie ein Passwort ein und notieren Sie es.
- ▶ Wiederholen Sie das eingegebene Passwort im Feld „Passwort bestätigen“.
- ▶ Bestätigen Sie Ihre Eingabe mit „Anwenden“.

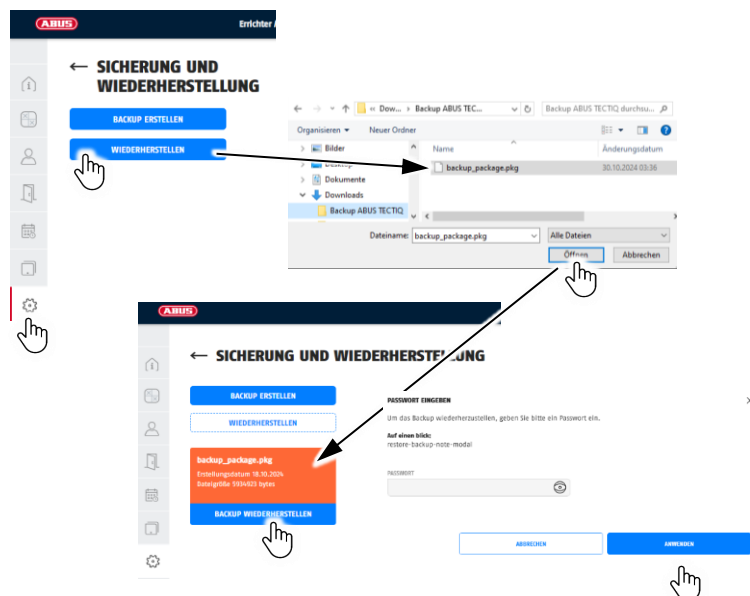




- ▶ Nach Erstellung des Backups laden Sie die Sicherung auf Ihren PC.
- ▶ Geben Sie den gewünschten Speicherort ein.
- ▶ Bestätigen Sie den Abschluss des Vorgangs durch Betätigen der Schaltfläche „Erledigt“.

TECTIQ Anlagendaten wiederherstellen

- ▶ Wählen Sie „Wiederherstellen“.
- ▶ Wählen Sie die gewünschte Sicherungsdatei auf Ihrem PC aus.
- ▶ Betätigen sie die Schaltfläche „Öffnen“.
- ▶ Ihr Backup wird im Access Manager zur Wiederherstellung angezeigt.
- ▶ Wählen Sie die Schaltfläche „Backup wiederherstellen“.
- ▶ Geben Sie das Passwort ein und wählen die Schaltfläche „Anwenden“.

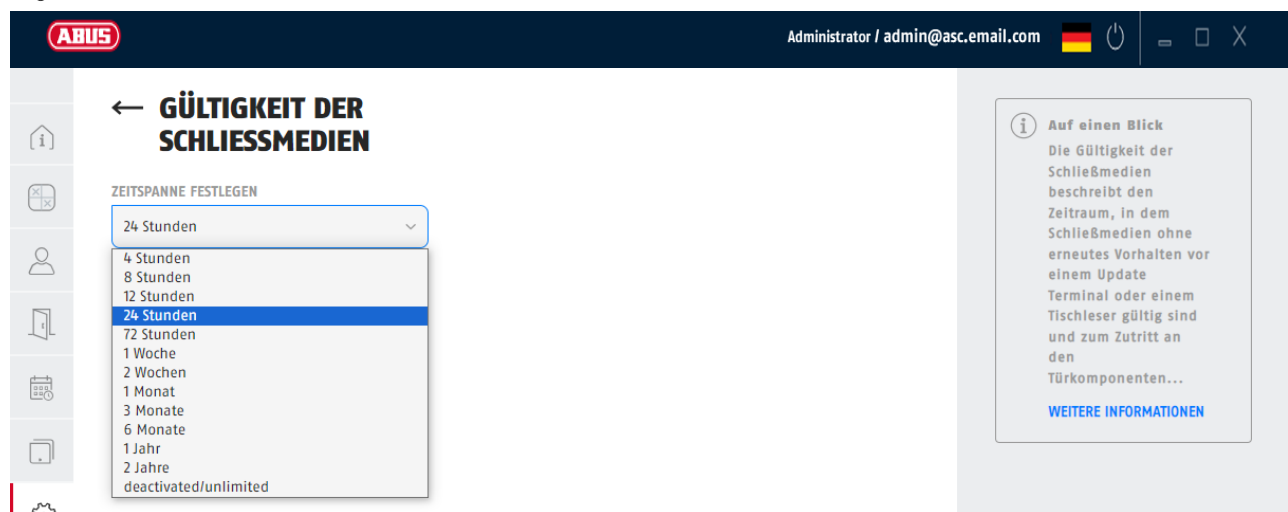


13.2.6. Gültigkeit der Schließmedien

Die Gültigkeit der TECTIQ Schließmedien kann zur Erhöhung der Sicherheit gegen unbefugte Nutzung begrenzt werden. Wenn die Funktion aktiviert ist, ist der Nutzer gehalten, seine Zutrittsberechtigung regelmäßig zu aktualisieren. Im Menü „Gültigkeit der Schließmedien“ bestimmen Sie das Zeitintervall, nach dem die Zutrittsberechtigung erneuert werden muss.

Nach Ablauf der Zeitspanne muss die Zutrittsberechtigung erneuert werden, indem das Schließmedium vor dem Online-Terminal oder am Tischleser präsentiert wird – was im normalen Betrieb, ohne Änderung der Personendaten, immer möglich ist.

Sie erreichen die Funktion über die Sicht Systemeinstellungen und die Schaltflächen Systemkonfiguration und Gültigkeit der Schließmedien.



► Wählen Sie das Zeitintervall aus dem Listenfeld „Zeitspanne festlegen“.

- Das typische und empfohlene Zeitintervall für einen Geschäftsbetrieb mit Angestellten beträgt zwischen 12 und 48 Stunden (entsprechend 1 bis 2 Tagen). Kurze Zeiten führen zu aktuelleren Daten im System, da häufiger Daten von den Türkomponenten in die Zugriffskontrollzentrale zurückgeschrieben werden. Die Sicherheit wird erhöht.
- Ein kurzes Zeitintervall von weniger als 12 Stunden empfiehlt sich z. B. für Gäste oder Handwerker, die nur kurzzeitig im gesicherten Bereich unterwegs sind.
- Längere Zeitintervalle sollten nur in Ausnahmefällen eingestellt werden.
- Ein unbegrenzter Zutritt sollte nicht für normale Schließmedien eingestellt werden, sondern z. B. nur für solche Schließmedien, die zu Sicherheitszwecken erstellt und – dem normalen Gebrauch entzogen - an einem sicheren Ort aufbewahrt werden.

