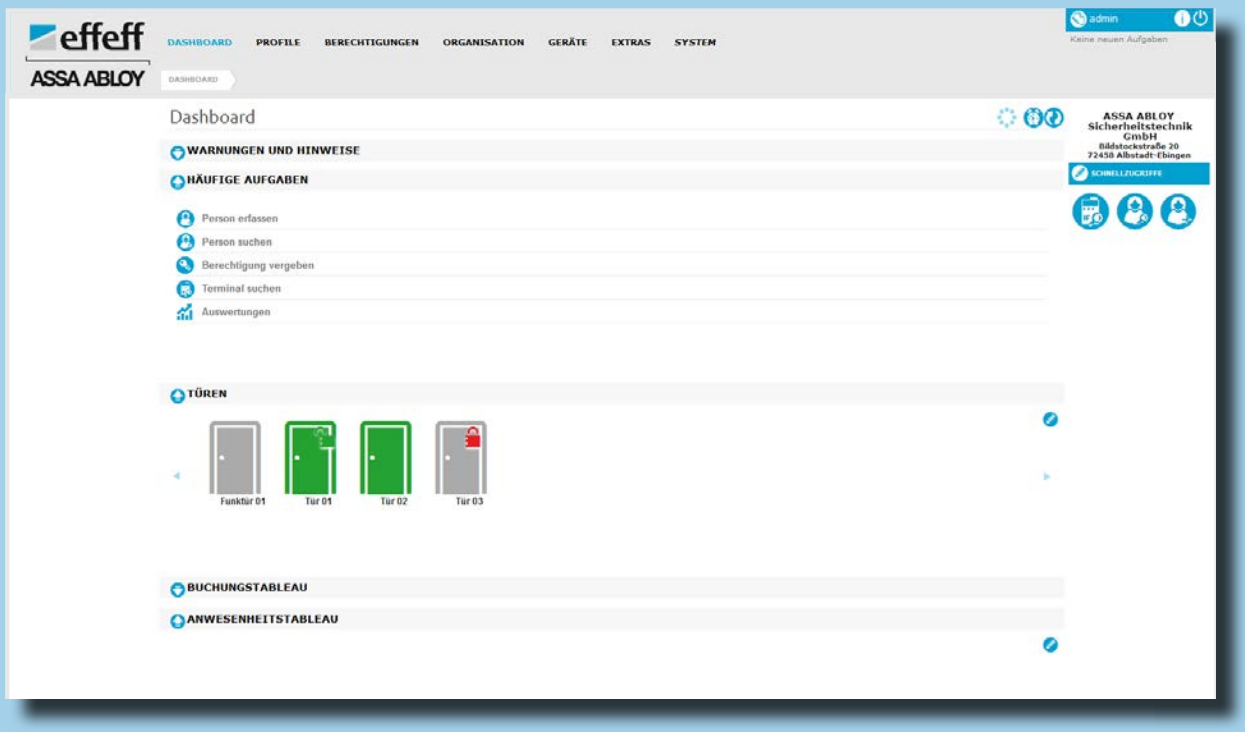
SCALA net



Software SCALA net

Benutzerhandbuch

D0104309

effeff
ASSA ABLOY

Experience a safer
and more open world

Lesen Sie diese Anleitung vor der Benutzung sorgfältig durch und bewahren Sie sie auf. Die Anleitung beinhaltet wichtige Informationen zum Produkt, insbesondere zum bestimmungsgemäßen Gebrauch, zur Sicherheit, Montage, Benutzung, Wartung und Entsorgung.

Geben Sie die Anleitung nach der Montage an den Benutzer und im Falle einer Weiterveräußerung mit dem Produkt weiter.

Softwareversion ab SCALA net V13

Diese Anleitung bezieht sich auf die angegebene Softwareversion.

Eine aktuelle Version dieser Anleitung ist im Internet verfügbar:
https://aa-st.de/file/d01043

Hinweis zu Produkten und Dienstleistungen Dritter

Alle in dieser Anleitung genannten Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

- Microsoft Windows® ist ein eingetragenes Warenzeichen der Microsoft® Corporation.
- Oracle™ ist ein eingetragenes Warenzeichen der ORACLE® Corporation.
- Java™ ist ein eingetragenes Warenzeichen der ORACLE® Corporation.
- OpenJDK ist ein eingetragenes Warenzeichen der ORACLE® Corporation.
- OpenWebStart ist eine Open-Source-Lösung der Karakun AG.
- Apache Tomcat™ and Tomcat™ sind eingetragene Warenzeichen der The Apache Software Foundation® Corporation.
- MIFARE™, DESFire™ und MIFARE™ classic sind eingetragene Warenzeichen der XP Semiconductors Austria GmbH Styria.
- LEGIC® Standard, LEGIC® prime und LEGIC® Advant sind eingetragene Warenzeichen der LEGIC Identsystem AG.
- OSS-Association e.V.® ist ein als Verein eingetragener Zusammenschluss von Herstellerunternehmen des Marktes für Sicherheitstechnik.
- ASSA ABLOY Aperio® ist ein eingetragenes Warenzeichen der ASSA ABLOY Sicherheitstechnik GmbH.
- ASSA ABLOY CLIQ® ist ein eingetragenes Warenzeichen der ASSA ABLOY Group.

Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung bezüglich Produkten und Dienstleistungen, die nicht von *ASSA ABLOY Sicherheitstechnik GmbH* hergestellt oder bereitgestellt werden. *ASSA ABLOY Sicherheitstechnik GmbH* macht sich diese Produkte und Dienstleistungen nicht zu eigen.

Herausgeber

ASSA ABLOY Sicherheitstechnik GmbH
Bildstockstraße 20
72458 Albstadt
DEUTSCHLAND
Telefon: +49 (0) 7431 / 123-0
E-Mail: albstadt@assaabloy.com
Internet: www.assaabloy.com/de

Dokumentennummer, -datum

D0104309 12.2024

Copyright

Inhaltsverzeichnis

Die Software SCALA net

Zutrittskontrollsystem für große Gebäudekomplexe

SCALA net ist ein Zutrittskontrollsystem für große Gebäudekomplexe mit unterschiedlichsten Gebäudebereichen. Die Software *SCALA net* steuert und kontrolliert auf einfache Weise Zugangsberechtigungen für Personen und Personengruppen zu geschützten Bereichen, zum Beispiel Haupt- oder Nebeneingängen von Gebäuden oder einzelnen Räumen wie Laboren, Entwicklungsabteilungen, Tresorräumen oder anderen sicherheitsrelevanten Bereichen. Auftretende Ereignisse und Alarme werden chronologisch gespeichert und können jederzeit ausgewertet werden.

Online-Lesertypen (nur SCALA Leser)

Es werden drei SCALA-Lesertypen unterschieden: Online-, Validier- und Segmentier-Leser. Dabei bieten alle drei Lesertypen immer mindestens die Online-Leser-Funktion. Validier- und Segmentier-Leser bieten zusätzliche Funktionen.

Online-Leser

Ein Online-Leser liest die Transponderkennung oder die UID eines vorgehaltenen Transponders und überträgt die Daten zum Controller.

Validier-Leser (nur SCALA Leser)

Ein Validier-Leser (auch Update-Leser oder Schreib-Leser genannt) speichert zutrittsrelevante Daten auf Transponder und liest eventuell vorhandene Ereignisse aus.

Segmentier-Leser (nur SCALA Leser)

Auf einem neuen Transponder muss eine festgelegte Datenstruktur (Applikation) angelegt werden. Ein Segmentier-Leser speichert einmalig diese Applikation auf einen Transponder und schreibt die in *SCALA net* hinterlegte Transponderkennung hinein. *SCALA net* identifiziert den Transponder anschließend immer anhand der Transponderkennung und nicht mehr anhand der UID (Seriennummer) des Transponders.

Der Zeitpunkt der Segmentierung wird in den Stammdaten des Transponders gespeichert.

Hinweis!

Keine unsegmentierten Transponder ausgeben: ASSA ABLOY empfiehlt Transponder grundsätzlich, zum Beispiel mit dem *SCALA Desktop-Codierer* zu segmentieren. Sodass kein unsegmentierter Transponder im Umlauf ist.

Online- und Offline-System

Mit *SCALA net* können Türen online und offline verwaltet werden, je nach Ausstattung mit Elektronikzylindern und -beschlägen.

Online

Online-Türen

Online-Türen sind über Draht oder Funk direkt mit *SCALA net* verbunden und werden wie auch die Ausweise zentral verwaltet. Wird ein Ausweis gelesen, erfolgt die Reaktion des Türcontrollers in Echtzeit. Die Berechtigung eines Ausweise wird sofort ausgewertet. Änderungen in *SCALA net* sind sofort wirksam, zum Beispiel geändert Zutrittsberechtigungen.

- *Online über Drahtverbindung:* Die Leser sind über ein Kabel an einen Türcontroller angeschlossen (Abb. 1 – 1).
- *Online über Funkverbindung:* Als Leser arbeiten hier elektronische Zylinder, Beschläge oder Schlösser, die per Funk mit einem Hub kommunizieren. Der Hub ist über ein Kabel an einen Türcontroller angeschlossen (– 2).

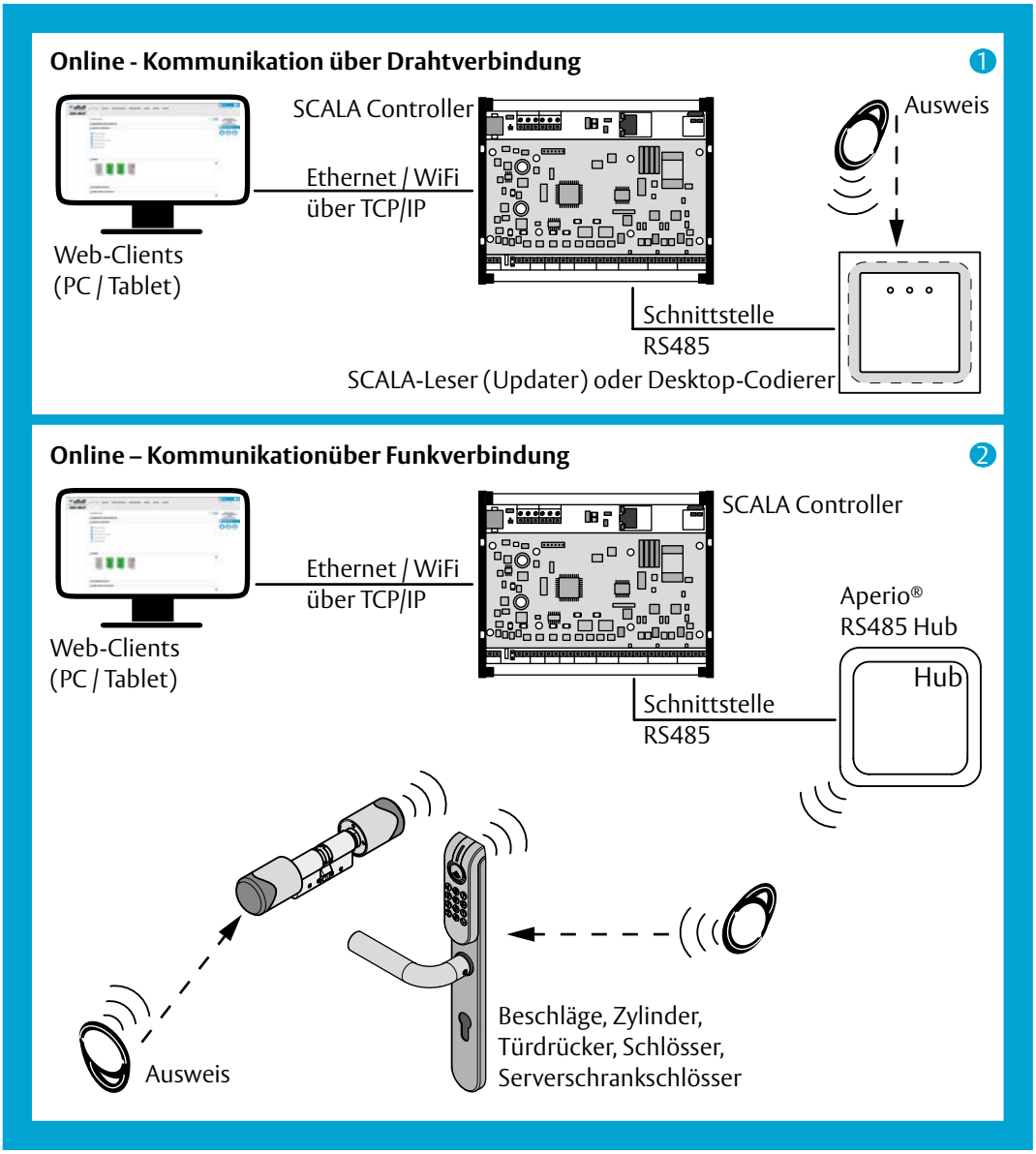


Abb. 1: Kommunikationswege bei Online-Türen

Offline

Offline-Türen

Offline-Türen haben keine Verbindung über Draht oder Funk zu *SCALA net*. Offline-Türen werden zentral verwaltet und anschließend werden die geänderten Daten über dazu vorbereitete Parameterkarten an die Offline-Türen übertragen und auch von dort gelesen.

Parameterkarten sind äußerlich normale Ausweise, die über eine besondere Datenstruktur verfügen. So vorbereiten dienen sie als *Schlossparameterkarte (SPK)*, *Protokolltransportkarte (PTK)* und *Blacklist-Karte (BLK)* (II – Hinweise, Begriffserklärung).

Anders als bei Online-Türen erfolgt die Datenübertragung nicht in Echtzeit. Die Kommunikation der Leser mit *SCALA net* erfolgt zeitversetzt, da die Daten über die Parameterkarten transportiert werden müssen. Die Parameterkarten werden an Online-Update-Lesern („Online“, Seite 8) beschrieben und an den Schließzylindern der Offline-Türen gelesen und umgekehrt.

Parameterkarten werden keiner Person zugeordnet und besitzen keine Zutrittsberechtigungen.

Für die Definition der Datenstruktur auf den Parameterkarten Unterstützt *SCALA net* zwei alternative Standards, die sich gegenseitig ausschließen:

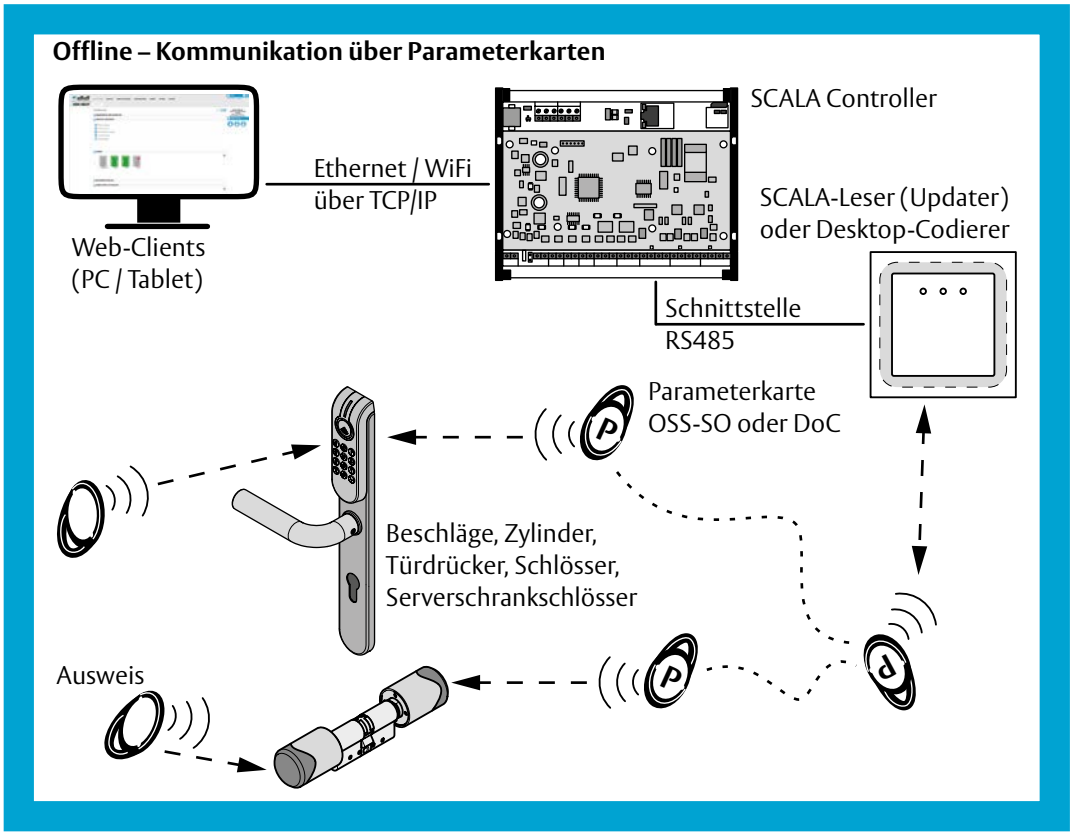
- OSS-SO Open Security Standards - Standard Offline oder
- *DoC* Data on Card

Vorteilhaft ist, dass ein einmal bestehendes Netzwerk ohne zusätzliche Verkabelung jederzeit um beliebig viele Offline-Türen erweitert werden kann.

Es kann jeweils nur eine aktive *Schlossparameterkarte (SPK)*, *Protokolltransportkarte (PTK)* und *Blacklist-Karte (BLK)* geben. Wird eine der Karte verloren, muss sie aus *SCALA net* gelöscht werden und anschließend neu angelegt werden.

Müssen viele Ausweise beschrieben und gelesen werden, empfiehlt *ASSA ABLOY Sicherheitstechnik* einen *Desktop-Codierer* als Update-Leser.

Abb. 2: Kommunikationswege bei Offline-Türen



Verschlüsselung der Kommunikation mit SCALA-Komponenten

Die Kommunikation über den RS485-Bus kann verschlüsselt erfolgen. Empfohlen wird eine Verschlüsselung für Bus-Teilnehmer, die eine Schließhardware ansteuern, um zum Beispiel eine Tür freizugeben.

Die Verschlüsselung wird von *SCALA net* kontrolliert. Die Verschlüsselungscodes (Code-Schlüssel) werden in SCALA net verwaltet und nach dem Top-Down-Prinzip an die Komponenten verteilt. Dabei wird die unverschlüsselte Komponenten-UID zur eindeutigen Zuordnung verwendet. Jede Komponente kann einen individuellen Schlüssel verwenden. Falls im Einzelfall eine Komponente manipuliert werden konnte, bleiben die anderen sicher.

Die Verschlüsselung muss für eine Komponente im Einzelfall aktiviert bzw. deaktiviert werden (Kapitel IV Systemkonfiguration - Verschlüsselung der Datenübertragung).

Arbeiten mit der Software SCALA net

Der Benutzer verwaltet und pflegt alle relevanten Zutrittskontrolldaten in logischen und zusammenhängenden Dialogschritten, die aufeinander aufbauen. Eine Fehlbedienung oder Fehleingabe wird durch Hilfestellungen weitestgehend verhindert. Die Bedienerführung ist intuitiv, wobei die Abläufe möglichst einheitlich wiederholt werden. Im Hintergrund laufen intelligente Plausibilitätsprüfungen zur permanenten Kontrolle der Eingabe ab.

Planung des Zutrittskontrollsystems

Entscheiden Sie je nach Sicherheitsanforderungen, wie Ihre Hardware ausgestattet werden soll, zum Beispiel *Türen*. Grundsätzlich gibt es *Online-Geräte* und *Offline-Geräte*, die sich in der Ausstattung, Verkabelung sowie in der erreichbaren Sicherheit unterscheiden („Online- und Offline-System“, Seite 8).

Es werden vier Sicherheitsstufen unterschieden (Tab. 1).

Tab. 1: Sicherheitsstufen

Hohe Sicherheit	Bei Online-Türen mit verkabeltem Wandleser, Rückmeldekontakt und zum Beispiel Motorschloss. Eine Zutrittsentscheidung im *SCALA Controller* erfolgt in Echtzeit.
Mittlere Sicherheit	Bei Online-Türen mit Aperio® Funk-Komponenten, ohne Verkabelung am Türblatt. Die Aperio® Komponenten kommunizieren in Echtzeit über einen Funk-Hub mit dem *SCALA Controller*. Eine Zutrittsentscheidung im *SCALA Controller* erfolgt in Echtzeit.
Mäßige Sicherheit	Bei Online-Türen mit Aperio® Offline-Komponenten, ohne Verkabelung am Türblatt. Die Zutrittsberechtigungen werden auf den Nutzer-Transponder geschrieben und haben eine zeitlich begrenze Gültigkeit, normalerweise für einen Tag. Über Validier-Leser („Validier-Leser (nur SCALA Leser)“, Seite 7) werden Berechtigungen auf den Transponder aktualisiert.
Geringe Sicherheit	bei Türen, die nicht über das Zutrittskontrollsystem verwaltet werden

Komponenten im Überblick

Die Software SCALA net

Die Software *SCALA net* ist auf einem Server (oder PC) des Unternehmens installiert und kommuniziert mit den *SCALA Controllern*. Die *Scala net* Datenbank enthält alle Informationen über das System. Mit der Software *SCALA net* werden alle Einstellungen des Zutrittskontrollsystems vorgenommen und verwaltet.
Änderungen im System können an mehreren Arbeitsplätzen gleichzeitig vorgenommen werden, da alle Clients gleichzeitig auf den Server zugreifen können.

SCALA Controller

Die *SCALA Controller* kommunizieren über TCP/IP mit dem *SCALA net Server*. Die Türkomponenten sind an den *SCALA Controllern* angeschlossen und werden durch diese gesteuert.
Die Konfiguration der Hardware wird durch die Software unterstützt.

Folgende Funktionen können genutzt werden:
- Verwendung von vordefinierten Standard-Konfigurationen,
- eigene Konfigurationen, die als Vorlage definiert sind,
- Konfigurationsdaten können grafisch angezeigt werden,
- Konfigurationsdaten können als PDF-Datei gedruckt werden und
- automatische Systemdokumentation.

Micro-SD-Karte für SCALA Controller

Die Micro-SD-Karte des zugehörigen *SCALA Controllers* wird direkt am Arbeitsplatz des Benutzers konfiguriert. Folgende Vorteile können genutzt werden:
- Automatisches Erstellen einer Micro-SD-Karte für einen *SCALA Controller*,
- keine Konfiguration des *SCALA Controllers* notwendig,
- Inbetriebnahme erfolgt über Einstecken der Micro-SD-Karte mit automatischer Anmeldung am definierten Server,
- einfacher Austausch (zum Beispiel bei Beschädigung oder Verlust) durch neue Micro-SD-Karte und
- Protokolle (LOG-Dateien) mit allen systemrelevanten Meldungen sind vorhanden.

Integrierter Webserver für SCALA Controller

Der integrierte *Webserver* für *SCALA Controller* dient der Ferndiagnose. Der *SCALA Controller* kann über seine IP-Adresse direkt angesprochen werden. Die Anmeldung (Login) erfolgt mit Benutzernamen und Passwort.

SCALA-Leser

Die *SCALA Leser* werden über den RS485-Bus mit dem *SCALA Controller* verbunden. Die *SCALA Leser* geben Transponder-Daten an den *SCALA Controller* weiter. Die Leser sind in unterschiedlichen Lesetechnologien und Bauformen verfügbar.

Weitere Türkomponenten

An *SCALA net* können unterschiedliche Türkomponenten angeschlossen und verwaltet werden, zum Beispiel Türöffner, Motorschlösser und Türkontakte.

Zubehör

Für das Zutrittskontrollsystem *SCALA net* gibt es verschiedene *SCALA Controller*, elektronische Schließzylinder und -beschläge, Motorschlösser, Lesegeräte, Türöffner und Identmittel.

Zu dieser Anleitung

Diese Anleitung wurde für eingewiesenes Personal mit PC-Grundkenntnissen geschrieben. Lesen Sie diese Anleitung, um das System sicher zu betreiben und die zulässigen Einsatzmöglichkeiten auszunutzen.

Die Anleitung gibt Ihnen auch Hinweise über die Funktion wichtiger Bauteile.

Zu den Abbildungen

Die Abbildungen sind mit der im Impressum genannten Softwareversion oder älteren Versionen erstellt worden. Zudem wurden viele Abbildungen bearbeitet und vereinfacht, um den beschriebenen Kontext zu verdeutlichen. Abweichungen in der farblichen Darstellung oder Gestaltung gegenüber der aktuellen Softwareversion sind möglich, haben aber keine Bedeutung für die Beschreibung der Softwareversion.

Hardware

Die Montage und Installation der Hardware wird in dieser Anleitung nicht beschrieben. Lesen Sie dazu die den Hardwarekomponenten beiliegenden Anleitungen und lassen Sie sich von *ASSA ABLOY Sicherheitstechnik* beraten.

Bedeutung der Symbole

Gefahr!

Sicherheitshinweis: Nichtbeachtung führt zu Tod oder schwerer Verletzung.

Warnung!

Sicherheitshinweis: Nichtbeachtung kann zu Tod oder schweren Verletzungen führen.

Vorsicht!

Sicherheitshinweis: Nichtbeachtung kann zu Verletzungen führen.

Achtung!

Hinweis: Nichtbeachtung kann zu Materialschäden führen und die Funktion des Produkts beeinträchtigen.

Hinweis!

Hinweis: Ergänzende Informationen zur Bedienung des Produkts.

Sicherheitshinweise

Warnung!

Lebensgefahr durch Stromschlag: Ein Stromschlag ist lebensgefährlich und kann zu schweren Verletzungen führen.
- Lassen Sie alle Arbeiten an elektrischen Anlagen und Anschlüssen durch eine Handwerksfachkraft erledigen.

Lebensgefahr durch fehlerhafte oder beschädigte elektrische Installation: Eine fehlerhafte oder beschädigte elektrische Installation kann lebensgefährlich sein und kann zu schweren Verletzungen führen oder auch Brände auslösen.
- Lassen Sie alle elektrischen Anlagen und Anschlüsse regelmäßig durch eine Handwerksfachkraft prüfen.
- Lassen Sie eine elektrische Anlage oder einen Anschluss sofort durch eine Handwerksfachkraft prüfen, wenn es Hinweise auf Fehlfunktionen gibt.

Achtung!

Sachbeschädigung durch fehlerhafte elektrische Installation: Durch einen fehlerhaften elektrischen Anschluss, zum Beispiel eine unpassende Spannungsversorgung, können elektrische Komponenten beschädigt oder zerstört werden.
- Lassen Sie alle Arbeiten an elektrischen Anlagen und Anschlüssen durch eine Handwerksfachkraft erledigen.

Datenverlust durch technischen Verschleiß: Die Systemkonfiguration kann durch technischen Verschleiß verloren gehen, zum Beispiel durch eine defekte Festplatte. Mit einer regelmäßigen Datensicherung lässt sich der Aufwand für eine Neukonfiguration minimieren.
- Erstellen Sie regelmäßig Datensicherungen (Backup).

Diebstahl oder Missbrauch von Dateien der Datensicherung: Die erstellten Datensicherungen werden in Dateien abgelegt und können anschließend frei kopiert werden.
- Speichern Sie Datensicherungsdateien immer so ab, dass ausschließlich autorisierte Personen auf die Dateien zugreifen können.

Sabotage und Datenmissbrauch durch öffentlich zugängliche Anmeldedaten: Werden Anmeldedaten öffentlich, können diese für Sabotage am System, Datendiebstahl und Datenmissbrauch verwendet werden.
- Beachten Sie, dass Anmeldedaten, insbesondere Passwörter, niemals laut ausgesprochen werden. Auch das Aufschreiben von Anmeldedaten ist unnötig. Hat ein Benutzer sein Passwort vergessen, löscht der Administrator das gespeicherte Passwort und vergibt ein neues.
- Sollte das Administrator-Passwort vergessen werden, kontaktieren Sie den Support.

Sicherheitslücken durch fehlende Updates und Kontrollen: Der Administrator muss sicherstellen, dass bekannte Sicherheitslücken geschlossen werden. ASSA ABLOY stellt bei Bedarf aktuelle Informationen im Internet bereit.
Regelmäßig – ASSA ABLOY empfiehlt monatlich – durchführen:
- Überprüfen Sie den ordnungsgemäßen Zustand der Daten und Buchungen.
- Beachten Sie die Informationen, die ASSA ABLOY im Internet bereit hält.
- Beachten Sie die vom Hersteller Ihres Endgeräts und des Betriebsystems im Internet bereitgestellten Informationen.

www.assaabloy.com/de

Bestimmungsgemäßer Gebrauch

SCALA net ist ein Zutrittskontrollsystem zum Steuern, Kontrollieren und Verwalten von Zutrittsberechtigungen für Personen zu geschützten Bereichen, zum Beispiel Haupt- oder Nebeneingängen von Gebäuden oder einzelnen Räumen wie Laboren, Entwicklungsabteilungen, Tresorräumen oder anderen sicherheitsrelevanten Bereichen.

SCALA net kontrolliert den Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen und protokolliert auftretende Ereignisse und Alarme zur späteren Auswertung.

Die Systemkonfiguration und -administration erfolgt über die Software *SCALA net*. Sie kann für beliebig viele Computer im Netzwerk lizenziert oder über das Internet eingesetzt werden.

Gesetzliche Bestimmungen, Normen, Richtlinien, Anleitungen und weitere Begleitdokumente zu angeschlossenen Türen und Komponenten müssen im Einzelnen beachtet, eingehalten und umgesetzt werden.

Die Erfassung und Verarbeitung personenbezogener Daten darf ausschließlich entsprechend der EU-Datenschutzgrundverordnung (DSGVO) erfolgen. Verantwortlich ist die „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; ...“ (DSGVO Art. 4)

Es muss geprüft und sichergestellt sein, dass alle Funktionen und Eigenschaften von angeschlossenen Türen und Komponenten, insbesondere in Flucht- und Rettungswegen (zum Beispiel Paniktüren und Notausgangstüren) und anderen sicherheitsrelevanten Bereichen entsprechend der jeweils zugehörigen Begleitdokumente vollständig funktionieren. Dies gilt unabhängig vom Funktionszustand des Zutrittskontrollsystems, zum Beispiel bei einem Stromausfall.

Vorgeschriebene Wartungsintervalle von angeschlossenen Türen und Komponenten sind von *SCALA net* unabhängig und müssen entsprechend der jeweiligen Normen, Richtlinien und Begleitdokumente durchgeführt werden.

SCALA net ist für die Nutzung entsprechend dieser Anleitung geeignet.

Jede darüber hinausgehende Verwendung gilt als nicht bestimmungsgemäß.

Entsorgung

Für Produkte, die mit dem Symbol (durchgestrichene Mülltonne) gekennzeichnet sind gilt:

Die geltenden Vorschriften zum Umweltschutz müssen eingehalten werden. Batterien, Akkumulatoren, Lampen, Elektrogeräte und auch personenbezogene Daten gehören nicht in den Hausmüll.

Altbatterien, Altakkumulatoren und Lampen müssen dem Gerät zerstörungsfrei entnommen werden und separat entsorgt werden.

Verpackung

Verpackungsmaterialien müssen der Wiederverwendung zugeführt werden. Das Verpackungsmaterial kann auch am Ort der Übergabe dem Vertreiber oder Fachhandwerker kostenlos zur Entsorgung überlassen werden.

Personenbezogene Daten

Personenbezogene Daten müssen vor der Entsorgung des Produkts gelöscht werden. Der Endnutzer ist dafür selbst verantwortlich.

Produkt

WEEE-Reg.-Nr. DE 69404980
Das Produkt ist nach dem Gebrauch als Elektronikschrott ordnungsgemäß zu entsorgen und zur stofflichen Wiederverwendung einer örtlichen Sammelstelle kostenlos zuzuführen.

Es bestehen grundsätzlich folgende weitere Möglichkeiten zur kostenlosen Entsorgung beim Vertreiber:

- Rückgabe eines funktionsähnlichen Altgeräts am Ort der Abgabe des Neugeräts.
- Rückgabe von maximal drei gleichartigen Altgeräten (max. Kantenlängen 25 cm) in einem Einzelhandelsgeschäft, ohne Verpflichtung zu einem Neukauf.

Die Rücknahmepflicht gilt für Vertreiber von Elektrogeräten mit einer Verkaufsfläche von größer 400 m² oder für Vertreiber von Lebensmitteln, die mehrmals im Kalenderjahr oder dauerhaft Elektrogeräte anbieten mit einer Gesamtverkaufsfläche von 800 m². Bei Online-Anbietern gelten die aufsummierten Lager- und Versandflächen für Elektrogeräte als Verkaufsfläche. Für weitere Details siehe ElektroG3 §17 (1)(2).

Vertreiber, die Fernkommunikationsmittel verwenden, müssen bei Auslieferung von Wärmeüberträgern, Bildschirmen, Monitoren und Geräten, die Bildschirme mit einer Oberfläche größer 100 Quadratzentimetern enthalten sowie Geräte, bei denen mindestens eine der äußeren Abmessungen mehr als 50 Zentimeter beträgt unentgeltlich abholen oder mitnehmen. Für Lampen und insbesondere kleinere Geräte müssen sie geeignete Rückgabemöglichkeiten in zumutbarer Entfernung gewährleisten.

Begriffserklärung

Tab. 2: Erläuterungen und Definitionen von Begriffen, Produkten und Bauteilen

Begriff	Beschreibung
Anti-Passback	Die Funktion *Anti-Passback* ist eine Zutrittswiederholsperre. Sie verhindert, dass ein Ausweis mehrmals zum Betreten eines Bereichs benutzt wird. Der Bereich muss zunächst verlassen werden, bevor der Ausweis wieder zum Betreten benutzt werden kann.
Benutzer	*Benutzer* bedienen *SCALA net*.
Administrator	Der *Administrator* ist ein spezieller Benutzer mit allen Berechtigungen. Er kann *SCALA net* ohne Einschränkungen benutzen.
Blacklist	Die *Blacklist* enthält alle ID-Mittel (Ausweise), denen die Gültigkeit entzogen wurde, zum Beispiel weil ein Ausweis verloren wurde oder eine Person keine Zutrittsberechtigung mehr haben soll.
CSV-Datei	Eine *CSV-Datei* (Character Separated Value) ist eine Datei in der Daten durch ein Trennzeichen (zum Beispiel ein Semikolon) getrennt zeilenweise abgelegt werden.
Dashboard	Das *Dashboard* ist eine Benutzeroberfläche, die nach dem Login angezeigt wird. Es ist die Zentrale innerhalb der Software, die den Benutzer über wichtige Systemereignisse informiert sowie einen Überblick über personenbezogene Daten und den Status von Türen gibt.
Erweiterungsmodul	Das *Erweiterungsmodul* ist eine optionale Hardwareerweiterung. Der *SCALA Controller* wird um sechs Anschlusspins erweitert.
Funktion	Eine *Funktion* ist eine Eigenschaft oder Fähigkeit einer Hardware, zum Beispiel eine Tür mit *DoC-System*.
Gruppen	In *Gruppen* werden Projekt- oder Arbeitsgruppen nach Personenbereichen organisatorisch zusammengefasst (heißen auch: *Organisationseinheiten*).
ID	ID ist das Identmittel, zum Beispiel ein Ausweis eventuell in Kombination mit einer PIN.
UID	Die *UID* ist herstellerseitig auf dem Ausweis gespeichert und – nicht immer – aufgedruckt.
ID-Mittel / *Ausweis* *Identmittel*	Ein *Ausweis* ist ein *Identmittel (ID-Mittel)* für eine Person. Ein Ausweis wird beim Vorhalten vom Leser gelesen. Hat die Person eine Zugangsberechtigung wird die Tür freigegeben.
Blacklist-Karte	Eine *Blacklist-Karte (BLK)* ist ein ID-Mittel zum Übertragen von Blacklist-Daten an alle Offline-Zylinder.
Schlossparameterkarte	Eine *Schlossparameterkarte (SPK)* ist ein ID-Mittel zum Übertragen von Daten an alle Offline-Zylinder, zum Beispiel Zeitmodelle.
Protokolltransportkarte	Eine *Protokolltransportkarte (PTK)* ist ein ID-Mittel zum Übertragen von Meldungen von einem Offline-Zylinder in die Software *SCALA web*.
UHF-Aktivierungskarte	Eine UHF-Aktivierungskarte ist ein ID-Mittel zum Aktivieren des Funkmoduls in der Offline Komponente

Tab. 2: Erläuterungen und Definitionen von Begriffen, Produkten und Bauteilen

Begriff	Beschreibung
Leser (Lesegerät)	*Leser* überprüfen in Ausweisen gespeicherte Identifikationsnummern. Ausweisdaten werden immer verschlüsselt vom *Lesegerät* in den *SCALA Controller* übertragen. Leser können, je nach Konfiguration, auch zum Schreiben von Daten auf Ausweise benutzt werden (Update-Leser).
Update-Leser *Online-Leser*	Ein *Update-Leser* ist ein *Online-Leser*, der die aktuell gültigen Offline-Zutrittsrechte auf die Ausweise schreibt.
Validier-Leser	Ein Validier-Leser (auch Update-Leser oder Schreib-Leser genannt) speichert zutrittsrelevante Daten auf Transponder und liest eventuell vorhandene Ereignisse aus.
Segmentier-Leser	Ein Segmentier-Leser speichert einmalig eine festgelegte Datenstruktur (Applikation) auf einen Transponder und schreibt die in *SCALA net* hinterlegte Transponderkennung hinein.
Mifare Classic Schlüsselkarte	Hauptprogrammierkarte für Mifare Classic Offline Komponenten. Mit dem Vorhalten einer Mifare Classic Schlüsselkarte wird die Offline Komponente dem System zugeordnet und initialisiert. Dabei werden Basisparameter wie Aufbau der/des Transponders, Schlüssel und Lock-Identität übertragen.
Offline	*Offline* ist ein *Zeitmodell* für Zylinder und Beschläge, die keine feste Verbindung zur Datenbank haben. Es sind bis zu 16 *Zeitmodelle* verarbeitbar
Online	*Online* ist ein *Zeitmodell* für Zylinder und Beschläge, die eine feste Verbindung zur Datenbank haben. Es sind bis zu 1024 *Zeitmodelle* verarbeitbar.
OSS–SO / DoC	*OSS–SO* und *DoC* sind Speicherstandards für die Kommunikation mit Offline-Lesern über Transponder.
OSS–SO *OSO*	Abkürzung für den *Open Securtiy Standards - Standard Offline* der OSS-Association e.V.® https://www.oss-association.com/standards/oss-standard-offline/
DoC	Abkürzung für *Data on Card*.
Person	*Personen* bekommen in *SCALA net* Zutrittsberechtigungen zugewiesen. *Personen* bedienen *SCALA net* nicht.
Revalidierungszeit	Nach Ablauf der *Revalidierungszeit* verlieren alle DoC-Ausweise ihre Gültigkeit. Ein Update-Leser mit Zugriff auf die aktuellen Berechtigungen aktiviert die Ausweise beim Vorhalten wieder. Ein kleinerer Wert bedeutet höhere Sicherheit. Typisch ist eine Revalidierungszeit von 1440 Minuten (= 24 Stunden). So dass die Gültigkeit von DoC-Ausweisen jeden Tag neu bestätigt werden muss.
RS485	Die serielle Schnittstelle *RS485* ist ein Standard für kabelgebundene, digitale Datenübertragungen über große Entfernungen.
SCALA Controller	Am *SCALA Controller* sind Hardware-Komponenten angeschlossen, zum Beispiel Leser oder Türöffner. Die Konfiguration erfolgt über die Software *SCALA net*. Die Konfigurationsdaten werden verschlüsselt auf der Micro-SD-Karte gespeichert.

Tab. 2: Erläuterungen und Definitionen von Begriffen, Produkten und Bauteilen

Begriff	Beschreibung
SCALA Eingangsmodul	Das *SCALA Eingangsmodul* ist eine optionale Hardwareerweiterung. Mit diesem Modul wird der *SCALA Controller* um acht Analog- / Digitaleingänge erweitert.
SCALA Relaismodul	Das *SCALA Relaismodul* ist eine optionale Hardwareerweiterung. Mit diesem Modul wird der *SCALA Controller* um acht Relaisausgänge erweitert. Pro *SCALA Controller* können bis zu vier *Relaismodule* und ein *Eingang* angeschlossen werden.
SCALA Türmodul	Das *SCALA Türmodul* ist eine optionale Hardwareerweiterung. Das Türmodul befindet sich direkt bei einer Tür. Die Komponenten wie Leser oder Türöffner werden direkt angeschlossen. Das Türmodul wird über eine RS485-Leitung mit dem Controller verbunden.
SCALA Wiegandmodul	Das *SCALA Wiegandmodul* ist eine optionale Hardwareerweiterung. Mit diesem Adapter können Lesegeräte mit einer Wiegandschnittstelle in das Zutrittskontrollsystem integriert werden.
Session Time-out	Erfolgt keine Benutzereingabe, wird der Benutzer nach Ablauf einer festgelegten Zeit automatisch abgemeldet (Logout). Die Zeit zum *Session Time-out* wird in den Konfigurationsdaten eingestellt.
Sperre	Eine *Sperre* bezeichnet systemintern eine Tür. Hier wird der Durchgang von A nach B grundsätzlich verwehrt.
Terminal	Ein *Terminal* bezeichnet entweder einen *SCALA Controller* mit den an ihn angeschlossenen Komponenten oder eine OSS-SO- / DoC-Komponente.
Toggle	Die Berechtigung die *Toggle*-Funktion (Toggle = Umschalten) zu nutzen, erlaubt einer Person, · eine Tür von *daueroffen* auf *verriegelt* (zu) oder · von *verriegelt* (zu) auf *daueroffen* umzuschalten
Transponderkennung Ausweisnummer	Die Bezeichnungen *Transponderkennung* und *Ausweisnummer* sind in *SCALA net* Synonyme. Die Ausweisnummer wird in *SCALA net* definiert und auf den Transponder codiert. Anschließend wird der Transponder anhand der codierten Ausweisnummer von *SCALA net* identifiziert. Aus Sicherheitsgründen sollte deshalb die *Ausweisnummer* nicht gleich der UID des Transponders gewählt werden.
Werkzeug	Ein *Werkzeug* ist ein Softwaremodul, das zum Beispiel über einen Menüpunkt aufgerufen wird.
Zeitbereich	Ein *Zeitbereich* besteht aus einem oder mehreren *Zeitintervallen* mit derselben Anfangs- und Endzeit.
Zeitintervall	Ein *Zeitintervall* ist ein Zeitraum bezogen auf einen Tag.
Zeitmodell	Ein *Zeitmodell* dient zur Festlegung bestimmter Zeitdaten in einem Profil. Es wird für die Erstellung eines Zutrittsrechtes in Verbindung mit einem Zutrittspunkt benötigt. Es wird zwischen den Zeitmodellen *Online* und *Offline* unterschieden.
ALWAYS	*ALWAYS* ist der Permanentzustand eines *Zeitmodells* innerhalb der Software *SCALA net*. Es ist rund um die Uhr und an allen Tagen (auch an Sondertagen) gültig.

Tab. 2: Erläuterungen und Definitionen von Begriffen, Produkten und Bauteilen

Begriff	Beschreibung
ZK-Element	Ein *ZK-Element* (Abkürzung für *Zutrittskontrollelement*) ist eine Komponente innerhalb eines Zutrittskontrollsystems, zum Beispiel ein *Lesegerät*, *Zutrittspunkt*, *Tür* oder *Ausweis*.
Zutrittspunkt	Ein *Zutrittspunkt* ist ein Punkt, an dem der Durchgang beantragt wird. Jede Tür kann zwei *Zutrittspunkte* haben, einen inneren und / oder einen äußeren.

SCALA net installieren

Hinweis!

Beschreibung für Microsoft Windows® Systeme: Die vorliegende Anleitung beschreibt ausschließlich die Installation und Konfiguration unter Microsoft Windows®.

Die Herstellerbedingungen müssen eingehalten werden: Für die Installation der Datenbank *Microsoft® SQL Server®* gelten die Herstellerbedingungen:
- Informieren Sie sich bitte aktuell über Webseiten des Herstellers.

Individuelle Installation ist erforderlich bei vorhandener Teilinstallation derselben Softwareversion: Eine *individuelle Installation* ist erforderlich, wenn
- bereits einzelne Komponenten installiert worden sind,
- mehrere Instanzen installiert werden sollen,
- auf eine schon vorhandene Datenbank zurückgegriffen werden soll oder
- bei einer SSL-Verschlüsselung („SSL-Verschlüsselung (optional)“, Seite 22).

Für die Installation werden die in Tab. 3 genannten Dateien benötigt.

Tab. 3: Installationsdateien

SCALA net 64-Bit-Version	Dateien
SCALA net Setup	*setup...-x64-... .exe* (64-Bit-Version)
Lizenzdatei und Lizenzschlüsseldatei	Die Lizenzdatei wird per Mail mit einem zugehörigen Lizenzschlüssel an den Kunden verschickt.

Informationen zur SSL-Zertifizierung https://ssl.de/ssl.html

SSL-Verschlüsselung (optional)

SCALA net ist für eine SSL-verschlüsselte Installation geprüft und zertifiziert (Impressum, Seite 2).

SSL-Zertifizierung

Das Management für Server-Zertifikate muss der SCALA-Lizenznehmer (Kunde) übernehmen.

Der Server wird vom Kunden bereitgestellt. Die Verwaltung des Servers und des SSL-Zertifikats liegt in der Verantwortung des Kunden bzw. des kundenseitigen IT-Beauftragten. Die Begutachtung des konkreten Servers ist Teil der SSL-Zertifizierung, da hier die kundenseitigen DNS-Namen und IP-Adressen des Servers berücksichtigt werden müssen.

Für die Durchführung einer SSL-Zertifizierung muss der Kunde eine autorisierte zertifizierende Stelle (CA) beauftragen und IT-seitig authentisieren.

SSL-Zertifikate sind in der Regel auf Grund der Sicherheitsrelevanz zeitlich befristet und müssen regelmäßig vom Kunden kostenpflichtig verlängert werden.

Installation mit SSL-Verschlüsselung

Nach der Software-Installation ist grundsätzlich kein aktuell gültiges SSL-Zertifikat hinterlegt. Trotzdem kann bereits bei der Installation (SCALA-Setup) der WebServer *Apache Tomcat™* für eine SSL-verschlüsselte Verbindung konfiguriert werden. Dabei wird ein zunächst selbst-signiertes Zertifikat erstellt. Dieses selbst-signierte Zertifikat muss der Kunde später durch das SSL-Zertifikat der zertifizierenden Stelle ersetzen.

Bis zur abgeschlossenen, vom Kunden beauftragten SSL-Zertifizierung, erhält dieser über den Zugang *https://< IP-Adresse des Servers >/scala*, zum Beispiel *https://localhost/scala*, immer eine Zertifikatsfehlermeldung. Dies ist kein Fehler im technischen Sinne, sondern weißt lediglich auf das Fehlen der SSL-Zertifizierung durch die dafür autorisierte zertifizierende Stelle (CA) hin.

Voraussetzungen für die Installation

Allgemeine Systemvoraussetzungen / Voraussetzungen für Server

In (Tab. 4) sind die Mindestanforderungen an den Server / den Computer aufgelistet.

Tab. 4: Anforderungen

Komponente Hardware	Beschreibung
Prozessor	· Mindestens: Zwei Prozessoren à 2,0 GHz · Empfohlen: Quad-Core CPU mit mindestens 3,0 GHz
RAM	· Mindestens: 8 GB · Empfohlen: 16 GB
Freier Speicherplatz	· Mindestens: 40 GB Festplattenspeicher · Empfohlen: 60 GB Festplattenspeicher
Weitere Hardware	· USB-Anschluss

In Tab. 5 sind die Systemvoraussetzungen für *SCALA net* aufgelistet.

Tab. 5: System-voraussetzungen

Komponente Software	Beschreibung
Softwarebetriebssysteme (für *SCALA net*)	· Microsoft Windows®
Webbrowser jeweils in aktueller Version	· Microsoft Edge · Google Chrome™ · Mozilla Firefox®
Server-Betriebssysteme	· Microsoft Windows® 2012 Server · Microsoft Windows® 2012 R2 Server · Microsoft Windows® 2016 Server · Microsoft Windows® 2019 Server
Betriebssysteme für lokale Installation auf Workstations	· ab Windows 10
Zugang zum Intranet oder Internet	Für Webserver muss ein Netzwerkzugang vorhanden sein: · zum Intranet **oder** · optional zum Internet

In Tab. 6 sind für die Kommunikation der SCALA net Dienste benötigten Ports in den Firewalls und/oder Proxyservern aufgelistet.

Tab. 6: Freizugebende Ports

Port	Beschreibung
8888	Kommunikation zwischen *SCALA net Server* und *SCALA net Controller*
8080	*SCALA net Webservice*
443	HTTPS-Verbindung
25	SMTP Nachrichtenversand
587	SMTP verschlüsselter Nachrichtenversand

Software installieren

Je nach Performance des Zielrechners beträgt die Installationsdauer zwischen fünf und dreißig Minuten.

Für die Installation sind Administratorberechtigungen notwendig.

1 Wählen Sie passend zum Betriebssystem die 32-Bit- oder 64-Bit-Variante des Installationsprogramms
   - *setup.....-x64-..... .exe* ist für ein 64-Bit-Betriebssystem
   - *setup.....-x86-..... .exe.* ist für ein 32 Bit-Betriebssystem.

⇨ Das Setup für die Software wird ausgeführt.

2 Folgen Sie den angezeigten Anweisungen.

⇨ Nach der erfolgreichen Installation wird *SCALA net* automatisch gestartet (Tab. 7)
(oder kann später gestartet werden, falls der automatische Start bei der Installation deaktiviert wurde).

⇨ *SCALA net* zeigt die Anmeldemaske, mit einem Hinweis, dass keine gültige Lizenz vorhanden ist.

Tab. 7: Dienste, die SCALA net zur Laufzeit benötigt

Dienst
ASSA ABLOY SCALA - Communication Server
ASSA ABLOY SCALA - MQService
ASSA ABLOY SCALA - Scheduler
ASSA ABLOY SCALA - WebServer
SQL-Server (ISACDB)
SQL Server Agent (ISACDB)
SQL Server Browser
SQL Server VSS Writer

Die Lizenzdatei beim ersten Start hochladen

Die Lizenzdatei wird von ASSA ABLOY mit einem Lizenzschlüssel (kurzer Text) geliefert. Nachdem die Lizenzen erfolgreich importiert wurden, sind die lizenzierten Module freigeschaltet und können benutzt werden.

1 Starten Sie SCALA net im Internet-Browser mit der
Adresse *https://localhost/scala.*
2 Melden Sie sich als Administrator an:
Benutzername: *admin*
Passwort: *Admin@AssaAbloy1*
(Groß- Kleinschreibung wird unterschieden)

Nach dem ersten Start wird die *Lizenzverwaltung* angezeigt.

3 Klicken Sie in das Feld *Lizenzdatei hochladen* und wählen Sie den Pfad zur Lizenzdatei aus.
4 Tragen Sie den Lizenzschlüssel ein.
5 Klicken Sie auf Import.

⇨ Nach erfolgreichem Import der Lizenzdatei zeigt *SCALA net* automatisch das *Dashboard* an.

IV – Inbetriebnahme

Diese Kapitel zeigt eine typische Reihenfolgen nach der Software-Installation.

Grundsätzlich: Im Verlauf der Bedienung werden typischerweise Meldungen zur weiteren Bedienung angezeigt: (Erfolgsmeldungen, Mißerfolgsmeldungen, Fehlermeldungen, kontext- und datenabhängige Meldungen). Die Meldungen müssen beachtet werden, eventuell sind Eingaben erforderlich.

Starten

Software starten

Nach erfolgreicher Installation können Sie die Software starten:

1 Starten Sie *SCALA net* im Internet-Browser mit der Adresse *https://localhost/scala*.
2 Melden Sie sich am Login mit folgendem Benutzer an.
Benutzername: *admin*
Passwort: *Admin@AssaAbloy1* (gilt nur bei der ersten Anmeldung)
(Groß- Kleinschreibung wird unterschieden)
⇨ Eventuell werden Meldungen angezeigt.

3 Beachten und befolgen Sie die angezeigten Informationen.
⇨ Das *Dashboard* wird angezeigt (Abb. 3–1).

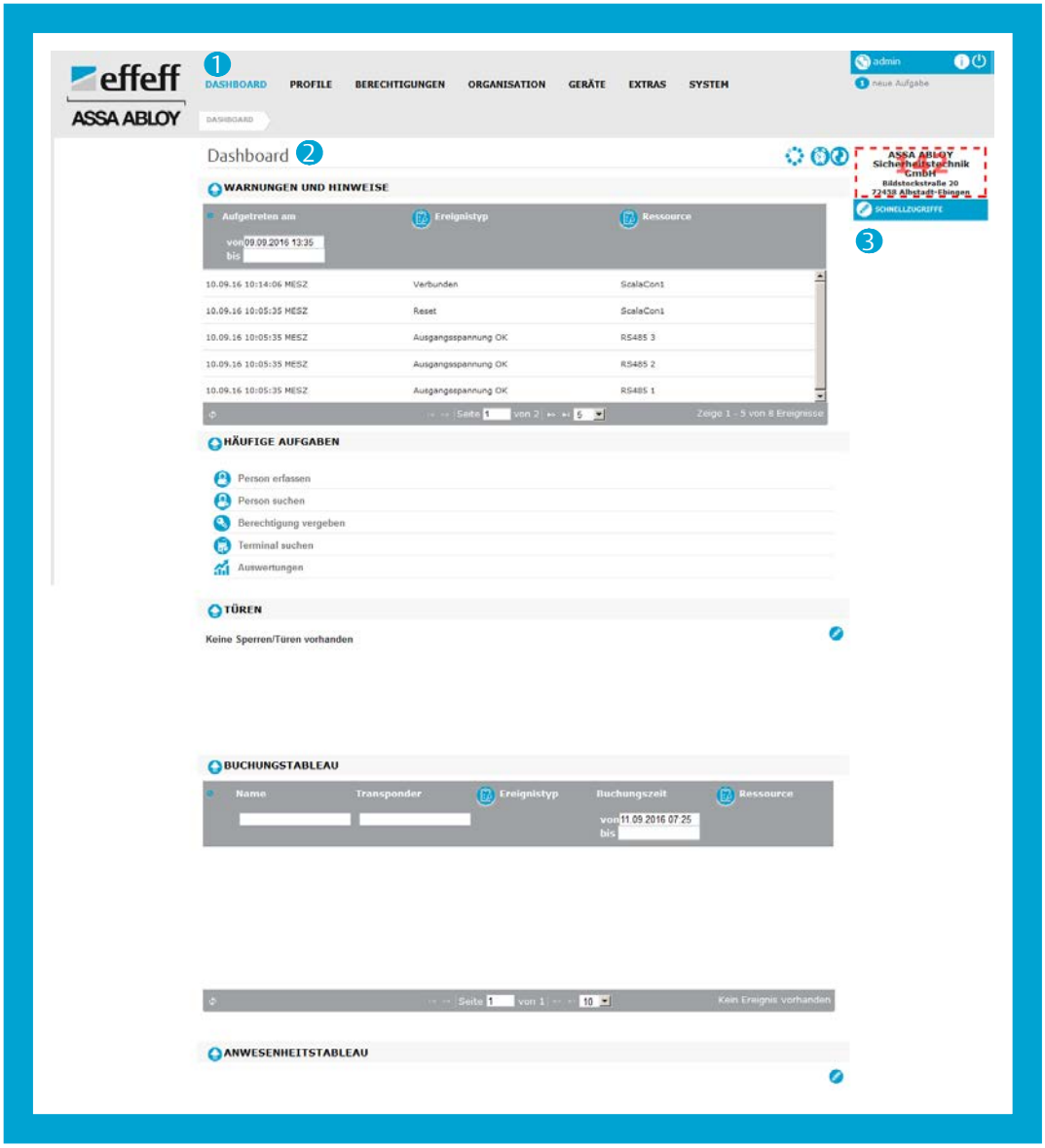


Abb. 3: SCALA net nach dem ersten Start
1 *Menü*
2 *Dashboard*
3 *Schnellzugriffe*

Benutzer

Benutzer (II – Hinweise, Begriffserklärung) bedienen *SCALA net*. Benutzer bekommen vom Administrator Berechtigungen zugewiesen (Tab. 8).

Benutzertypen

Tab. 8: Benutzertypen und ihre Eigenschaften

	Beschreibung
Systembenutzer (Benutzer)	Der *Benutzer* kann *SCALA net* entsprechend seiner individuellen Berechtigungen benutzen. Die Berechtigungen werden von einem Administrator festgelegt.
Systembenutzer mit allen Rechten (Administrator)	Der *Administrator* ist ein spezieller Benutzer mit allen Berechtigungen. Er kann *SCALA net* ohne Einschränkungen benutzen. Die Berechtigungen sind alle automatisch gesetzt und können nicht verändert werden.

Benutzer-Stammdaten erfassen

1 Klicken Sie auf **SYSTEM** / **Benutzer**.
⇨ Die *Benutzerliste* wird angezeigt.
2 Klicken Sie auf Erfassen.
3 Wählen Sie in der Vorauswahl den Benutzertyp, im Regelfall *Systembenutzer*.
Je nach Lizenz stehen weitere Benutzertypen zur Auswahl.
4 Erfassen Sie die Stammdaten zu dem neuen Benutzer.
5 Klicken Sie auf Speichern.
⇨ Sie haben neue Benutzer-Stammdaten erfasst.

Benutzer-Stammdaten bearbeiten

1 Klicken Sie auf **SYSTEM** / **Benutzer**.
⇨ Die *Benutzerliste* wird angezeigt.
2 Klicken Sie in der Benutzerliste auf den zu bearbeitenden Benutzer.
3 Ändern Sie die Stammdaten zu dem neuen Benutzer.
4 Klicken Sie auf Speichern.
⇨ Sie haben die Benutzer-Stammdaten geändert.

Benutzer-Stammdaten löschen

1 Klicken Sie auf **SYSTEM** / **Benutzer**.
⇨ Die *Benutzerliste* wird angezeigt.
2 Klicken Sie in der Benutzerliste auf den zu bearbeitenden Benutzer.
3 Klicken Sie auf Löschen.
⇨ Sie haben die Benutzer-Stammdaten gelöscht.

Benutzerrolle / Zuweisen von Berechtigungen

In der Benutzerrolle werden die Berechtigungen für Benutzergruppen festgelegt.

Benutzerrolle anlegen

1 Klicken Sie auf **SYSTEM** / **Benutzerrolle**.

⇨ Die *Benutzerrollenliste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Definieren Sie die Benutzerrolle.

3.1 Setzen Sie die Berechtigungen für die Benutzerrolle,
- konfigurieren Sie das Hauptmenü (Module hinzufügen oder entfernen),
- konfigurieren Sie das Dashboard (Dashboard-Bereiche hinzufügen oder entfernen)

4 Klicken Sie auf Speichern.

⇨ Sie haben eine neue Benutzerrolle erfasst.

oder alternativ

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

⇨ Die *Benutzerliste* wird angezeigt.

2 Wechseln Sie auf die Registerkarte BERECHTIGUNGEN.

3 Klicken Sie auf  .

⇨ Die Eingabemaske *Benutzerrolle erfassen* wird angezeigt.

4 Definieren Sie die Benutzerrolle.

4.1 Setzen Sie die Berechtigungen für die Benutzerrolle,
- konfigurieren Sie das Hauptmenü (Module hinzufügen oder entfernen),
- konfigurieren Sie das Dashboard (Dashboard-Bereiche hinzufügen oder entfernen)

5 Klicken Sie auf Speichern.

⇨ Sie haben eine neue Benutzerrolle erfasst.

Dashboard

Das **DASHBOARD** ist eine spezielle Bedienoberfläche mit einer Übersicht und der individuell anpassbaren Schnellzugriffsleiste.

Schnellzugriffe konfigurieren

Einige Menüpunkte lassen sich als Schnellzugriffe festlegen. Die Funktionen sind dann mit einem Klick erreichbar.

1 Klicken Sie auf  .

⇨ Eine *Auswahlliste* wird angezeigt.

2 Markieren Sie die Funktionen, die als Schnellzugriff angezeigt werden sollen.

⇨ Sie haben die Schnellzugriffe konfiguriert.

Dashboard konfigurieren

Es können Dashboard-Bereiche auf- und zugeklappt werden.

Beim Beenden wird der Zustand des Dashboards für den angemeldeten Benutzer automatisch gespeichert und beim nächsten Start wird der letzte Zustand des Dashboards wieder hergestellt.

Grundlagen zu Netzwerkadressen

Im SCALA-Netzwerk werden Daten zwischen den *SCALA Controllern* und dem Server ausgetauscht. Diese Netzwerkteilnehmer haben IP-Adressen, um Quelle und Ziel von Datenpaketen zu benennen.

Zwei systematische Möglichkeiten statische IP-Adressen oder DHCP-Server

Innerhalb eines Netzwerkes muss jede IP-Adresse eindeutig sein. Es gibt zwei systematische Möglichkeiten IP-Adressen festzulegen:

- Zuweisung von statischen IP-Adressen durch einen Administrator,
- Zuweisung von dynamischen IP-Adressen über DHCP-Server.

ASSA ABLOY Sicherheitstechnik GmbH empfiehlt, eine Mischform aus beiden Möglichkeiten zu vermeiden und sich grundsätzlich für eine der beiden Varianten zu entscheiden.

Ein gemeinsames logisches Netzwerk

IP-Adresse nach IPv4-Systematik

Eine IP-Adresse nach IPv4-Systematik besteht immer aus vier Zahlenblöcken zwischen 0 und 255, zum Beispiel:

192 . 168 . 100 . 12

Zwei Netzwerkteilnehmer eines physikalischen Netzwerks können Daten austauschen, wenn sie zu einem gemeinsamen Subnetz und einem gemeinsamen logischen Netzwerk gehören. Das Subnetz wird über die Subnetzmaske festgelegt, die auch aus vier Zahlenblöcken besteht, zum Beispiel:

Subnetzmaske

255 . 255 . 255 . 0

Sind die ersten drei Zahlenblöcke der IP-Adressen bei allen Netzwerkteilnehmer gleich, so gehören diese zum selben Subnetz und zum selben logischen Netzwerk, so dass alle Netzwerkteilnehmer miteinander kommunizieren können. Im vierten Zahlenblock muss jeder Netzwerkteilnehmer eine eindeutige Adressnummer haben, zum Beispiel

IP-Adressen in einem logischen Netzwerk

192 . 168 . 100 . 12
192 . 168 . 100 . 10
192 . 168 . 100 . 200

Hinweis: Die Adressen 192 . 168 . XXX . 0 und 192 . 168 . XXX . 255 sind in der Netzwerktechnik reserviert und dürfen nicht verwendet werden.

Mehrere logische Netzwerke

Innerhalb eines Subnetzes können mehrere logische Netzwerke definiert werden, so dass nur die Netzwerkteilnehmer innerhalb eines logischen Netzwerkes miteinander kommunizieren können. Der dritte Zahlenblock der IP-Adresse definiert die Zugehörigkeit eines Netzwerkteilnehmers zu einem logischen Netzwerk, zum Beispiel:

IP-Adressen in mehreren logischen Netzwerken

Logisches Netzwerk 1	Logisches Netzwerk 2	Logisches Netzwerk 3
192 . 168 . 1 . 100	192 . 168 . 2 . 10	192 . 168 . 100 . 10
255 . 255 . 1 . 101	192 . 168 . 2 . 101	192 . 168 . 100 . 101
255 . 255 . 1 . 102	192 . 168 . 2 . 200	192 . 168 . 100 . 101
. . .	. . .	. . .

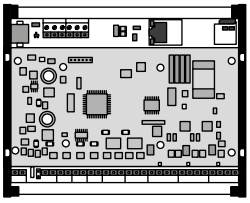
Statische IP-Adressen

Wird die systematische Möglichkeit *statische IP-Adressen* gewählt, muss sich der Administrator selbst um die Vergabe der IP-Adressen bei jedem Netzwerkteilnehmer kümmern und er muss selbst auf die Eindeutigkeit achten. Wird nach Konfiguration der *SCALA Controller* die statische *IP-Adresse* am Server geändert, müssen die *SCALA Controllern* wieder neu konfiguriert werden.

IP-Adressen über DHCP-Server

Wird die systematische Möglichkeit dynamische *IP-Adressen über DHCP* gewählt, vergibt der DHCP-Server die IP-Adressen automatisch. Diese Option muss auch am Server eingeschaltet sein.

SCALA Controller



Im Zentrum der Kommunikation von Software und Hardware stehen die *SCALA Controller*, an denen alle Komponenten (Leser, Türmodule, Türöffner usw.) angeschlossen sind. .

Controller erfassen

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ Die *Terminal-Liste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie die Art des Terminals – in diesem Beispiel **SCALA net (SCALA Controller)**.

4 Erfassen Sie die Stammdaten zu dem neuen *SCALA Controller*.
In diesem Beispiel ist der *SCALA Controller* mit dem Namen *ScalaCon1* benannt.

5 Klicken Sie auf Speichern.

⇨ Sie haben einen *SCALA Controller* erfasst.

Der *SCALA Controller* muss die IP-Adresse oder den Namen des Kommunikationsservers (Server) kennen. Server ist der Rechner, auf dem die Software *SCALA net* installiert wurde. Über die Software *SCALA net* wird eine ZIP-Datei erstellt, deren Inhalt auf die SD-Karte kopiert werden muss.

Hinweis!

Reihenfolge der Handlungen bei der Konfiguration einhalten: Die Reihenfolge der Handlungen bei der Konfiguration ist nicht beliebig und muss eingehalten werden..

- Erst die IP-Adresse des *SCALA Controllers* konfigurieren.
- Danach die SD-Karte initialisieren.

Die IP-Adressse des Controllers konfigurieren

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der *SCALA Controller* angezeigt. Der *SCALA Controller* ist noch nicht betriebsbereit, deshalb ist er mit einem roten Punkt gekennzeichnet.

⇨ Dem *SCALA Controller* muss eine IP-Adresse zugewiesen werden. Die IP-Adresse des *SCALA Controller* muss so gewählt werden, dass Sie zum Subnetz des Servers passt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste – in diesem Beispiel *ScalaCon1*..

3 Klicken Sie auf PARAMETER.

4 Geben Sie die IP-Konfiguration ein.

5 Klicken Sie auf Speichern.

⇨ Die SD-Karte des *SCALA Controllers* muss nun initialisiert werden.

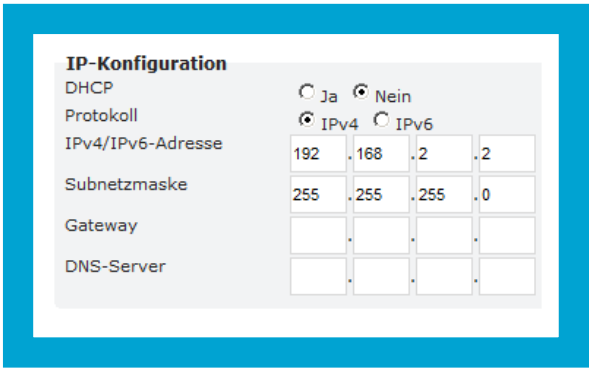


Abb. 4: IP-Konfiguration

Die SD-Karte initialisieren

Bevor die SD-Karte initialisiert werden kann, muss die IP-Adresse des *SCALA Controllers* konfiguriert sein.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der bereits erfasste *SCALA Controller* angezeigt. Der *SCALA Controller* ist noch nicht betriebsbereit, deshalb ist er mit einem roten Punkt gekennzeichnet.

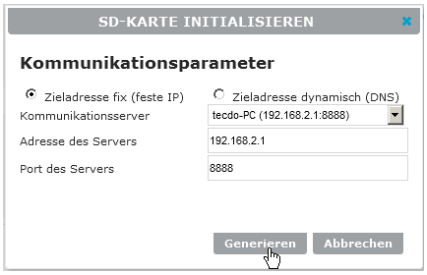
⇨ Die SD-Karte muss initialisiert werden.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste – in diesem Beispiel *ScalaCon1*.

3 Klicken Sie auf SD-Karte initialisieren.

4 Geben Sie die Kommunikationsparameter ein.

statische IP-Adresse	dynamische IP-Adresse
Hat der Server eine statische Zieladresse, geben Sie diese ein.	Hat der Server eine dynamische Zieladresse, geben Sie den Namen des Servers ein.



5 Klicken Sie auf **Generieren**.

⇨ Es wird eine ZIP-Datei generiert.

6 Speichern Sie die ZIP-Datei.

7 Entnehmen Sie die SD-Karte aus dem *SCALA Controller*.

7.1 Drücken Sie die SD-Karte in die Halterung bis es klickt.

⇨ Die SD-Karte ist nun gelöst.

7.2 Ziehen Sie die Karte aus der Halterung.

8 Entpacken Sie den Inhalt der ZIP-Datei auf der SD-Karte (Abb. 5).

9 Setzen Sie die SD-Karte wieder in den *SCALA Controller* ein.

10 Starten Sie *SCALA net* und den *SCALA Controller* neu.

⇨ Die SD-Karte ist initialisiert, so dass der *SCALA Controller* mit dem Server kommunizieren kann.

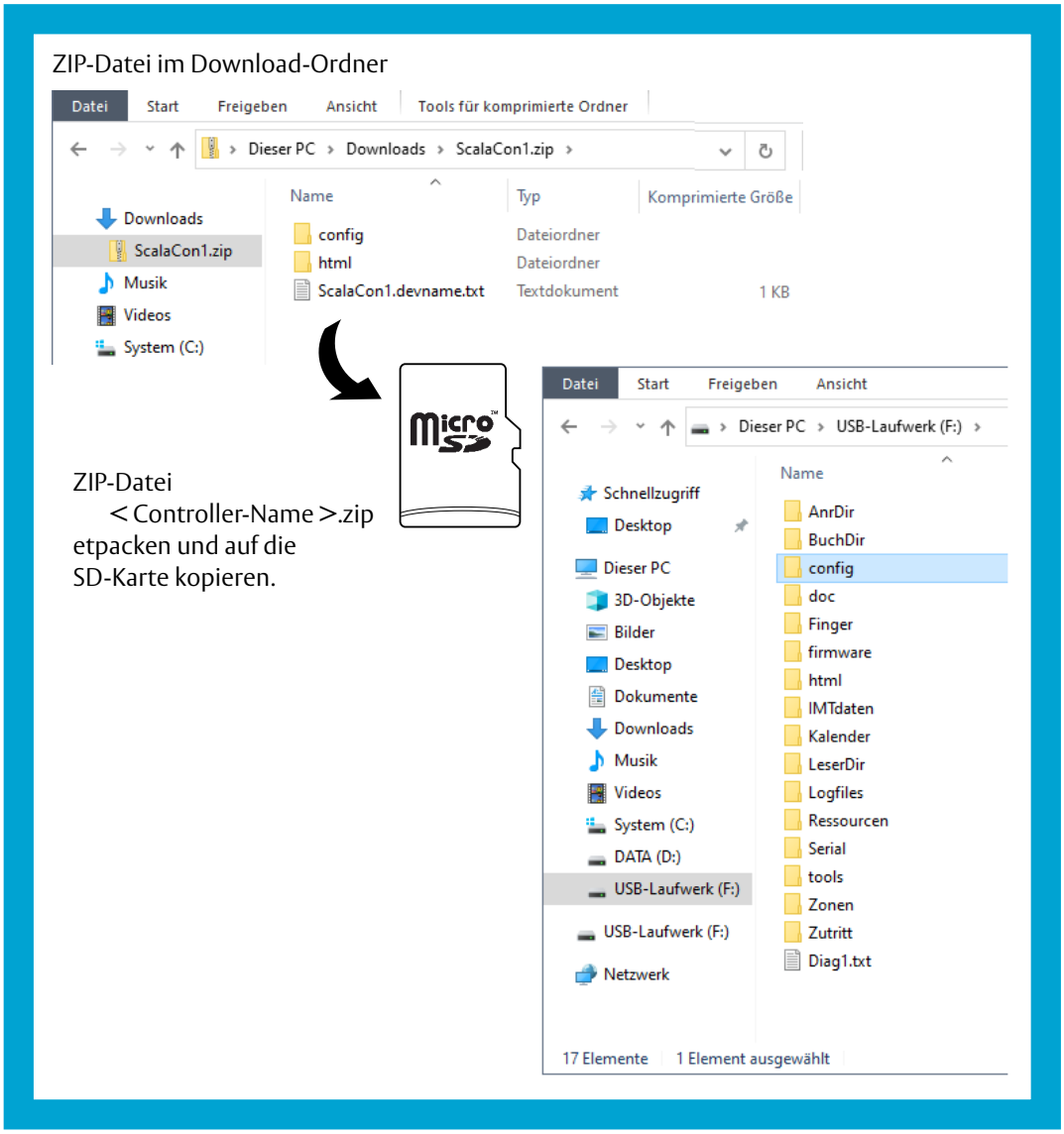
⇨ Es dauert etwas bis die Konfiguration des Controllers abgeschlossen ist. Während dieses Vorgangs piept der Controller mehrmals.

⇨ Der *SCALA Controller* ist in der Terminal-Liste mit einem grünen Punkt gekennzeichnet.

Hinweis!

IP-Adresse des Servers ist unbekannt: Falls Sie die IP-Adresse des Servers nicht kennen, kann diese über die Windows-Netzwerkeinstellungen ermittelt werden oder über die Windows-Eingabeaufforderung mit dem dem Befehl *ipconfig*.

Abb. 5: ZIP-Datei in Config-Ordner entpacken



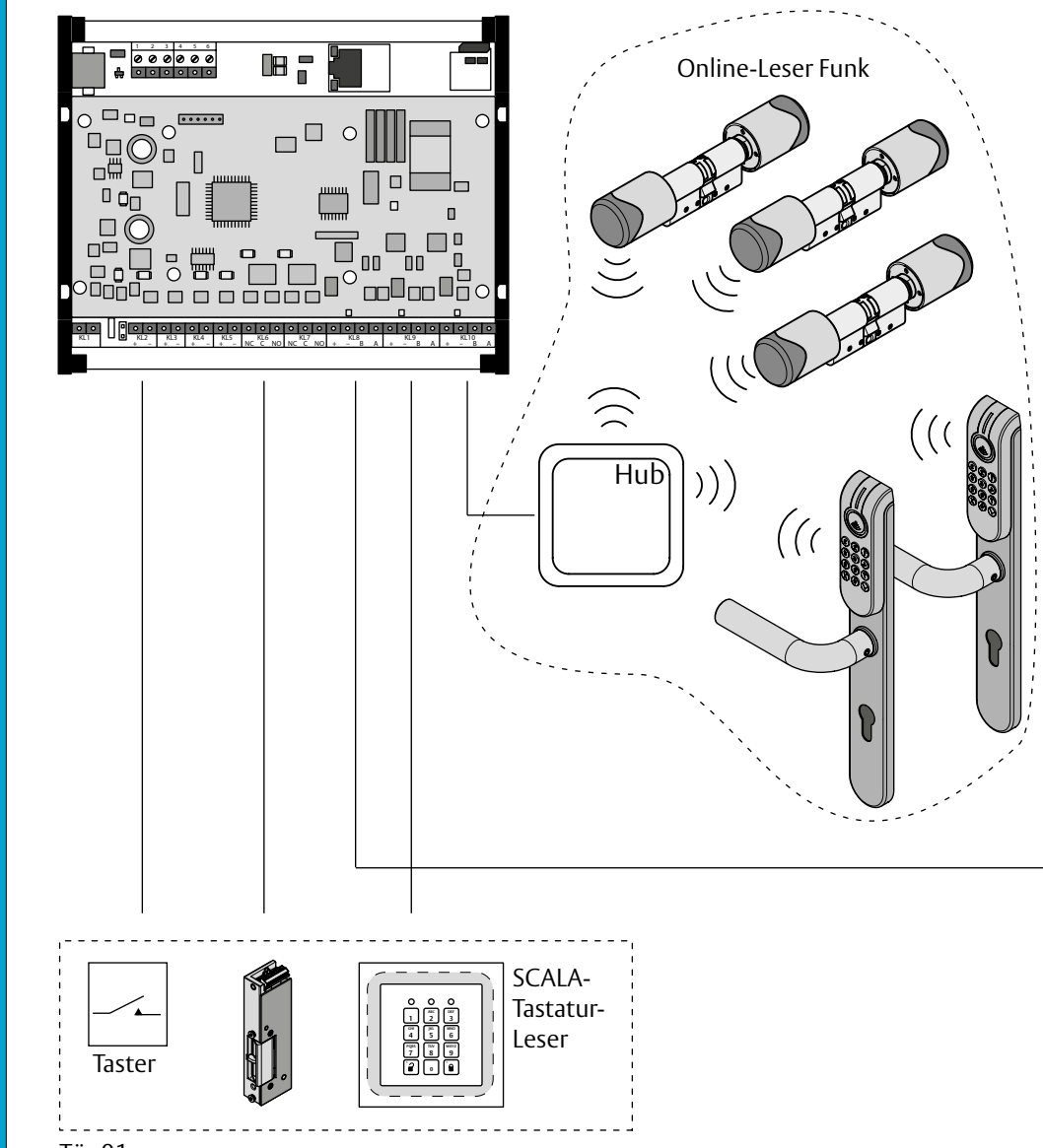
Falls es nicht funktioniert

Problem	Hinweise zur Lösung
SCALA Controller bleibt in der Terminal-Liste mit einem roten Punkt gekennzeichnet	· Halten Sie sich an die vorgegeben Handlungsreihenfolge. · Prüfen Sie die Netzwerkverbindung. · Wechseln Sie das Verbindungskabel. · Konfigurieren Sie *SCALA Controller* und *SCALA Server* im selben Subnetz. Beispiel: Bei der typischen Subnetzmaske 255.255.255.0 · dürfen sich nur die letzten Zahlen der IP-Adressen unterscheiden (Beispiel: 192.168.1.1 und 192.168.1.2) und · müssen sich die letzten Zahlen der beiden IP-Adressen unterscheiden. · Prüfen Sie, ob die Firmware aktuell ist.

Ein Anschlussbeispiel

Im Nachfolgenden wird beschrieben, wie die an den *SCALA Controller* angeschlossenen Komponenten in *SCALA net* erfasst und konfiguriert werden. Bei der Beschreibung wird von den in Abb. 6 dargestellten Gegebenheiten ausgegangen.

Abb. 6: Beispiel eines SCALA Controllers an dem mehrere Komponenten angeschlossen sind



Hinweis!

Reihenfolge bei Identifizierung zur Freigabe – erst PIN, dann Ausweis: Bei einem PIN-Ausweis-Leser muss immer zuerst die PIN eingegeben und erst danach der Ausweis vorgehalten werden.