13.2.7. Datenschutz und rechtliche Themen

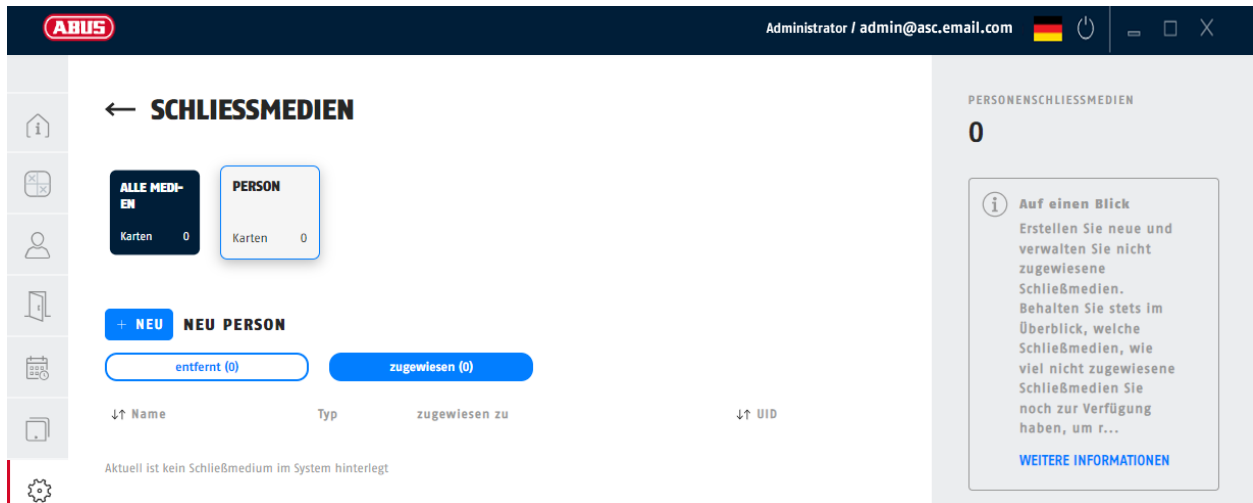
Alle Themen mit rechtlicher Relevanz finden Sie in der Sicht Systemeinstellungen unter den Schaltflächen Systeminformationen und Datenschutz und Rechtliche Themen.



13.3. Schließmedien

Die Sicht Schließmedien bietet die Übersicht über alle der Anlage bekannten Schließmedien. Hierzu gehören neben aktuell Personen zugewiesenen Schließmedien auch gesperrte oder solche, die bereits Personen zugewiesen waren.

Sie erreichen die Funktion über die Sicht Systemeinstellungen und die Schaltfläche Schließmedien.

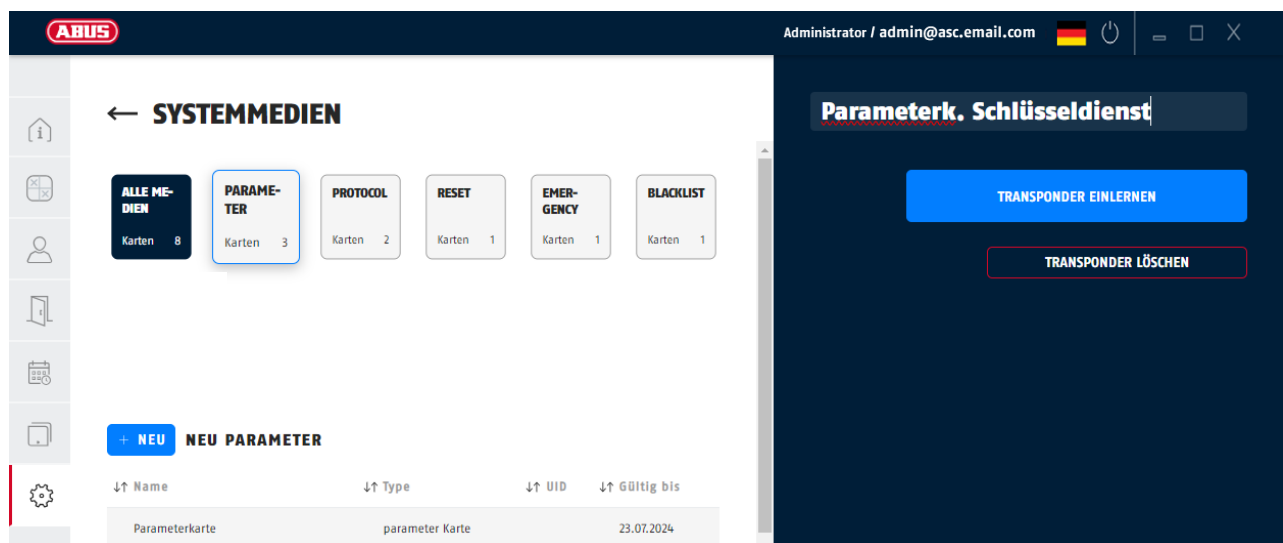


13.4. Systemmedien

Die Sicht Systemmedien verwaltet alle Medien mit Systemfunktionen. Systemmedien sind in der Regel nicht Personen zugeordnet und sollten sicher, vor unbefugtem Zugriff geschützt, aufbewahrt werden. Hierzu gehören:

- Parameterkarten
- Protokollkarten
- Resetkarten
- Notöffnungstransponder
- Blacklistkarten

Sie erreichen die Funktion über die Sicht Systemeinstellungen  und die Schaltfläche  Systemmedien.

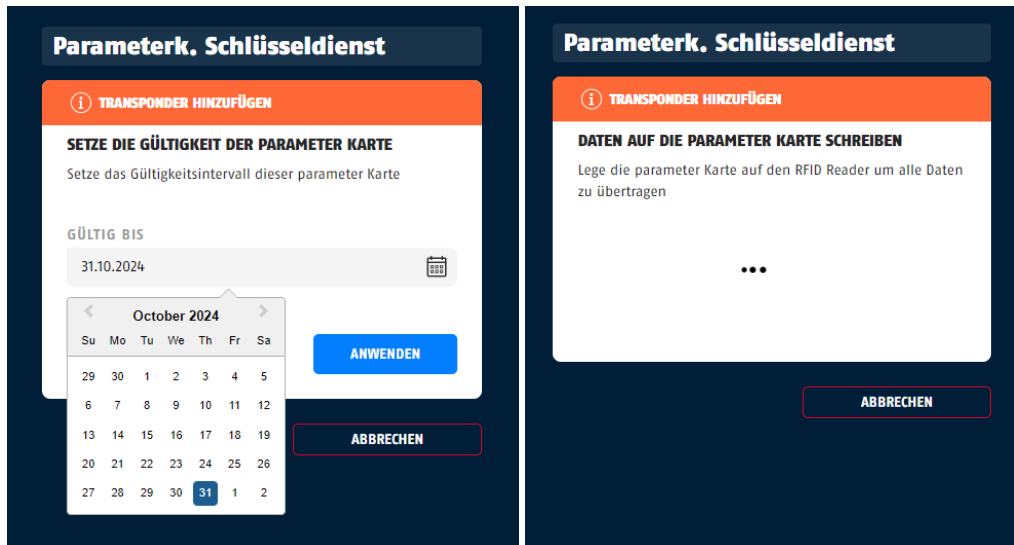


Fügen Sie neue Systemmedien hinzu:

- ▷ Wählen Sie den gewünschten Medientyp aus, indem Sie die betreffende Schaltfläche betätigen.
- ▷ Betätigen Sie die Schaltfläche „+Neu“.
- ▷ Geben Sie eine Bezeichnung für das Systemmedium ein.

Nach dem Hinzufügen können Sie weitere Einstellungen vornehmen.

- ▷ Betätigen Sie die Schaltfläche „Transponder einlernen“.
- ▷ Setzen Sie ein Gültigkeitsintervall für das Systemmedium.
Achtung: Wählen Sie ein sinnvolles Zeitintervall. Treffen Sie die geeigneten Maßnahmen, dass Sie die Gültigkeit des betreffenden Systemmediums rechtzeitig verlängern.
- ▷ Schließen Sie den Vorgang ab, indem Sie das Medium beschreiben. Befolgen Sie hierzu die Anweisungen im Editierbereich.

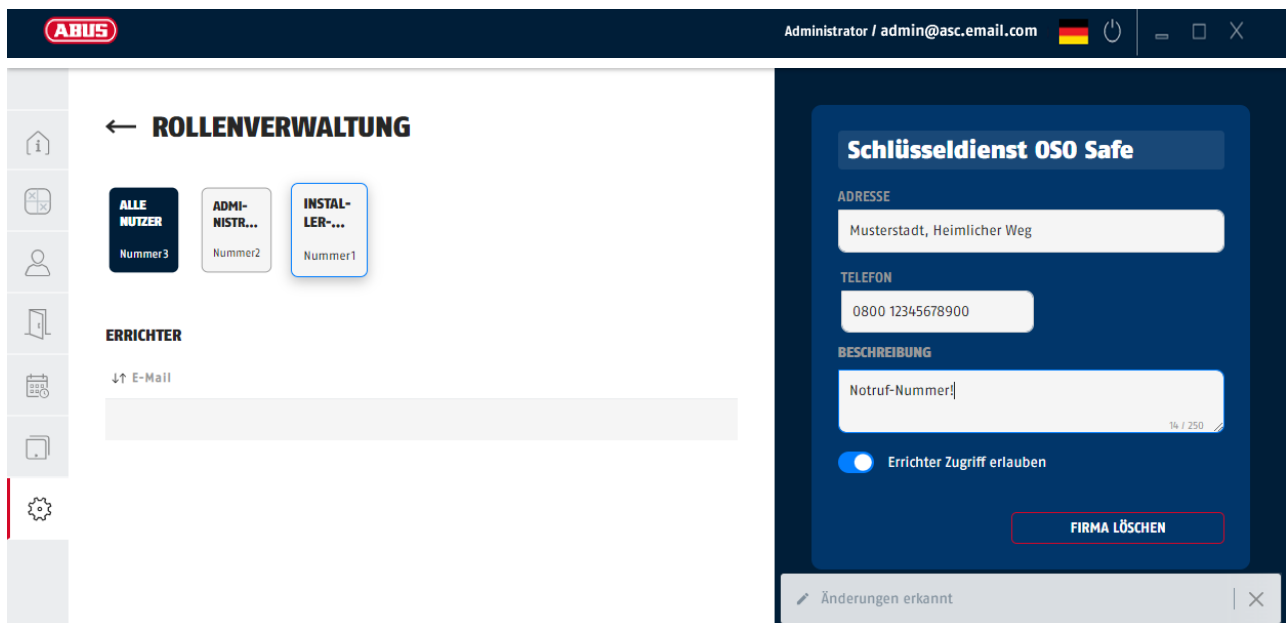


13.5. Rollenverwaltung

TECTIQ erlaubt zwei Nutzer-Rollen, die als Ansprechpartner in der TECTIQ Zutrittskontrollzentrale hinterlegt werden:

- Der Administrator ist der Betreiber der Anlage, z. B. der Eigentümer der Liegenschaft, Facility Manager.
- Der Installateur ist der Facherrichter, z. B. ein autorisierter ABUS Fachhandelspartner.

Sie erreichen die Funktion über die Sicht Systemeinstellungen und die Schaltfläche Rollenverwaltung.



14. LED-Signale

Inhalt

- 14.1. LED-Signale an Türkomponenten
- 14.2. LED-Signale am Update Terminal
- 14.3. LED-Signale am Tischleser

14.1. LED-Signale an Türkomponenten

		Zutritt gewährt.
	(je 0,1 s)	Zutritt verweigert. Schließmedium abgelaufen oder keine Berechtigung für die Tür.
		Batteriewarnung, Zutritt gewährt mit 5 Sekunden Verzögerung
		Falsches oder fremdes Schließmedium / Lesefehler
		Allgemeiner Fehler
	(je 0,3 s)	Hardware-Fehler
		Leistungsunterbrechung (bei TECTIQ Beschlag)
	(1 s)	Motor-Fehler, wenn Öffnungs-Zeit abgelaufen. Tür bleibt offen. Wenn der Fehler 5× in Folge auftritt, startet das Gerät neu.
		Langes Leuchten (1 s), gefolgt von schnellem Blinken: Motor-Fehler, Gerät startet neu, bis der Fehler beseitigt ist.
	Permanent	Software-Fehler, Gerät ist außer Betrieb.
		Software-Fehler, Gerät muss neu programmiert werden.
		Gerät startet neu (z. B. nach Batteriewechsel oder Fehler)
	(5 s)	Leuchten für 5 Sekunden nach Neustart: Gerät enthält keine Daten.

Beim Umgang mit Systemmedien

		Schnelles Blinken (0,1 s / 0,3 s) Schreib-/Lesevorgang läuft.
		0,5 s Vorgang erfolgreich beendet.
		0,5 s Vorgang nicht erfolgreich.

Beim Umgang mit Admin App

	Smartphone mit Admin App und Anlagenberechtigung identifizieren
	4× kurz blinken: Keine Berechtigung; Vorgang abgebrochen
	Langsam blinken: Schreibvorgang läuft. Wenn der Vorgang erfolgreich war, startet das Gerät anschließend neu.






14.2. LED-Signale am Update Terminal

	Zutrittsrechte wurden aktualisiert. Systemmedium erfolgreich beschrieben. Eine vorhandene Tür wird geöffnet.
(je 0,1 s)	Bei Schließmedium: Zutritt verweigert. Bei Systemmedium: Medium wird beschrieben.
(0,5 s)	Bei Schließmedium: Zutrittsrechte wurden nicht aktualisiert. Bei Systemmedium: Schreibvorgang fehlgeschlagen.
(0,1 s)	Falsches oder fremdes Schließmedium / Lesefehler / Verbindungsstörung zwischen Leseinheit und Steuereinheit.
	Allgemeiner Fehler
...	Keine Verbindung zur Zutrittskontrollzentrale; Terminal ist offline.
	Anlagenstörung. Keine Verbindung zur Zutrittskontrollzentrale; Terminal ist offline. Kein Zutritt möglich.
	Software-Update läuft zwischen Zentrale und Leseinheit (oder über Smartphone mit Admin App)
	Leseinheit startet neu.
	Leseinheit verbindet sich mit Steuereinheit
(5 s)	Leuchten für 5 Sekunden nach Neustart: Gerät enthält keine Daten.