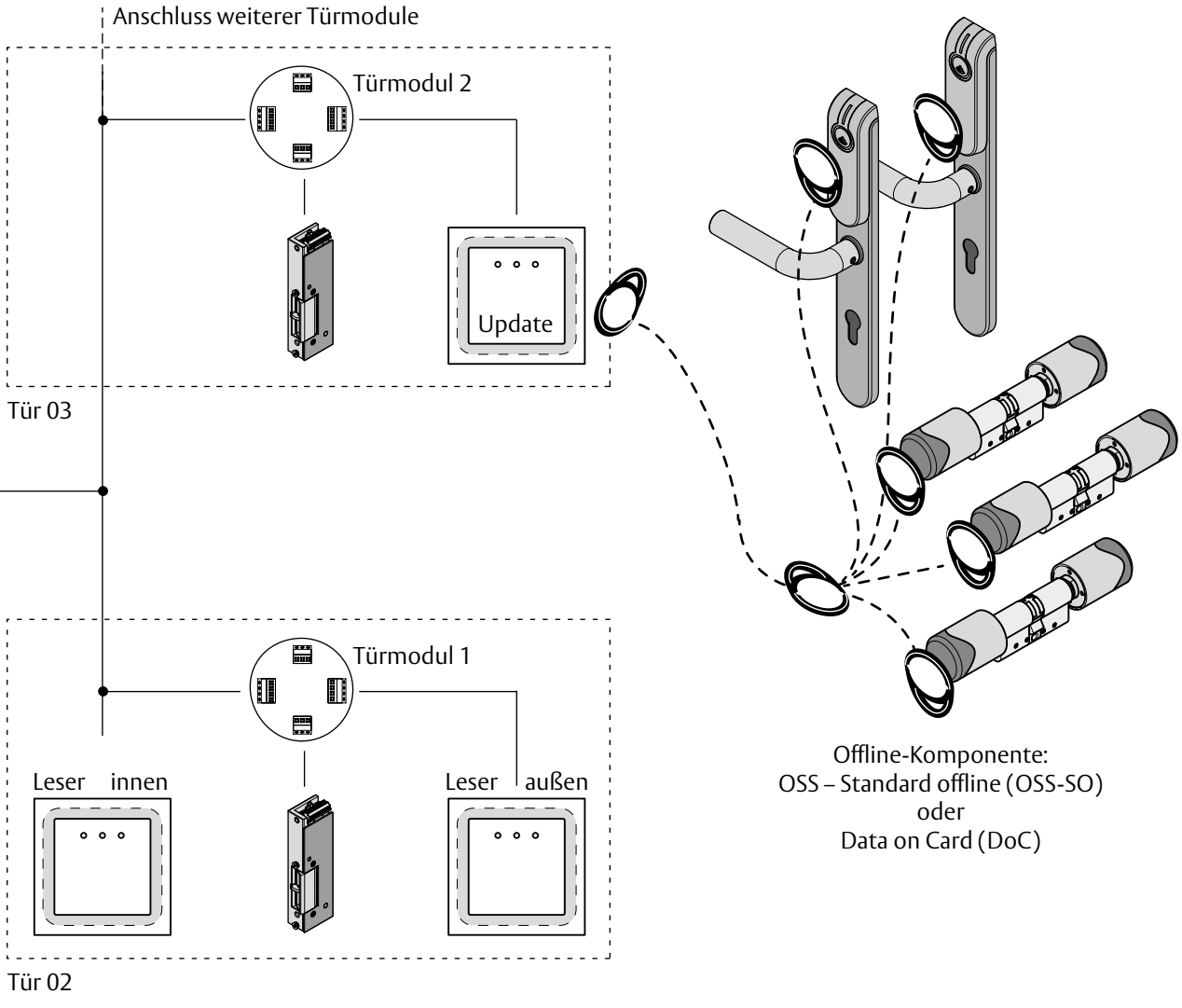
Die Verdrahtung ist vereinfacht dargestellt.

Wie die Komponenten angeschlossen werden, ist in den jeweils beiliegenden Anleitungen beschrieben.

Achtung!

Sachschaden durch Überlastung der Relais am Controller:
Die maximale Belastbarkeit der Relais darf nicht überschritten werden (siehe Technische Daten zum Controller).

- *ASSA ABLOY* empfiehlt: Schließen Sie die Türöffner grundsätzlich an separate Stromversorgungen an.



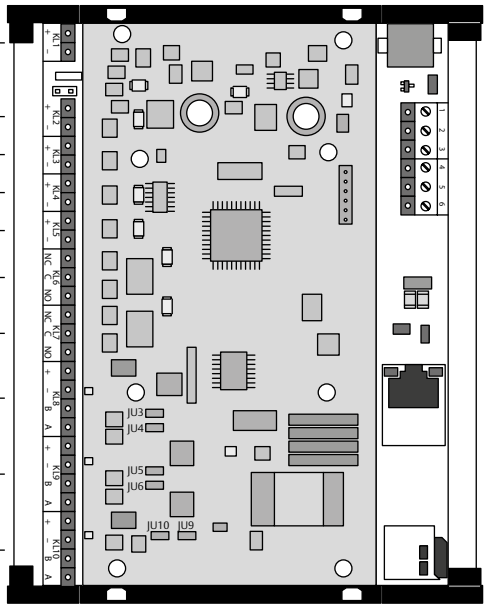
Offline-Komponente:
OSS – Standard offline (OSS-SO)
oder
Data on Card (DoC)

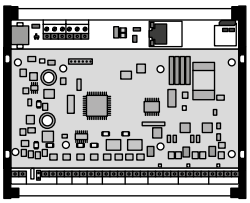
Eingänge / Ausgänge / Schnittstellen

Der *SCALA Controller* ist mit vier Eingängen, zwei Ausgängen (Relais) und drei seriellen Schnittstellen ausgestattet, die wie folgt benannt sind:

Tab. 9: werkseitige Bennenungen

SCALA net	am Controller
· Spannungs-versorgung	· KL1
· In 1 (...)	· KL2
· In 2 (...)	· KL3
· In 3 (...)	· Kl4
· In 4 (...)	· Kl5
· Out 1 (...)	· KL6
· Out 2 (...)	· KL7
· RS485 1 (RS485)	· KL8
· RS485 1 (RS485)	· KL9
· RS485 1 (RS485)	· KL10





Serielle Schnittstellen umbenennen

Die werkseitigen Benennungen der seriellen Schnittstellen können geändert werden.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

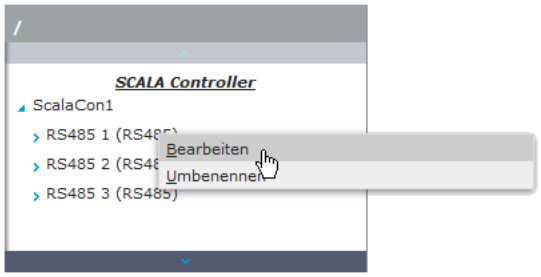
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü (Rechtsklick) zur seriellen Schnittstelle auf **Bearbeiten**.



5 Benennen Sie die serielle Schnittstelle. (In den nachfolgenden Beispielen werden die werkseitig vergebenen Benennungen verwendet.)

Adressierung von Leser und Türmodulen

Achtung!

Funktionseinschränkung bei falscher Adressierung von SCALA-Komponenten: Allen SCALA-Komponenten, die an derselben Schnittstelle angeschlossen sind, müssen eindeutige Adressen zugewiesen werden.

- Konfigurieren Sie die Adressen der Komponenten, wie es in den jeweils dort beiliegenden Anleitungen und in der Anleitung zum *SCALA Adresskodierer* (D01119xx SCALA Adresskodierer) beschrieben ist.

Alle angeschlossenen SCALA-Komponenten müssen immer eindeutig adressierbar sein (Adresse 1 bis 8). Werden mehrere SCALA-Komponenten an einer Schnittstelle des *SCALA Controllers* betrieben, so müssen die Adressen konfiguriert werden. Dabei werden jeder SCALA-Komponente eindeutige Adressnummern zugewiesen (Abb. 7).

Hinweis!

Technische Änderungen vorbehalten: Entnehmen Sie die werkseitig eingestellten Adressen den jeweils dem Produkt beiliegenden Anleitungen:

Werkseitig sind folgende Adressen eingestellt:

- die SCALA Leser — die Adresse 1
- die SCALA Türmodule — die Adresse 3,
- die SCALA BLE-Türmodule — die Adresse 3,
- die SCALA 8-fach Relais-Module — die Adresse 5,
- die SCALA Eingangsmodul — die Adresse 6,
- die SCALA WIEGAND-Module — die Adresse 7.

Das *SCALA net Erweiterungsmodul* und das *SCALA net WLAN Modul* haben keine Adresse, da diese direkt auf den Controller aufgesteckt werden.

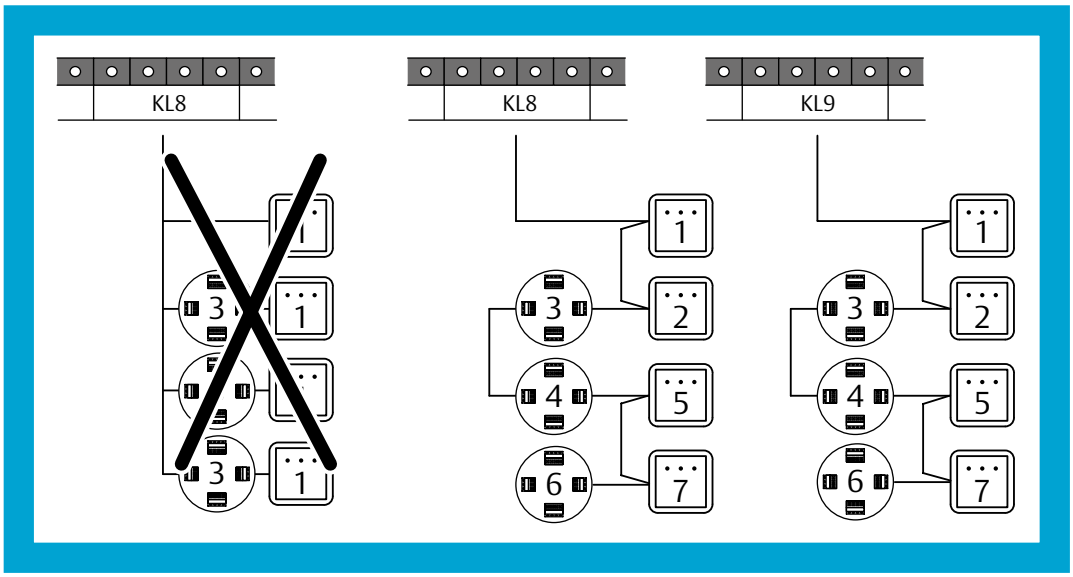


Abb. 7: Beispiel zur Adressvergabe an den seriellen Schnittstellen

Adresskonfiguration (optional)

Nachfolgend wird am Beispiel eines Lesers beschrieben, wie die Adresse einer SCALA-Komponente geändert werden kann.

Voraussetzung

Software OpenWebStart

Die Software *OpenWebStart* muss installiert sein, damit Bus-Adressen (Adresse) für SCALA-Komponenten über den Adresskonfigurator gesetzt werden können.

Download: https://openwebstart.com/

Achtung!

Zerstörung der SCALA-Komponente bei falscher Spannungsversorgung: Damit die Adresse geändert werden kann, muss der SCALA-Leser
- mit Spannung versorgt sein und
- über einen RS485-auf-USB-Wandler mit dem Rechner verbunden sein.

Bei Verwendung einer ungeeigneten Spannungsquelle, kann der SCALA-Leser zerstört werden. Verwenden Sie ein Spannungsversorgung die zum SCALA-Leser passen, entsprechend der dem Produkt beiliegenden Anleitung.

Funktionsprinzip

Die Datei *descriptor.jnlp* der Software *SCALA net* wird heruntergeladen und editiert.

Die Datei descriptor.jnlp herunterladen

1 Klicken Sie auf **GERÄTE** / **LESER** .

⇨ In der *Leserliste* werden die angelegten Lesern angezeigt.

2 Wählen Sie den Leser, dessen Adresse geändert werden soll.

3 Klicken Sie auf **STAMMDATEN** .

4 Kicken Sie auf das Symbol .

⇨ Die Datei *descriptor.jnlp* zum ausgewählten Leser wurde heruntergeladen.

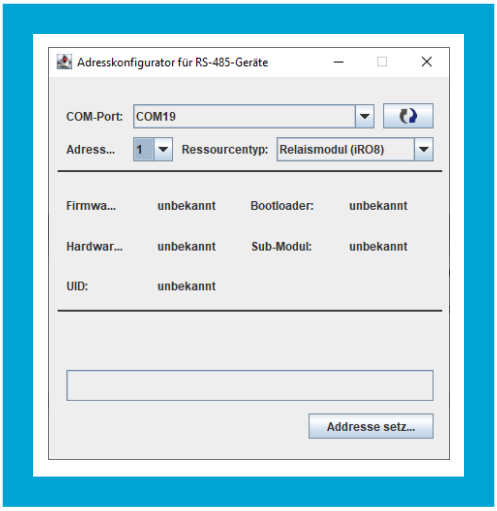


Abb. 8: Adresskonfigurator

Die Adresse ändern

1 Schließen Sie den SCALA-Leser an eine passende Spannungsquelle an

2 Verbinden Sie den SCALA-Leser über einen RS485-auf-USB-Wandler mit dem SCALA-Rechner.

3 Öffnen Sie die Datei *descriptor.jnlp*, zum Beispiel per Doppelklick.

⇨ Der *Adresskonfigurator für RS-485-Geräte* wird gestartet (Abb. 8).

4 Konfigurieren Sie die Adresse.

5 Klicken Sie auf Adresse setz... .

⇨ Die Adresse wurde geändert

⇨ Sie können die den SCALA Leser nun anschließen und verenden.

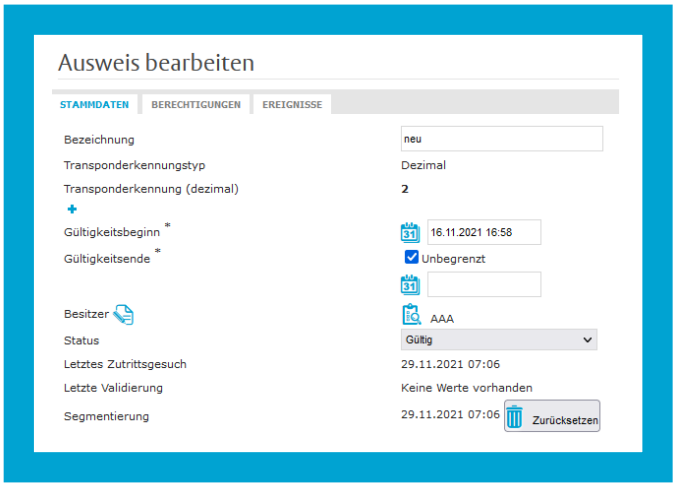
Segementier-Leser

Eine UID kann ausgespäht und emuliert werden. Dies ist ein Sicherheitsrisiko, das durch eine Segmentierung beseitigt werden kann.

Segmentier-Leser (nur SCALA Leser)

Auf einem neuen Transponder muss eine festgelegte Datenstruktur (Applikation) angelegt werden. Ein Segmentier-Leser speichert einmalig diese Applikation auf einen Transponder und schreibt die in *SCALA net* hinterlegte Transponderkennung hinein. *SCALA net* identifiziert den Transponder anschließend immer anhand der Transponderkennung und nicht mehr anhand der UID (Seriennummer) des Transponders.

Abb. 9: Transponderdaten nach Segmentierung



Nach einer erfolgreichen Segmentierung eines Transponders wird dessen UID-Datensatz im *SCALA Controller* gelöscht. Der Zeitpunkt der Segmentierung wird in den Transponder-Stammdaten gespeichert.

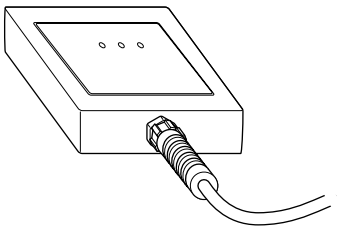
Eine Segmentierung kann in *SCALA net* in den Transponderdaten zurückgesetzt werden.

Bei einer Segmentierung wird zum Abschluss geprüft, dass die Applikation vollständig auf den Transponder übertragen wurde.

Da Segmentierung und Validierung getrennt werden, verkürzt sich die Dauer einer Validierung.

Hinweis!

Keine unsegmentierten Transponder ausgeben: ASSA ABLOY empfiehlt Transponder grundsätzlich, zum Beispiel mit dem *SCALA USB-Desktop-Codierer* zu segmentieren. Sodass kein unsegmentierter Transponder im Umlauf ist.



Einen Leser als Segmentier-Leser definieren

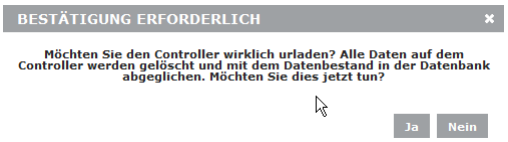
1 Legen Sie einen Leser an (im Nachfolgenden beschrieben).
2 Klicken Sie unter *Leser bearbeiten* auf STAMMDATEN .
3 Aktivieren Sie die *Transponder-Segmentierung*.

4 Klicken Sie auf Speichern.

⇨ Der Leser arbeitet nun als Segmentierer.

Funktionen und Standardaktionen im Überblick

Tab. 10: Standardaktionen

Standardaktion	Beschreibung / Bedeutung	
SD-Karte	Die Standardaktion *SD-Karte* speichert Kommunikationdaten auf die SD-Karte im Controller. Die SD-Karte ist eindeutig mit der Hardware des Controllers verknüpft. Ein Wechsel der SD-Karte ist nur nach Bestätigung eines berechtigten Benutzers in möglich. Erfolgt keine Bestätigung, kommuniziert der Controller zwar mit *SCALA net*, die Bestätigung ermöglicht jedoch erst die Funktionen der Zutrittskontrolle.	
Urladen	*Urladen* löscht alle Daten eines Controllers und gleicht den Datenbestand mit der Datenbank ab. Die Daten werden neu geschrieben. 	
Anschlussplan herunterladen	Über *Anschlussplan herunterladen* wird die verdrahtete Konfiguration ausgedruckt. Diese Funktion dient der Information, aber auch als Hilfe bei einer Fehlersuche.	
Steuerkommando	*Neustart (Softwarereset)*:	Erzwingt einen Neustart des Controllers.
	Permanentspeicher löschen:	Löscht den Speicherbereich für permanente Daten im Controller.
	SD-Karte prüfen (Checkdisk):	Überprüft das Dateisystems der SD-Karte im Controller und behebt gefundene Fehler.
	Protokoll laden:	Das Geräteprotokoll des Controllers wird an den Server gesendet.
	Freien Speicher abfragen:	Anzeige des freien Speichers auf der SD-Karte im Controller.
	Anstehende Buchungen abfragen:	Anzeige der aktuell anstehenden Buchungen.

Hinweis!

Pflichtfelder müssen korrekt und vollständig ausgefüllt werden: Pflichtfelder sind in der Software *SCALA net* mit einem * markiert. Diese Felder müssen ausgefüllt werden.
Manche Standardaktionen (und andere Eingabeparameter) erfordern eine ganz bestimmte Eingabe, um erfolgreich abgeschlossen werden zu können. So muss bei der Standardaktion *Erfassen* der vollständige Name eingegeben werden, damit Sie die Standardaktion *Erfassen* verlassen können. Auch können an bestimmten Stellen nur numerische und / oder alphanumerische Eingaben erlaubt sein. Das System gibt Ihnen an, wenn Sie eine nicht systemkonforme Eingabe getätigt haben und weist Sie auf die Regeln hin.

Darstellung von Pflichtfeldern

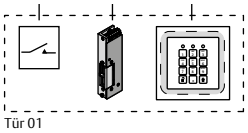
Bezeichnung *

Typ *

Urladen bei unerwartetem Verhalten: Verhält sich das System nicht wie erwartet oder werden Daten angezeigt, die veraltet zu sein scheinen, kann das daran liegen, dass das System noch nicht alle Vorgänge verarbeitet hat. Dies ist im Normalfall kein Problem und dient der Performance des Gesamtsystems.

- Verwenden Sie die Funktion Urladen um einen sofortigen Datenabgleich zwischen Controller und Datenbank zu erzwingen. Das Urladen benötigt je nach Datenbankgröße und anstehenden Verarbeitungsprozessen einige Sekunden Zeit.

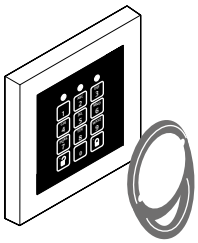
Beispiel Tür 01



Tür 01

Türen –Beispiel Tür 01

In diesem Beispiel wird eine Tür mit einem Tastaturleser, einem Türöffnertaster und einem Türöffner angelegt (Abb. 6 – Tür 01).



Einen Tastaturleser hinzufügen

In diesem Beispiel ist der Leser an der seriellen Schnittstelle KL9 (Tab. 9) angeschlossen.

Der Leser kann nun zu *SCALA net* hinzugefügt werden.

Im Nachfolgenden wird beschrieben, wie ein Ausweisleser angelegt wird und im zweiten Schritt eine PIN-Tastatur. Die Beschreibung zum Ausweisleser ist typisch für jeden Leser, ob mit oder ohne Tastatur.

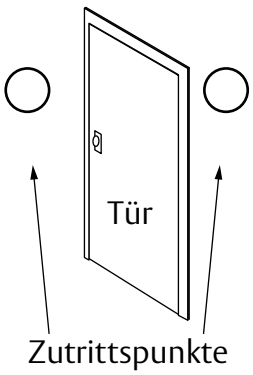
Es wird gezeigt wie ein Einmal-Code für eine PIN-Tastatur vergeben wird.

Hinweis!

Ein Tastaturleser muss als Ausweisleser und als PIN-Tastatur angelegt werden: Der Tastaturleser besteht aus zwei Komponenten,
- dem Ausweisleser und
- der PIN-Tastatur.

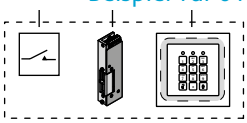
Beide Komponenten müssen separat als *Leser* und *PIN-Tastatur* in *SCALA net* hinzugefügt werden.

Tür – Zutrittspunkt – Leser



SCALA net unterscheidet zwischen Türen und Zutrittspunkten.
Eine *Sperre/Tür* kann mehrere Zutrittspunkte haben.
An den Zutrittspunkten befinden sich Leser und/oder Türöffner.

Beispiel Tür 01



Tür 01

Den Tastaturleser hinzufügen – als Ausweisleser

1 Klicken Sie auf **GERÄTE** / **Terminal**.

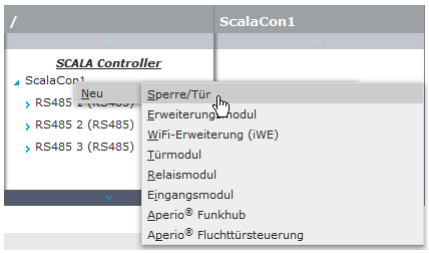
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

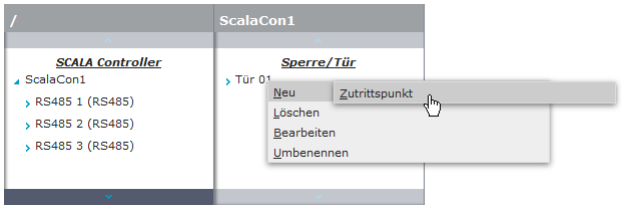
⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf **Neu** und weiter auf **Sperre/Tür**.



5 Benennen Sie die neue Tür.

6 Klicken Sie im Kontextmenü zur Tür auf **Neu** und weiter auf **Zutrittspunkt**.



7 Benennen Sie den neuen Zutrittspunkt.
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung.

8 Klicken Sie im Kontextmenü zum Zutrittspunkt auf **Neu** und weiter auf **Leser**.

9 Benennen Sie den neuen Leser und wählen Sie die passenden Konfigurationsdaten zum angeschlossenen Leser aus (zum Beispiel Lesertyp MIFARE oder PHG (Peter Hengstler)).
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung des Lesers.

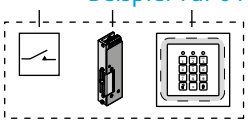
⇨ Die linke LED am Leser signalisiert:
- leuchtet gelb — Der Leser ist betriebsbereit.
- leuchtet nicht — Der Leser wurde nicht konfiguriert.

⇨ Oberhalb der Anschlussleiste am *SCALA Controller* signalisiert eine LED:
- leuchtet grün — Der Leser wurde erfolgreich hinzugefügt.
- leuchtet rot — Der Leser wurde nicht erfolgreich konfiguriert.
- blinkt rot — Der Leser wurde nicht erfolgreich hinzugefügt.
  Eine mögliche Ursache: Es wurde der falsche Lesertyp ausgewählt.

10 Testen Sie den Leser, indem Sie einen unbenutzten Ausweis vorhalten.

⇨ Die rechte LED am Leser signalisiert:
- leuchtet rot — Der Leser funktioniert ordnungsgemäß.
- leuchtet nicht — Der Leser funktioniert nicht ordnungsgemäß.

Beispiel Tür 01



Tür 01

Den Tastaturleser hinzufügen – als PIN-Tastatur

Der Tastaturleser wurde bereits als Ausweisleser angelegt.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf.

5 Klicken Sie im Kontextmenü zum Zutrittspunkt auf **Neu** und weiter auf **PIN-Tastatur**.

6 Benennen Sie die neue PIN-Tastatur und wählen Sie die passenden Konfigurationsdaten zum angeschlossenen Leser aus (in diesem Beispiel heißt der assoziierte Leser *Tür 01 Leser*). *ASSA ABLOY Sicherheitstechnik* empfiehlt eine eindeutige Benennung der Tastatur.

⇨ Die Leser signalisiert durch Piep-Signale, dass die Konfiguration übernommen wurde.

7 Testen Sie den Leser, indem Sie eine Nummerntaste drücken.

⇨ Der Leser bestätigt die Eingabe:

- mit Piep-Signal Der Leser funktioniert ordnungsgemäß.
- kein Signal Der Leser funktioniert nicht ordnungsgemäß.

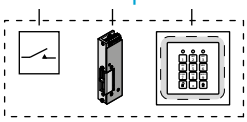
Abb. 10: Tastaturleser werden als Leser und auch als PIN-Tastatur hinzugefügt

Achtung!

Funktionsausfall bei falscher Baudrate an PHG-Lesern: PHG-Leser arbeiten mit einer Baudrate von 9600 und funktionieren nicht bei einer falsch eingestellten Baudrate.

- Stellen Sie für die Schnittstelle, an der der PHG-Leser angeschlossen ist, die Baudrate auf 9600 ein („Die Baudrate einstellen (PHG-Leser)“, Seite 43).

Beispiel Tür 01



Tür 01

Die Baudrate einstellen (PHG-Leser)

1 Klicken Sie auf **GERÄTE** / **Terminal**.

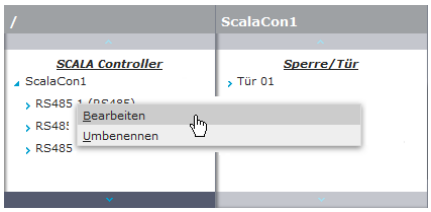
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zur *Schnittstelle* auf **Bearbeiten**.



5 Wählen Sie die Baudrate 9600 aus.

6 Klicken Sie auf **Speichern**.

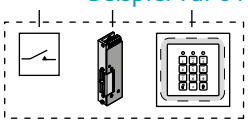
⇨ Die Baudrate für den PHG-Leser ist eingestellt.

Achtung!

Funktionsstörungen, wenn SCALA-Leser und PHG-Leser an einer Schnittstelle betrieben werden: PHG-Leser arbeiten mit einer Baudrate von 9600 SCALA-Leser mit einer Baudrate von 115200.

- Betreiben Sie PHG-Leser getrennt von SCALA-Lesern an unterschiedlichen Schnittstellen.

Beispiel Tür 01



Tür 01

Einen Ausgang zuweisen, zum Beispiel Türöffner

In diesem Beispiel ist der elektrische Türöffner an Ausgang 1 KL6 (Tab. 9) am *SCALA Controller* angeschlossen (Abb. 6 – Tür 01).

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf.

5 Klicken Sie im Kontextmenü zum Zutrittspunkt auf Bearbeiten.

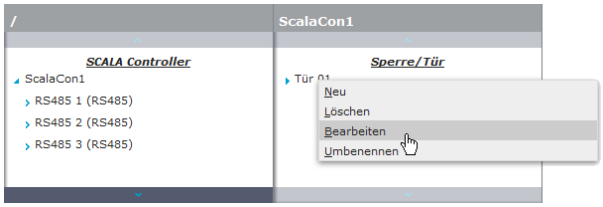
6 Klicken Sie auf AUSGÄNGE.

7 Wählen Sie den passenden Ausgang aus, in diesem Beispiel Out 1 (ScalaCon1).

8 Klicken Sie auf Speichern.

9 Klicken Sie auf **>SCALA CONTROLLER BEARBEITEN>**

10 Klicken Sie im Kontextmenü zur Sperre / Tür auf Bearbeiten.



11 Klicken Sie auf AUSGÄNGE.

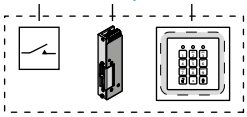
12 Wählen Sie den passenden Ausgang aus, in diesem Beispiel Out 1 (ScalaCon1).

13 Klicken Sie auf Speichern.

⇨ Der Türöffner ist nun betriebsbereit.

⇨ Der Türöffner kann nach Hinzufügen des Türöffnertasters getestet werden.

Beispiel Tür 01



Türöffnertaster hinzufügen

In diesem Beispiel ist der Türöffnertaster an Eingang 1 KL2 (Tab. 9) am *SCALA Controller* angeschlossen.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

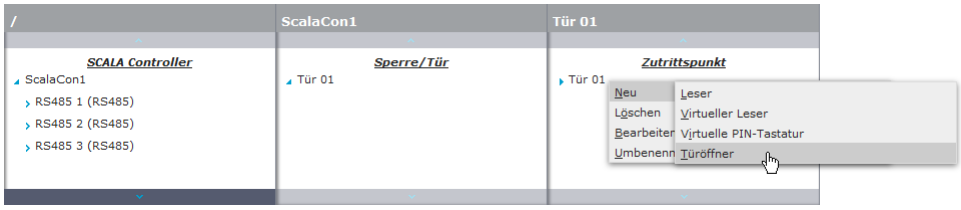
2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf.

5 Klicken Sie im Kontextmenü zum Zutrittspunkt auf Neu und weiter auf Türöffner.



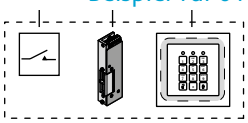
6 Benennen Sie den neuen Türöffnertaster und wählen Sie den passenden Eingang zum angeschlossenen Taster aus (in diesem Beispiel heißt der Eingang *In 1 (ScalaCon1)*).
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung des Tasters.

7 Klicken Sie auf Speichern.

⇨ Der Türöffnertaster ist nun betriebsbereit.

8 Testen Sie den angeschlossenen Türöffner und den Türöffnertaster.
- Der Türöffner entriegelt nach Betätigen des Türöffnertaster und verriegelt nach der eingestellten Türöffnungszeit (unter ***Zutrittspunkt*** / Tür 01 / Bearbeiten / STAMMDATEN).

Beispiel Tür 01



Tür 01

Freigabe-Logik konfigurieren

Bei einem Tastaturleser gibt es zwei Möglichkeiten zur Freigabe einer Tür. Die Freigabe erfolgt

- nach Vorhalten eines gültigen Ausweises
  ODER
  nach Eingabe einer gültigen PIN.
- nach Vorhalten eines gültigen Ausweises
  UND
  nach Eingabe einer gültigen PIN.

Welche Freigabe-Logik gilt, wird über die Erfassungselemente eingestellt.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf.

5 Klicken Sie im Kontextmenü des angelegten Zutrittspunkts (hier *Tür 01*) auf Bearbeiten.

6 Klicken Sie auf ERFASSUNGSELEMENTE.

7 Zum Hinzufügen einer Komponente, klicken Sie auf .

8 Fügen Sie den Leser je nach Freigabe-Logik hinzu:

UND-Logik

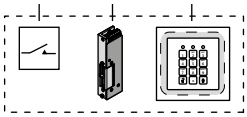
UND-Logik: Leser und Tastatur stehen in **einer Zeile** der Matrix

ODER-Logik

ODER-Logik Leser und Tastatur stehen in **einer Spalte** der Matrix

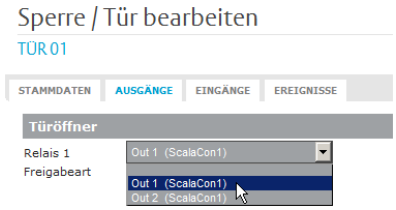
9 Klicken Sie auf Speichern.

Beispiel Tür 01



Tür 01

Falls es nicht funktioniert

Problem	Hinweise zur Lösung
Der Türöffner reagiert nicht, wenn der Türöffnertaster betätigt wird	1 Prüfen Sie, ob der Türöffnertaster unter den Erfassungselementen eingetragen ist: 1.1 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf. 1.2 Klicken Sie im Kontextmenü des angelegten Zutrittspunkts (hier *Tür 01*) auf Bearbeiten. 1.3 Klicken Sie auf ERFASSUNGSELEMENTE. 2 Falls der Taster nicht aufgeführt ist, klicken Sie auf ⊕. 3 Fügen Sie den Taster hinzu.  4 Klicken Sie auf Speichern. 5 Wiederholen Sie den Test.
Der Türöffner reagiert nicht, wenn der Türöffnertaster betätigt wird	1 Prüfen Sie, ob der Türöffner unter AUSGÄNGE in den Daten zur Tür eingetragen ist: 1.1 Klappen Sie alle Komponenten bis ***Sperre/Tür*** auf. 1.2 Klicken Sie im Kontextmenü der angelegten Tür (hier *Tür 01*) auf Bearbeiten. 1.3 Klicken Sie auf AUSGÄNGE. 2 Falls der Taster nicht aufgeführt ist, tragen Sie ihn ein  3 Klicken Sie auf Speichern. 4 Wiederholen Sie den Test.

Hinweis!

Reihenfolge bei Identifizierung zur Freigabe – erst PIN, dann Ausweis: Bei einem PIN-Ausweis-Leser muss immer zuerst die PIN eingegeben und erst danach der Ausweis vorgehalten werden.

Personen anlegen

Ausweise / Personen

Zu diesem Zeitpunkt ist es sinnvoll wenigstens eine Person anzulegen, um die hinzugefügten Komponenten zu testen. Nach Vorhalten eines berechtigten Ausweises oder nach Eingabe einer gültigen PIN muss die zum Leser gehörende Tür freigegeben werden.

Ausweise und Personen sind miteinander eindeutig verbunden, da jede Person einen Ausweis erhält.

Die Berechtigungen werden in einer Matrix zugewiesen (Abb. 11). Links im Zeilenkopf sind die Personen aufgelistet (1), rechts im Spaltenkopf sind die Türen aufgelistet (2), im Kreuzungspunkt von Zeile und Spalte werden die Berechtigungen durch Mausklick zugewiesen (3).

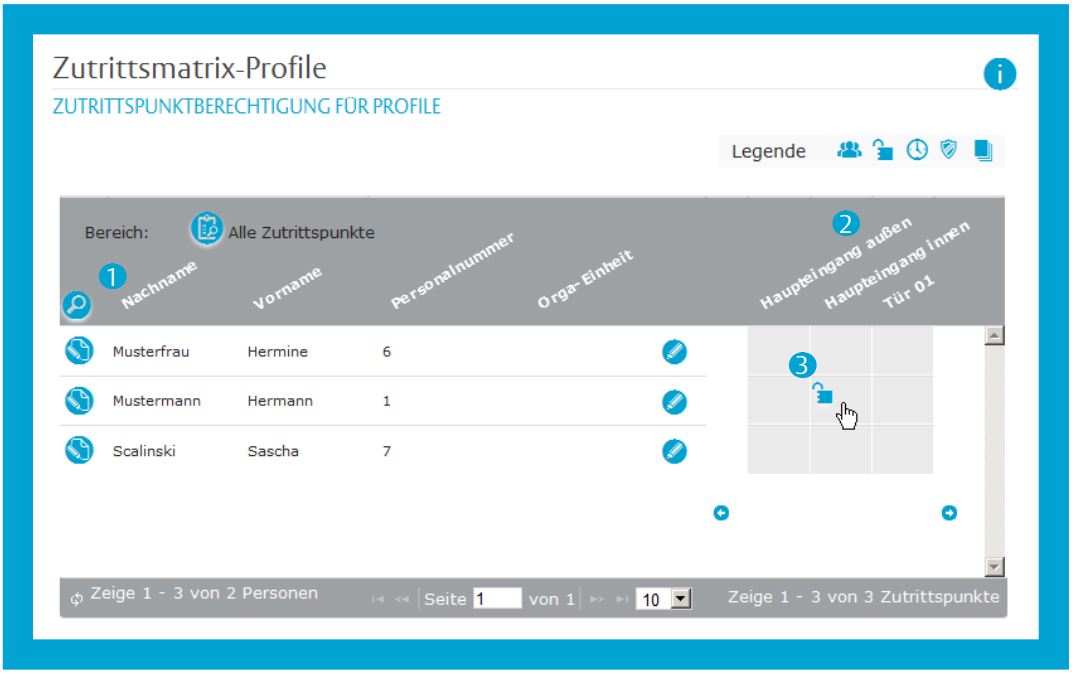


Abb. 11: Prinzip der Zutrittsmatrix

Transponderkennung – Ausweisnummer – UID

Die Bezeichnnungen Transponderkennung und Ausweisnummer sind in *SCALA net* Synonyme.

Die Ausweisnummer wird in *SCALA net* definiert und auf den Transponder codiert. Anschließend wird der Transponder anhand der codierten Ausweisnummer von *SCALA net* identifiziert. Aus Sicherheitsgründen sollte deshalb die Ausweisnummer nicht gleich der UID des Transponders gewählt werden.

Ausweisnummer in Windows-Zwischenablage kopieren

Wenn Ausweise erfasst werden, muss immer die Ausweisnummer eingegeben werden, die gegebenenfalls auf den Ausweisen aufgedruckt ist. Die Ausweisnummer ist sehr lang und es kann zu Abschreibfehlern kommen. Einfacher ist es, die Ausweisnummer in die Windows-Zwischenablage zu kopieren und später von dort zu übernehmen.

1 Halten Sie den Ausweis vor einen Leser, dies wird von *SCALA net* protokolliert.
2 Klicken Sie auf **EXTRAS** / **Ereignis-Log**.

⇨ Es wird die Tabelle *Ereignis-Log* angezeigt.
In der ersten Zeile ist ein Ereignis des Ereignistyps *Ausweis unbekannt* aufgelistet.

3 Kopieren Sie die Ausweisnummer aus der Spalte *Ereignisdaten* in die Windows-Zwischenablage.

Personen anlegen

Eine Person anlegen

1 Kopieren Sie die Ausweisnummer in die Windows-Zwischenablage
(„Ausweisnummer in Windows-Zwischenablage kopieren“, Seite 49).
2 Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Profile**.

⇨ Es wird die *Zutrittsmatrix-Profile* mit den bereits erfassten Personen angezeigt.