Beim Umgang mit Systemmedien oder Admin App

	Schnelles Blinken (0,1 s / 0,3 s) Schreib-/Lesevorgang läuft.
	0,5 s Vorgang erfolgreich beendet.
	0,5 s Vorgang nicht erfolgreich.

14.3. LED-Signale am Tischleser

	Rotes Dauerleuchten	Einschalten/Initialisieren/Keine Verbindung
	Grünes Dauerleuchten	Betriebsbereit / Vorgang erfolgreich
	Kurzes rotes Blinken (0,1 s / 0,3 s)	Falsches Medium (falsche oder fehlende Anlagennummer)
	Grünes Blinken	Schreib-/Lesevorgang aktiv
	Langsames rotes Blinken (0,3 s / 0,3 s)	Vorgang nicht erfolgreich

ABUS TECTIQ

ANHANG

15. Protokolle

Der TECTIQ Accessmanager stellt Protokolle zur Dokumentation und als Aufgabenliste zum Download bereit.

15.1. Schlüsselausgabeprotokoll (Muster)



ABUS SECURITY CENTER

SCHLÜSSELAUSGABEPROTOKOLL

ERSTELLT: 07/09/2024 04:47:33

EMPFÄNGER

Benutzername: Hermann Hufschmidt
Kommentar: Zugriffskarte
UID: 044542f2937480

ÜBERGABE

Datum

Signatur

RÜCKGABE

Datum

Signatur

ZUSÄTZLICHE VEREINBARUNG

16. Übersicht – TECTIQ Türkomponenten

Anforderung	Wandleser / Update Terminal	Elektronischer Zylinder	Elektronischer Beschlag
Einseitige Zutrittskontrolle	Ja	Ja	Ja
Zweiseitige Zutrittskontrolle	Ja	Ja	Nein
Für Außentüren	Ja	Ja	Ja
Für Innentüren	Ja	Ja	Ja
Für Türöffner/Türsummer	Ja	Keine Einschränkung	Keine Einschränkung
Für motorisch angetriebene Türen	Ja	Keine Einschränkung	Nein
Für Karusselltüren, Türkreuze	Ja	Keine Einschränkung	Nein
Türblattstärke	Keine Einschränkung	Außen/Innen 30 ... 90 mm	32 mm ... 121 mm
Für FH-Türen	Keine Einschränkung	Ja	Ja
Schließfunktion	Entfällt	Ja	Mit SVP-Schloss und /oder Beschlag mit mechanischem Override
Für Fluchtwege geeignet	Keine Einschränkung, abhängig von der Tür	Ja (nur einseitige Variante)	Ja
Für Garagentore	Mit Antrieb: ja	Ja (Halbzylinder)	Nein
Einbau	Unterputz- / Aufputzdose	In Tür mit Einsteckschloss	In Tür mit Einsteckschloss
Für skandinavische Türen	Keine Einschränkung	Ja	Ja
Für Türen mit Schweizer Rundzylinder	Keine Einschränkung	Ja	Ja
Unabhängige Batterieversorgung	Nein (mit USV: ja)	Ja	Ja
Batterielaufzeit	Entfällt	Bis zu 3 Jahre oder 65.000 Schließzyklen	Bis zu 3 Jahre oder 90.000 Schließzyklen
Versorgung via 230 V	Ja (über Netzteil)	Nein	Nein
Versorgung via PoE	Ja	Nein	Nein
Umgebungstemperatur	-10 ... +60 °C / Innenleser -20 ... +70 °C / Außenleser	-25 ... +65 °C	-25 ... +65 °C
Schutzart (EN 60529)	IP44 / 67	IP67	IP54 (Standard; andere Varianten: IP55)
Notöffnung mit Notöffnungstransponder	Ja	Ja	Ja
Notbestromung bei Ausfall aller Komponenten	Abhängig von der Tür	Ja, über USB-Anschluss	Ja, über USB-Anschluss
Verlängerung Zutrittsberechtigung	Ja (Update Terminal)	Nein	Nein

17. Wer macht was und wann?




Was?	Wer?	Wann?	Anmerkungen
Nutzer anlegen	Admin Facherrichter	Bei Bedarf Bei Errichten	
Nutzer ändern	Admin	Bei Bedarf	
Nutzer entfernen	Admin	Bei Bedarf	Empfehlung: Nutzer nicht entfernen, sondern sperren.
Nutzer sperren	Admin	Bei Bedarf	Nutzer sperren oder Schließmedium
Schließmedium sperren	Admin	Bei Bedarf/Verlust	
Neues Schließmedium erstellen	Admin	Bei Bedarf	
TECTIQ Projekt anlegen	Facherrichter	Bei Errichten	
TECTIQ Projekt planen	Bauherr Facherrichter	Bei Errichten	
TECTIQ Projekt konfigurieren	Facherrichter	Bei Errichten	
TECTIQ Projekt in Betrieb nehmen	Facherrichter	Bei Errichten	
Türen anlegen	Facherrichter	Bei Errichten Bei Umbau	Vorhangschloss durch Admin
Türen ändern	Facherrichter	Bei Umbau	Ändern von Türgruppen auch durch Admin
Türkomponenten zuweisen	Facherrichter Ggf. Admin	Bei Errichten Bei Umbau	Vorhangschloss durch Admin
Türen umbauen	Facherrichter	Bei Umbau	
Türen programmieren	Facherrichter Admin	Bei Errichten/Umbau	Admin bei Vorhangschloss oder bei Änderung von Türgruppen
Zutrittsberechtigung bearbeiten	Admin Facherrichter	Bei Bedarf Bei Errichten	
Störungsbehebung Batteriewechsel Keine Verbindung Gerätedefekt	Betreiber Facherrichter Facherrichter	Bei Batteriewarnung Bei Störungsmeldung Bei Funktionsstörung	Gerätedefekte oder Reparaturen nur durch Facherrichter
Wartung	Facherrichter		Siehe Montageanleitungen
Reparatur	Facherrichter		Siehe Montageanleitungen
Firmware Update	Admin	Bei Meldung im Access Manager	
Türkomponente tauschen	Facherrichter	Bei Defekt	
Programmieren von Schließmedien	Facherrichter Admin	Bei Errichten Bei Bedarf	
Zentrale Neustart	Admin	Auf Anforderung durch ABUS Support.	
Netzwerk-Reset	Facherrichter	Bei Fehler in der IP-Adresse, wenn kein Zugriff auf die Zentrale möglich ist	Ohne DHCP in der Anlage muss die Erreichbarkeit der Zentrale geprüft und wieder hergestellt werden.
Werks-Reset	Facherrichter	Auf Anforderung durch ABUS Support.	Bei Betätigen werden sämtliche Daten gelöscht! Unbedingt vorher die Daten sichern!

18. TECTIQ Dokumentation – Hinweise und Symbole

Dieses Handbuch enthält neben allgemeinen technischen Beschreibungen wichtige Hinweise, die unbedingt beachtet werden sollen. Textliche Auszeichnungen und zusätzliche Elemente signalisieren die Wichtigkeit dieser Passagen.