3 Klicken Sie auf Neue Person.
4 Geben Sie die Personaldaten ein.
4.1 Übernehmen Sie dabei die Ausweisnummer aus der Windows-Zwischenablage.
oder
Schreiben Sie die Nummer vom Ausweis ab.

⇨ Die neu angelegte Person wird in der Zutrittsmatrix angezeigt.

Einer Person Berechtigungen zuweisen

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Profile**.

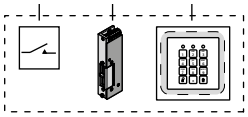
⇨ Es wird die *Zutrittsmatrix-Profile* mit den bereits erfassten Personen angezeigt.

2 Weisen Sie der Person Berechtigungen zu.

⇨ Die zugewiesenen Zutrittsberechtigungen werden in der Zutrittsmatrix angezeigt (Abb. 11 – 3) und sind sofort gültig.

⇨ Sie können mit dem Ausweis die bisherige Konfiguration testen.

Beispiel Tür 01



Tür 01

Einmal-Code

Unabhängig von Personen und Ausweisen ist es möglich, einen Einmal-Code für einen Zutrittspunkt zu vergeben, zum Beispiel für Boten oder Personen, die wenige Zutrittsberechtigungen in einem begrenzten Zeitrahmen benötigen.

Eigenschaften des Einmal-Code:

- der Einmal-Code kann frei festgelegt werden,
- es kann ein Gültigkeitszeitraum angegeben werden,
- bei Bedarf kann der Code auch mehrfach verwendet werden,
  - die Anzahl der Nutzungen ist einstellbar,
  - *SCALA net* zeigt die maximale Anzahl der Nutzungen und die Anzahl der Zutritte an.

Voraussetzungen

Am Zutrittspunkt befindet sich ein Tastaturleser.

Einen Einmal-Code festlegen

1 Klicken Sie auf **GERÄTE** / **Zutrittspunkt**.

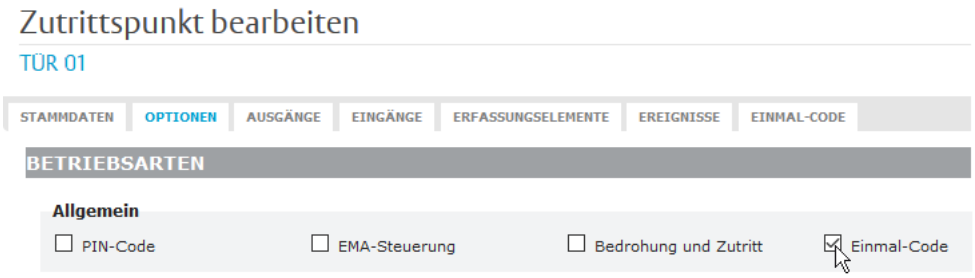
⇨ Es wird die *Zutrittspunktliste* mit den bereits erfassten Zutrittspunkten angezeigt.

2 Klicken Sie auf den zu bearbeitenden Zutrittspunkt.

3 Klicken Sie auf **OPTIONEN**.

⇨ Es werden die **Betriebsarten** angezeigt

4 Setzen Sie die Option *Einmal-Code*.



⇨ Anschließend wird zusätzlich die Registerkarte **EINMAL-CODE** angezeigt.

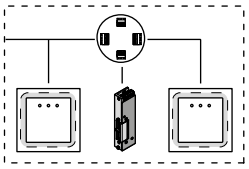
5 Klicken Sie auf **EINMAL-CODE**.

6 Klicken Sie auf , um die Einmal-Code-Nummer zu vergeben.

7 Geben Sie die Daten zur Gültigkeit ein.

⇨ Der Einmal-Code kann innerhalb des Gültigkeitszeitraums für die vorgegebene maximale *Anzahl Nutzungen* verwendet werden (1). Die tatsächliche Anzahl der Nutzungen wird ebenfalls angezeigt (2)

Beispiel Tür 02



Tür 02

Türen – Beispiel Tür 02

In diesem Beispiel wird eine Tür mit zwei Lesern angelegt. Ein Leser ist direkt an der seriellen Schnittstelle KL8 angeschlossen, der zweite Leser und der Türöffner sind an einem Türmodul angeschlossen und das Türmodul auch an der seriellen Schnittstelle KL8 (Tab. 9) am *SCALA Controller* (Abb. 6 – Tür 02).

Folgende Adressvergabe („Adressierung von Leser und Türmodulen“, Seite 35) ist typisch für eine Tür mit zwei Lesern und einem Türmodul:

- Leser 1 Adresse 1 (werkseitig bereits eingestellt)
- Leser 2 Adresse 2 (muss konfiguriert werden)
- Türmodul Adresse 3 (werkseitig bereits eingestellt)

Türmodul an Tür 02 hinzufügen

1 Klicken Sie auf **GERÄTE** / **Terminal**.

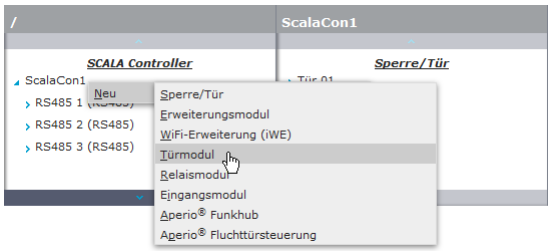
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN .

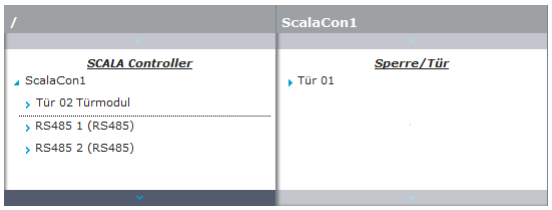
⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf Neu und weiter auf Türmodul.

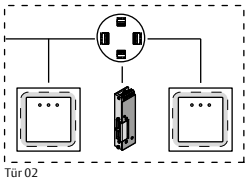


5 Benennen Sie das neue Türmodul.

⇨ Das Türmodul wird als Schnittstelle aufgeführt.



Beispiel Tür 02



Leser an Tür 02 außen hinzufügen

1 Klicken Sie auf **GERÄTE** / **Terminal**.

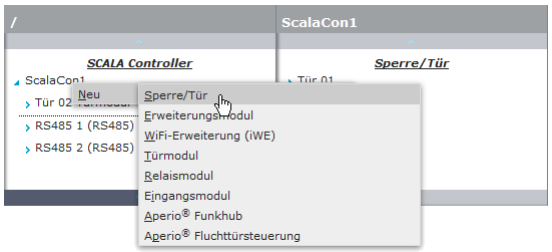
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf **Neu** und weiter auf **Sperre/Tür**.

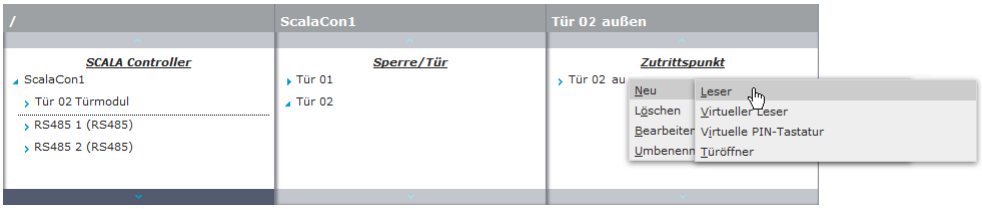


5 Benennen Sie die neue Tür.

6 Klicken Sie im Kontextmenü zur Tür auf **Neu** und weiter auf **Zutrittspunkt**.

7 Benennen Sie den neuen Zutrittspunkt.
ASSA ABLOY Sicherheitstechnik empfiehlt die Benennung der Tür zu übernehmen.

8 Klicken Sie im Kontextmenü zum Zutrittspunkt auf **Neu** und weiter auf **Leser**.



9 Benennen Sie den neuen Leser und wählen Sie die passenden Konfigurationsdaten zum angeschlossenen Leser aus (in diesem Beispiel ist der Lesertyp MIFARE).
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung des Lesers.

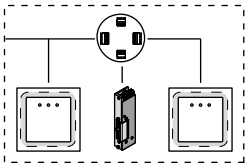
⇨ Die linke LED am Leser signalisiert:
- leuchtet gelb — Der Leser hat Betriebsspannung.
- leuchtet nicht — Der Leser wurde nicht konfiguriert.

⇨ Oberhalb der Anschlussleiste am Controller signalisiert eine LED:
- leuchtet grün — Der Leser wurde erfolgreich hinzugefügt.
- leuchtet rot — Der Leser wurde nicht erfolgreich konfiguriert.
- blinkt rot — Der Leser wurde nicht erfolgreich hinzugefügt.
  Eine mögliche Ursache: Es wurde der falsche Lesertyp ausgewählt.

10 Testen Sie den Leser, indem Sie einen unbenutzten Ausweis vorhalten.

⇨ Die rechte LED am Leser signalisiert:
- leuchtet rot — Der Leser funktioniert ordnungsgemäß.
- leuchtet nicht — Der Leser funktioniert nicht ordnungsgemäß.

Beispiel Tür 02



Tür 02

Leser an Tür 02 innen hinzufügen

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der Terminal-Liste wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf **STAMMDATEN**.

⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

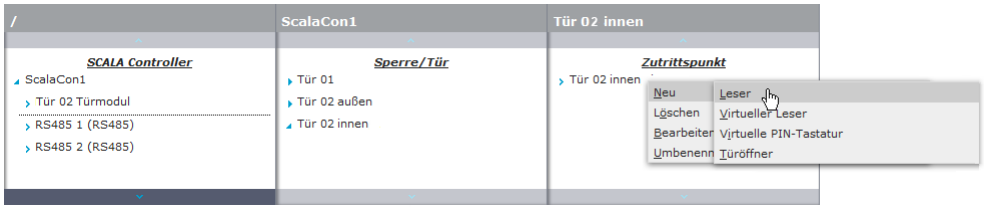
4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf Neu und weiter auf Sperre/Tür.

5 Benennen Sie die neue Tür.

6 Klicken Sie im Kontextmenü zur Tür auf Neu und weiter auf Zutrittspunkt.

7 Benennen Sie den neuen Zutrittspunkt.
ASSA ABLOY Sicherheitstechnik empfiehlt die Benennung der Tür zu übernehmen.

8 Klicken Sie im Kontextmenü zum Zutrittspunkt auf Neu und weiter auf Leser.



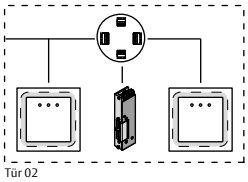
9 Benennen Sie den neuen Leser und wählen Sie die passenden Konfigurationsdaten zum angeschlossenen Leser aus (in diesem Beispiel ist der Lesertyp MIFARE).
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung des Lesers.

⇨ Die linke LED am Leser signalisiert:
- leuchtet gelb — Der Leser hat Betriebsspannung.
- leuchtet nicht — Der Leser wurde nicht konfiguriert.

10 Testen Sie den Leser, indem Sie einen unbenutzten Ausweis vorhalten.

⇨ Die rechte LED am Leser signalisiert:
- leuchtet rot — Der Leser funktioniert ordnungsgemäß.
- leuchtet nicht — Der Leser funktioniert nicht ordnungsgemäß.

Beispiel Tür 02



Türöffner hinzufügen

In diesem Beispiel ist der elektrische Türöffner am Türmodul angeschlossen (Abb. 6 – Tür 02). Der Türöffner wird von den Lesern auf beiden Türseiten angesteuert

1 Klicken Sie auf **GERÄTE** / **Terminal**.

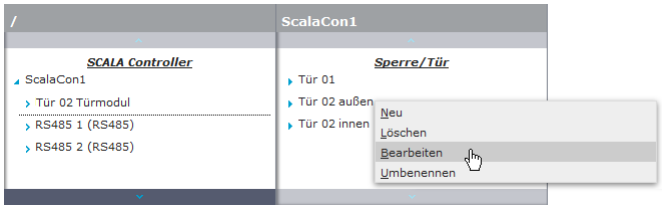
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

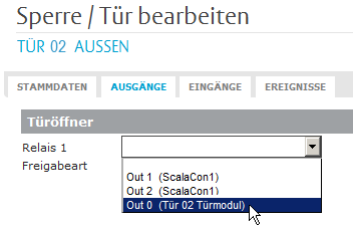
⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klappen Sie alle Komponenten bis ***Sperre/Tür*** auf.



5 Klicken Sie im Kontextmenü zur Tür auf Bearbeiten.

6 Klicken Sie auf AUSGÄNGE.



7 Wählen Sie in der Auswahlliste zum Türöffner das Türmodul aus.

8 Klicken Sie auf Speichern.

⇨ Der Türöffner ist nun betriebsbereit, da er über das Türmodul angesteuert wird.

9 Wechseln Sie zu den Stammdaten des *SCALA Controllers*:

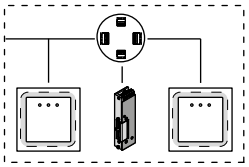
9.1 Klicken Sie in der Navigationsleiste auf **> SCALA CONTROLLER BEARBEITEN >**

10 Wiederholen Sie die Vorgehensweise ab Schritt 5 bis Schritt 8 für den Leser auf der anderen Türseite.

⇨ Der Türöffner ist nun betriebsbereit.

⇨ Der Türöffner kann nach Hinzufügen einer Person mit passender Berechtigung getestet werden.

Beispiel Tür 02



Tür 02

Falls es nicht funktioniert

Problem	Hinweise zur Lösung
An den Lesern leuchten keine LEDs.	1 Prüfen Sie, ob an den beiden Leser unterschiedliche Adressen konfiguriert wurden. 1.1 Entfernen Sie einen Leser von der Schnittstelle. ⇨ Leuchtet anschließend am anderen Leser die linke LED gelb, so haben beide Leser die gleiche Adresse. ⇨ Wenden Sie sich an den Support.
Der Leser hat Betriebsspannung (linke LED leuchtet gelb) aber beim Vorhalten eines Ausweises passiert nichts.	1 Prüfen Sie, ob der Leser unter den Erfassungselementen eingetragen ist: 1.1 Klappen Sie alle Komponenten bis ***Zutrittspunkt*** auf. 1.2 Klicken Sie auf den angelegten Zutrittspunkt (hier *Tür 02*) und weiter auf Bearbeiten. 1.3 Klicken Sie auf ERFASSUNGSELEMENTE. 2 Falls der Leser nicht aufgeführt ist, klicken Sie auf ⊕. 3 Fügen Sie den Taster hinzu.  4 Klicken Sie auf Speichern. 5 Wiederholen Sie den Test.

Türmodul – Ein zweites Türmodul

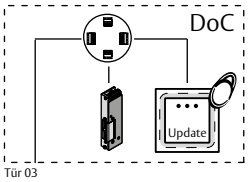
Es ist möglich mehr als ein Türmodul anzuschließen

Das Türmodul ist an der seriellen Schnittstelle KL8 (Tab. 9) am *SCALA Controller* angeschlossen. An der seriellen Schnittstelle KL8 sind bereits zwei Leser, ein Türmodul und ein Türöffner angeschlossen („Türen – Beispiel Tür 02“, Seite 51).

Folgende Adressvergabe („Adressierung von Leser und Türmodulen“, Seite 35) ist typisch für eine Tür mit einem zweiten Türmodul und einem weiteren Leser:

- Türmodul Adresse 4 (muss konfiguriert werden)
- Leser Adresse 5 (muss konfiguriert werden)

Beispiel Tür 03



Tür 03

Türen – Beispiel Tür 03 Data-on-Card- bzw. OSO-Bereich vorbereiten

In diesem Beispiel wird eine Tür mit einem Türmodul, einem Update-Leser ohne Tastatur und einem Türöffner angelegt (Abb. 6– Tür 03).

In diesem Beispiel wird angenommen, dass der Update-Leser außen montiert ist. Der Update-Leser wird im Verlauf des Beispiels zu einem OSO-Bereich (oder DoC) hinzugefügt. Die Gültigkeit aller Ausweise in einem OSO-Bereich läuft automatisch nach einer eingestellten Revalidierungszeit ab, die typische Revalidierungszeit beträgt 1440 Minuten (= 24 Stunden). Beim Betreten des Gebäudes werden die Ausweise am Update-Leser wieder aktualisiert und sind dann wieder für einen Tag gültig.

OSS-Standard-Offline-Bereich oder Data-On-Card-Bereich

Ein zweites Türmodul hinzufügen

1 Legen Sie das Türmodul wie beschrieben an („Türen – Beispiel Tür 02“, Seite 51).
2 Fügen Sie den Türöffner wie beschrieben hinzu.

⇨ Der Update-Leser für den OSO-Bereich (oder DoC) ist vorbereitet.
⇨ Der OSO-Bereich mit den Offline-Lesern kann nun angelegt werden.

Türen – Beispiel Offline-Leser / Data on Card (DoC) oder OSS-SO (OSO)

Über *DoC* bzw. *OSO* werden die Offline-Leser eingebunden. Diese Leser (in diesem Beispiel Schließzylinder) sind nicht direkt über Kabel oder Hub mit dem *SCALA Controller* verbunden. Der Datentransfer erfolgt über die Transponder.

In diesem Beispiel wird ein Offline-Bereich (DoC- oder OSO-Bereich) angelegt (Abb. 6 – Offline-Leser).

Der Offline-Bereich („Bereiche“, Seite 65) funktioniert so, dass die Ausweise automatisch nach Ablauf eines Tages ihre Gültigkeit verlieren. Ein Ausweis ist nach Ablauf eines Tag erst wieder berechtigt, wenn er an Tür 02 über den Update-Leser aktualisiert wurde, anschließend ist er wieder für 24 h berechtigt (Auto-Revalidierungszeit).

Der in diesem Beispiel verwendete Update-Leser wurde bereits in Beispiel Tür 02 angelegt („Türen – Beispiel Tür 03 Data-on-Card- bzw. OSO-Bereich vorbereiten“, Seite 56).

Offline-Bereich (DoC-Bereich bzw. OSO-Bereich) erfassen

1 Klicken Sie auf **ORGANISATION** / **Bereich**.

⇨ Die *Bereichsliste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie das System **Aperio® DoC (Aperio® Komponente)** bzw. **Aperio® OSO (SCALA Controller)**

4 Erfassen Sie die Stammdaten zu dem neuen Bereich.

4.1 Geben Sie eine eindeutige Benennung ein (in diesem Beispiel *Offline-Bereich 01*).

4.2 Geben Sie die Auto-Revalidierungszeit vor (in diesem Beispiel 1440 Minuten = 24 Stunden).

5 Klicken Sie auf Speichern.

⇨ Sie haben einen Offline-Bereich erfasst.

Berechtigungsschreiber festlegen

Zum Offline-Bereich gehört mindestens ein Online-Berechtigungsschreiber (Update-Leser).

6 Klicken Sie auf .

7 Wählen Sie den Update-Leser aus (in diesem Beispiel *Tür 03*).

8 Klicken Sie auf Speichern.

⇨ Sie haben einen Update-Leser für den Offline-Bereich festgelegt.

Offline-Leser erfassen

Zum Offline-Bereich gehört mindestens ein Offline-Leser. Dieser wird als Terminal erfasst.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ Es wird die Terminal-Liste angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie **Offline Komponente (Aperio® DoC, Aperio® OSO)**.

4 Erfassen Sie die Stammdaten zum Offline Leser.

4.1 Geben Sie eine eindeutige Benennung ein (in diesem Beispiel *Offline 0101*).

5 Klicken Sie auf Speichern.

6 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ Der Offline-Leser wird in der Terminal-Liste aufgeführt. Er ist mit einem roten Punkt gekennzeichnet.

Den Offline-Leser zum Offline-Bereich hinzufügen

1 Klicken Sie auf **ORGANISATION** / **Bereich**.

⇨ Die *Bereichsliste* wird angezeigt.

2 Klicken Sie auf den neu angelegten Offline-Bereich (in diesem Beispiel *Offline-Bereich 01*)
3 Klicken Sie ZUTRITTSPUNKTE.
4 Klicken Sie auf .
5 Wählen Sie den neu angelegten Offline-Leser aus (in diesem Beispiel *Offline 0101*).
6 Klicken Sie auf Speichern.

⇨ Der Offline-Leser wurde einem Offline-Bereich hinzugefügt.
⇨ Es können nun Berechtigungen für diese Offline-Tür vergeben werden.

Einer Person Berechtigungen zuweisen

Auch für die Offline-Türen müssen Berechtigungen an Personen vergeben werden.

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Profile**.

⇨ Es wird die *Zutrittsmatrix* mit den bereits erfassten Personen angezeigt.

2 Weisen Sie den Personen Berechtigungen für die Offline-Zylinder zu.

⇨ Die zugewiesenen Zutrittsberechtigungen für Offline-Zylinder werden in der Zutrittsmatrix angezeigt (Abb. 11 – 3).
⇨ Die Zutrittsberechtigungen sind aber erst gültig, wenn sie über einen DoC-Parameterausweis an die Offline-Zylinder übertragen wurden.

DoC-Parameterausweis erfassen

Die Verbindung zu den Offline-Türen erfolgt über Parameterausweise (I – Allgemeine Beschreibung, Online- und Offline-System). Ein Parameterausweis muss zuerst in *SCALA net* erfasst werden.

1 Kopieren Sie die Ausweisnummer in die Windows-Zwischenablage
(„Ausweisnummer in Windows-Zwischenablage kopieren“, Seite 49).
2 Klicken Sie auf **PROFILE** / **Parameterausweise**.

⇨ Die *Parameterausweisliste* wird angezeigt.

3 Klicken Sie auf Erfassen.
4 Erfassen Sie die Stammdaten zu dem neuen Parameterausweis.
4.1 Übernehmen Sie dabei die Ausweisnummer aus der Windows-Zwischenablage.
oder
Schreiben Sie die Nummer vom Ausweis ab.

DoC-Parameterausweis als Ausweistyp zuweisen

4.2 Wählen Sie *DoC-Parameterausweis* unter *Typ* der Ausweiskarte aus.
5 Klicken Sie auf Speichern.

⇨ Sie haben einen DoC-Parameterausweis erfasst. Er kann nun für die Übertragung von Daten auf Offline-Zylinder verwendet werden.
⇨ Der Ausweis wird in der Parameterausweisliste aufgeführt.

DoC-Parameterausweis benutzen

Daten für die Übertragung auf DoC-Parameterausweis vorbereiten

1 Klicken Sie auf **ORGANISATION** / **Bereich**.

⇨ Die *Bereichsliste* wird angezeigt.

2 Klicken Sie auf den Bereich, dem der Offline-Leser zugewiesen wurde (in diesem Beispiel *DoC-Bereich 01*).

⇨ *DoC-Bereich bearbeiten* wird angezeigt.

⇨ Zur Kontrolle:

- Unter **STAMMDATEN** muss mindestens ein Berechtigungsschreiber (Update-Leser) aufgeführt sein.
- Unter **ZUTRITTSPUNKTE** muss mindestens ein Offline-Leser aufgeführt sein.

3 Klicken Sie auf DoC-Komponenten parametrieren.

⇨ Die Auswahl des Parameterausweises wird angezeigt.

4 Wählen Sie den Ausweis aus.

⇨ Die Daten werden für die Übertragung vorbereitet.

5 Warten Sie bis die Datenübertragung bestätigt ist.

Daten auf DoC-Parameterausweis übertragen

Die nachfolgenden Handlungen müssen nicht sofort erledigt werden, sondern können auch mit zeitlichem Abstand erfolgen. Die Offline-Leser sind aber erst aktualisiert, wenn alle Handlungsschritte vollständig ausgeführt wurden.

6 Halten Sie den Doc-Parameterausweis vor einen Update-Leser, bis die aufleuchtende blaue LED wieder erlischt.

⇨ Die mittlere LED am Update-Leser leuchtet, solange die Daten übertragen werden.

⇨ Die rechte LED am Update-Leser signalisiert:

- blinkt rot — Die Daten wurden nicht ordnungsgemäß übertragen.
- leuchtet grün — Die Daten wurden ordnungsgemäß auf den DoC-Parameterausweis übertragen.

Daten auf Offline-Leser übertragen

Die nachfolgende Handlung muss nicht sofort erledigt werden, sondern kann auch mit zeitlichem Abstand erfolgen. Die Offline-Leser sind aber erst aktualisiert, wenn alle Handlungsschritte vollständig ausgeführt wurden.

7 Halten Sie den Doc-Parameterausweis vor jeden Offline-Leser der aktualisiert werden soll.

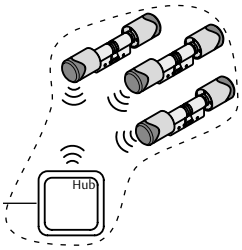
⇨ Die LED am Offline-Leser signalisiert:

- blinkt rot — Die Daten wurden nicht ordnungsgemäß übertragen.
- leuchtet grün — Die Daten wurden ordnungsgemäß auf den Offline-Leser übertragen.

Falls es nicht funktioniert

Problem	Hinweise zur Lösung
Die DoC-Parameterkarte wird nicht ordnungsgemäß beschrieben.	1 Prüfen Sie, ob Sie den richtigen Ausweis beschreiben. 1.1 Vergleichen Sie die Ausweisnummer.
Der Offline-Leser reagiert nicht.	1 Prüfen Sie den Zustand der Batterie im Leser.

Beispiel Funktür



Türen –Beispiel Funktüren

Funk-Leser sind über einen Funkhub (Hub) mit *SCALA net* verbunden, der Hub ist am *SCALA Controller* angeschlossen. Der Hub kann an den seriellen Schnittstellen KL9 oder KL10 angeschlossen werden.

Einen Funkhub hinzufügen

In diesem Beispiel ist der Funkhub an der seriellen Schnittstelle KL10 (Tab. 9) angeschlossen.

Die LED am Funkhub signalisiert:
- blinkt abwechselnd lange grün und kurz rot Der Hub ist betriebsbereit.

Der Funkhub kann nun zu *SCALA net* hinzugefügt werden.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

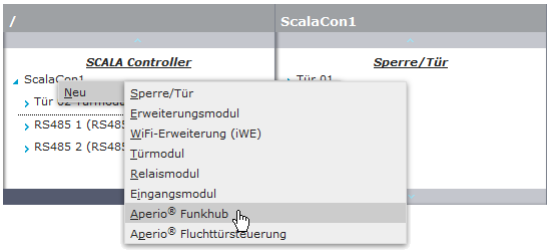
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

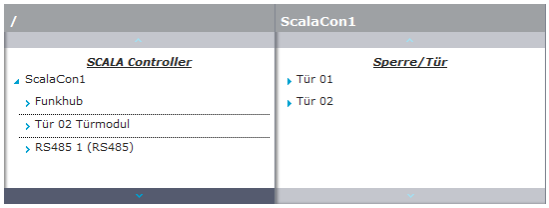
⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf Neu und weiter auf Aperio® Funkhub.



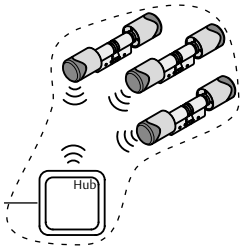
5 Geben Sie die Daten zum Funkhub ein.
- 5.1 Benennen Sie den neuen Hub.
- 5.2 Geben Sie die serielle Schnittstelle an, an der der Hub angeschlossen ist (in diesem Beispiel *KL10*).

⇨ Der Funkhub wird als Schnittstelle aufgeführt.



⇨ Die LED am Funkhub signalisiert:
- blinkt abwechselnd lange grün und zweimal kurz rot Der Hub ist betriebsbereit.

Beispiel Funktür



Einen Online Funk-Zylinder hinzufügen

Nachdem der Funkhub zu *SCALA net* hinzugefügt wurde, können die Funk-Zylinder (Aperio Komponente) hinzugefügt werden.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

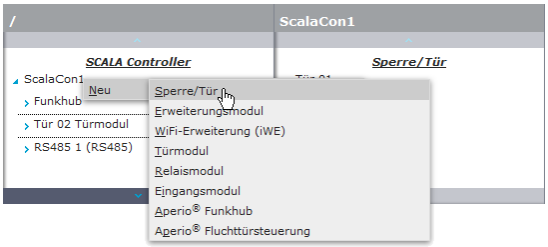
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

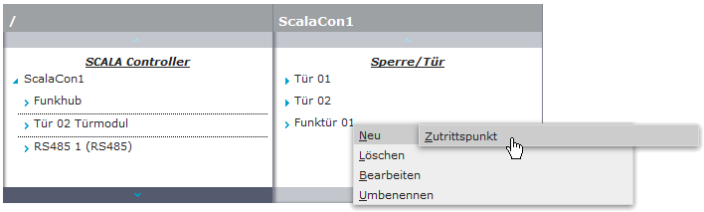
⇨ Im unteren Bildbereich wird die konfigurierte Hardware angezeigt.

4 Klicken Sie im Kontextmenü zum *SCALA Controller* auf Neu und weiter auf Sperre/Tür.



5 Benennen Sie die neue Funktür.

6 Klicken Sie im Kontextmenü zur Funktür auf Neu und weiter auf Zutrittspunkt.



7 Benennen Sie den neuen Zutrittspunkt.
ASSA ABLOY Sicherheitstechnik empfiehlt die Benennung der Funktür zu übernehmen.

8 Klicken Sie im Kontextmenü zum Zutrittspunkt auf Neu und weiter auf Aperio Komponente.

9 Benennen Sie den neuen Funkzylinder.
ASSA ABLOY Sicherheitstechnik empfiehlt eine eindeutige Benennung des Funkzylinders.

⇨ Die LED am Funkhub signalisiert:
- leuchtet grün — Der Hub ist betriebsbereit und hat eine Verbindung zum Funkzylinder.

⇨ Oberhalb der Anschlussleiste am Controller signalisiert eine LED:
- leuchtet grün — Der Hub und der Funkzylinder wurden erfolgreich hinzugefügt.
- leuchtet rot — Der Hub und der Funkzylinder wurden nicht erfolgreich hinzugefügt.
- blinkt rot — Der Leser wurde nicht erfolgreich hinzugefügt.
  Eine mögliche Ursache: Es wurde eine falsche Adresse ausgewählt.

Einer Person Berechtigungen zuweisen

1 Weisen Sie den Personen Berechtigungen für die Funktür zu
(„Einer Person Berechtigungen zuweisen“, Seite 49)

Zeitmodell

Zeitmodelle

Über Zeitmodelle können Zutrittsberechtigungen zeitlich eingeschränkt werden. Zum Beispiel, keine Zutrittsberechtigung an Feiertagen oder in den Nachtstunden.

SCALA net beinhaltet die Standard-Zeitmodelle IMMER/ALWAYS, jeweils vom Typ *Online* und *Offline*, diese beinhalten keine zeitlichen Einschränkungen.

Ein Zeitmodell anlegen

In diesem Beispiel wird ein Zeitmodell für Werktage angelegt. Die Zutrittszeit ist von Montag bis Donnerstag 06:00 Uhr bis 18:00 Uhr und Freitags von 06:00 Uhr bis 13:00 Uhr. (Abb. 12). Die Feiertage werden nachfolgend über Feiertagslisten ergänzt.

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zeitmodell**.

⇨ Die *Zeitmodellliste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie den Typ aus

⇨ Eine leere Zeitmodellmatrix wird angezeigt

4 Benennen sie das Zeitmodell.

5 Doppelklicken Sie in die Zeile *Montag*.

⇨ Es wird ein Zeitbereich in die Zeile eingetragen, der Zeitbereich muss nun berabeitet werden.

6 Tragen Sie die Freigabezeiten in die Zeitmodellmatrix ein, in diesem Beispiel für Montag bis Freitag.

6.1 Markieren Sie den Zeitbereich.

6.2 Ändern Sie die *Von-Zeit* und die *Bis-Zeit*.

7 Klicken Sie auf Speichern.

⇨ Sie haben ein Zeitmodell erfasst (Abb. 12).

- Das Kürzel wird automatisch vergeben.
- Die Aufteilung in gleiche Zeitbereiche erfolgt auch automatisch.

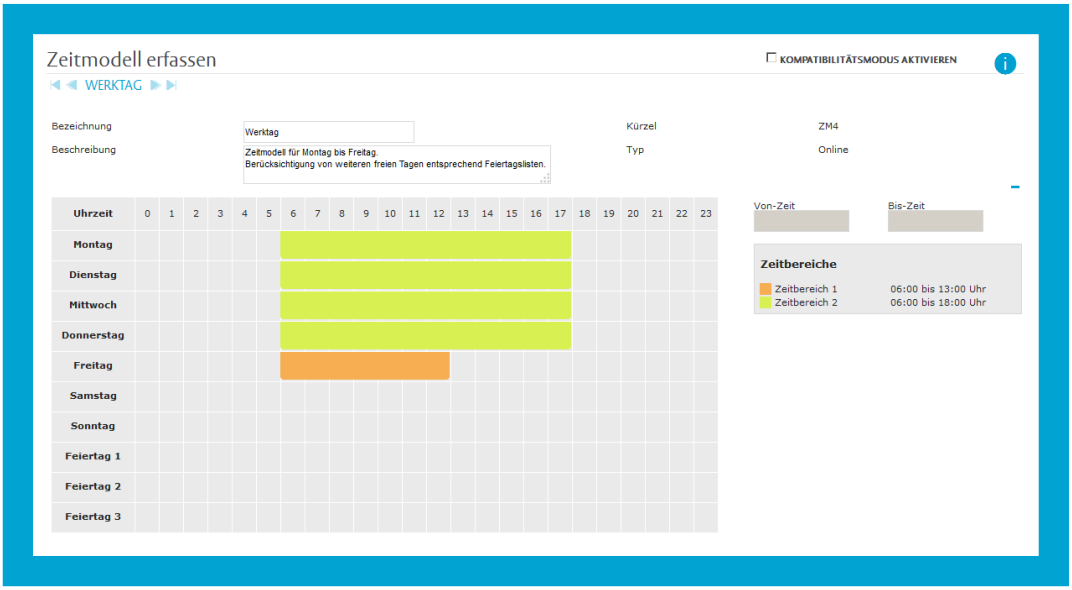
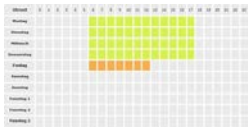


Abb. 12: Ein einfaches Zeitmodell

Zeitmodell



Feiertagsliste anlegen

Damit in einem Zeitmodell Feiertage berücksichtigt werden, muss zuerst mindestens eine Feiertagsliste angelegt werden.

In der Feiertagsliste können drei Typen von Feiertagen definiert werden. Diese entsprechen in den Zeitmodellen den Tagestypen *Feiertag 1* (= Typ 1) bis *Feiertag 3* (= Typ 3).

1 Klicken Sie auf **SYSTEM** / **Kalender**.
⇨ Die *Kalenderliste* wird angezeigt.
2 Klicken Sie auf Erfassen.
3 Geben Sie die Stammdaten ein.
4 Klicken Sie auf Speichern.
⇨ Die Feiertagsliste wird generiert und angezeigt.
⇨ Allen Feiertagen wurde automatisch der Typ 1 zugewiesen.
⇨ Falls in den Stammdaten das Bundesland ausgewählt wurde, enthält die Liste alle Feiertage des Bundeslandes.

Feiertagsliste erweitern

Es können weitere Feiertage zur Feiertagsliste ergänzt werden. So können zum Beispiel Betriebsferien eingetragen werden. Die Betriebsferientage werden dann wie Feiertage behandelt.

1 Klicken Sie auf **SYSTEM** / **Kalender**.
⇨ Die *Kalenderliste* wird angezeigt.
2 Klicken Sie auf die zu bearbeitende Feiertagsliste.
⇨ Die *Feiertagsliste* wird zur Bearbeitung geöffnet.
3 Klicken Sie auf .
4 Bearbeiten Sie die neue Zeile.
4.1 Es ist organisatorisch sinnvoll, die individuellen Feiertage von den regulären Feiertagen zu trennen.
Wählen Sie deshalb *Typ 2* oder *Typ 3* für die Betriebsferien.

Organisatorisch sinnvoll: die individuellen Feiertage von den regulären Feiertagen trennen

5 Klicken Sie auf .
6 Klicken Sie auf Speichern.
⇨ Die Feiertagsliste enthält nun auch weitere, individuelle Feiertage.

Feiertagsliste aktivieren

Die Feiertagsliste wird ignoriert, wenn Sie nicht für den jeweiligen *SCALA Controller,* für den sie gelten soll, aktiviert wird.

1 Klicken Sie auf **GERÄTE** / **Terminal**.
⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.
2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.
3 Klicken Sie auf STAMMDATEN.
4 Wählen Sie den *Feiertagskalender* aus.
⇨ Die Feiertagsliste ist nun aktiviert.
⇨ Die in der Feiertagsliste eingetragenen Tage werden nun im Zeitmodell berücksichtigt.
⇨ Falls erforderlich, können Zutrittsberechtigungen für diese Feiertage wie für die anderen Tage vergeben werden („Ein Zeitmodell anlegen“, Seite 62). Falls kein Zeitbereich eingetragen ist, hat die Person, der das Zeitmodell zugewiesen ist, kein Zutrittsrecht.

Zeitmodell

Zutrittsvergabe mit Zeitmodellen aktivieren

Damit Zeitmodelle zugewiesen werden können, muss diese Eigenschaft in *SCALA net* aktiviert sein.

Diese Eigenschaft wird normalerweise einmal eingestellt und anschließend nicht mehr geändert.

1 Klicken Sie auf **SYSTEM** / **Systemkonfiguration**.

⇨ Die *Systemkonfiguration* wird angezeigt.

2 Klicken Sie auf ZUTRITTSKONTROLLE.

3 Wählen Sie für Zutrittsvergabe *Matrix mit Zeitmodell*.

4 Klicken Sie auf Speichern.

⇨ Es können nun die Zeitmodelle den Personen zugewiesen werden.

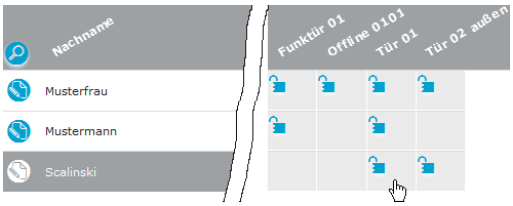
Ein Zeitmodell einer Person zuweisen

Damit das Zeitmodell wirksam wird, muss es den Personen und Türen zugewiesen werden.

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Profile**.

⇨ Die *Zutrittsmatrix-Profile* wird angezeigt.

2 Klicken Sie in die zu bearbeitende Matrixzelle.



3 Der Dialog *Zutrittsberechtigung für ...* wird angezeigt.
In der Titelzeile ist die ausgewählte Person (Zeile der Matrix) und die ausgewählte Tür (Spalte der Matrix) genannt.

4 Klicken Sie auf ZUTRITTSBERECHTIGUNGEN.

5 Markieren Sie das gültige Zeitmodell für die in der Kopfzeile genannte Person und Tür.

6 Klicken Sie auf OK.

⇨ Sie haben eine Person und eine Tür mit einem Zeitmodell verbunden.

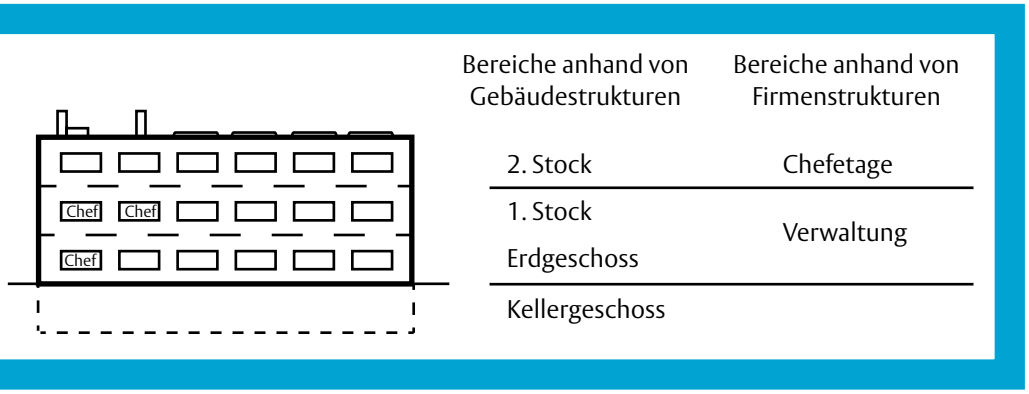
Bereiche

Organisatorische Strukturen

In *SCALA net* können Türen bzw. Leser in Bereichen organisiert werden. Ein Offline-Bereich (DoC- bzw. OSO-Bereich) wurde in dieser Kurzanleitung bereits angelegt („Türen – Beispiel Tür 03 Data-on-Card- bzw. OSO-Bereich vorbereiten“, Seite 56). Es können aber auch weitere Bereiche angelegt werden, zum Beispiel Online-Bereiche oder Bereiche, die Gebäudestrukturen wiederspiegeln, zum Beispiel Bereiche nach Etagen aufgeteilt.

Bereiche können sich auch überschneiden, zum Beispiel könnten die vier Bereiche Kellergeschoss, Erdgeschoss, 1. Stock und 2. Stock zu den Bereichen Kellergeschoss, Verwaltung mit Erdgeschoss und 1. Stock und Chefetage mit 2. Stock und einzelnen Räumen aus anderen Etagen zusammengefasst werden (Prinzipielles Beispiel in Abb. 13).

Abb. 13: Prinzipielles Beispiel mit sich überschneidenden Bereichen anhand von Gebäudestrukturen und Firmenstrukturen



Hinweis!

Bei aktivierter Bereichswechselkontrolle werden Bewegungsdaten protokolliert: Die optionale Bereichswechselkontrolle wird unter **GERÄTE** / **Terminal** auf der Registerkarte **PARAMETER** aktiviert. SCALA net protokolliert die Bewegungen von Ausweisen (Personen) an den festgelegten Ein- und Austrittspunkten.

Offline-Bereiche / DoC-Bereich oder OSO-Bereich

Zu einem Offline-Bereiche gehört ein Update-Leser

Offline-Leser müssen in mindestens einem DoC- bzw. OSO-Bereich zusammengefasst werden. Zu einem Offline-Bereich gehört immer mindestens ein Berechtigungsschreiber (Update-Leser). Dies muss bei der Planung von Bereichen berücksichtigt werden.

Es muss ein Update-Leser dem Offline-Bereich zugeordnet werden („Türen – Beispiel Offline-Leser / Data on Card (DoC) oder OSS-SO (OSO)“, Seite 57).

Hinweis!

Update-Leser löschen: Wurde ein Update-Leser einem Bereich zugeordnet und Zutrittsberechtigungen vergeben, so kann der Leser erst wieder aus dem Bereich gelöscht werden, nachdem alle Zutrittsberechtigungen für diesen Leser gelöscht wurden („Ausweise / Personen“, Seite 48).

Planung

Zur Planung von Bereichen empfiehlt es sich zunächst eine tabellarische Darstellung anzufertigen (Prinzipielles Beispiel in Abb. 14).

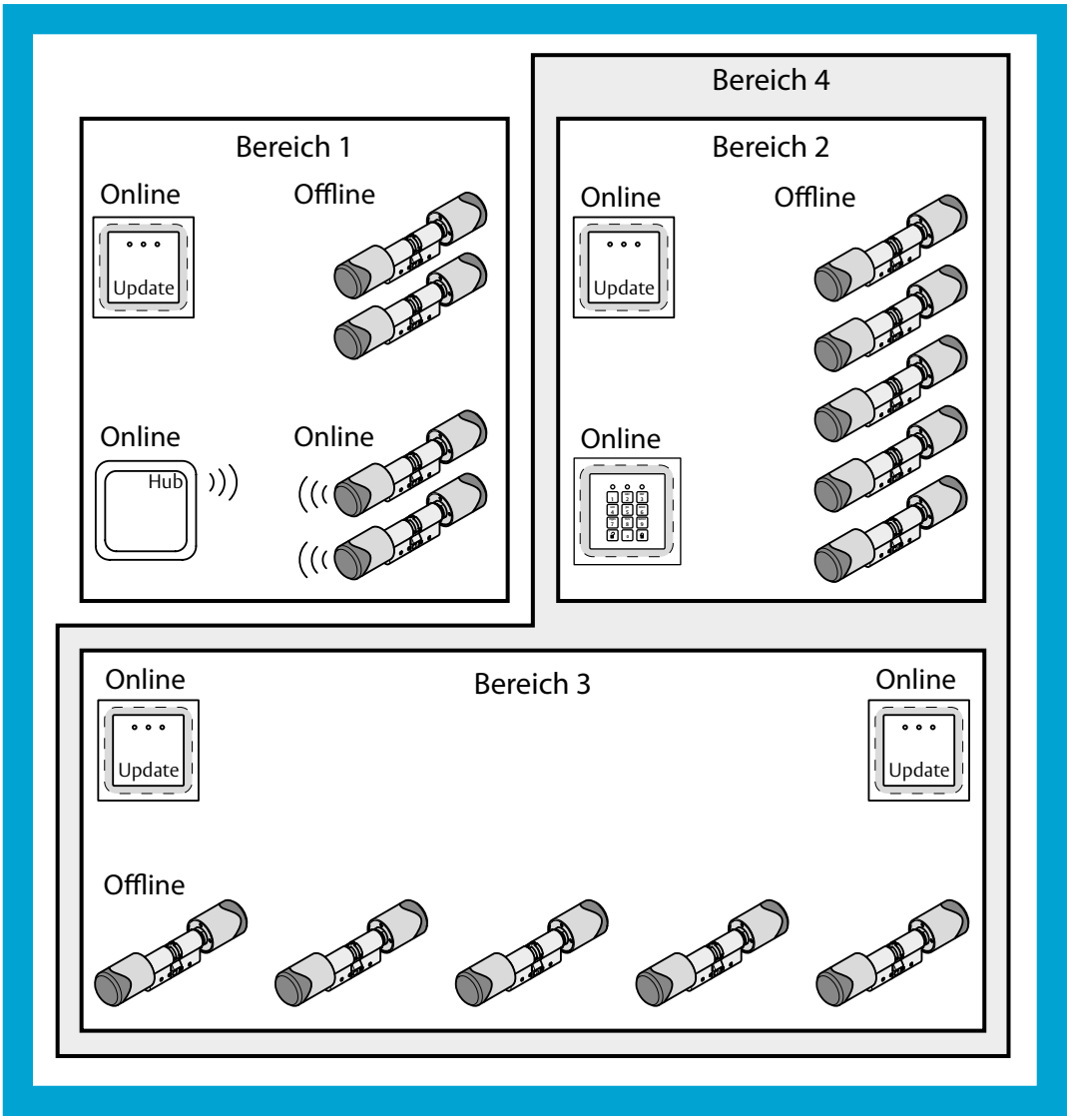


Abb. 14: Prinzipielles Beispiel einer Planung von Bereichen

Einen Bereich erfassen

1 Klicken Sie auf **ORGANISATION** / **Bereich**.

⇨ Die Bereichsliste wird angezeigt.

2 Klicken Sie auf Erfassen.
3 Wählen Sie das System **SCALA net (SCALA Controller)**.
4 Erfassen Sie die Stammdaten zu dem neuen Bereich.
5 Klicken Sie auf Speichern.

⇨ Sie haben einen Bereich erfasst.

Mandanten

SCALA net ist eine mandantenfähige Software. Mandanten sind eine weitere Möglichkeit die Nutzung des Systems zu strukturieren.

Definition: Mandanten in der Informationstechnik

Sicherlich verbinden viele Leser mit dem Begriff *Mandanten* einen Auftraggeber, zum Beispiel eines Rechtsanwalts oder Steuerberaters, also eine natürliche Person. Dies ist hier nicht gemeint.

Definition

In der Informationstechnologie ist ein Mandant die oberste Ordnungsinstanz in einem IT-System. Der Mandant ist eine datentechnisch und organisatorisch geschlossene Einheit im IT-System. Jeder Mandant kann nur seine eigenen Daten sehen.

Vorteile von Mandantensystemen sind:
- die zentrale Installation und Wartung,
- der geringere Speicherbedarf für Daten (da mehrere Mandanten die mandantenübergreifenden Daten gemeinsam verwenden),
- sowie geringere Lizenzkosten.

Tab. 11: Mandantenübergreifende und mandantenunabhängige Daten

Mandantenübergreifende Daten	Mandantenabhängige Daten
Mandantenübergreifende Daten sind Daten, die für alle Mandanten gemeinsam verwaltet werden:	Mandantenabhängige Daten sind Daten, die für jeden Mandanten individuell verwaltet werden:
in SCALA net	
Ausweislänge Raumzonen-Zutrittspunkt-Zuordnung Zeitmodelle allgemeine Systemparameter	Terminals Türen Zutrittspunkte Leser Personenberechtigungen Gruppenberechtigungen Identifizierungsmerkmale Skripte Transponderdefinitionen Auswertungen

Der Standardmandant

Der Standardmandant wird immer mit der Hauptlizenz freigeschaltet. Der Standardmandant beinhaltet die Basiskonfiguration und die mandantenübergreifenden Daten.

Hauptmandant und Arbeitsmandant

Der Hauptmandant ist der einem Benutzer grundsätzlich zugewiesene Mandant. Arbeitsmandant ist der Mandant, in dem der Benutzer gerade arbeitet. Es ergeben sich folgende Möglichkeiten:

ohne Mandanten	*SCALA net* ohne Mandanten nutzen	Werden keine weiteren Mandanten angelegt, bleibt der Standardmandant als einziger Mandant im Hintergrund und ist für die Benutzung nicht weiter von Bedeutung. Alle Administratoren und andere Benutzer haben automatisch den Standardmandanten als Hauptmandanten. Hauptmandant und Arbeitsmandant sind für alle Benutzer und Administratoren identisch.	
mit Mandanten	*SCALA net* mit Mandanten strukturieren	Administratoren	**Administratoren haben den Standardmandanten als Hauptmandanten zugeordnet**. Sie können alle Mandanten sehen und zur Bearbeitung zwischen den Arbeitsmandanten wechseln.
		Benutzer	**Benutzer haben nicht den Standardmandaten als Hauptmandanten zugeordnet**, sondern einen anderen Mandanten. Sie können andere Mandanten nicht sehen und nur die mandantenabhängigen Daten ihres eigenen Mandanten bearbeiten. Hauptmandant und Arbeitsmandant sind identisch.

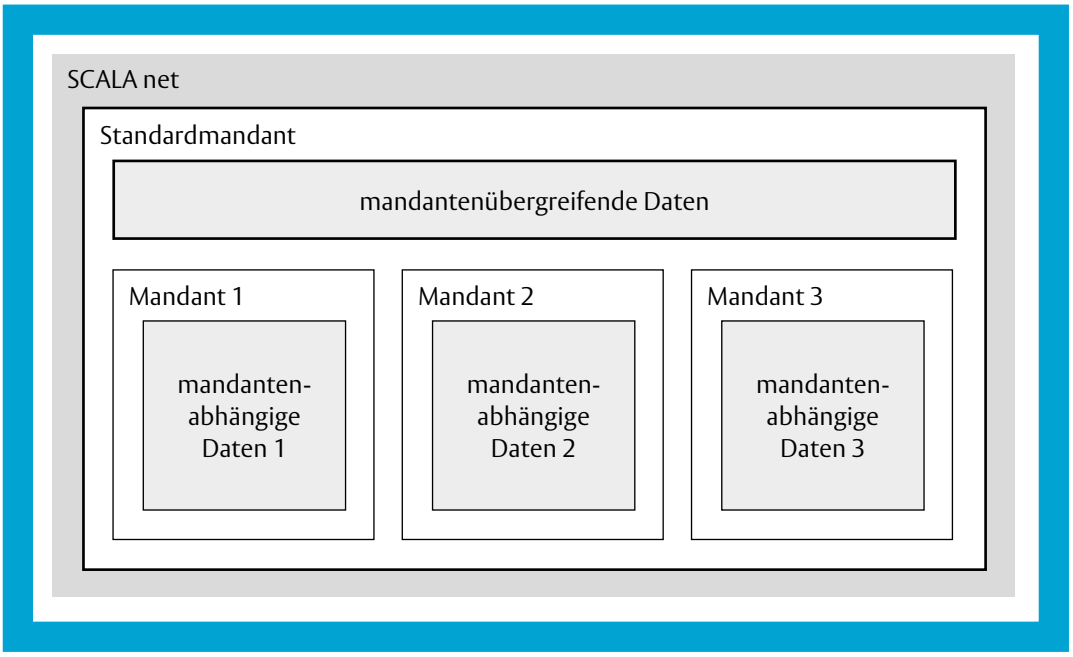


Abb. 15: Beispiel einer Systematik beim Strukturieren mit Mandanten

Einen Mandanten erfassen

1 Klicken Sie auf **SYSTEM** / **Mandanten**.

⇨ Die Mandantenliste wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Erfassen Sie die Stammdaten zu dem neuen Mandanten.

4 Klicken Sie auf Speichern.

⇨ Sie haben einen Mandanten erfasst.

⇨ Dieser neue Mandant ist den Administratoren automatisch zusätzlich zugewiesen.

Einem Benutzer eine Mandantenberechtigung zuweisen

Administratoren haben automatisch alle Mandanten Berechtigungen zugewiesen bekommen. Allen anderen Benutzern müssen die Mandanten zugewiesen werden.

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

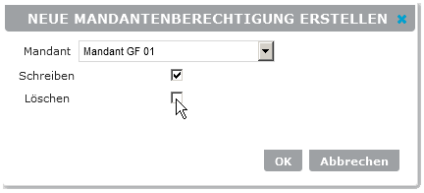
⇨ Die Benutzerliste wird angezeigt.

2 Klicken Sie auf den zu bearbeitenden Benutzer.

3 Klicken Sie auf MANDANTENBERECHTIGUNGEN.

4 Klicken Sie auf .

5 Wählen Sie den Mandanten aus und weißen Sie die Berechtigungen zu.



6 Klicken Sie auf Speichern.

⇨ Sie haben einem Benutzer einen Mandanten zugewiesen.

V Systemkonfiguration

In diesem Kapitel wird beschrieben, wie SCALA net lokalisiert und aktualisiert werden kann. Darunter fallen grundsätzliche Einstellungen zum Kalenders, zu Benutzern und Benutzerrollen, zu Transpondern, aber auch die Aktualisierung von Firmware und die Erweiterung von Lizenzen.

Systemkonfiguration

Achtung!

Gefahr eines Systemausfalls: Falsche Systemkonfigurationen können zu Funktionsausfällen oder Funktionseinschränkungen führen.

- Informieren Sie sich sorgfältig, bevor Sie Systemkonfigurationen bearbeiten.
- Erstellen Sie zur Sicherheit ein Backup des aktuellen Systems, bevor Sie Änderungen vornehmen („Backup / Datensicherung“).

Hinweis!

Die Konfiguration ist abhängig von den erworbenen Lizenzen: Nicht-lizenzierte Funktionen können nicht ausgeführt werden. Die Lizenzen sind über die erworbene Lizenzdatei fest vorgegeben. Werkseitig voreingestellte Standarddaten (grau dargestellt) können bei fehlender Lizenz nicht geändert werden.

- Erweitern Sie bei Bedarf den Funktionsumfang. Dazu können Sie Lizenzen nachbestellen.

Backup / Datensicherung

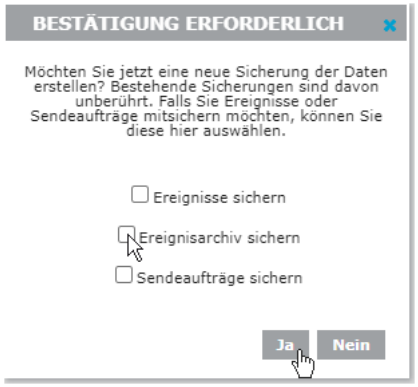
Die Datenbank sichern / Ein Backup erstellen

1 Klicken Sie auf **SYSTEM** / **Datenbankmanagement**.

⇨ Informationen über die aktuell verwendete Datenbank werden angezeigt.

2 Klicken Sie auf Backup.

⇨ Der Dialog *Bestätigung erforderlich* wird angezeigt.



3 Wählen Sie bei Bedarf zusätzlich zu sichernde Optionen aus.

4 Klicken Sie auf Ja.

5 Folgen Sie den weiteren Anweisungen.

⇨ Die Datenbank wird gesichert und in einer Backup-Datei abgelegt.

Die Datenbank wiederherstellen / Ein Backup einspielen

1 Klicken Sie auf **SYSTEM** / **Datenbankmanagement**.

⇨ Informationen über die aktuell verwendete Datenbank werden angezeigt.

2 Klicken Sie auf Datei hochladen.

3 Folgen Sie den weiteren Anweisungen.

⇨ Die Datenbank wird anhand der ausgewählten Backup-Datei wieder hergestellt.

Firmware Update

Es ist empfehlenswert die Firmware des Controllers regelmäßig zu aktualisieren.

SCALA PARTNERSHIP Extranet

Aktuelle Firmware Releases werden von *ASSA ABLOY Sicherheitstechnik GmbH* zertifizierten SCALA-Systempartnern über das *SCALA PARTNERSHIP Extranet* bereitgestellt.

Die Controller-Firmware aktualisieren

1 Klicken Sie auf **GERÄTE** / **Firmware-Verwaltung**.

⇨ Die *Firmware-Verwaltung* wird angezeigt.
Es werden die bereits installierten Versionen aufgelistet.

2 Klicken Sie auf Erfassen.

⇨ *Firmware erfassen* wird angezeigt.

3 Geben Sie in die Daten ein.
- 3.1 Geben Sie eine sprechende Bezeichnung* ein, die später in der Firmware-Verwaltungsliste angezeigt wird.
- 3.2 Wählen Sie den passenden Typ* der Firmware, zum Beispiel *Firmware SCALA Controller*.
- 3.3 Falls Sie weitere Controller hinzufügen wollen und mit der neuen Firmware betreiben wollen:
  Legen Sie die neue Firmware als Gerätestandard fest.
  Die neue Firmware wird dann allen in die SCALA-net-Umgebung eingebundenen Controllern automatisch zugewiesen.

4 Klicken Sie in das Textfeld Hochladen.

⇨ Ein Dateiauswahldialog wird angezeigt.

5 Wählen Sie die von *ASSA ABLOY Sicherheitstechnik GmbH* gelieferte Installationsdatei aus.

6 Klicken Sie auf Speichern.

⇨ *Firmware bearbeiten* wird angezeigt.

7 Klicken Sie auf Geräte aktualisieren.

⇨ Die Geräte werden aktualisiert. Das kann einige Minuten dauern.

⇨ Nach erfolgreicher Aktualisierung ist der Controller in der angezeigten Liste grün abgehakt.

⇨ Die Controller-Firmware ist aktualisiert.

Lizenzverwaltung

Zur Nutzung von *SCALA net* muss eine gültige Lizenz importiert werden. Dadurch wird der Funktionsumfang von *SCALA net* festgelegt.

Die Lizenz wird von *ASSA ABLOY Sicherheitstechnik GmbH* in zwei Dateien geliefert, eine LIC-Datei mit der codierten Lizenzbeschreibung und eine TXT-Datei mit dem Lizenzschlüssel als Klartext. Die LIC-Datei muss importiert werden, zusätzlich muss der Lizenzschlüssel eingegeben werden.

Eine Lizenz importieren

1 Klicken Sie auf **SYSTEM** / **Lizenzverwaltung**.

⇨ Die *Lizenzverwaltung* wird angezeigt.

2 Wechseln Sie auf die Registerkarte **IMPORT**.

3 Klicken Sie in das Texteingabefeld Lizenzdatei hochladen.

⇨ Ein Dateiauswahldialog wird angezeigt.

4 Wählen Sie die von *ASSA ABLOY Sicherheitstechnik GmbH* gelieferte LIC-Datei aus.

5 Kopieren Sie den Lizenzschlüssel aus der von *ASSA ABLOY Sicherheitstechnik GmbH* gelieferten TXT-Datei in das Texteingabefeld Lizenzschlüssel.

6 Klicken Sie auf Import.

⇨ Es wird eine Erfolgsmeldung angezeigt, wenn die Lizenz erfolgreich importiert wurde.

7 Ändern Sie das Passwort.

⇨ Die Lizenz wurde importiert. *SCALA net* arbeitet nun mit dem lizenzierten Funktionsumfang.

⇨ Die Kundendaten und die Lizenzdaten mit den freigeschalteten Modulen werden auf der Registerkarte **LIZENZDETAILS** angezeigt.

Kalender und Zeitmodelle

Zeitmodelle

Der Kalender dient als Grundlage für die Verwaltung von Zeitmodellen. Über Zeitmodelle können Zutrittsberechtigungen zeitlich eingeschränkt werden. Zum Beispiel, keine Zutrittsberechtigung an Feiertagen oder in den Nachtstunden.

Standard-Zeitmodelle IMMER/ALWAYS

SCALA net beinhaltet die Standard-Zeitmodelle IMMER/ALWAYS, jeweils vom Typ *Online* und *Offline*, diese beinhalten keine zeitlichen Einschränkungen.

Feiertagslisten

Der Kalender dient zum Verwalten von Feiertagslisten. In den Feiertagslisten werden auch Betriebsferien und lokale oder individuelle Feiertage und besondere Werktage eingetragen, zum Beispiel Tage, an denen ein Gebäude abweichend von der Regel geschlossen bleibt oder der Zugang abweichend geregelt werden soll.

Feiertage in drei Typen kategorisieren

Bei Bedarf können drei Typen von Feiertagen unterschieden werden. Es ist nicht zwingend notwendig, aber empfehlenswert, um zum Beispiel zwischen gesetzlichen Feiertagen, Betriebsferien und weiteren besonderen Tagen organisatorisch zu unterscheiden.

Kalender und Zeitmodell verbinden

Die über den Kalender angelegten Feiertagslisten werden erst dann vom System ausgewertet, wenn die Feiertagsliste einem Zeitmodell zugeordnet ist. Das Zeitmodell muss einem Controller zugeordnet sein (Abb. 16).

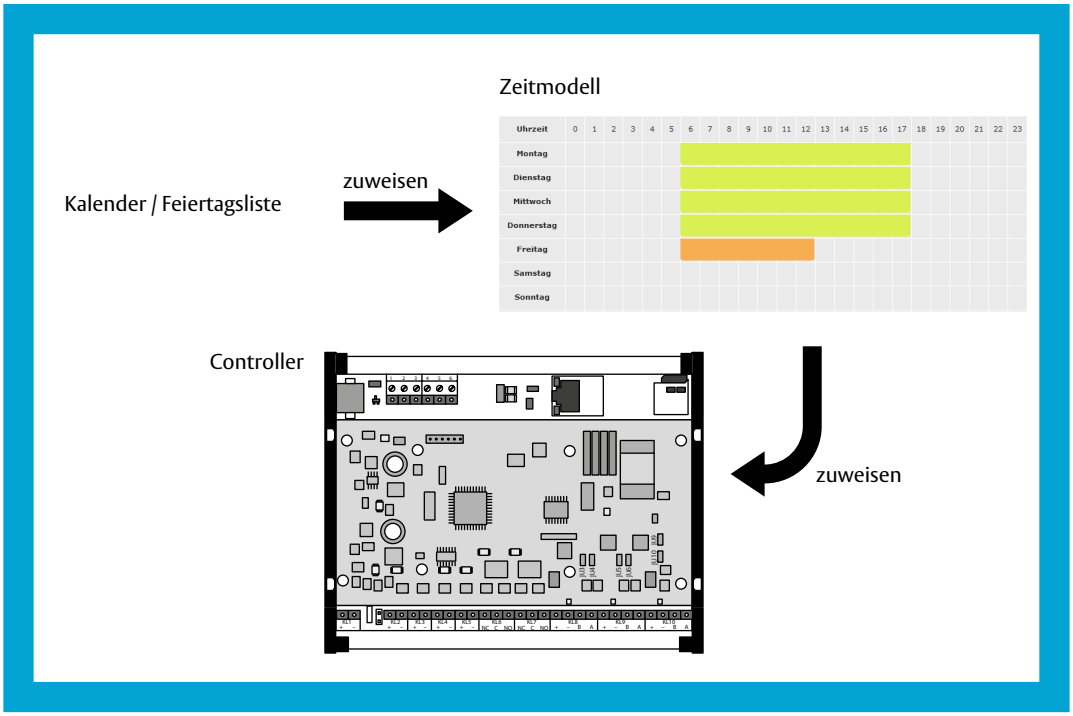


Abb. 16: Prinzipieller Zusammenhang von Kalender, Zeitmodell und Controller

Feiertagsliste anlegen

1 Klicken Sie auf **SYSTEM** / **Kalender**.

⇨ Die *Kalenderliste* wird angezeigt.
Im unkonfigurierten System sind noch keine Kalender angelegt.

2 Klicken Sie auf Erfassen.

3 Klicken Sie auf STAMMDATEN.

4 Geben Sie die Stammdaten ein (Tab. 12).

5 Klicken Sie auf Speichern.

⇨ Die Feiertagsliste wird generiert und angezeigt (Abb. 17).

⇨ Allen Feiertagen wurde automatisch der *Typ 1* zugewiesen.

⇨ Falls in den Stammdaten das Bundesland ausgewählt wurde, enthält die Liste alle Feiertage des Bundeslandes.

Tab. 12: Feiertagsliste konfigurieren

Parameter	Beschreibung
Name	Individuelle Benennung der Feiertagsliste.
Gültigkeit	Feiertage bis zum eingetragenen Jahr. Kann nicht bearbeitet werden.
Land *Provinz*	Angeben, um die gesetzlichen Feiertage zu übernehmen.

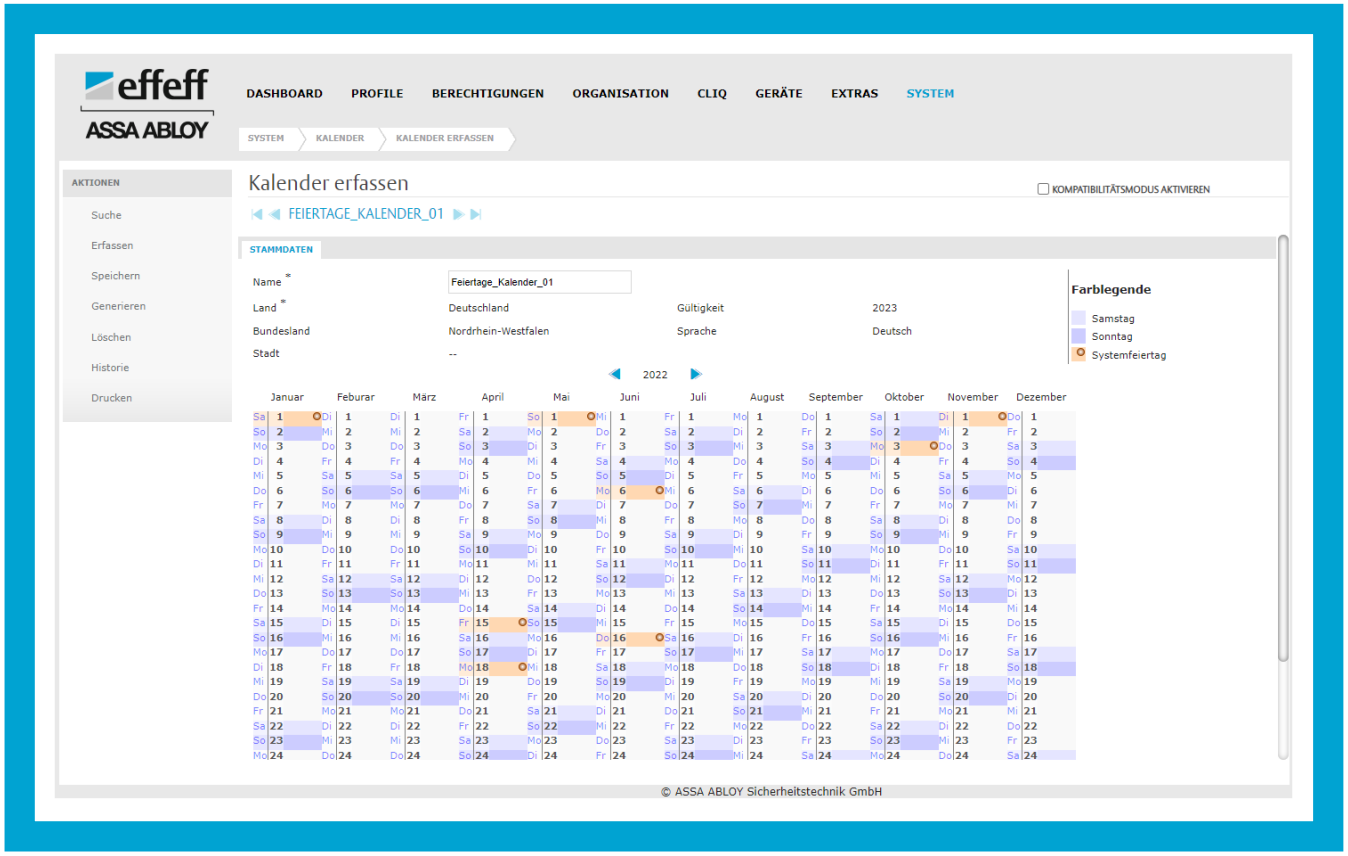


Abb. 17: Kalender mit den in SCALA net festgelegten Feiertagen für das gewählte Bundesland und Jahr

Feiertagsliste erweitern – Feiertag anlegen

1 Klicken Sie auf **SYSTEM** / **Kalender**.

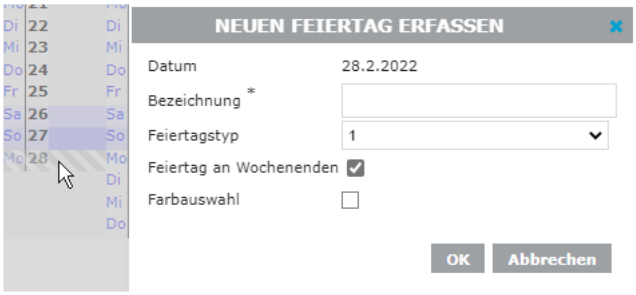
⇨ Die *Kalenderliste* wird angezeigt.

2 Klicken Sie auf die zu bearbeitende Feiertagsliste.

⇨ Die *Feiertagsliste* wird zur Bearbeitung geöffnet.

3 Klicken Sie auf einen Tag, der als zusätzlicher Feiertag festgelegt werden soll.

⇨ Der Dialog *Neuen Feiertag erfassen* wird angezeigt.

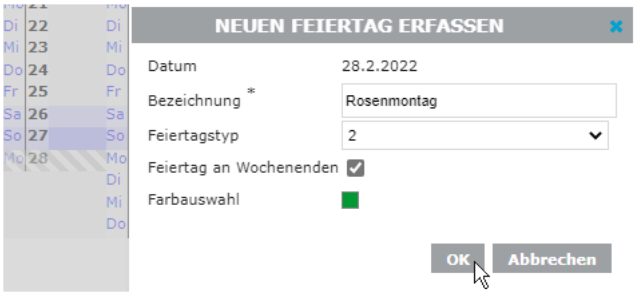


4 Geben Sie die Daten ein:

4.1 Geben Sie eine eindeutige Bezeichnung ein.

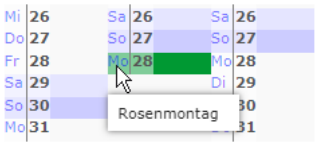
4.2 Wählen Sie *Typ 2* oder *Typ 3* für *Betriebsferien* (Tab. 13 – *Typ*).

4.3 Wählen Sie eine Darstellungsfarbe aus



5 Klicken Sie auf **OK**.

⇨ Die Feiertagsliste enthält nun einen weiteren, individuelle Feiertag.



6 Klicken Sie auf Speichern.

Tab. 13: Feiertag konfigurieren

Parameter	Beschreibung
Bezeichung *Datum*	Individuelle Benennung und Zeitpunkt des Tages (zum Beispiel Feiertag oder Werksferientag)
Typ	Automatisch wird *Typ 1* zugewiesen. Bei Bedarf kann zwischen drei Typen von Feiertagen unterschieden werden. Es ist möglich, die drei Typen in unterschiedlichen Zeitmodellen gesondert zu berücksichtigen. Es ist organisatorisch sinnvoll, die individuellen Feiertage von den regulären Feiertagen zu trennen.

Ein Zeitmodell anlegen

In diesem Beispiel wird ein Zeitmodell für Werktage angelegt. Die Zutrittszeit ist von Montag bis Donnerstag 06:00 Uhr bis 18:00 Uhr und Freitags von 06:00 Uhr bis 13:00 Uhr. (Abb. 18). Die Feiertage werden nachfolgend über Feiertagslisten ergänzt.

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zeitmodell**.

⇨ Die *Zeitmodellliste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie den Typ aus

⇨ Eine leere Zeitmodellmatrix wird angezeigt

4 Benennen sie das Zeitmodell.

5 Doppelklicken Sie in die Zeile *Montag*.

⇨ Es wird ein Zeitbereich in die Zeile eingetragen, der Zeitbereich muss nun bearbeitet werden.

6 Tragen Sie die Freigabezeiten in die Zeitmodellmatrix ein, in diesem Beispiel für Montag bis Freitag.

6.1 Markieren Sie den Zeitbereich.

6.2 Ändern Sie die *Von-Zeit* und die *Bis-Zeit*.

7 Klicken Sie auf Speichern.

⇨ Sie haben ein Zeitmodell erfasst (Abb. 18).

- Das Kürzel wird automatisch vergeben.
- Die Aufteilung in gleiche Zeitbereiche erfolgt auch automatisch.

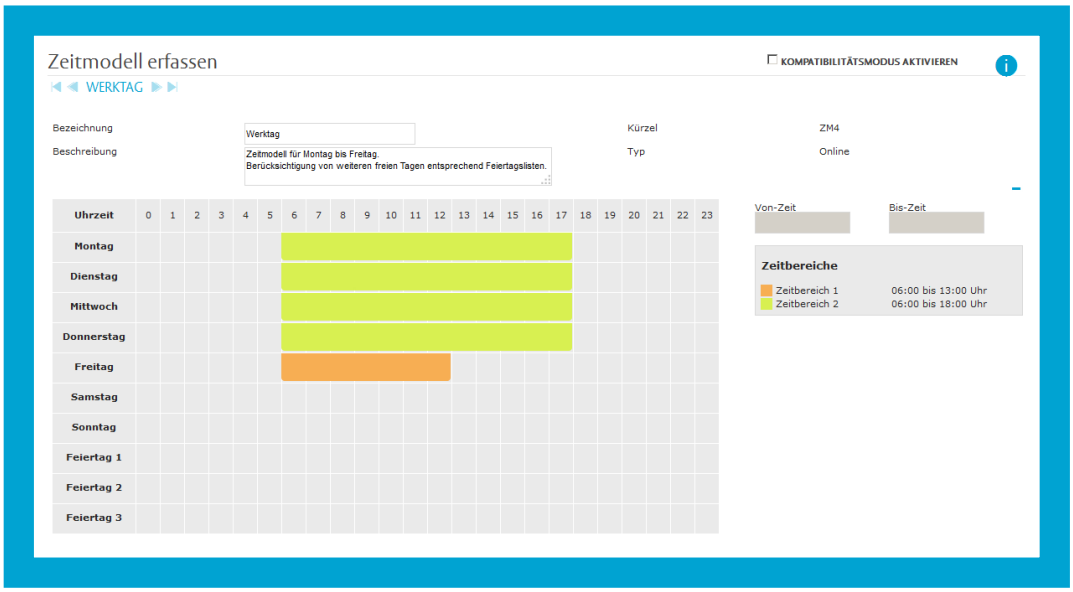


Abb. 18: Ein einfaches Zeitmodell

Feiertagsliste aktivieren

Die Feiertagsliste wird ignoriert, wenn Sie nicht für den jeweiligen *SCALA Controller,* für den sie gelten soll, aktiviert wird.

1 Klicken Sie auf **GERÄTE** / **Terminal**.

⇨ In der *Terminal-Liste* wird der betriebsbereite *SCALA Controller* angezeigt.

2 Klicken Sie auf den zu konfigurierenden *SCALA Controller* in der Terminal-Liste.

3 Klicken Sie auf STAMMDATEN.

4 Wählen Sie den *Feiertagskalender* aus.

⇨ Die Feiertagsliste ist nun aktiviert.

⇨ Die in der Feiertagsliste eingetragenen Tage werden nun im Zeitmodell berücksichtigt.

⇨ Falls erforderlich, können Zutrittsberechtigungen für diese Feiertage wie für die anderen Tage vergeben werden („Ein Zeitmodell anlegen“, Seite 77). Falls kein Zeitbereich eingetragen ist, hat die Person, der das Zeitmodell zugewiesen ist, kein Zutrittsrecht.

Feiertage generieren

Durch die Funktion *Feiertage generieren*, werden alle Feiertage überschrieben, die nicht selbst erfasst wurden. Dies kann zum Beispiel beim Wechsel eines Bundeslandes notwendig sein.

1 Klicken Sie auf **SYSTEM** / **Kalender**.

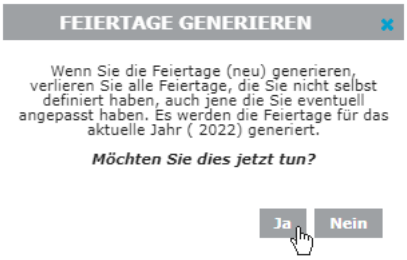
⇨ Die *Kalenderliste* wird angezeigt.

2 Klicken Sie auf die zu bearbeitende Feiertagsliste.

⇨ Die *Feiertagsliste* wird zur Bearbeitung geöffnet.

3 Klicken Sie Generieren.

⇨ Der Dialog *Feiertage generieren* wird zur Bestätigung angezeigt.



4 Klicken Sie auf Ja wenn Sie die Feiertage überschreiben wollen:

Selbstdefinierte Feiertage automatisch fortschreiben

SCALA net schreibt die Feiertage passend zum gewählten Bundesland automatisch in die nachfolgenden Jahre fort. Optional kann dies auch für selbstdefinierte Feiertage aktiviert werden. Dies ist aber nur sinnvoll, wenn in jedem Jahr das gleiche Datum belegt wird, zum Beispiel für Betriebsferien zwischen Weihnachten und Neujahr. („Zeitaufträge“, Seite 98)

1 Klicken Sie auf **SYSTEM** / **Systemkonfiguration**.
2 Klicken Sie auf SYSTEM.
3 Aktivieren Sie die Option *Eigene Feiertage fortschreiben*.
4 Klicken Sie auf Speichern.

Zeitzone einrichten

werkseitig für Deutschland auf Europe/Berlin eingestellt

Die Zeitzone ist werkseitig für Deutschland auf *Europe/Berlin* eingestellt.

1 Klicken Sie auf **SYSTEM** / **Systemkonfiguration**.
2 Klicken Sie auf SYSTEM.
3 Wählen sie die passende *Standard Zeitzone* aus.
4 Klicken Sie auf Speichern.