Warnung vor Personenschäden

Warnhinweise weisen auf **Gefahren für Leib und Leben** hin. Warnhinweise unterscheiden nach dem Schweregrad der Gefahr und nutzen eines der folgenden Signalwörter:

Symbol	Signalwort	Bedeutung
	GEFAHR!	Bezeichnet eine unmittelbare Gefahr, die, wenn sie nicht vermieden wird, den Tod oder eine schwere Verletzung zur Folge hat!
	WARNUNG!	Bezeichnet eine mögliche Gefahr, die, wenn sie nicht vermieden wird, den Tod oder eine schwere Verletzung zur Folge haben kann.
	VORSICHT!	Bezeichnet eine mögliche Gefahr, die, wenn sie nicht vermieden wird, eine geringfügige oder mäßige Verletzung zur Folge haben kann.



Warnung vor Sachschäden

Bei Nichtbeachten der Hinweise können **Sachschäden** am Produkt, dem Gebäude oder in Folge fehlerhafter Funktion entstehen, die ihrerseits Folgeschäden nach sich ziehen können.

Symbol	Signalwort	Bedeutung
	HINWEIS	Weist auf eine Möglichkeit zur Beschädigung des Produkts oder am Gebäude hin.
	Wichtig	Weist auf mögliche Fehlfunktionen in Folge fehlerhafter Montage oder Inbetriebnahme hin.
	INFO	Gibt zusätzliche wichtige oder nützliche Informationen.

Weitere Symbole

Bei besonderen Gefahren oder Hinweisen kann – anstelle des allgemeinen Warnsymbols – ein konkretes Symbol verwendet werden:

	GEFAHR!	Gefahr durch elektrischen Schlag
	HINWEIS	Beschädigung des Produkts durch elektrostatische Entladung

Weitere Auszeichnungen

- Textpassagen mit einem vorangestellten Punkt • sind Teil einer Aufzählung.
- ▷ Textpassagen mit einem vorangestellten Dreieck markieren einen Handlungsschritt: Hier müssen Sie etwas tun. Bitte halten Sie die Reihenfolge der Handlungsschritte ein – soweit nicht anders vermerkt.

Weitere Dokumentationen

Beachten Sie des Weiteren die produktbegleitenden Dokumentationen der ABUS TECTIQ Produkte und die ausführlichen Montageanleitungen, die Sie jederzeit aktuell unter abus.com beziehen können.

19. Sicherheitshinweise

19.1. Allgemeine Sicherheitshinweise



GEFAHR!

Gefahr durch elektrischen Schlag!

Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung elektronischer Geräte. Elektrischer Schlag kann zum Tod führen.

- Vor Arbeiten am Gerät freischalten.
- Spannungsführende Teile in der Umgebung abdecken!



WARNUNG!

Explosionsgefahr!

Montieren und Betreiben der Geräte in explosionsgefährdeten Bereichen kann zu schweren Verletzungen oder Tod führen.

- Montieren und betreiben Sie die Geräte nicht in explosionsgefährdeten Bereichen.



VORSICHT!

Verletzungsgefahr durch Verschlucken von Kleinteilen!

Kinder können Kleinteile verschlucken.

- Halten Sie Kleinteile wie Schrauben oder Schließmedien fern von Kindern.



VORSICHT!

Quetschgefahr durch motorisch betriebene Türen in der Einbauumgebung!

Motorisch betriebene Türen können zu Verletzungen führen.

- Schalten Sie während der Arbeiten motorisch betriebene Türen in der unmittelbaren Umgebung frei.
- Sichern Sie Ihre Baustelle zu allen Seiten vor dem Zutritt unbeteiligter Personen.
- Benutzen Sie Ihre persönliche Schutzausrüstung.

19.2. Sicherheitshinweise für Flucht- und Rettungswege



WARNUNG!

Schwere Verletzungen oder Tod möglich, wenn Fluchttüren oder Brandschutztüren aufgrund unsachgemäßer Montage oder Wartung nicht einwandfrei funktionieren!

Schlecht montierte oder gewartete Schließzylinder oder Beschläge können die Funktion von Fluchttüren und Brandschutztüren beeinträchtigen. In Notfällen können hierdurch gefährliche Situationen mit schweren oder tödlichen Verletzungen entstehen.

- Lassen Sie Flucht- und Brandschutztüren mit den montierten Komponenten ausschließlich durch Fachpersonal montieren und warten.
- Beachten und befolgen Sie alle Herstellerhinweise bei der Montage und Wartung der Türen, Schlösser, Schließzylinder und Beschläge.
- Stellen Sie sicher, dass in Flucht- und Rettungswegen ausschließlich hierfür geeignete Komponenten montiert sind. Achten Sie insbesondere auf die Kompatibilität der verbauten Komponenten. Beachten Sie die Zertifikate der Hersteller.
- Halten Sie die vorgeschriebenen Wartungsintervalle von Türen, Schlössern und Schließzylindern ein.
- Tauschen Sie Schließzylinder und Beschläge an Flucht- und Brandschutztüren nach Erreichen der Höchstzahl an Schließzyklen aus.

19.3. Sicherer Umgang mit Batterien



WARNUNG! Gefahr durch unsachgemäßen Umgang mit Batterien!

Batterien können überhitzen und Brände verursachen.

Beschädigungen oder das Aussetzen großer Hitze können Brände oder Explosionen verursachen und zu schweren Verletzungen, Verbrennungen oder Verätzungen führen.

Beim Auslaufen können gefährliche Stoffe freigesetzt werden, die Ihre Gesundheit beeinträchtigen.

- Batterien nicht verpolen. Beachten Sie die Polarität (+/-).
- Batterien nicht aufladen, öffnen, ins Feuer werfen oder kurzschließen.
- Neue und gebrauchte Batterien nicht zusammen verwenden.
- Nicht zusammen mit anderen Batterietypen verwenden.
- Batterien nur vollständig entladen und mit abgeklebten Polen zurückgeben.
- Batterien von Kindern fernhalten.

19.4. Fachgerechte Installation



Die hier beschriebenen Produkte/Systeme dürfen nur von Personen installiert und gewartet werden, die für die jeweilige Aufgabenstellung qualifiziert sind.

Für elektrische Installationen ist die Qualifikation einer Elektrofachkraft erforderlich.

Qualifiziertes Personal für die Installation und Wartung des Systems ist i. d. R. ein geschulter ABUS Fachhandelspartner.

20. Glossar

Access Manager

Der TECTIQ Access Manager ist eine leistungsfähige und umfassende Verwaltungssoftware für das ABUS TECTIQ Zutrittskontrollsystem. Er wird u.a. zur Inbetriebnahme, Ersteinrichtung und Übergabe des TECTIQ Zutrittskontrollsystems an den Betreiber und für die Anlage von Nutzern, Erteilung von Zugangsberechtigungen, Erstellung von Zeitplänen sowie die Verwaltung von Schließmedien und Systemmedien eingesetzt.