Benutzer

Administrator und Benutzer

Systembenutzer bedienen *SCALA net*. Einfache Systembenutzer (*Benutzer*) bekommen vom *Administrator* Berechtigungen zugewiesen (Tab. 14). Ein *Administrator* ist ein Systembenutzer mit Zugang zu allen lizenzierten Berechtigungen.

Benutzertypen

Tab. 14: Benutzertypen und ihre Eigenschaften

	Beschreibung
Systembenutzer (Benutzer)	Der *Benutzer* kann *SCALA net* entsprechend seiner individuellen Berechtigungen benutzen. Die Berechtigungen werden von einem Administrator festgelegt.
Systembenutzer mit allen Rechten (Administrator)	Der *Administrator* ist ein spezieller Benutzer mit allen Berechtigungen. Er kann *SCALA net* ohne Einschränkungen benutzen. Die Berechtigungen sind alle automatisch gesetzt und können nicht verändert werden.

Benutzerrollen

Benutzertypen entsprechen systemeigene Benutzerrollen

Prinzipiell sind die oben genannten *Benutzertypen* bereits systemseitig vorgegebene *Benutzerrollen*. Wenn keine weiteren Benutzerrollen definiert wurden, dann muss jedem Benutzer der Benutzertyp *Systembenutzer* zugewiesen werden (Abb. 19 –1). Für *Benutzer mit allen Rechten* muss die Option *Administrator* gesetzt sein (2).

Benutzerseitig definierte Benutzerrollen

Administratoren oder andere Benutzer mit der zugewiesenen Berechtigung können weitere Benutzerrollen anlegen, zum Beispiel für bestimmte Abteilungen, Geschäftsfelder, Gebäudebereiche oder Tätigkeitsfelder im Gebäude. Diesen Benutzerrollen können Berechtigungen zugewiesen oder entzogen werden. Dabei können Berechtigungen in einem Arbeitsgang für ganze Module oder nur für Teile von Modulen zugewiesen oder entzogen werden.

Benutzer

Nachdem die Benutzerrollen definiert wurden, können diese Benutzern zugewiesen werden.

So können Benutzer in Gruppen organisiert werden. Es gibt zum Beispiel mehrere Benutzer, die am Empfang arbeiten. Alle diese Benutzer haben über die Benutzerrolle *Empfang* dieselben Berechtigungen zugewiesen bekommen. Sollen im Nachhinein diesen Benutzern Berechtigungen zugewiesen oder entzogen werden, geschieht dies über die Benutzerrolle *Empfang* für alle gleichzeitig.

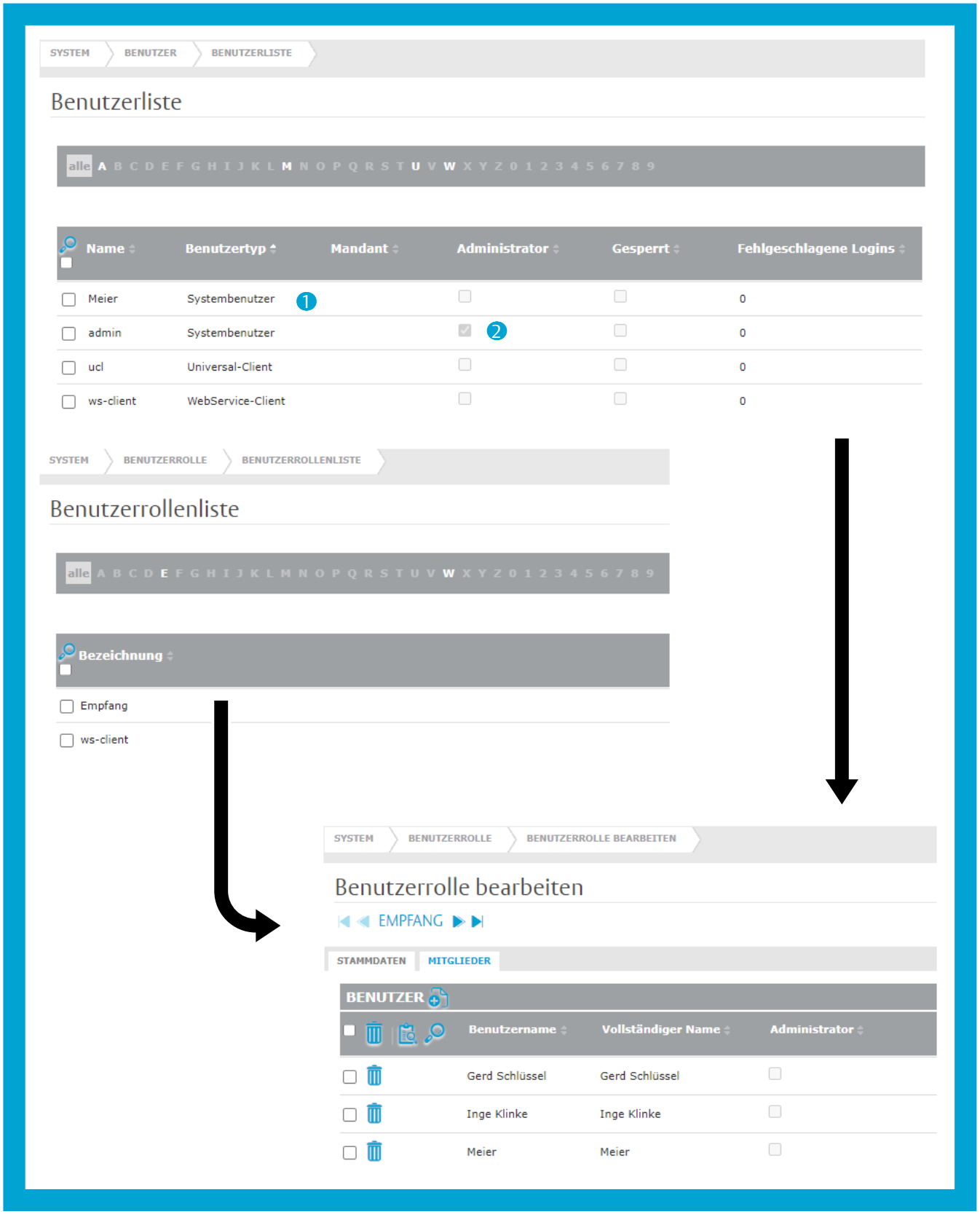


Abb. 19: Darstellung von Benutzerrollen und Benutzern

Benutzer-Stammdaten erfassen

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

⇨ Die *Benutzerliste* wird angezeigt.

2 Klicken Sie auf Erfassen.
3 Wählen Sie in der Vorauswahl den Benutzertyp, im Regelfall *Systembenutzer*.
Je nach Lizenz stehen weitere Benutzertypen zur Auswahl.
4 Erfassen Sie die Stammdaten zu dem neuen Benutzer.
5 Klicken Sie auf Speichern.

⇨ Sie haben neue Benutzer-Stammdaten erfasst.

Benutzer-Stammdaten bearbeiten

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

⇨ Die *Benutzerliste* wird angezeigt.

2 Klicken Sie in der Benutzerliste auf den zu bearbeitenden Benutzer.
3 Ändern Sie die Stammdaten zu dem neuen Benutzer.
4 Klicken Sie auf Speichern.

⇨ Sie haben die Benutzer-Stammdaten geändert.

Benutzer-Stammdaten löschen

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

⇨ Die *Benutzerliste* wird angezeigt.

2 Klicken Sie in der Benutzerliste auf den zu bearbeitenden Benutzer.
3 Klicken Sie auf Löschen.

⇨ Sie haben die Benutzer-Stammdaten gelöscht.

Benutzerrolle / Zuweisen von Berechtigungen

In der Benutzerrolle werden die Berechtigungen für Benutzergruppen festgelegt.

Benutzerrolle anlegen

1 Klicken Sie auf **SYSTEM** / **Benutzerrolle**.

⇨ Die *Benutzerrollenliste* wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Definieren Sie die Benutzerrolle.

3.1 Setzen Sie die Berechtigungen für die Benutzerrolle,
- aktivieren / deaktivieren Sie Module für das Hauptmenü und das Dashboard (Abb. 20),

4 Klicken Sie auf Speichern.

⇨ Sie haben eine neue Benutzerrolle erfasst.

oder alternativ

1 Klicken Sie auf **SYSTEM** / **Benutzer**.

⇨ Die *Benutzerliste* wird angezeigt.

2 Wechseln Sie auf die Registerkarte BERECHTIGUNGEN.

3 Klicken Sie auf .

⇨ Die Eingabemaske *Benutzerrolle erfassen* wird angezeigt.

4 Definieren Sie die Benutzerrolle.

4.1 Setzen Sie die Berechtigungen für die Benutzerrolle,
- aktivieren / deaktivieren Sie Module für das Hauptmenü und das Dashboard (Abb. 20),

5 Klicken Sie auf Speichern.

⇨ Sie haben eine neue Benutzerrolle erfasst.

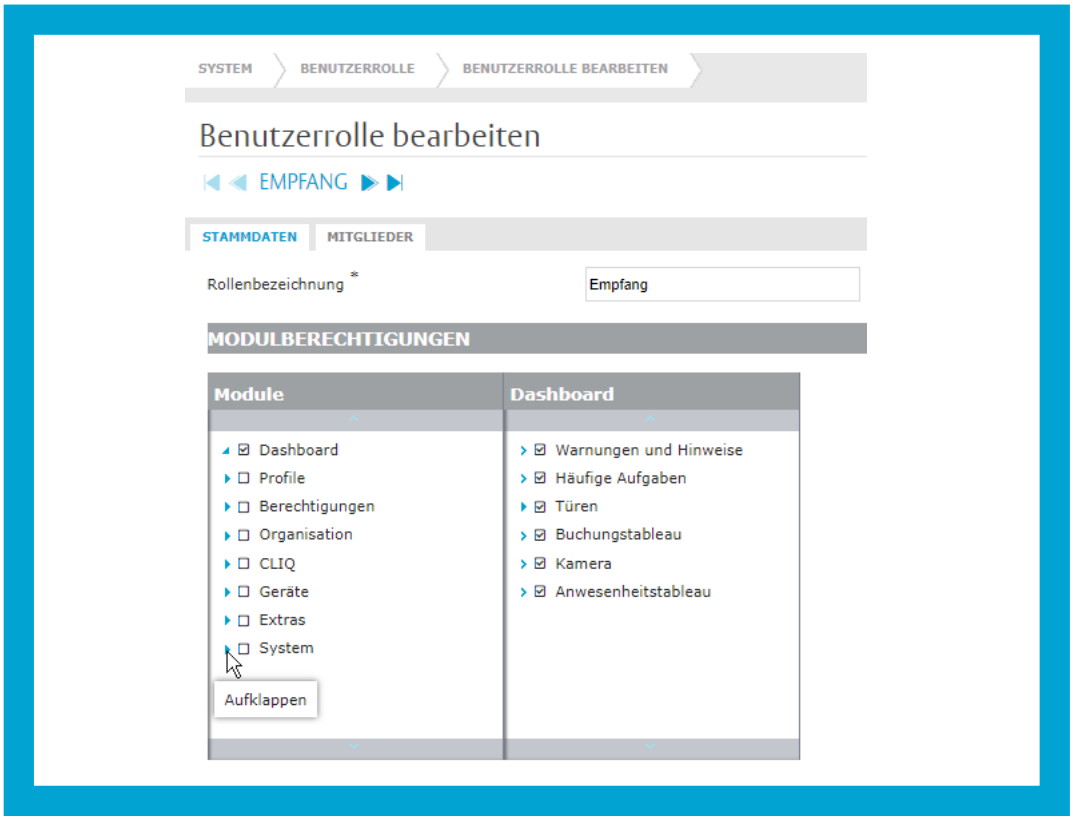


Abb. 20: Benutzerrolle konfigurieren

Dashboard

Das **DASHBOARD** ist eine spezielle Bedienoberfläche mit einer Übersicht und der individuell anpassbaren Schnellzugriffsleiste.

Schnellzugriffe konfigurieren

Einige Menüpunkte lassen sich als Schnellzugriffe festlegen. Die Funktionen sind dann mit einem Klick erreichbar.

1 Klicken Sie auf .

⇨ Eine *Auswahlliste* wird angezeigt.

2 Markieren Sie die Funktionen, die als Schnellzugriff angezeigt werden sollen.

⇨ Sie haben die Schnellzugriffe konfiguriert.

Dashboard konfigurieren

Es können Dashboard-Bereiche auf- und zugeklappt werden.

Beim Beenden wird der Zustand des Dashboards für den angemeldeten Benutzer automatisch gespeichert und beim nächsten Start wird der letzte Zustand des Dashboards wieder hergestellt.

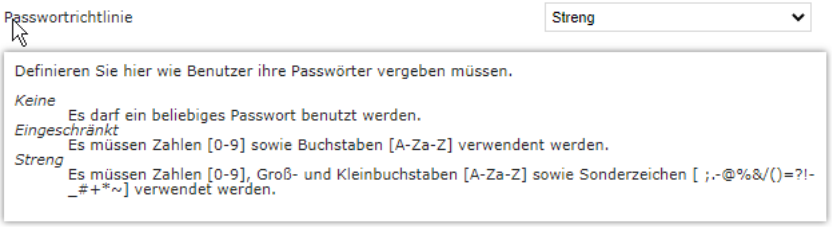
Systemkonfiguration

Über die *Systemkonfiguration* werden grundlegende Parameter zum Verhalten von *SCALA net* festgelegt.

Hinweis!

Nicht alle Optionen werden beschrieben: Im Nachfolgenden werden die Optionen zur Systemkonfiguration erläutert. Dabei werden sich selbsterklärende Optionen oder Optionen, die leicht über die vorhanden Tooltips verstanden werden können hier nicht weiter erklärt.

- Falls Ihnen die Benennung einer Option unklar ist, lesen Sie den vorhanden Tooltip dazu.
  Ein Tooltip wird geöffnet, wenn Sie den Mauszeiger unbewegt auf die Benennung legen.



Das System (SCALA net) konfigurieren

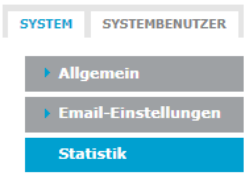
1 Klicken Sie auf **SYSTEM** / **Systemkonfiguration**.

⇨ Der Bereich *Systemkonfiguration* wird angezeigt, bestehend aus mehreren Registern, die wieder in Abschnitte aufgeteilt sind.

2 Konfigurieren Sie die Optionen (Abb. 21ff).
  2.1 Klicken Sie jeweils auf das zu bearbeitende Register.
  2.2 Klicken Sie auf ▸, um den Abschnitt zu wechseln.

3 Klicken Sie auf Speichern.

⇨ Sie haben die Systemkonfiguration geändert.



Systemkonfiguration – System

Tab. 15: Beschreibung zu Abb. 21

Konfigurierbarer Parameter	Beschreibung
Allgemein	
Standard Zeitzone	Festlegen der Standard-Zeitzone „Zeitzone einrichten“, Seite 79
Personalnummer automatisch	Eine Personalnummer im Personalstammsatz automatisch generieren und manuelle Eingabe deaktivieren.
Eigene Feiertage fortschreiben	Die selbstdefinierten Feiertage bei einem Jahreswechsel automatisch fortgeschrieben, zum Beispiel bei einer festen Betriebsruhe zwischen den Jahren).
Sendeaufträge optimieren	Sendeaufträge werden automatisch auf Redundanz geprüft und die Datenmenge vermindert
 *4-Augenprinzip (Ereignisse)* und *automatische Abmeldung [min]*	Zum Einsehen nicht-anonymisierter Ereignisse ist eine zusätzliche Anmeldung einer berechtigten Person notwendig. Die Legitimation durch die zweite Person endet nach Ablauf der vorgegebenen Zeit automatisch
Web-Service-Schnittstelle aktiv	SOAP-Schnittstelle zur Kommunikation mit Fremdsystemen zum Anlegen, Ändern und Löschen von Personen, Personengruppen und Transpondern sowie Ereignisabfragen.
E-Mai-Einstellungen	
mehrere Optionen	Die richtigen Eingaben zu diesen Parametern müssen beim lokal zuständigen Administrator erfragt werden.
Statistik	
Systemstatistik aktiv Aufzeichnungsrate [s] Aufbewahrung [h]	Bei aktivierter Systemüberwachung werden Kennzahlen des Systems in festgelegten Intervallen (*Aufzeichnungsrate*) erfasst, zum Beispiel die CPU-Auslastung und die Speicherauslastung. Nach Ablauf der Aufbewahrungsdauer werden die Daten automatisch gelöscht. Die gesammelten Daten können eingesehen werden über **SYSTEM** / **Systemkonfiguration**. Kann bei einer Fehlersuche hilfreich sein („Systemdiagnose durchführen“, Seite 102)

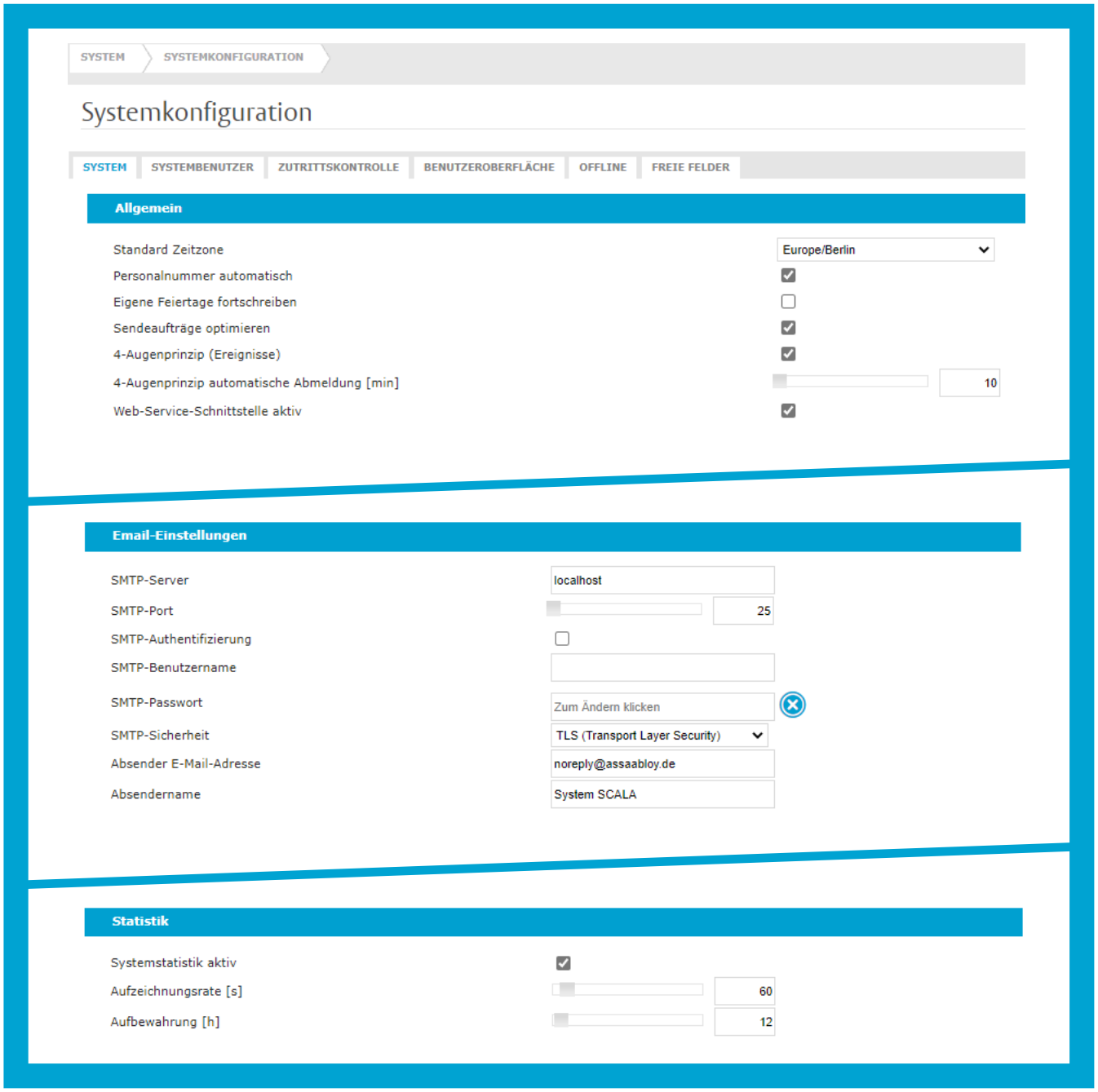


Abb. 21: Darstellung der Optionen im Bereich System / Systemkonfiguration Register System

Systemkonfiguration – Systembenutzer

Tab. 16: Beschreibung zu Abb. 22

Konfigurierbarer Parameter	Beschreibung
Allgemein	
Passwortlänge	Minimale Länge eines Passworts.
Passwortgültigkeit [d]	Nach Ablauf der genannten Zeit in Tagen muss das Passwort geändert werden.
Anzahl Loginversuche	Die maximale Anzahl falscher Passworteingabe. Bei einer weiteren falschen Eingabe wird der Zugang für diesen Benutzer gesperrt. Bei Anzahl 0 sind unbegrenzt viele falsche Eingaben erlaubt.
Passwortrichtlinie	Regeln für den Aufbau Passworts. Die aktuellen Regeln werden ein Tooltip (Mauszeiger halten) angezeigt (–1).

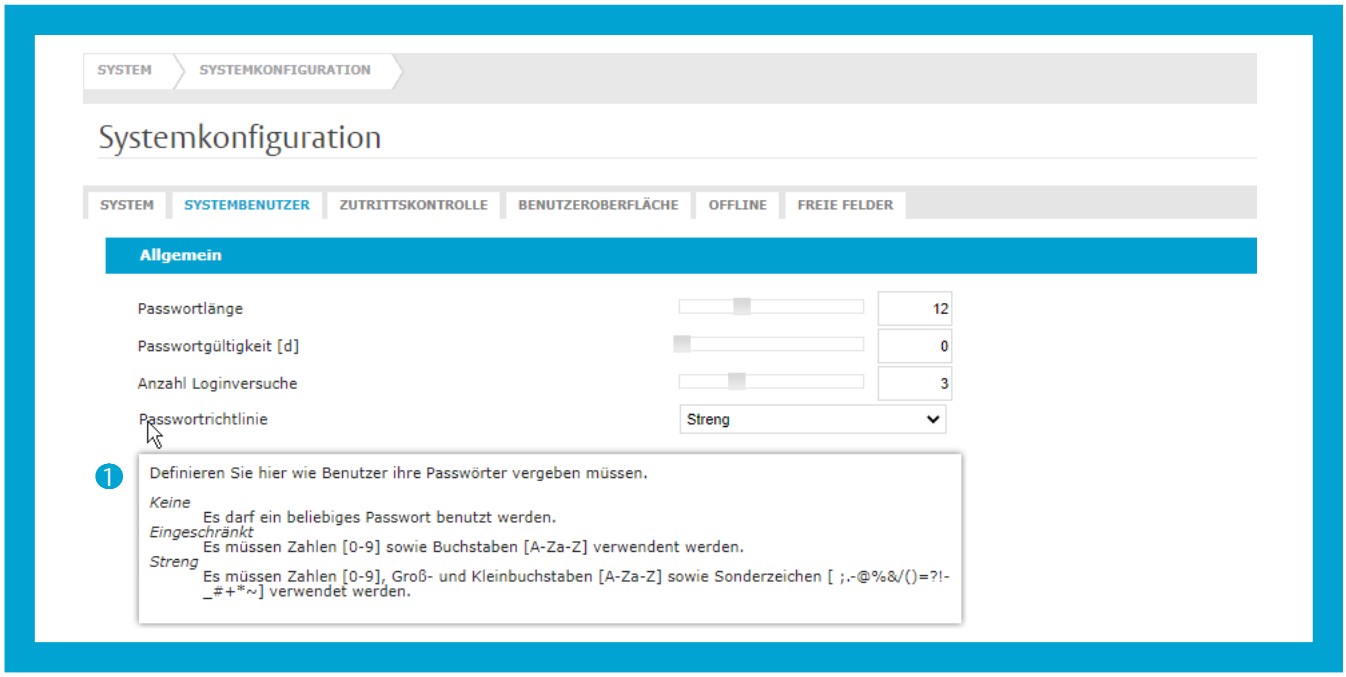


Abb. 22: Darstellung der Optionen im Bereich System / Systemkonfiguration Register Systembenutzer

Systemkonfiguration – Zutrittskontrolle

Tab. 17: Beschreibung zu Abb. 23

Konfigurierbarer Parameter	Beschreibung
Allgemein	
Zutrittsvergabe	Modus zur Vergabe von Zutrittsberechtigungen ein: · *Matrix ohne Zeitmodell*, · *Matrix mit Zeitmodell*
Raumzonen Zutrittspunkt Zuordnung	1 : 1 Zutrittsberechtigung nur am Zutrittspunkt. n : m Zutrittsberechtigung in einer Raumzone. Die Zutrittspunkte sind in Raumzonen gruppiert.
Maximale Buchungsaufbewahrung	Nach Ablauf der Dauer in Tagen werden Buchungen automatisch gelöscht. Bei Anzahl 0 wird nicht gelöscht.
Ablauf von Benutzerkommandos	Über einige Terminals können vom Benutzer Kommandos an das System gesendet werden. Die Gültigkeit eines Kommandos läuft nach der vorgegebenen Dauer ab, zum Beispiel weil ein Kommando wegen einer technischen Störung nicht unmittelbar gesendet werden konnte. Bei Dauer 0 wird diese Einschränkung deaktiviert.
Anzahl Whitelist-Einträge	Die maximale Anzahl an Whitelist-Einträgen.
Transponder	
mehrere Optionen	Je nach verwendetem Transponder müssen hier die passenden Einstellungen vorgenommen werden.
Ausweis lernen	Bei aktivierter Option wird ein bisher unbekannter Transponder in die Datenbank aufgenommen und kann anschießend einer Person zugewiesen werden.
Code	
mehrere Optionen	Einstellmöglichkeiten zur Auswertung von PIN-Codes
Alarmendziffer *Bedrohungscode errechnen* *Alarmendziffer subtrahieren*	Eine PIN-Endziffer, die bei Eingabe einen Alarm auslöst. Bei Vorgabe -1 ist die Funktion deaktiviert. Bei Aktivierung wird die Alarmziffer durch Addition der Alarmziffer berechnet. Bei zusätzlicher Aktivierung wird die Alarmziffer durch Subtraktion der Alarmziffer berechnet.

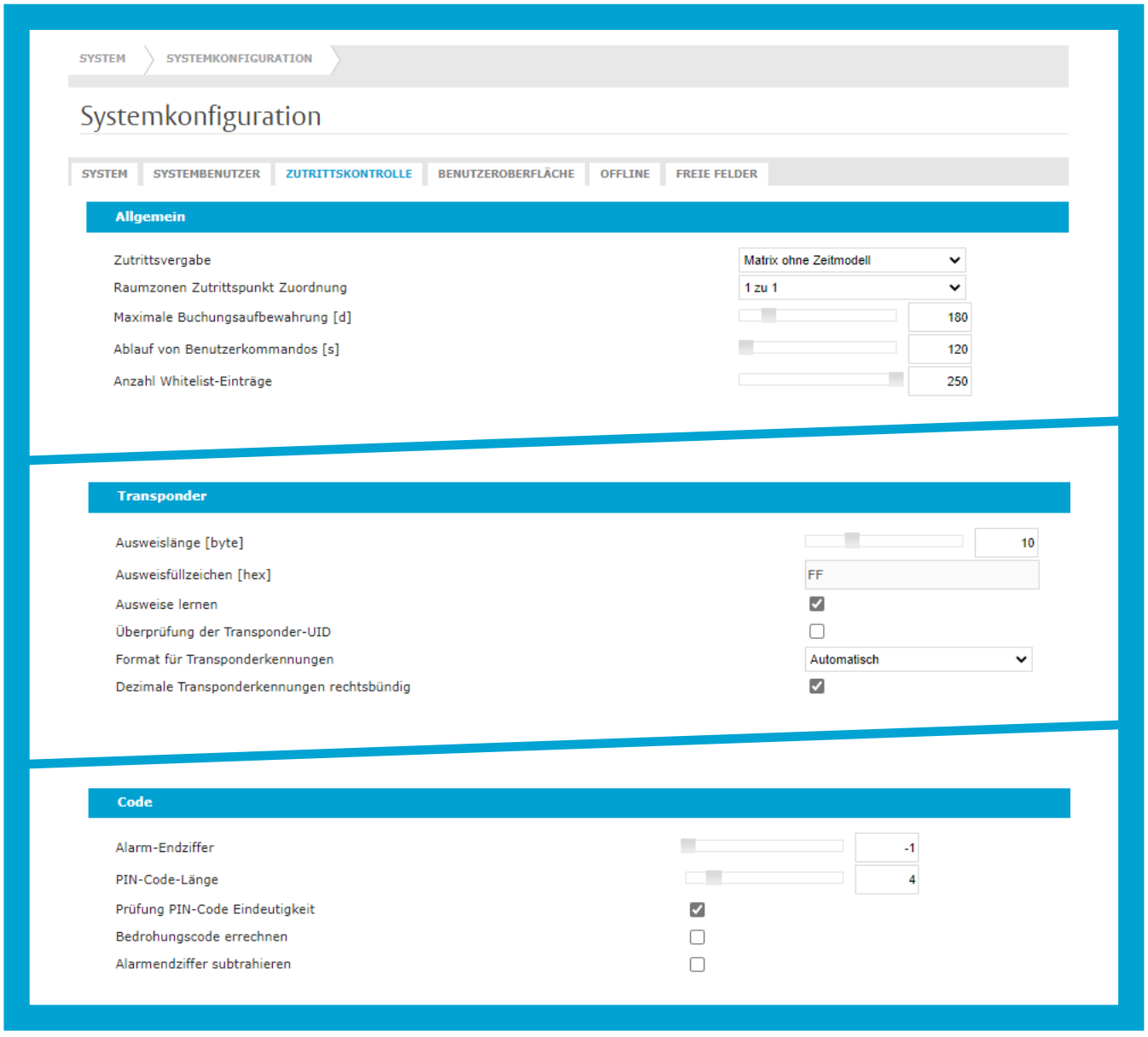


Abb. 23: Darstellung der Optionen im Bereich System / Systemkonfiguration Register Zutrittskontrolle

Systemkonfiguration – Benutzeroberfläche

Die werkseitigen Einstellungen sind für die meisten Benutzer gut geeignet. Es ist aber möglich das Verhalten der Benutzeroberfläche an individuelle Bedürfnisse anzupassen. Für Personen mit körperlichen Einschränkungen kann es sinnvoll sein, die Zeiten bis zum Ausblenden von zum Beispiel Dialogen und Fehlermeldungen zu verlängern.

Tab. 18: Beschreibung zu Abb. 24

Konfigurierbarer Parameter	Beschreibung
Allgemein	
mehrere Optionen	Vorgabe von Zeiten, bis Info-Dialoge, Warndialoge und Fehlerdialoge ausgeblendet werden. Die Dialoge werden ohne Bestätigung durch den Benutzer geschlossen. Bei Dauer 0 wird der jeweilige Dialogtyp nur nach Bestätigung durch den Benutzer geschlossen..
Inhaltsbeschränkungen aufheben	Erlaubt dem Browser unbeschränkt Inhalte zu laden. (siehe nachfolgenden Warnhinweis).

Achtung!

Inhaltsbeschränkungen nicht dauerhaft aufheben: Die Option *Inhaltsbeschränkungen aufheben* sollte nicht dauerhaft aktiviert bleiben, da sie eine Sicherheitslücke öffnet.

- Deaktivieren Sie diese Option, sobald sie nicht mehr aktiv benötigt wird.

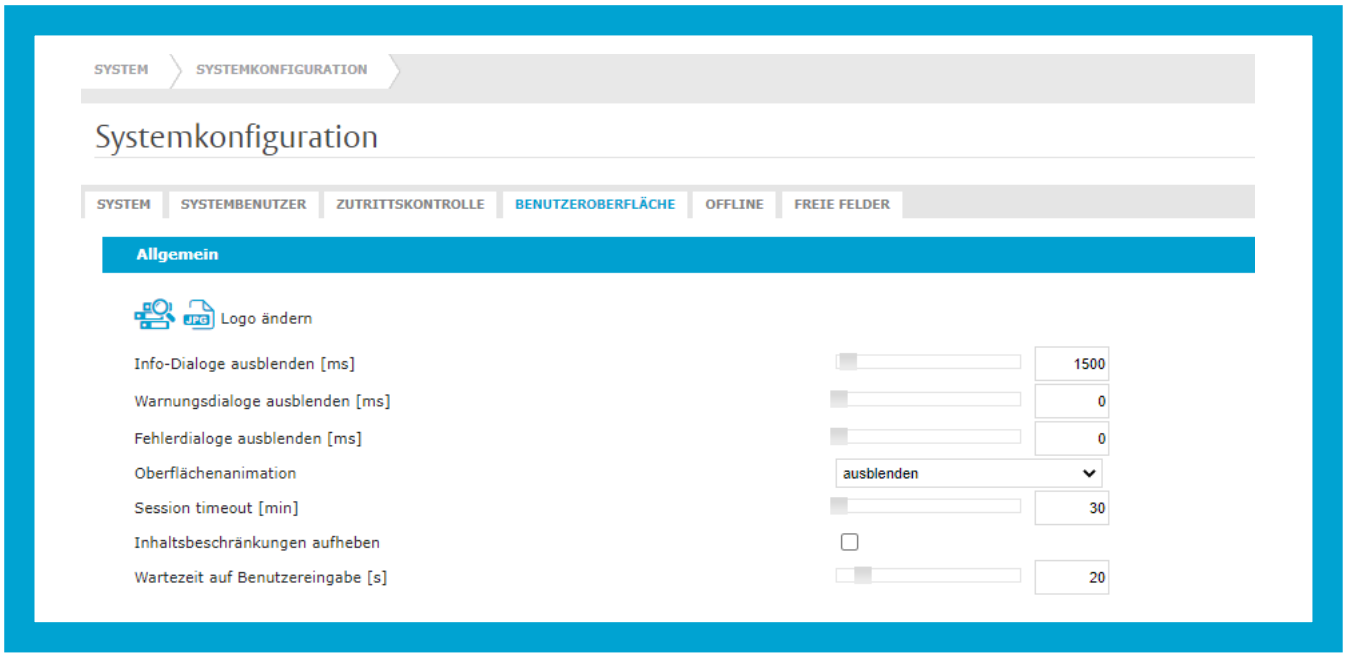


Abb. 24: Darstellung der Optionen im Bereich System / Systemkonfiguration Register Benutzeroberfläche

Systemkonfiguration – Offline

Offline-Türen

Offline-Türen haben keine Verbindung über Draht oder Funk zu *SCALA net*. Offline-Türen werden zentral verwaltet und anschließend werden die geänderten Daten über dazu vorbereitete Parameterkarten an die Offline-Türen übertragen und auch von dort gelesen. Eine Kommunikation in Echtzeit ist nicht möglich. (Kapitel I - Online- und Offline-System)

Für die Definition der Datenstruktur unterstützt *SCALA net* zwei alternative Standards, die sich gegenseitig ausschließen:

- OSS-SO *Open Securtiy Standards - Standard Offline* der OSS-Association e.V.® oder
- *DoC* *Data on Card* der ASSA ABLOY Gruppe

Tab. 19: Beschreibung zu Abb. 25

Konfigurierbarer Parameter	Beschreibung
DoC	
DoC Offline-System	Aktiviert das Data on Card Offline System
OSO Offline	
OSO Offline-System	Aktiviert das *OSS Offline-System*

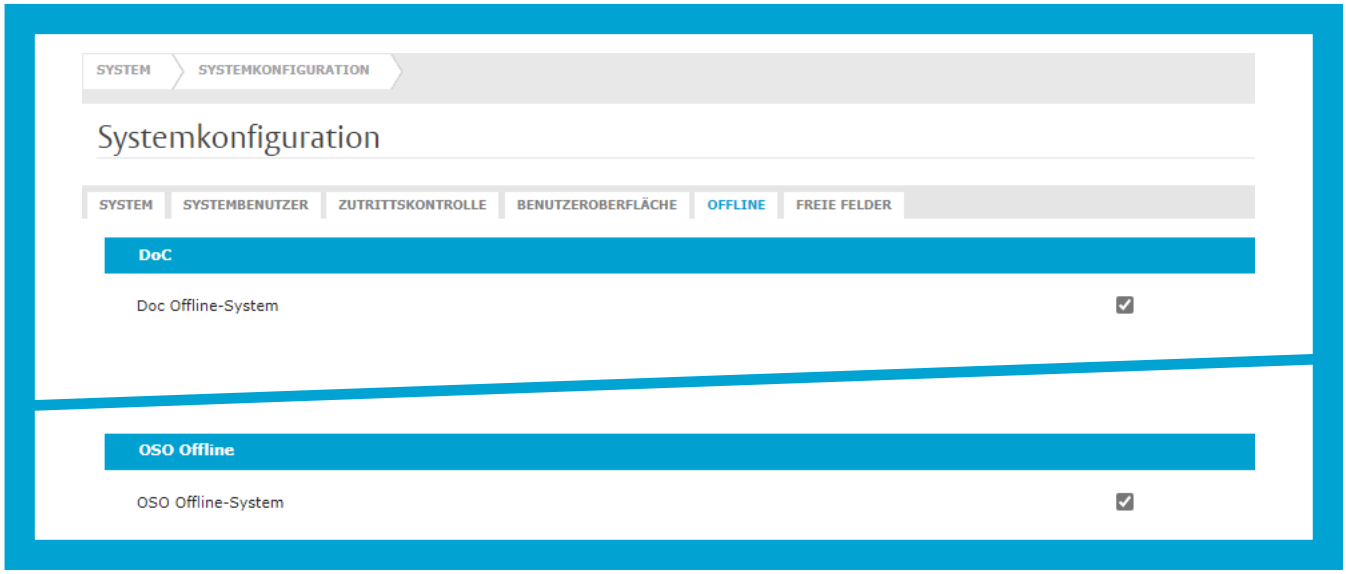


Abb. 25: Darstellung der Optionen im Bereich System / Systemkonfiguration Register Systembenutzer

Systemkonfiguration – Freie Felder

Freie Felder bieten die Möglichkeit über Freitext weitere Eigenschaften zur Definition von Benutzern hinzuzufügen, zum Beispiel zur Verwendung als individuelle Suchkriterien:

Tab. 20: Beschreibung zu Abb. 26

Konfigurierbarer Parameter	Beschreibung
Textfelder Datumsfelder Optionsfelder	Aktivieren Sie diese Option und geben Sie einen Bezeichner an, der als Beschriftung des freien Feldes angezeigt wird. Falls *In Suche anzeigen* aktiviert ist, kann das Feld auch in Suchmasken verwendet werden.
Auswahlfelder	Bei Auswahlfeldern muss die Auswahlliste zusätzlich definiert werden.

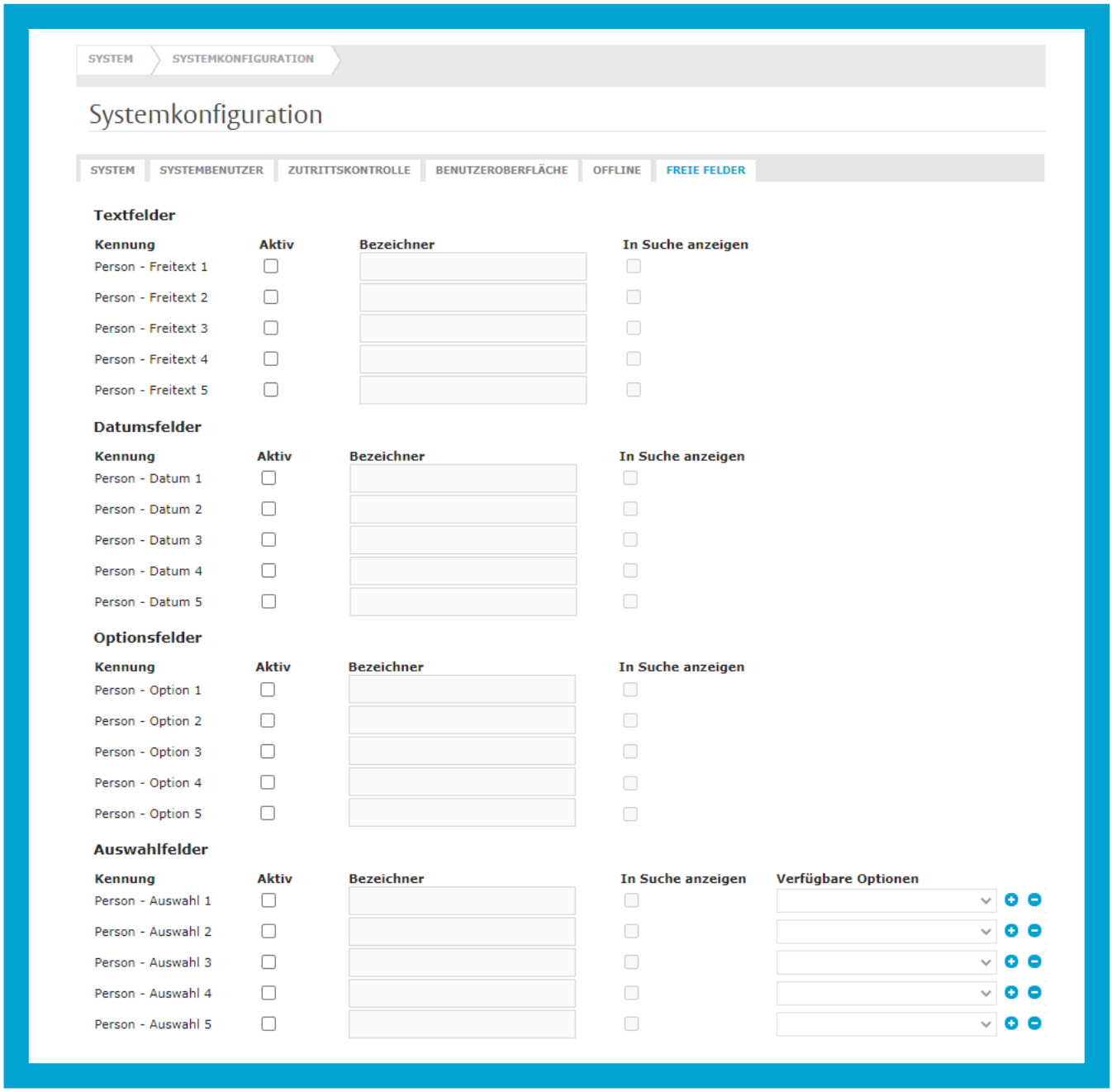


Abb. 26: Darstellung der Optionen im Bereich System / Systemkonfiguration Register Freie Felder

Transponder

Damit *SCALA net* mit den Transpondern kommunizieren kann, muss ein Transpondertyp vorgegeben werden.

Einen Transpondertypen festlegen

1 Klicken Sie auf **SYSTEM** / **Transponder**.

⇨ Die Transponder-Liste wird angezeigt.

2 Klicken Sie auf Erfassen.

3 Wählen Sie einen der angezeigten Transpondertypen aus.

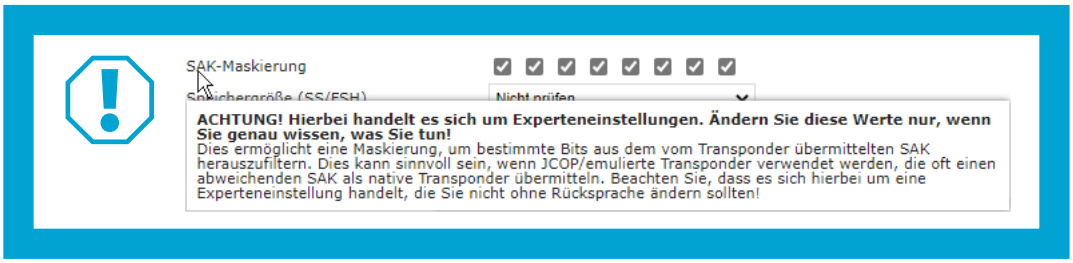
⇨ Das Fenster < *ausgewählter Transpondertyp* > *Transponder erfassen* wird angezeigt (Abb. 28).

Achtung!

Werkseitig vorgegebene Expertenkonfiguration: Mehrere der konfigurierbaren Parameter sind werkseitig vordefiniert (Abb. 27).

- Informieren Sie sich sorgfältig, bevor Sie Transpondertypen konfigurieren.
- Erstellen Sie zur Sicherheit ein Backup des aktuellen Systems, bevor Sie Änderungen vornehmen („Backup / Datensicherung“, Seite 71).

Abb. 27: Konfigurieren der Transpondertypen erfordert Expertenwissen



Tab. 21: Beschreibung zu Abb. 28

Konfigurierbarer Parameter	Beschreibung
mehrere Optionen	Werkseitig vorgegebene Expertenkonfiguration, siehe Tooltip im Einzelfall (Abb. 27).
Bezeichnung	Individuelle Benennung des Transponders
Transpondertyp	*Transpondertyp* festlegen, der nachträglich nicht mehr verändert werden kann.

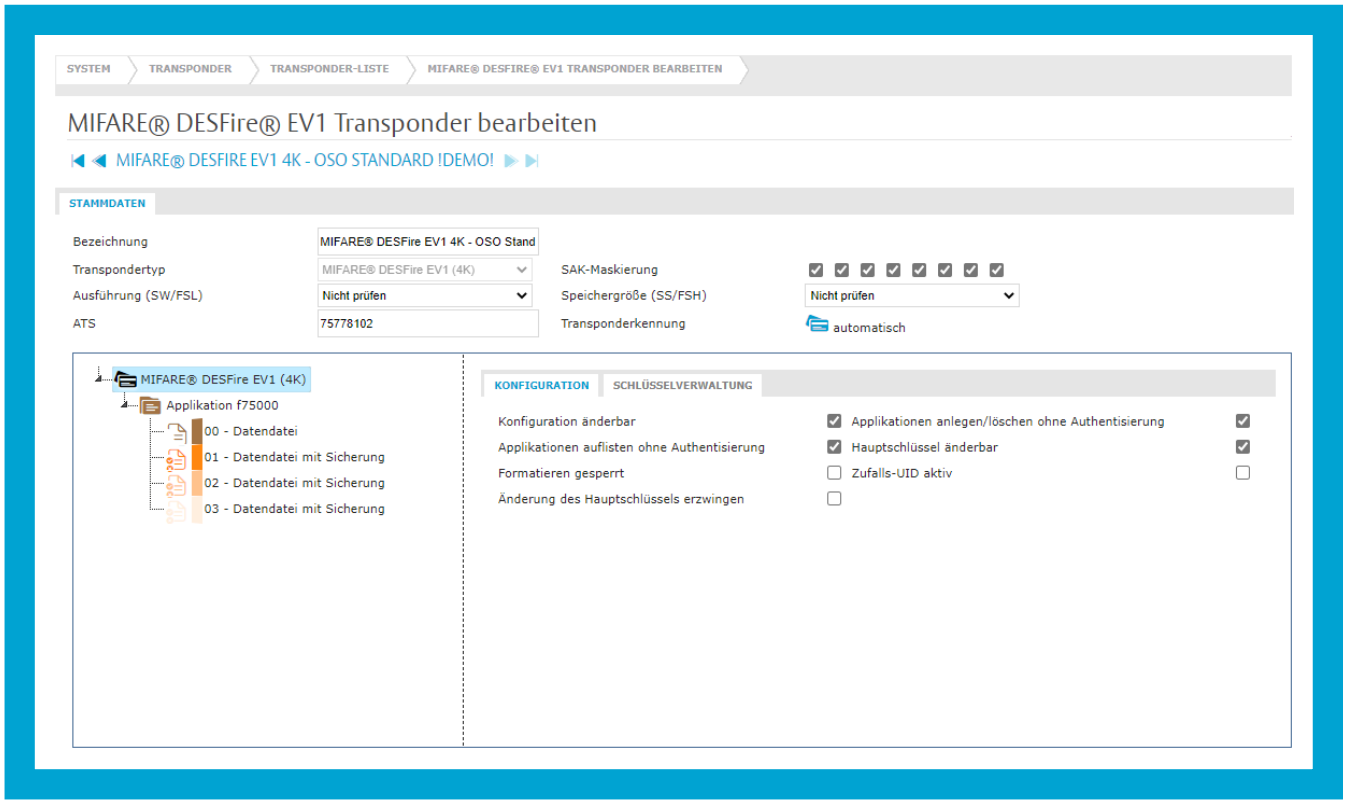


Abb. 28: Transpondertypen konfigurieren

Zeitaufträge

Routine-Aufgaben können per Zeitauftrag automatisiert werden, zum Beispiel den Feiertagskalender automatisch fortschreiben.

Einen Zeitauftrag konfigurieren

1 Klicken Sie auf **SYSTEM** / **Zeitauftrag**.

⇨ Die Zeitauftragsliste wird angezeigt.

2 Klicken Sie auf Erfassen.

⇨ Die Eingabemaske *Zeitauftrag erfassen* wird angezeigt (Abb. 29).

3 Definieren Sie den neuen Zeitauftrag.

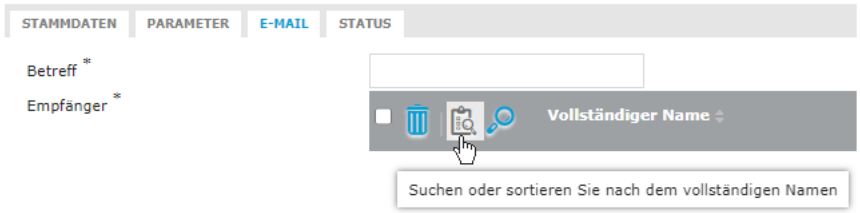
3.1 Damit der Zeitauftrag wirksam wird, muss folgendes angegeben werden:
- eine Benennung (Abb. 29 –1),
- ein Zeitauftragstyp (–2)
- eine Ausführungszeit incl. Wiederholungsintervall oder ein Wochentag (–3),

4 Klicken Sie auf Speichern.

⇨ Sie haben Sie haben einen Zeitauftrag angelegt.

⇨ Es werden nun weitere Register angezeigt.

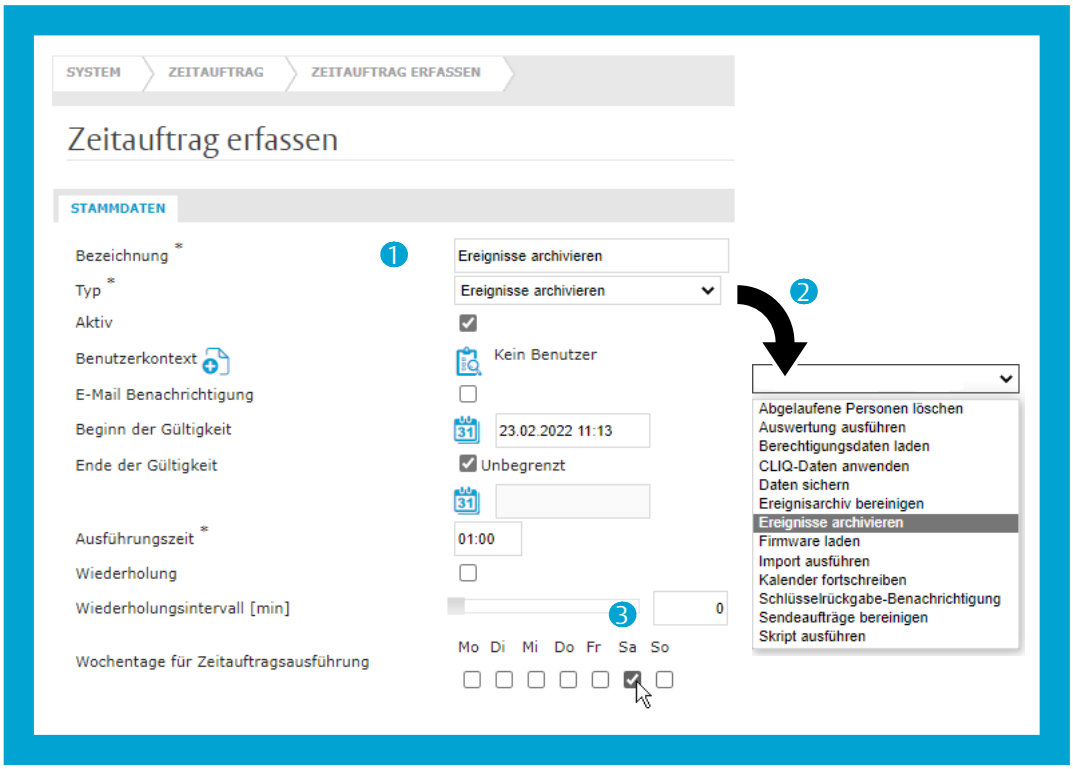
5 Legen Sie weitere Details zum Zeitauftrag fest.
Zum Beispiel E-Mail-Empfänger falls E-Mail-Benachrichtigung aktiviert wurde.



6 Klicken Sie auf Speichern.

⇨ Der Zeitauftrag ist sofort wirksam.

Abb. 29:
Einen Zeitauftrag konfigurieren



Verschlüsselung der Datenübertragung

Die Kommunikation über den RS485-Bus kann verschlüsselt erfolgen. Empfohlen wird eine Verschlüsselung für Bus-Teilnehmer, die eine Schließhardware ansteuern, um zum Beispiel eine Tür freizugeben.

Die Verschlüsselung wird von *SCALA net* kontrolliert (Abb. 30). Die Verschlüsselungscodes (Code-Schlüssel) werden in SCALA net verwaltet und nach dem Top-Down-Prinzip an die Komponenten verteilt. Dabei wird die unverschlüsselte Komponenten-UID zur eindeutigen Zuordnung verwendet. Jede Komponente kann einen individuellen Schlüssel verwenden. Falls im Einzelfall eine Komponente manipuliert werden konnte, bleiben die anderen sicher.

Controller ab Firmware 9.6.1
Angeschlossene Komponenten ab Firmware 9.5.1

Folgende Komponenten unterstützen die verschlüsselte Kommunikation über den RS485-Bus:

- SCALA Controller — ab Firmware 9.6.1
- SCALA Türmodul,
- SCALA 8fach-Relaismodul,
- SCALA 8fach-Eingangsmodul,
- SCALA MIFARE-Leser;
- SCALA Bluetooth-Modul V4

— ab Firmware 9.5.1

Hinweis!

Die Verschlüsselung ist controllerspezifisch: Nach Aktivierung der Verschlüsselung können die Komponenten nicht mehr an einem anderen Controller oder in einer anderen Anlage verwendet werden. Deshalb muss Folgendes beachtet werden:

- Die Verschlüsselung muss deaktiviert werden, bevor eine Komponente oder der Controller ausgetauscht wird oder an den Support geschickt wird.
- Installationsarbeiten erfolgen im Normalfall bei unverschlüsselter Kommunikation.
- Die Verschlüsselung wird erst nach dem vollständigen Abschluss von Installationsarbeiten eingeschaltet.

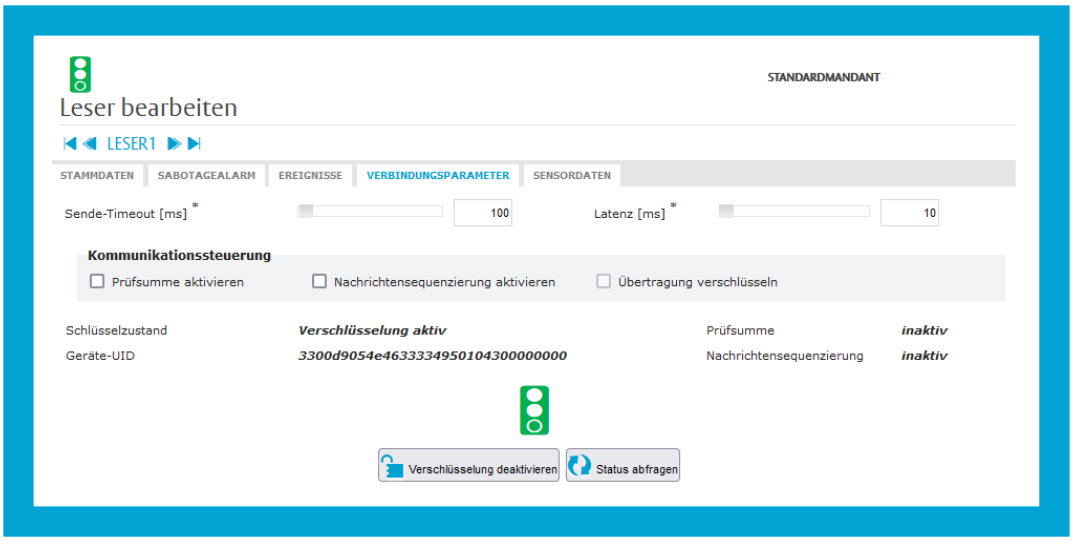


Abb. 30: Verschlüsselung

Beispiel Leser: Verschlüsselung aktivieren / deaktivieren

1 Klicken Sie auf **GERÄTE** / **LESER** .

⇨ In der *Leserliste* werden die angelegten Lesern angezeigt.

2 Wählen Sie den Leser, dessen Kommunikation verschlüsselt werden soll.

3 Klicken Sie auf **VERBINDUNGSPARAMETER** .

4 Klicken Sie auf Verschlüsselung aktivieren bzw. auf Verschlüsselung deaktivieren .

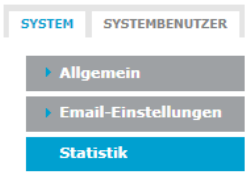
⇨ Die Kommunikation mit der Komponente wird nun verschlüsselt bzw. nicht mehr verschlüsselt.

Problem – Ursache – Lösung

Sollte *SCALA net* nicht wie erwartet funktionieren, sollten folgende Maßnahmen durchgeführt werden, bevor der Support von *ASSA ABLOY* kontaktiert wird.

Systemdiagnose durchführen

1 Aktivieren Sie die Systemstatistik, für eine Systemdiagnose.
- 1.1 Klicken Sie auf **SYSTEM** / **Systemkonfiguration**.
- ⇨ Der Bereich *Systemkonfiguration* wird angezeigt.
- 1.2 Klicken Sie auf STAMMDATEN.
- 1.3 Klicken Sie auf ▸, um den Abschnitt **Statistik** zu öffnen.
- 1.4 Schalten Sie die *Systemstatistik* aktiv



2 Klicken Sie auf Speichern.

⇨ Sie haben die Systemstatistik für eine spätere Systemdiagnose aktiviert.

3 Arbeiten Sie einige Zeit mit *SCALA net*, um Daten zu sammeln.

4 Klicken Sie auf **SYSTEM** / **Systemdiagnose**.

⇨ Der Bereich *Systemdiagnose* wird angezeigt (Abb. 31).

⇨ Prüfen Sie die statistischen Daten, die auf mehren Registern zusammengefasst sind.

5 Falls gefunden, beseitigen Sie die Fehlerursache.

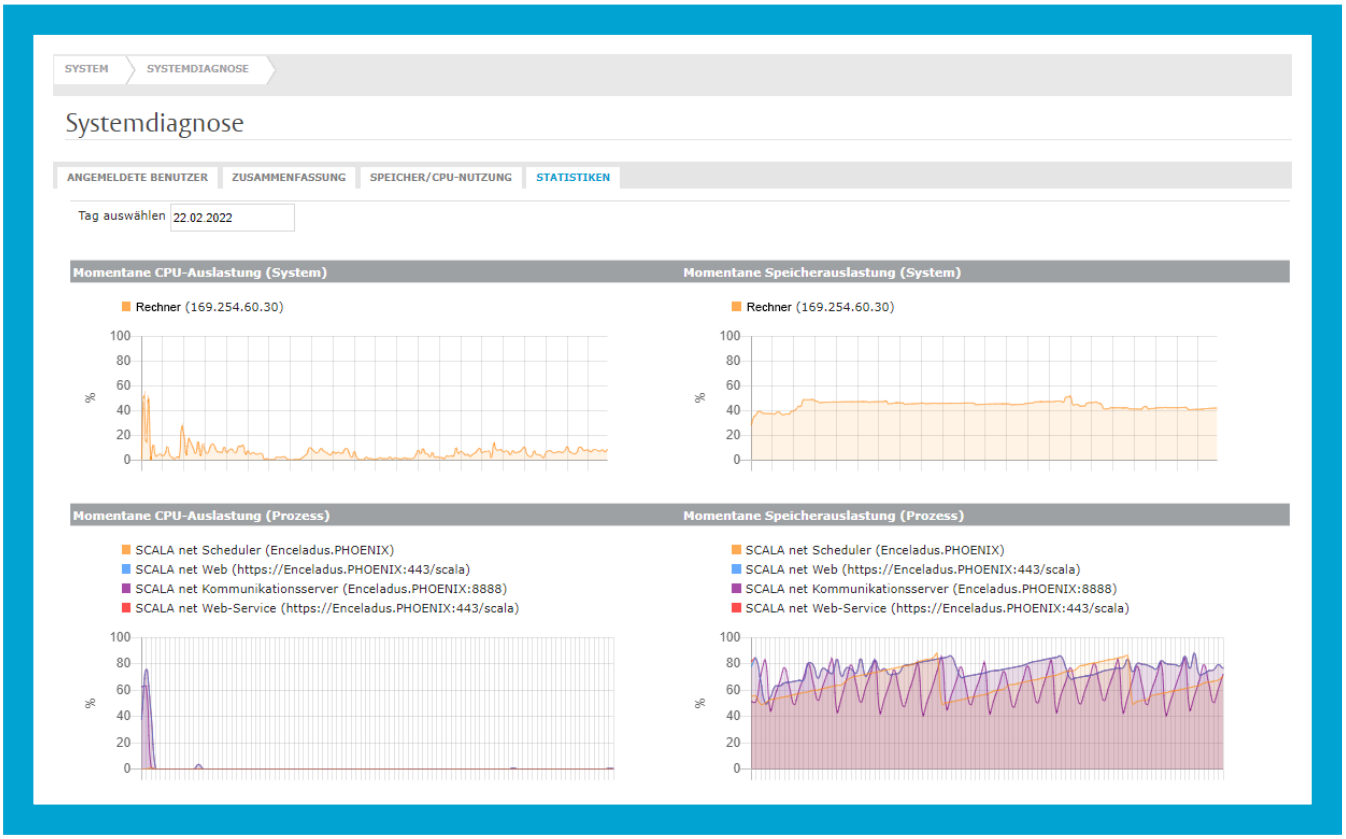


Abb. 31: Darstellung statistischer Daten in der Systemdiagnose

VI – Bedienung / Arbeiten mit SCALA net

Dieses Kapitel beschreibt die Bedienung anhand von Beispielen.

Planung

Schon bei kleinen Gebäudekomplexen sollte im voraus geplant werden, um zu verhindern, dass das Zutrittskontrollsystem zweimal angelegt werden muss. Je größer der zu verwaltende Gebäudekomplex und je komplizierter die Organisation, der sich darin bewegenden Menschen, Firmen, Gruppen, Fahrzeugen usw., desto aufwändiger ist eine spätere Umstrukturierung des Zutrittskontrollsystems. Eine sorgfältige Planung ist also notwendig.

Gruppen und Orga-Einheiten

Gruppen und Orga-Einheiten fassen bestimmte Personengruppen organisatiorisch zusammen.

So können Zutrittsberechtigungen durch Zuordnen von Personen zu Gruppen bzw. zu Orga-Einheiten organisiert nach vorgegebener Struktur und Hierarchie erteilt werden.

Gruppen und Orga-Einheiten erfassen

1 Klicken Sie auf **ORGANISATION** und dann auf **Gruppen/Orga-Einheiten**.
2 Wählen Sie im Vorauswahl-Fenster *Gruppe*.
3 Klicken Sie auf **GRUPPENMITGLIEDER**.

⇨ Bearbeiten Sie eine Gruppe, indem Sie Personen zur Gruppe hinzufügen oder entfernen

Zutrittsberechtigung erteilen

Sie können hier jedem aufgeführten Offline-Zutrittspunkt nur ein Zeitmodell zuordnen und damit der Gruppe an den gewählten Zutrittspunkten nur eine ALWAYS Zutrittsberechtigung erteilen.

Mehrfache Zuordnung von Zeitmodellen

Eine Mehrfach-Zuordnung von Zeitmodellen muss individuell **Personen** durchgeführt werden.

Darstellung von Zutrittspunkten

Zutrittspunkte werden in der Spalte *Berechtigungen* mit einem Kontrollkästchen dargestellt.

24-Stunden-Zutrittsberechtigung

Bei einer 24-Stunden-Zutrittsberechtigung verwendet *SCALA net* das *ALWAYS* Zeitmodell, welches standardmäßig 24 Stunden Zutritt gewährt.

Personen

Grundsätzlich können Sie jeder Person individuelle Zutrittsrechte, Ausweise und Gruppenmitgliedschaften sowie Organisationseinheiten zuordnen.

Es werden folgende Elemente erfasst und verwaltet:
- Adress-, Kontakt- und Gültigkeitsdaten (Stammdaten)
- Berechtigungen
- Identifizierungsmerkmale wie PIN-Code und Transponder
- Ereignisse
- Dokumente
- Gruppenmitgliedschaften
- spezielle Offline Funktionen aktivieren
- Blacklist

Personen können über das Menü **PROFILE** / **Personen** erfasst werden, alternativ auch über eine Zutrittsmatrix unter **BERECHTIGUNGEN** oder über den Excel®-Import.

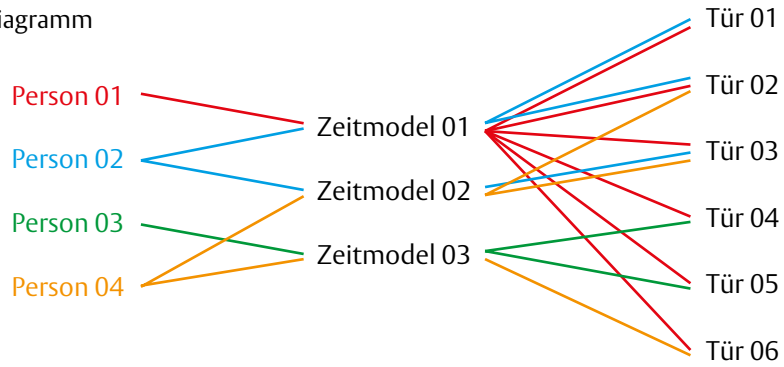
Die Zutrittsberechtigungen (Berechtigungen) werden in einer Matrix zugewiesen (Abb. 32). In den Zeilenköpfen sind die Personen aufgelistet, in den Spaltenköpfen sind die Türen aufgelistet, im Kreuzungspunkt von Zeile und Spalte werden die Berechtigungen über Zeitmodelle zugewiesen.

Arbeitsreihenfolge

Daraus ergibt sich eine Arbeitsreihenfolge: Bevor Berechtigungen an Personen zugewiesen werden können, müssen Türen und Zeitmodelle angelegt sein.

Abb. 32: Verknüpfung von Personen und Türen über Zeitmodelle

Liniendiagramm



Matrix-Darstellung in SCALA net

	Tür 01	Tür 02	Tür 03	Tür 04	Tür 05	Tür 06
Person 01	Zeitmdl. 01	Zeitmdl. 01	Zeitmdl. 01	Zeitmdl. 01	Zeitmdl. 01	Zeitmdl. 01
Person 02	Zeitmdl. 01	Zeitmdl. 01	Zeitmdl. 02	–	–	–
Person 03	–	–	–	Zeitmdl. 03	Zeitmdl. 03	–
Person 04	–	Zeitmdl. 02	Zeitmdl. 02	–	–	Zeitmdl. 03

Person erfassen

Hinweis!

Pflichtfelder: Der Nachname, die Personalnummer sowie Beginn und Ende der Gültigkeit sind Pflichtangaben.
Personalnummer: Die Personalnummer kann von *SCALA net* automatisch vergeben werden. Dies wird unter **SYSTEM** **Systemkonfiguration** festgelegt.

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.
⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.
1.1 Falls nicht, klicken Sie auf Suche.
2 Klicken Sie auf Erfassen.
⇨ Die Eingabemaske **PERSON ERFASSEN** wir angezeigt
3 Geben Sie die Daten zur Person ein
4 Klicken Sie auf Speichern.
⇨ Sie haben eine Person erfasst.

Person löschen

Hinweis!

Löschen bei Buchungen nicht möglich: Eine Person kann nicht gelöscht werden, wenn Buchungen zur Person vorliegen, zum Beispiel, der zugeordnete Ausweis wurde an einem Leser erfasst.

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.
⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.
1.1 Falls nicht, klicken Sie auf Suche.
2 Klicken Sie in der Personenliste auf die zu löschende Person.
3 Klicken Sie auf Löschen.
⇨ Sie haben eine Person gelöscht.

Person sperren / entsperren

Personen können jederzeit gesperrt und entsperrt werden. Wird eine Person gesperrt, hat dies folgende Auswirkungen:

- Der Person werden alle Berechtigungen entzogen.
- Die zugeordneten Ausweise bleiben gültig, werden jedoch bei einem Buchungsversuch ignoriert.

weiterhin gültige Ausweise werden ignoriert

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.
⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.
1.1 Falls nicht, klicken Sie auf Suche.
2 Klicken Sie in der Personenliste auf die zu sperrende Person.
3 Setzen Sie die Checkbox *Gesperrt*.
⇨ Sie haben eine Person gesperrt / entsperrt.

Berechtigungen

Nachdem eine Person erfasst wurde, können Berechtigungen festgelegt werden. Dazu werden der Person Türen und Zeitmodelle zugewiesen. Durch die Verknüpfung einer Person mit einer Tür über ein Zeitmodell erhält die Person Zutrittsberechtigungen

Berechtigungen zuweisen / entziehen

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie in der Personenliste auf die zu bearbeitende Person.

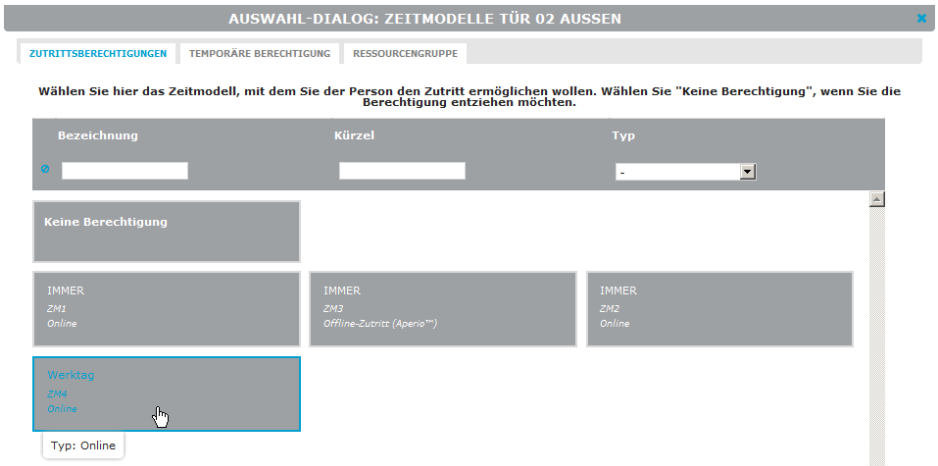
3 Klicken Sie auf BERECHTIGUNGEN.

⇨ Es wird eine Tabelle angezeigt. In den Spaltenköpfen werden die Türen aufgelistet, für die Zutrittsberechtigungen festgelegt werden können. Die Verbindung von Person und Tür erfolgt über die Zuweisung eines Zeitmodells.

4 Klicken Sie im Kontextmenü (Rechtsklick) zu einer Tür auf Zutrittsberechtigung ändern.

5 Weisen Sie der Person und Tür ein Zeitmodell zu.

- Klicken Sie auf ein Zeitmodell, um Zutrittsberechtigungen zuzuweisen.
- Klicken Sie auf Keine Berechtigung, um Zutrittsberechtigungen zu entziehen.



6 Klicken Sie auf OK.

7 Klicken Sie auf Speichern.

⇨ Sie haben eine Person und eine Tür über ein Zeitmodell verknüpft. Die Person hat nun Zutrittsberechtigungen für die Tür, zu den im Zeitmodell definierten Zeiten.

Bereits bestehende Berechtigungen auf Personen übertragen

Bestehende Berechtigungen, Gruppenmitgliedschaften und die OSO-Einstellungen (oder DoC) einer Person können auf ein andere Person übertragen werden, zum Beispiel beim Neuanlegen von Personen.

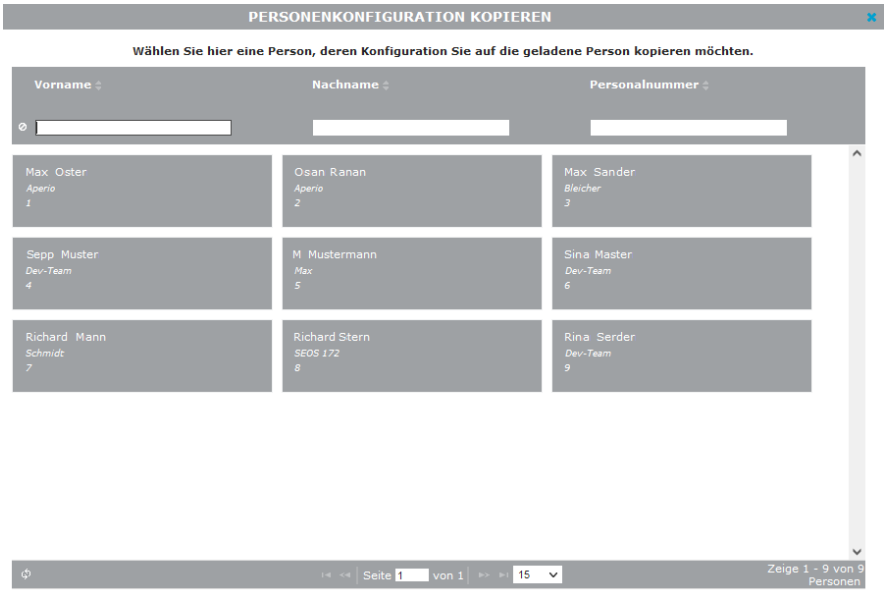
1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie auf Kopieren.

3 Klicken Sie in der Personenliste auf die Person, der sie bestehende Berechtigungen zuordnen wollen.



4 Wählen Sie die Person, deren Berechtigungen, Gruppenmitgliedschaften und OSO-Einstellungen (oder DoC) kopiert werden sollen.

⇨ Die Berechtigungen, Gruppenmitgliedschaften und OSO-Einstellungen (oder DoC) werden übertragen.

Gruppenmitgliedschaften

Über *Gruppenmitgliedschaften* werden einzelne Personen Organisationseinheiten und Gruppen zugeordnet, zum Beispiel der Organisationseinheit *Abteilung* (Abb. 33).

Wenn mehreren Personen organisatorisch ein einheitliches Zutrittsrecht an Türen gewährt werden kann, so ist es sinnvoll, diese Personen zu Organisationseinheiten oder Gruppen zusammenzufassen. Alle Berechtigungen, die für Organisationseinheiten oder Gruppen definiert sind, gelten automatisch für die zugehörigen Person.

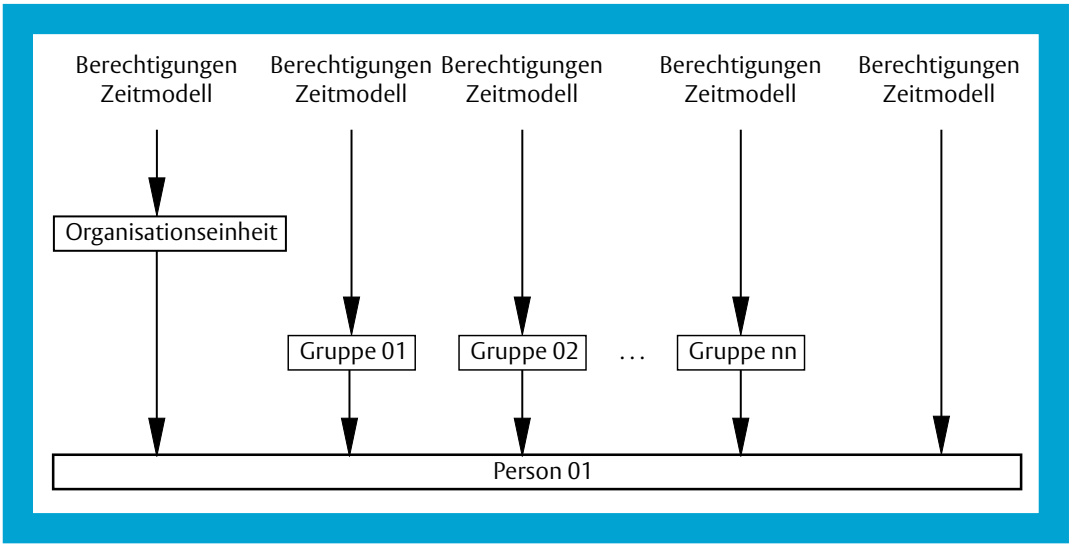
Eine Person kann nur maximal einer Organisationseinheit, aber mehreren Gruppen zugewiesen sein. Eine Person kann auch Gruppen zugewiesen werden, ohne zu einer Organisationseinheit zu gehören.

Organisationseinheiten oder Gruppen können direkt in den Personendaten über die GRUPPENMITGLIEDSCHAFTEN erstellt werden.

Berechtigungen, die eine Person über die Organisationseinheiten oder über Gruppen erhalten hat, sind in der individuellen Matrix zur Person unter BERECHTIGUNGEN sichtbar, können aber dort nicht verändert werden.

Die Bearbeitung von Personendaten bzgl. Organisationseinheiten und Gruppen ist weitgehend gleich. Im Nachfolgenden ist das Hinzufügen von Personen zu einer Organisationseinheit, das Erstellen einer Organisationseinheit über *Person bearbeiten* und das Entfernen einer Personen aus einer Organisationseinheit beschrieben und gilt analog für das Arbeiten mit Gruppen.

Abb. 33: Berechtigungen über Gruppen organisieren



Person(en) einer Organisationseinheit hinzufügen

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie in der Personenliste auf die Person, die aus einer Organisationseinheit entfernt werden soll.

3 Klicken Sie auf GRUPPENMITGLIEDSCHAFTEN.

⇨ Es werden die Organisationseinheit und die Gruppen angezeigt.

Voraussetzung für die weitere Bearbeitung

Voraussetzung für die weitere Bearbeitung:
Die Person wurde noch keiner Organisationseinheit zugewiesen.