Administrator, Admin

Administrator (kurz Admin) des TECTIQ Zutrittskontrollsystems ist eine vom Betreiber festgelegte Person, die für die Verwaltung der Nutzer, der Türkomponenten und der Schließmedien verantwortlich ist. Der Administrator vergibt im Auftrag des Betreibers Zutrittsrechte, trägt neue Personen in die Anlage ein und gibt Schließmedien aus. Hierfür steht ihm der TECTIQ Access Manager – eine leistungsfähige und umfassende Verwaltungssoftware für das ABUS TECTIQ Zutrittskontrollsystem zur Verfügung. Der Administrator ist der erste Ansprechpartner für alle Belange, weist Nutzer in die Anlage ein und sperrt Schließmedien bei Verlust. Der Betreiber kann mehrere Administratoren bestimmen.

Aktoren

Elektromechanische Komponenten, wie elektrische Türöffner, Türantriebe, Vereinzelungsanlagen. Die Aktoren werden von den Steuereinheiten der TECTIQ Update Terminals angesteuert.

Aufgabenliste

Vom Zutrittskontrollsystem automatisch generierte Liste mit zu erledigenden Aufgaben (z.B. offene Parametrierung von Türkomponenten, Batteriewechsel etc.). Die Aufgabenliste wird auf dem Dashboard des TECTIQ Access Managers angezeigt.

Berechtigung

Eine Person erhält die grundsätzliche Zutrittsberechtigung zu ausgewählten gesicherten Bereichen, wenn Sie hierzu autorisiert ist – i. d. R. durch den Besitz eines persönlichen Schließmediums. Zutrittsberechtigungen für die gesicherten Bereiche werden auf dem Schließmedium gespeichert und haben eine begrenzte Gültigkeit. Sie müssen aktualisiert und validiert werden (am Update Terminal) und können mithilfe eines voreingestellten Zeitplans verknüpft werden.

Beschlag

Siehe „Elektronischer Beschlag“

Blacklistkarte

Systemmedium zur Übertragung einer Sperrliste auf die betroffenen Türkomponenten.

Data-on-Card

Zutrittsberechtigungen werden auf den Schließmedien und nicht in den Offline Türkomponenten gespeichert. Hierdurch sind Änderungen von Zutrittsberechtigungen schnell und einfach zu verwalten.

Einsatzkräfte

Einsatzkräfte sind Mitarbeiter des Rettungsdienstes oder der Feuerwehr, die im Notfall Zutritt zum gesicherten Gebäude benötigen. Für Einsatzkräfte reserviert TECTIQ einen Notöffnungstransponder, der z. B. in einem Schlüsseldepot am Objekt oder bei der Einsatzzentrale hinterlegt ist.

Elektronischer Beschlag

Elektronische Beschläge geben nach der Kontrolle der Zutrittsberechtigung die Bedienung der Drücker frei. Sie sind in verschiedenen Ausführungen verfügbar.

Elektronischer Schließzylinder

Elektronische Schließzylinder koppeln nach der Kontrolle der Zutrittsberechtigung die Schließfunktion ein. Hierdurch kann der Zutrittsberechtigte die Tür öffnen und verriegeln.

Ereignisliste

Vom Zutrittskontrollsystem automatisch generierte Ereignisliste mit Informationen zur Nutzung und Anlagenbetreuung. Angezeigt werden u.a. Meldungen über erteilte oder verweigerte Zutrittsversuche, erfolgte Software-Aktualisierungen, Beschreiben von Schließmedien, Hinzufügen oder Löschen von Türkomponenten. Die Ereignisliste wird auf dem Dashboard des TECTIQ Access Managers angezeigt.

Facherrichter

Der Facherrichter ist der fachkundige Mitarbeiter des registrierten ABUS Fachhandelspartners, der die Zutrittskontrollanlage plant, umsetzt, programmiert und die Administratoren in die Anlage einweist.

Gesicherter Bereich

Bereich, der mittels geeigneter mechanischer oder anderer Mittel gegen unberechtigten Zutritt gesichert ist.

Gruppenberechtigung

Zutrittsberechtigungen zu Türgruppen oder einzelnen Türen können Personengruppen zugewiesen werden. Gruppenberechtigungen werden an die Mitglieder der Personengruppe vererbt. Sie können danach individuell für jede Person verändert werden. Werden Gruppenberechtigungen verändert, sind gegebenenfalls individuelle Berechtigungen neu einzustellen.

Gültigkeit, Gültigkeitsintervall

Die Gültigkeit von Zutrittsberechtigungen kann im Access Manager eingeschränkt werden. Es werden nachfolgende Möglichkeiten unterschieden:

Die generelle Personengültigkeit wird über das Anfangsdatum und Enddatum eingestellt (z.B. Firmeneintritt bis Renteneintritt, Beginn und Ende von Wartungen oder Reparaturen, Beginn und Ende einer zeitlich befristeten Beschäftigung). Wird kein Startdatum gesetzt, gilt die Berechtigung ab Anlage des Nutzers im System. Wird kein Enddatum gesetzt, ist die generelle Gültigkeit der Person nicht eingeschränkt.

Die Gültigkeit des TECTIQ Schließmediums ist in der Regel zeitlich begrenzt und muss nach Ablauf des einstellbaren Gültigkeitsintervalls an einem Update Terminal verlängert werden.

Gültigkeitsprüfung

Türkomponenten prüfen, ob Schließmedien aktuell gültig sind. Für Türgruppen besteht die Möglichkeit, die Gültigkeitsprüfung zu deaktivieren. Dies ist sinnvoll, um Personen, die über ein Schließmedium verfügen, z.B. die Zufahrt auf das Betriebsgelände an einer Parkplatzschanke zu ermöglichen.

Notöffnungstransponder

Der Notöffnungstransponder dient zur Notöffnung aller TECTIQ Türkomponenten mit der Sonderfunktion „Dauerhaft geöffnet“. Er ermöglicht Einsatzkräften den Zutritt zum gesicherten Gebäude oder Bereich. Der Notöffnungstransponder wird in der Regel in einem Feuerwehr-Schlüsseldepot am Objekt verwahrt.

Nutzer

Nutzer des TECTIQ Zutrittskontrollsystems ist eine vom Betreiber für den Zugang zu geschützten Bereichen berechtigte Person. Die Zugangsberechtigung gilt im Rahmen des vom Betreiber festgelegten Regelwerks für die für den Nutzer freigegebenen Bereiche. Der Nutzer erhält ein Schließmedium, auf das seine aktuellen Zutrittsberechtigungen vor der Nutzung übertragen werden. Die Speicherdauer der Zutrittsberechtigung auf dem Schließmedium kann vom Betreiber des Zutrittskontrollsystems eingestellt werden. Nutzer werden im TECTIQ Access Manager als „Person“ eingetragen. Personen können in Personengruppen mit gleichen Zutrittsberechtigungen zusammengefasst werden.

Parameterkarte

Die TECTIQ Parameterkarte ist ein Systemmedium und dient der Übertragung von Konfigurationsdaten aus der Zutrittskontrollzentrale auf die Türkomponente. Sowohl bei der Erstprogrammierung als auch bei Änderungen wird die Parameterkarte mit dem Tischleser beschrieben und vor Ort von der jeweiligen Komponente ausgelesen.

Person, Personengruppe

Nutzer und Inhaber eines TECTIQ Schließmediums in einer TECTIQ Zutrittskontrollanlage. Personen können als Personengruppen zusammengefasst und mit gleichen Rechten versehen werden. Die Einstellungen einer Personengruppe werden an die enthaltenen Personen vererbt.

Personengültigkeit

Siehe „Gültigkeit“

Protokollkarte

Die TECTIQ Protokollkarte ist ein Systemmedium. Sie liest Protokolldaten aus den TECTIQ Türkomponenten aus. Jede TECTIQ Türkomponente – Beschlag, Zylinder oder Wandleser – speichert bis zu 900 Einträge. Diese Einträge beinhalten z. B. erteilten oder verweigerten Zutritt, Batteriewarnungen oder -wechsel.

Resetkarte

TECTIQ Systemmedium zum Rücksetzen von TECTIQ Türkomponenten. Mit dem Rücksetzen wird die TECTIQ Türkomponente aus dem TECTIQ Zutrittskontrollsystem entfernt. Beim ersten Präsentieren der Resetkarte an der Türkomponente wird die Komponente zurückgesetzt. Beim zweiten Präsentieren erfolgt die Rücksetzung der Türkomponente auf Werkseinstellungen (Auslieferungszustand). Die systemspezifische Anlagennummer bleibt erhalten.

Schließmedium

Ein TECTIQ Schließmedium ist ein Transponder zum Öffnen und/oder Verschließen eines mit einer TECTIQ Türkomponente gesicherten Bereiches. Elektronische Schließmedien enthalten Daten zur Zutrittsberechtigung, die mit geeigneten Geräten gelesen und beschrieben werden. Die Daten sind durch spezielle Verschlüsselungstechniken geschützt.

Schließplan

Der Schließplan zeigt die aktuellen Berechtigungen für Personen/Personengruppen und Türen/Türgruppen übersichtlich an. Im Schließplan können Personen und Personengruppen Zutrittsberechtigungen zu Türen oder Türgruppen erteilt, geändert oder entzogen werden.

Schließzylinder

Siehe „Elektronischer Schließzylinder“

Schranke

Eine Schranke versperrt die Zufahrt zum Betriebsgelände. Schranken können über Türgruppen so eingestellt werden, dass durch Präsentieren des Schließmediums eine Öffnung ohne Gültigkeitsprüfung für das Schließmedium stattfindet.

Sperrliste

Liste in der Zutrittskontrollzentrale in der gesperrte Schließmedien gespeichert sind. Die Sperrliste muss mittels Blacklistkarte auf die Türkomponente übertragen werden, um den unbefugten Zutritt zum gesicherten Bereich zu verhindern. Die Sperrung des Schließmedium ist erst nach Übertragung wirksam.

Sperrtage

Sperrtage sind Tage, an denen die zugewiesene Zutrittsberechtigung nicht gültig ist (z.B. während Betriebsferien, an Feiertagen und sonstigen betriebsfreien Tagen).

Systemmedium

TECTIQ Systemmedien sind – wie Schließmedien – elektronische Transpondersysteme und haben spezielle Aufgaben in einer TECTIQ Anlage (Parameterkarte, Protokollkarte, Blacklistkarte, Resetkarte, Notöffnungstransponder)

Systemkomponenten

Aufeinander abgestimmte Bestandteile des ABUS TECTIQ Zutrittskontrollsystems. Systemkomponenten sind die

Komponenten im System, die nicht direkt einem Zutritt an einer Tür zugeordnet werden. In erster Linie betrifft das Update Terminals.

TECTIQ Anlage

Kurzbezeichnung für ein auf die lokalen Gegebenheiten abgestimmtes TECTIQ Zutrittskontrollsystem.

Tischleser

Der TECTIQ Tischleser dient zum Lesen und Beschreiben von Schließmedien und Systemmedien. Der TECTIQ Tischleser wird zur Inbetriebnahme des Systems, bei Änderungen und zum Erteilen von Zugriffsrechten benötigt. Er wird über einen USB-Anschluss an den Computer angeschlossen, auf dem die Schließsoftware TECTIQ Access Manager läuft. Optional kann der TECTIQ Tischleser die Funktion des TECTIQ Update Terminals zur Aktualisierung von Zutrittsberechtigungen auf den Schließmedien übernehmen.

Tür, Türgruppe

In einer TECTIQ Anlage steht eine Tür gleichbedeutend mit der Leseinheit einer Türkomponente. Komponenten mit zwei Leseinheiten – z. B. doppelseitige Schließzylinder oder Wandleser – werden in der Software Access Manager als zwei Türen geführt. Türen können in der Software als Türgruppen zusammengefasst und mit gleichen Rechten versehen werden. Die Einstellungen einer Türgruppe werden an die enthaltenen Türen vererbt.

Türkomponenten

TECTIQ Türkomponenten arbeiten elektronisch und ermöglichen berechtigten Personen den Zutritt zu einem gesicherten Bereich. Zu den Türkomponenten zählen elektronische Schließzylinder, elektronische Beschläge und Wandleser.

Update Terminal

Das TECTIQ Online Update Terminal ist über Netzwerk mit der Zutrittskontrollzentrale verbunden. Es besteht aus einem Wandleser, kombiniert mit dem zugehörigen Steuergerät. Das Online Update Terminal dient zum Lesen und Beschreiben von Schließmedien und Systemmedien, Aktualisieren von Zutrittsrechten und Weiterleiten von Informationen, Ereignissen und Rückmeldungen der Offline Türkomponenten (erfolgte Zutritte, Batteriewarnungen etc.) an die TECTIQ Zutrittskontrollzentrale.

Optional kann das Online Update Terminal einen Türöffner oder einen Türantrieb ansteuern.

Vereinzelungsanlagen

Vereinzelungsanlagen sind bauliche Anlagen zur Zutrittssteuerung zu einem Raum oder Gelände, z.B. Drehkreuze.

Vertrauenspersonen

Vertrauenspersonen genießen in ihrem Bereich besonderes Vertrauen, z. B. Betriebs- oder Personalräte, Mobbing-Beauftragte oder medizinisches Personal.

Wandleser

Der TECTIQ Wandleser ist eine Türkomponente zum Ansteuern von elektronischen Schließkomponenten, wie elektronische Türöffner, Türantriebe und Tore. Er besteht aus Leseinheit und Steuereinheit und wird durch Präsentieren des Schließmediums betätigt.

Zeitplan

Über Zeitpläne kann die Zutrittsberechtigung auf einzustellende Zeitintervalle (z.B. montags bis mittwochs, 9:00 Uhr bis 16:00 Uhr) begrenzt werden. Ein Zeitplan kann mehrere Zeitintervalle enthalten. Jeder Zeitplan kann zusätzlich bis zu 30 Sperrtage enthalten.

Jeder Person ist nur ein Zeitplan zuzuweisen. Er kann über die Personengruppe an die Person vererbt werden oder als individueller Zeitplan für eine Person eingerichtet werden.

Zutrittsberechtigung

Eine Person erhält die grundsätzliche Zutrittsberechtigung zu ausgewählten gesicherten Bereichen, wenn Sie hierzu autorisiert ist – i. d. R. durch den Besitz eines persönlichen Schließmediums. Zutrittsberechtigungen für die

gesicherten Bereiche werden auf dem Schließmedium gespeichert und haben eine begrenzte Gültigkeit. Sie müssen aktualisiert und validiert werden (am Update Terminal) und können mithilfe eines voreingestellten Zeitplans verknüpft werden.

Zutrittskontrollsystem, auch: Zutrittssystem

Das ABUS TECTIQ Zutrittskontrollsystem ist ein flexibles und skalierbares, elektronisches Sicherheitssystem, das es Betreibern gewerblicher und öffentlicher Gebäude und Objekte nahezu jeder Größe ermöglicht, mittels elektronischer Schließmedien Personen den Zugang zu gesicherten Bereichen im Rahmen des vom Betreiber festgelegten Regelwerks zu gewähren.

Das Zutrittskontrollsystem besteht aus den Komponenten TECTIQ Zutrittskontrollzentrale, TECTIQ Access Manager, TECTIQ Tischleser, TECTIQ Systemkomponenten, TECTIQ Türkomponenten sowie TECTIQ Schließ- und Systemmedien.

Zutrittskontrollzentrale, auch: Zentrale

Die TECTIQ Zutrittskontrollzentrale ist Kern des Zutrittskontrollsystems. Auf ihrer Hardware laufen sämtliche Datenbanken, Konfigurationen und Services. Sie speichert die zu steuernden Türen, die Nutzer der Anlage und deren Zutrittsrechte. Die TECTIQ Zutrittskontrollanlage wird mit dem Accessmanager entsprechend des Bedarfs des Betreibers eingerichtet und verwaltet. Der Access Manager läuft auf einem PC und greift über eine sichere Verbindung auf die Zutrittskontrollzentrale zu. Mit dem Access Manager und einem TECTIQ Tischleser werden die Daten aus der Zutrittskontrollzentrale auf Schließmedien und Systemmedien übertragen. In Anlagen mit TECTIQ Update Terminals kommuniziert die TECTIQ Zutrittskontrollzentrale über feste gesicherte Verbindungen direkt mit den Schließmedien und Systemmedien.

21. Stichwortverzeichnis

- Access Manager 9, 17, 35, 53, 54
- Access Manager – Oberfläche 65
- Admin App 9, 59
- Aktualisieren von Zutrittsrechten 55
- Aktualisierung 9, 15
- Aktualisierungsvorgang 57
- Anlagennummer 109
- Arbeitsbereich 65
- Aufgabenliste 73
- Batteriewarnungen 73
- Bedienschritte 14
- berechtigte Personen 10
- berechtigter Nutzer 56
- Beschlag 9, 10, 47
- Bestimmungsgemäße Verwendung 53
- Blacklistkarte 13, 28, 58
- Connect ID 38
- Dashboard 40, 65
- Data-on-Card 10
- Datenschutz 116
- Datensicherheit 13
- Datensicherung 113
- Datum und Uhrzeit 39
- Diebstahl 12
- durchgängige Berechtigung 50
- Editierbereich 65
- Elektronischer Beschlag 56
- Elektronischer Schließzylinder 56
- Elektronisches Vorhangeschloss 57
- Empfangsquittung 19
- Ereignisliste 13, 74
- Ereignisse 12
- Fachhandelspartner 12
- Fernzugriff 12
- Firmware 40
- Firmware Update 112
- Freigabedauer 46
- Gerätename 109
- gesicherter Bereich 10, 56
- Gesicherter Bereich 15
- Gruppenberechtigung 83
- Gruppenberechtigungen 25, 78
- Gültigkeit 10, 11
- Gültigkeit der Schließmedien 115
- Gültigkeit der Zutrittsrechte 88
- Gültigkeit des Schließmediums 24, 89
- Gültigkeitsprüfung 93
- Individuelle Zutrittsberechtigungen 78
- IP Adresse 109
- Kompaktmontage 34
- LED-Signale 16, 119
- Leitungsführung 34
- Listen 70
- Löschen eines Nutzers 24
- Netzwerkeinstellung 110
- Netzwerkeinstellungen 41
- neue Nutzer 19
- Notöffnungstransponder 28, 58
- offline 10
- Offline Türkomponenten 56
- Online Account 36
- Online Terminal 104
- Online Update Terminal 55
- Parameterkarte 28, 48, 57
- Passwortschutz 13
- permanente Zutrittsberechtigung 23
- Person 10
- Personen 49, 80
- Personengruppe 49
- Personengruppen 10, 25, 81
- persönliches Schließmedium 10
- Protokolldaten 11
- Protokollkarte 28, 58
- Relaiskonfiguration 46
- Resetkarte 28, 58
- Rollenverwaltung 118
- Schließanlagensoftware 9
- Schließmedien 9, 57, 116
- Schließmedien programmieren 51
- Schließmedium 11
- Schließmedium hinzufügen 89
- Schließplan 9, 22, 75
- Schließzylinder 9, 15
- Schlüsselausgabeprotokoll 90
- Schnell Tasten 69
- Schranke 93
- Seriennummer 109
- Sichten 65
- Skalierbarkeit 12
- Sperrliste 13, 71
- Sperrtage 11, 100
- Sperrung 13
- Sperrung des Schließmediums 16, 71
- Sperrung eines Schließmediums 29
- Statusmeldungen 12
- Systemaufbau 60
- Systemeinstellungen 28, 107
- Systemkomponenten 33, 103
- Systemmedien 9, 42, 57, 117
- Systemmeldungen 12
- Systemstatus 68
- Systemwarnungen 72
- Technische Daten 63
- Terminal Verbindungsstörungen 74
- Tischleser 9, 55
- Türen 45, 91
- Türfunktion freigeben 15
- Türgruppen 45, 91
- Türkomponente hinzufügen 96
- Türkomponenten 9, 10, 11, 45, 91
- Türkomponenten programmieren 48
- Uhrzeit 39
- Unbefugte Zutrittsversuche 13, 71
- Update Terminal 9, 11, 34, 41
- Update Terminal als Türkomponente 46
- Validierung 9, 10
- Vereinzelungsanlage 10, 131, 134
- Verlust 12

Verlust eines Schließmediums 71
verriegeln 15
Verschlüsselungsverfahren 13
Verwaltung der Zutrittsberechtigungen 17, 19
Verwaltung von Systemmedien 17
Wandleser 9, 46, 55, 56
Wiederherstellung 113
Zeiteinstellungen 111
Zeitintervall 99
Zeitplan 23, 32, 83
Zeitpläne 9, 10, 11, 48, 98
Zutrittsberechtigung 75
Zutrittsberechtigung ändern 15
Zutrittsberechtigungen 10, 11, 50
Zutrittskontrollanlage 11, 17, 33
Zutrittskontrollsoftware 35, 53
Zutrittskontrollsystem 9, 60
Zutrittskontrollzentrale 9, 11, 37, 53
Zylinder 10, 47

ABUS | Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel.: +49 82 07 959 90-0
Fax: +49 82 07 959 90-100

sales@abus-sc.com

©
Alle Rechte vorbehalten.

11 / 2024