4 Klicken Sie auf .

Personen hinzufügen

5 Fügen Sie Personen der Organisationseinheit hinzu.
Sie können mehrere Personen markieren (Shift- und Strg-Taste drücken) um diese gleichzeitig hinzuzufügen.

6 Klicken Sie auf Speichern.

⇨ Sie habe eine oder mehrere Personen einer Organisationseinheit zugewiesen.

⇨ Die Personen übernehmen dadurch alle Berechtigungen der Organisationseinheit zusätzlich.

Eine Person aus einer Organisationseinheit entfernen

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie in der Personenliste auf die Person, die aus einer Organisationseinheit entfernt werden soll.

3 Klicken Sie auf GRUPPENMITGLIEDSCHAFTEN.

⇨ Es werden die Organisationseinheit und die Gruppen angezeigt.

4 Klicken Sie auf .

Personen entfernen

5 Wählen Sie *Keine Organisationseinheit* um die Person aus der Organisationseinheit zu entfernen.

6 Klicken Sie auf Speichern.

⇨ Sie haben eine Person aus einer Organisationseinheit entfernt.

⇨ Die Person verliert dadurch alle Berechtigungen, die sie ausschließlich über die Organisationseinheit erhalten hatte.

Organisationseinheit erstellen und einer Person zuweisen

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie in der Personenliste auf die Person, die einer neu zu erstellenden Organisationseinheit zugewiesen werden soll.

3 Klicken Sie auf GRUPPENMITGLIEDSCHAFTEN.

⇨ Es werden die Organisationseinheit und die Gruppen angezeigt.

Voraussetzung für die weitere Bearbeitung

Voraussetzung für die weitere Bearbeitung:
Die Person wurde noch keiner Organisationseinheit zugewiesen.

4 Klicken Sie auf  .

⇨ Die Eingabemaske *Organisationseinheiten erfassen* wird angezeigt. Diese kann auch über **ORGANISATION** / **Gruppen / Orga-Einheiten** und Erfassen geöffnet werden.

Organisationseinheit anlegen

5 Definieren Sie die Organisationseinheit.

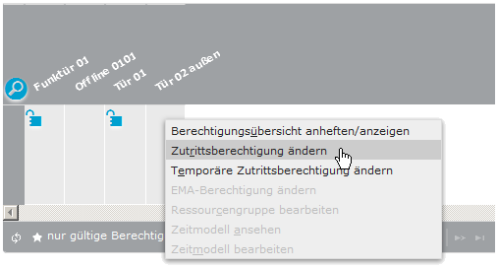
6 Klicken Sie auf Speichern.

⇨ Die Eingabemaske *Organisationseinheiten* hat die Registerkarte BERECHTIGUNGEN zusätzlich erhalten.

7 Klicken Sie auf BERECHTIGUNGEN.

Berechtigungen festlegen

8 Legen Sie Berechtigungen fest („Berechtigungen zuweisen / entziehen“, Seite 111)



9 Klicken Sie auf Speichern.

⇨ Der Organisationseinheit wurden Berechtigungen zugewiesen.

10 Klicken Sie auf GRUPPENMITGLIEDER.

11 Klicken Sie auf  .

Personen hinzufügen

12 Fügen Sie Personen der Organisationseinheit hinzu.
Sie können mehrere Personen markieren (Shift- und Strg-Taste drücken) um diese gleichzeitig hinzuzufügen.

13 Klicken Sie auf Speichern.

⇨ Sie haben eine Organisationseinheit erstellt.

⇨ Sie haben der Organisationseinheit Berechtigungen zugewiesen

⇨ Sie habe die Person, über die Sie die Organisationseinheit erstellt haben, und eventuell weitere Personen der neu erstellten Organisationseinheit zugewiesen.

14 Klicken Sie in der Navigationsleiste auf 〉**PERSON BEARBEITEN**〉 um wieder die Registerkarte GRUPPENMITGLIEDSCHAFTEN anzuzeigen.

Identifizierungsmerkmale

Identifizierungsmerkmale einer Person sind PIN-Codes und Ausweise.

Ausweise

UID = Unique Identifier

Herstellerseitig ist auf jedem Ausweis eine eindeutige Seriennummer, die UID (Unique Identifier), gespeichert, die nicht verändert werden kann. Oft ist die UID auch auf dem Ausweis aufgedruckt.

Je nach Lizenz können
- mehrere Ausweise einer Personen zugeordnet werden,
- zusätzlich zur jeweiligen UID individuelle Ausweisnummer auf die Ausweise geschrieben werden, zum Beispiel
  - der Name der Person oder
  - eine andere alphanumerische Bezeichnung.

Optional: Individuelle Ausweisnummern

Über die individuelle Ausweisnummer können Ausweise einfacher identifiziert und bei Bedarf gesperrt und wieder freigegeben werden. Eine einmal vergebene Ausweisnummer kann nachträglich nicht mehr verändert werden. Die Länge der Ausweisnummer wird im Feld *Ausweislänge [byte]* unter **SYSTEM** / **Systemkonfiguration** / **ZUTRITTSKONTROLLE** festgelegt.

PIN-Codes

Die 3- bis 9-stelligen PIN-Codes können
- manuell durch berechtigte Benutzer eingegeben werden oder
- automatisch vergeben werden.

Bei der manuellen Vergabe von PIN-Codes sind die PIN-Codes dem Ersteller bekannt. Der Ersteller muss den PIN-Code der betroffenen Person mitteilen.

Je nach Systemkonfiguration werden manuell erstellte PIN-Codes nicht automatisch auf Eindeutigkeit geprüft. So können dieselben PIN-Codes an mehrere Personen vergeben werden.

Automatisch vergeben PIN-Codes werden auch automatisiert per E-Mail an die betroffene Person verschickt. Mit der E-Mail wird auch eine Anleitung zum Ändern des PIN-Codes an einem Tastatur-Leser verschickt.

Einen Ausweis einer Personen zuweisen

1 Halten Sie den Ausweis vor einen beliebigen Leser.

⇨ Die LED am Leser leuchtet rot und signalisiert eine Fehlbuchung.

2 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

2.1 Falls nicht, klicken Sie auf Suche.

3 Klicken Sie in der Personenliste auf die Person, die einen Ausweis erhalten soll.

4 Klicken Sie auf  .

⇨ Es wird der Auswahl-Dialog *Nicht im System vorhandene Ausweisnummer* angezeigt.

5 Markieren Sie die Ausweisnummer.

6 Klicken Sie auf OK.

7 Klicken Sie auf Speichern.

⇨ Sie haben der Person einen (evtl. weiteren) Ausweis zugewiesen.

Alternative Vorgehensweise

1 Klicken Sie auf **PROFILE** und dann auf **Ausweise**.

⇨ Die *Ausweisliste* wird angezeigt, in der alle angelegten Ausweise aufgeführt sind.

2 Klicken Sie auf Erfassen.

3 Die Eingabemaske *Ausweis erfassen* wird angezeigt.

4 Geben Sie die STAMMDATEN ein.
Falls Sie die Ausweisnummer nicht eintippen wollen:

4.1 Halten Sie den Ausweis vor einen beliebigen Leser.

⇨ Die LED am Leser leuchtet rot und signalisiert eine Fehlbuchung.

4.2 Klicken Sie auf  .

⇨ Es wird der Auswahl-Dialog *Nicht im System vorhandene Ausweisnummer* angezeigt.

4.3 Klicken Sie auf eine Ausweisnummer.

5 Klicken Sie auf Speichern.

6 Klicken Sie in der Navigationsleiste auf 〉**AUSWEISE**〉 um wieder die *Ausweisliste* anzuzeigen.

7 Klicken Sie in der Ausweisliste auf den Ausweis, der einer Person zugeordnet werden soll.

8 Klicken Sie auf  hinter *Besitzer*.

9 Klicken Sie auf eine Person.

10 Klicken Sie auf Speichern.

⇨ Sie haben den Ausweis einer Person zugewiesen.

Die Ausweisdaten ändern, z.B. Gültigkeit oder Aktivieren / Deaktivieren

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie in der Personenliste auf die Person, deren Ausweis gesperrt werden soll.

3 Klicken Sie auf  .

⇨ Es wird ein Dialog zur Bearbeitung der Ausweisdaten angezeigt.

4 Ändern Sie die Daten, zum Beispiel
- Gültigkeitsende oder
- den Status (zum Beispiel auf *Gültig* oder *Gesperrt*).
  Jeder Status, außer gültig, deaktiviert den Ausweis.

5 Klicken Sie auf **OK**.

6 Klicken Sie auf **Speichern**.

⇨ Sie haben die Daten zu einem Ausweis bearbeitet.

Mehrere Ausweise einer oder mehreren Personen zuweisen

Nachfolgend wird beschrieben wie auf effiziente Weise mehrere Ausweise einer Person oder mehreren Personen zugewiesen werden können.

Das Prinzip:

SCALA net merkt sich eingelesene Ausweise, auch dann, wenn diese noch nicht im System bekannt sind und beim Einlesen lediglich eine Fehlbuchung erzeugen. Diese Eigenschaft kann man nutzen , mehrere Ausweise nacheinander einlesen und anschließend die eingelesenen UIDs den Personen zuweisen.

Ausweise einlesen

1 Legen Sie die Ausweise bereit, die an Personen vergeben werden sollen.
2 Halten Sie einen nach dem anderen Ausweis vor einen beliebigen Leser.
  2.1 Halten Sie einen Ausweis vor den Leser.
  ⇨ Die LED am Leser leuchtet rot und signalisiert eine Fehlbuchung.
  2.2 Warten Sie bis die rote LED wieder erlischt.

Personen erfassen

3 Falls noch nicht alle Personen, die einen Ausweis erhalten sollen, im System erfasst sind: Erfassen Sie alle Personen, die einen Ausweis erhalten sollen („Person erfassen“, Seite 114).

Die eingelesenen Ausweise den Personen zuweisen

4 Wechseln Sie wieder in die *Personenliste* über **PROFILE** / **Personen** und evtl. Suche.
5 Klicken Sie eine Person an, die einen Ausweis erhalten soll.
6 Klicken Sie auf  .
⇨ Es wird der Auswahl-Dialog *Nicht im System vorhandene Ausweisnummer* angezeigt
7 Markieren Sie eine Ausweisnummer.
8 Klicken Sie auf OK.
9 Klicken Sie auf Speichern.
⇨ Sie haben der Person einen (evtl. weiteren) Ausweis zugewiesen
10 Wiederholen Sie die Schritte 4 bis 9 bis alle Ausweise zugewiesen sind

PIN Code manuell vergeben

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie auf die Person, die einen PIN-Code erhalten soll.

Unter der Rubrik *PIN-Code* kann ein PIN-Code angelegt werden.

3 Klicken Sie auf  .

⇨ Es wird der Dialog *PIN-Code definieren* angezeigt

4 Geben den neuen PIN-Code ein.

5 Teilen Sie der betroffenen Person den neuen PIN-Code mit.

⇨ Es wurde ein neuer PIN-Code manuell vergeben.

PIN Code automatisch vergeben und per E-Mail zusenden

Voraussetzung

Die E-Mail-Adresse der betroffenen Person ist unter STAMMDATEN eingetragen.

1 Klicken Sie auf **PROFILE** und dann auf **Personen**.

⇨ Die *Personenliste* wird angezeigt, in der alle angelegten Personen aufgeführt sind.

1.1 Falls nicht, klicken Sie auf Suche.

2 Klicken Sie auf die Person, die einen PIN-Code erhalten soll.

Unter der Rubrik *PIN-Code* kann ein PIN-Code angelegt werden.

3 Klicken Sie auf  .

⇨ Es wurde ein neuer PIN-Code automatisch vergeben und versendet.

Berechtigungen über eine Zutrittsmatrix vergeben

Zutrittsmatrix

Über eine Zutrittsmatrix werden Zutrittsberechtigungen zugewiesen und die dazugehörige Elemente verwaltet. In einer Zutrittsmatrix werden Personen, Gruppen sowie Organisationseinheiten durch Zuordnung eines Zeitmodells Berechtigungen für Zutrittspunkte zugewiesen:

- Zutrittsmatrix-Profile — auf Personen bezogene Bearbeitung
- Zutrittsmatrix-Gruppen — auf Gruppen bezogene Bearbeitung

Funktionsprinzip einer Zutrittsmatrix

In den Zeilenköpfen sind die Personen oder Gruppen aufgelistet (Abb. 35–1), in den Spaltenköpfen sind Zutrittspunkte aufgelistet (2), im Kreuzungspunkt von Zeile und Spalte werden die Berechtigungen durch Mausklick zugewiesen (3). Beim Zuweisen einer Berechtigung wird immer ein Zeitmodell zugewiesen.

Für die Funktion einer Zutrittsmatrix werden also immer drei Komponenten benötigt:

- Personen oder Gruppen — in der Zeile (1)
- Zutrittspunkte — in der Spalte (2)
- Zeitmodelle — am Kreuzungspunkt (3)

Matrix aufrufen

1 Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Profile**.
oder
Klicken Sie auf **BERECHTIGUNGEN** / **Zutrittsmatrix-Gruppen**.

⇨ Die Zutrittsmatrix wird angezeigt.
⇨ Es möglich zwischen den Matrizen zu wechseln.
⇨ Bei Bedarf können über die Matrizen Personen, Gruppen und Zeitmodelle angelegt werden

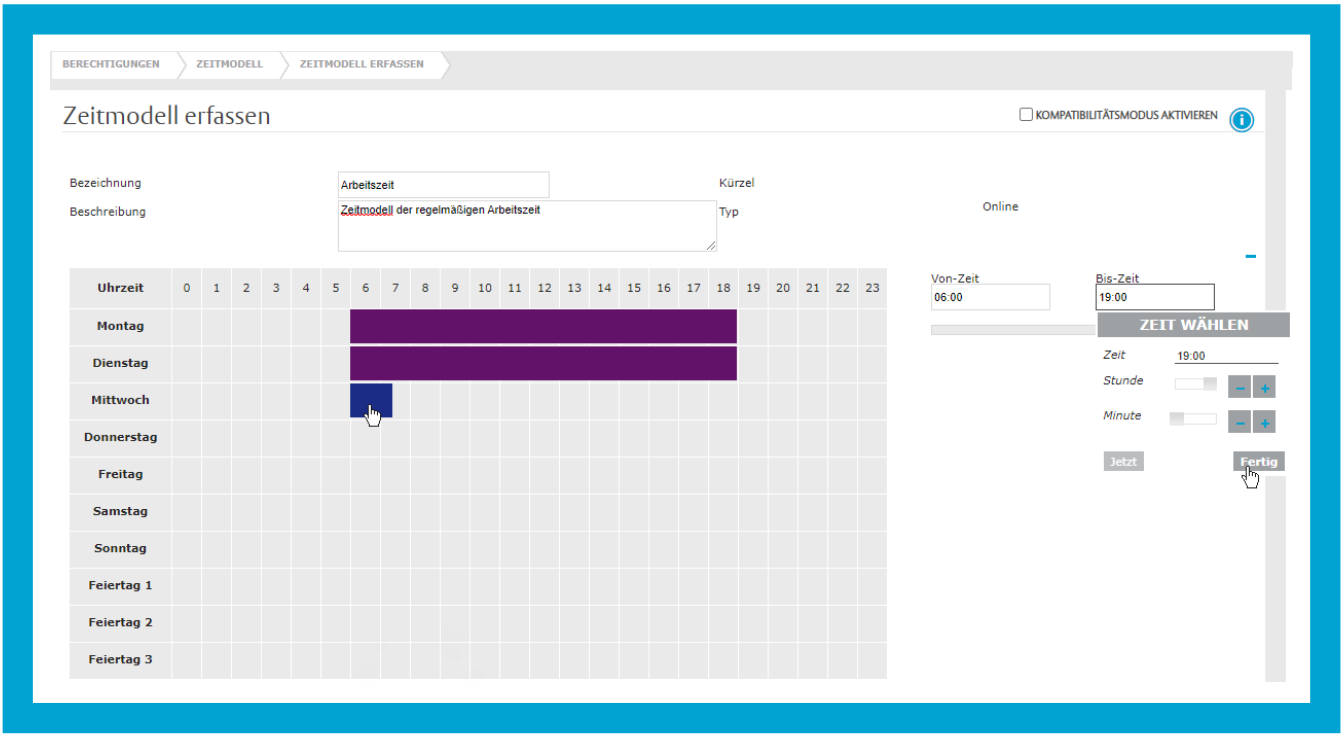


Abb. 34: Zeitmodell erfassen

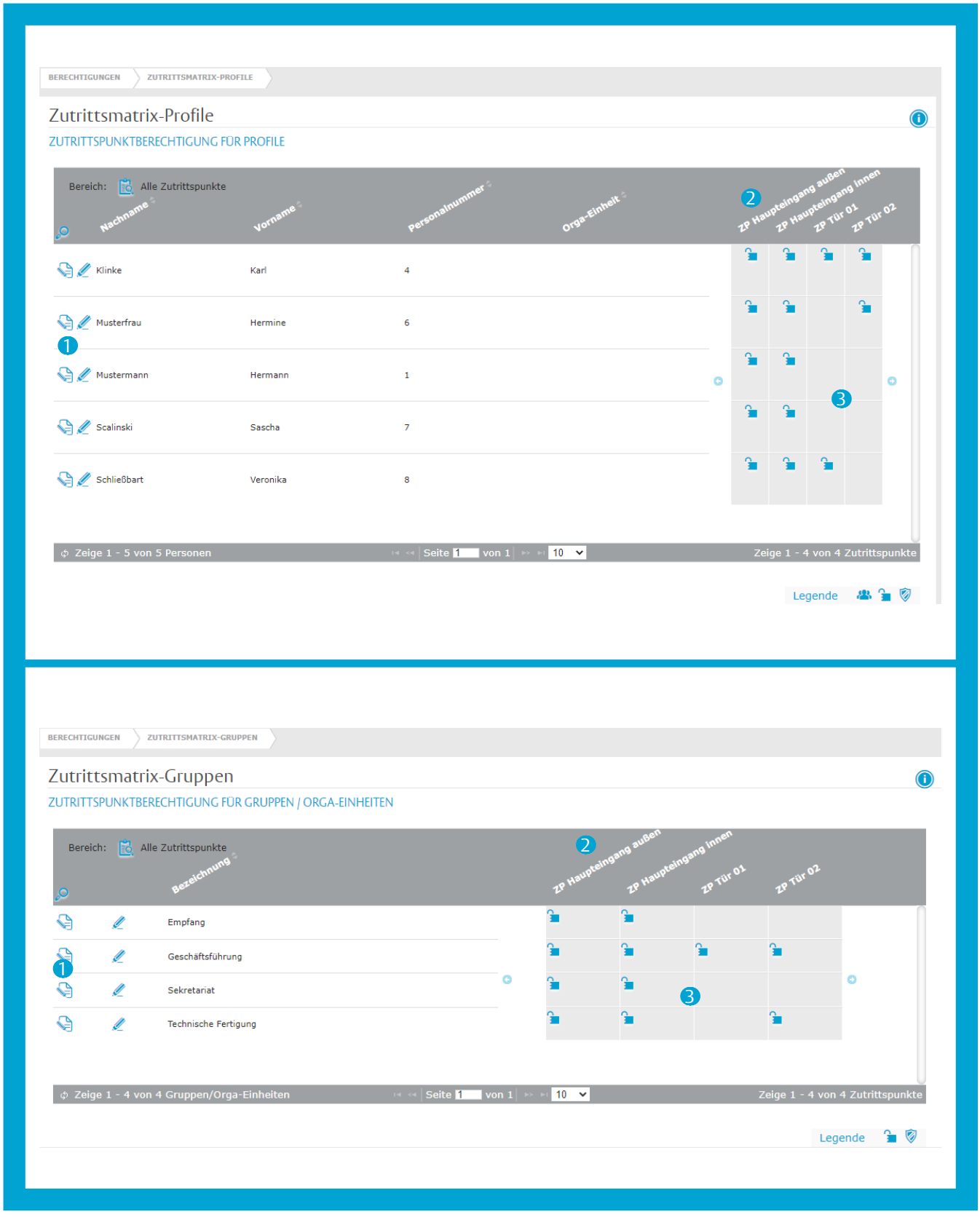


Abb. 35: Beispiele für die Zutrittsmatrix Profile und die Zutrittsmatrix Gruppen

LDAP-Schnittstelle

Einführung

Mit der LDAP-Schnittstelle verfügt SCALA net neben den Datenimportmöglichkeiten via MS Excel-Dateien und CSV-Dateien über eine weitere Möglichkeit Personendaten zu importieren.

Im Folgenden wird die Einrichtung und Anwendung eines solchen Imports in Verbindung mit einem Microsoft Active Directory auf Windows Server 2019 Version 3 beschrieben.

Diese Anbindung kann für zwei unterschiedliche Zwecke genutzt werden:

- Datenquelle für Personenimporte: Import von Personendaten zur automatischen Erfassung von Personen, für die in SCALA net entsprechende Zutrittsberechtigungen erstellt werden können. Details finden Sie im Abschnitt „Personenimport aus LDAP-Verzeichnis“.
- Datenquelle zur Authentifizierung von SCALA net-Benutzern: Zur Authentifizierung bei SCALA net wird eine Verknüpfung zwischen dem SCALA net-Benutzer und dem Active Directory hergestellt. Somit kann sich der SCALA net-Benutzer bei seiner Anmeldung mit den gewohnten Windows-Anmeldedaten einloggen. Details finden Sie im Abschnitt „Login gegen LDAP-Verzeichnis“.

Hinweise!

Single Sign-on: Eine Single Sign On (SSO) Anmeldung ist nicht möglich.
Sprachgebrauch LDAP-Verzeichnis bzw. LDAP-Server: In der Regel ist die Rede von einem Verzeichnisdienst, der einen Zugriff via LDAPv3 anbietet

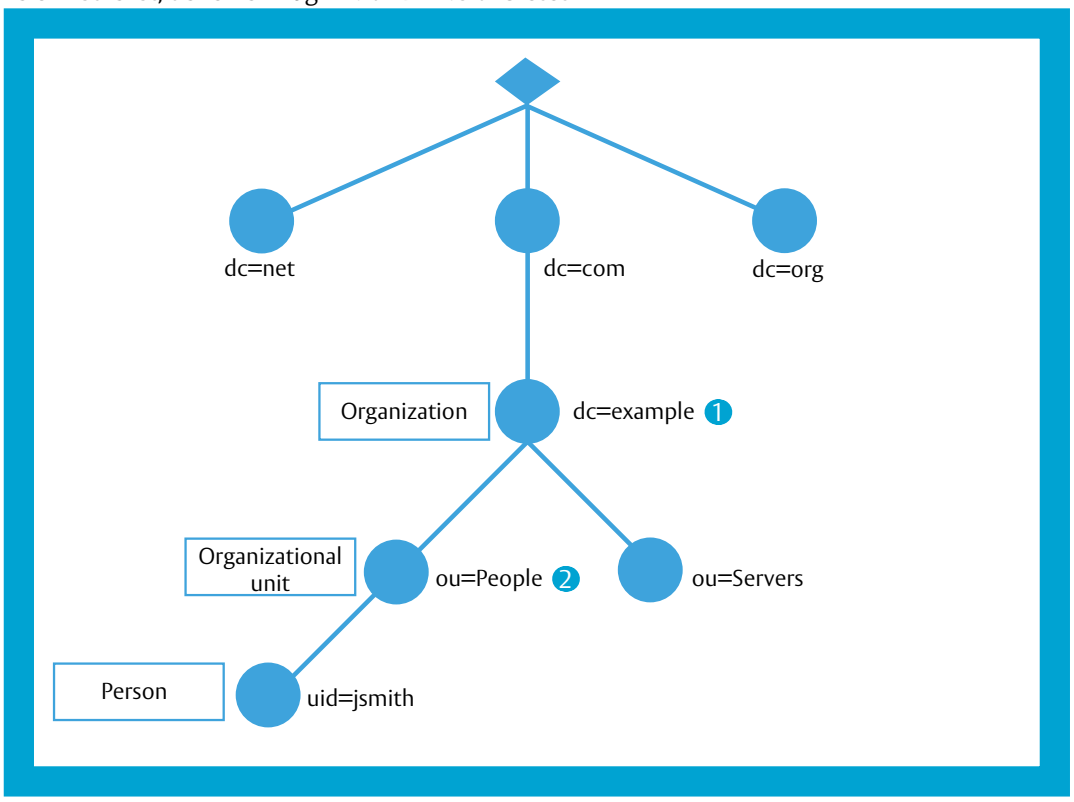


Abb. 36: LDAP-Verzeichnis

Allgemeines

Seit langer Zeit gibt es bei Java das sogenannte JNDI (Java Naming and Directory Interface). Es ähnelt in Aufbau und Verwendung sehr einem LDAP-Verzeichnis und dient einer Software zur dynamischen Ermittlung verfügbarer Dienste. Ein Anbieter eines Dienstes registriert diesen in einem JNDI-Verzeichnis und macht ihn damit öffentlich. Interessenten können das JNDI-Verzeichnis nach bestimmten Diensten durchsuchen. Ähnlich funktionieren LDAP-Verzeichnisse. Sie werden in der Regel von Unternehmen verwendet, um ihre Mitarbeiter bzw. deren Benutzerkonten zu verwalten.

Das LDAP-Verzeichnis

Das Verzeichnis ist hierarchisch aufgebaut und beginnt mit einem sogenannten Domain-Context (dc). Im Beispiel lautet dieser Kontext *example.com* (Abb. 36–1). Darunter kann beliebig verzweigt werden, indem weitere Container oder Objekte eingetragen werden. Ein Container wäre zum Beispiel eine Gruppe oder Organisationseinheit (hier: *People*) (Abb. 36–2).

Objekte können unterschiedliche Ausprägungen haben. Jedem LDAP-Verzeichnis liegt ein konkretes Schema zugrunde. Dieses kann auch kundenspezifisch angepasst werden und orientiert sich in der Regel an RFC 2251 (https://www.rfc-editor.org/rfc/rfc2251). Jede Implementierung bringt jedoch auch ihre Besonderheiten mit sich.

Objekte werden durch eine Reihe von Attributen definiert. Dabei kann eine mehr oder weniger komplexe Vererbung zwischen den verschiedenen Objekttypen im Spiel sein. Aufgabe eines Personenimports aus einer solchen Quelle ist es daher, die richtigen Objekte zu finden und deren Attribute auf die entsprechenden Eigenschaften im Objektmodell von SCALA net abzubilden.

Je nach Verwendungszweck der LDAP-Anbindung von SCALA net ergeben sich folgende Aufgaben:

- Personenimport aus einem LDAP-Verzeichnis: Die Aufgabe eines Personenimports aus einer solchen Quelle besteht also darin, die richtigen Objekte zu finden und deren Attribute auf die entsprechenden Eigenschaften im Objektmodell von SCALA net abzubilden.
- Authentifizierung gegen ein LDAP-Verzeichnis: Für die Authentifizierung gegen eine solche Struktur können verschiedene Protokolle verwendet werden. Für die Java-Welt sind dies die einfache Benutzername/Passwort-Authentifizierung und die Kerberos-Authentifizierung über das gleichnamige Protokoll in der Version 5.

Personenimport aus LDAP-Verzeichnis

Konfigurieren eines LDAP-Personenimports

Grundsätzlich sei vorausgeschickt: Um die richtige Konfiguration für die Anforderungen des Kunden zu finden ist die Mitarbeit des Kunden bzw. seiner IT-Abteilung erforderlich. Eine Konfiguration kann einmal angelegt werden, um später immer wieder aufgerufen und ausgeführt zu werden.

LDAP Import-Konfiguration erfassen

1 Klicken Sie auf **EXTRAS** und dann auf **Import**.
⇨ Die *Liste der Import-Konfigurationen* wird angezeigt, in der alle angelegten Konfigurationen aufgeführt sind.
2 Klicken Sie auf Erfassen .
⇨ Die Eingabemaske DATEIAUSWAHL wird angezeigt.

Hinweis!

Erfassung: In SCALA net kann zwar ein LDAP-Import in der bekannten Maske **EXTRAS** / **Import** erfasst werden. Da ein LDAP-Verzeichnis über eine URL adressiert wird, kann keine Vorlage in Form einer Datei ausgewählt werden.

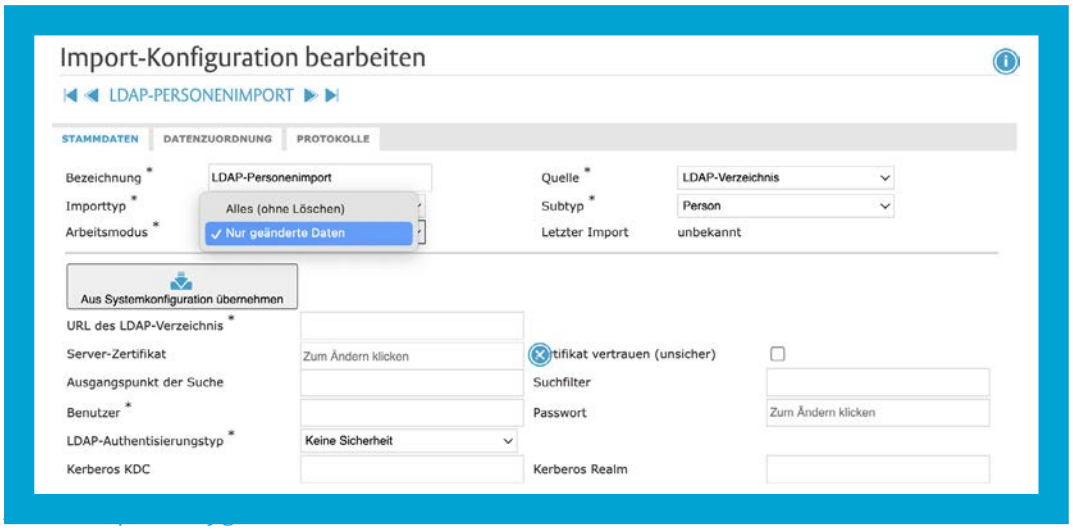
3 Lassen Sie das Eingabefeld leer und klicken Sie auf Erfassen
⇨ Die Eingabemaske IMPORT-KONFIGURATION ERFASSEN wird angezeigt.
4 Erfassen Sie die Daten zur Import-Konfiguration
5 Wählen Sie als Importtyp *Mitarbeiter*
6 Wählen Sie als Quelle *LDAP-Verzeichnis*
7 Wählen Sie als Arbeitsmodus *Nur geänderte Daten*, um die seit dem letzten Import geänderten Datensätze abzurufen und zu importieren.
7.1 Wählen Sie *Alles (ohne Löschen)*, um alle vorhandenen Daten abzurufen und zu integrieren.

Hinweise!

Auswahl der zu Importierenden Daten: Der Vorteil bei einem LDAP-Import gegenüber einem dateibasierten Import liegt darin, dass nur die Änderungen am Datenbestand seit dem letzten Import übertragen werden können. Daher kann zwischen einem Import seit dem letzten Import geänderten Datensätze und einem vollständigen Import aller Daten gewählt werden.

Import aller Daten (ohne Löschen): Früher importierte Daten, die im Quellsystem zwischenzeitlich gelöscht wurden, werden bei diesem Import nicht aufgerufen. Sie werden anschließend auch nicht gelöscht. Daher der Zusatz „ohne Löschen“.

Aus Systemkonfiguration übernehmen: Wenn Sie bereits in der **Systemkonfiguration** eine entsprechende LDAP-Authentisierung angelegt haben, erscheint nach dem Speichern die Schaltfläche *Aus Systemkonfiguration übernehmen*. Andernfalls erscheinen im unteren Teil der Eingabemaske nur die Felder für die zur Konfiguration notwendigen Parameter.



8 Klicken Sie auf Speichern.

⇨ Sie haben die Import-Konfiguration gespeichert und können nun weitere Daten eingeben.

Hinweis!

Aus Systemkonfiguration übernehmen: Wenn Sie bereits in der **Systemkonfiguration** eine entsprechende LDAP-Authentisierung angelegt haben, erscheint nach dem Speichern die Schaltfläche *Aus Systemkonfiguration übernehmen*. Damit können Sie die bereits angelegten Daten mit einem Klick übernehmen.

9 Klicken Sie auf die Schaltfläche *Aus Systemkonfiguration übernehmen*

10 Klicken Sie auf Speichern.

10.1 Alternativ geben Sie die *URL des LDAP-Verzeichnis* in folgender Form ein: *ldap(s)://server:port*

10.2 Definieren Sie den *Ausgangspunkt der Suche*, um die Datenmenge für die Suche einzuschränken, zum Beispiel: *DC=com,DC=example,DC=people,DC=uid* (siehe Abb. 36, Seite 118)

10.3 Wählen Sie den *LDAP-Authentisierungstyp* aus.

Hinweise!

Zertifikat: Für das TLS-Protokoll kann es erforderlich sein, das vom LDAP-Server verwendete Zertifikat zu pinnen. Dazu wird das Zertifikat in SCALA net hochgeladen und der Verbindung zum Server nur dann vertraut, wenn das vom Server gesendete Zertifikat mit diesem Zertifikat übereinstimmt. Zertifikatspinning ist nur dann notwendig, wenn das vom LDAP-Server verwendete Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle stammt. Wenn das Unternehmen über eine eigene PKIX-Struktur und eine eigene Root-CA verfügt, könnte eine mögliche Lösung auch darin bestehen, das Zertifikat der Stammzertifizierungsstelle in dem Key-Store des von den Java Diensten verwendeten Java Development Kits aufzunehmen.

LDAP Authentisierungstpyen

- Keine Sicherheit
- Einfache Sicherheit: Eingabe von Benutzer und Passwort erforderlich
- Kerberos V5: Eingabe von Benutzer und Passwort erforderlich

11 Geben Sie bei Bedarf den *Benutzer* ein (Bind-Benutzer: zum Beispiel *cn=MikeMac,dc=example,dc=com*)
12 Geben Sie für diesen *Benutzer* ein *Passwort* ein
13 Klicken Sie auf Speichern.
⇨ Sie haben die Stammdaten des LDAP Personenimports erfasst. SCALA net kontaktiert das LDAP-Verzeichnis mit den Parametern, um das Schema abzurufen. Die so erfasste LDAP-Import Konfiguration kann später immer wieder aufgerufen und mit einem Klick auf Import starten ausgeführt werden.

LDAP Import-Konfiguration ausführen

1 Klicken Sie auf die gewünschte Import-Konfiguration.
⇨ Sie gelangen in die Bearbeitungsmaske der gewählten Import-Konfiguration.
2 Klicken Sie auf auf Import starten
⇨ Sie haben die gewählte LDAP-Import Konfiguration gestartet.

Hinweise!

Änderung relevanter Parameter: Bei der Änderung folgender relevanter Parameter wird das LDAP-Verzeichnis erneut kontaktiert:
- URL des LDAP-Verzeichnisses,
- Ausgangspunkt der Suche
- Benutzer
- Passwort Authentisierungstyp
- Zertifikat

Scheitern beim Abrufen des Schemas: Überprüfen Sie die Einstellungen und/oder evtl. die Konfiguration des LDAP-Verzeichnisses bzw. der zwischengeschalteten Netzwerkkomponenten. Insbesondere bei der Verwendung von Kerberos ist es wichtig, dass die DNS-Auflösung korrekt funktioniert. Außerdem kann es notwendig sein, den sogenannten Login-Realm für den Kerberos-Dienst zu definieren, falls dieser nicht aus dem DN oder dem User-Prinzipal abgeleitet werden kann.

Abruf von Objekttypen beim Personenimport

Für den Personenimport ruft SCALA net das Schema für ganz bestimmte Objekttypen ab: inetOrgPerson, organizationalPerson, person. Diese Typen sind durch RFC 2798 (https://www.rfc-editor.org/rfc/rfc2798) und RFC 2256 (https://www.rfc-editor.org/rfc/rfc2256.html) definiert.

Dort steht Folgendes:

The inetOrgPerson object class is a general purpose object class that holds attributes about people. The attributes it holds were chosen to accommodate information requirements found in typical Internet and Intranet directory service deployments. The inetOrgPerson object class is designed to be used within directory services based on the LDAP protocol.

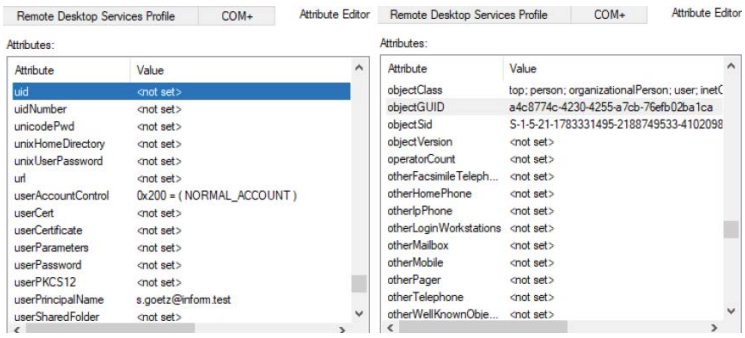
In RFC 2256 sind außerdem die Attribute für *organizationalPerson* und *person* festgelegt:

7.7. person
(2.5.6.6 NAME ‚person' SUP top STRUCTURAL MUST (sn $ cn)
MAY (userPassword $ telephoneNumber $ seeAlso $ description))

7.8. organizationalPerson
(2.5.6.7 NAME ‚organizationalPerson' SUP person STRUCTURAL
MAY (title $ x121Address $ registeredAddress $

destinationIndicator $
preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
telephoneNumber $ internationaliSDNNumber $
facsimileTelephoneNumber $
street $ postOfficeBox $ postalCode $ postalAddress $
physicalDeliveryOfficeName $ ou $ st $ l))

Durch die Abfrage des Schemas kann SCALA net nun einen Vorschlag für die Abbildung der LDAP-Attribute auf die Eigenschaften des SCALA net-Objektmodells machen. Im Gegensatz zu EXCEL oder CSV, wo die Zuordnung einer Spalte der Datei zu einer SCALA net-Eigenschaft nicht einfach antizipiert werden kann, ist die Verwendung der LDAP-Attribute festgelegt. Zum Beispiel gibt es nicht viel Spielraum für die Verwendung von Attributen wie *carLicense*, *jpegPhoto* oder *givenName*. Andere Attribute hingegen können in größerem Umfang verwendet werden. So definiert LDAP das Attribut *uid* oder auch *userid*, das in diesem Kontext einen Anmeldenamen darstellt. Dieser sollte hinreichend unterscheidbar sein, um als eindeutiges Merkmal zur Identifizierung eines Datensatzes zu dienen. Leider kommt hier die Eigenart der LDAP-Implementierungen ins Spiel. So wird im Microsoft Active Directory genau dieses Attribut nicht so gepflegt, wie es spezifiziert ist. Genauer gesagt wird es überhaupt nicht automatisch gefüllt.



SCALA net versucht, solche Implementierungsunterschiede auszugleichen. Da es jedoch kaum öffentlich zugängliche Dokumentationen zu den Schemata der einzelnen Verzeichnisdienste gibt (mit Ausnahme von Microsoft Active Directory, das über eine sehr gute Dokumentation verfügt), ist dies nur schwer möglich. Es ist daher nicht garantiert, dass der von SCALA net gemachte Vorschlag zur Verwendung der LDAP-Attribute automatisch zum Erfolg führt. Wie in Abb. 38, Seite 124 zu sehen ist, werden nur wenige Attribute von SCALA net automatisch vergeben. Da jedes Unternehmen sein Verzeichnis individuell pflegt, kann es natürlich immer sein, dass diese Zuordnungen für den konkreten Anwendungsfall nicht passen.

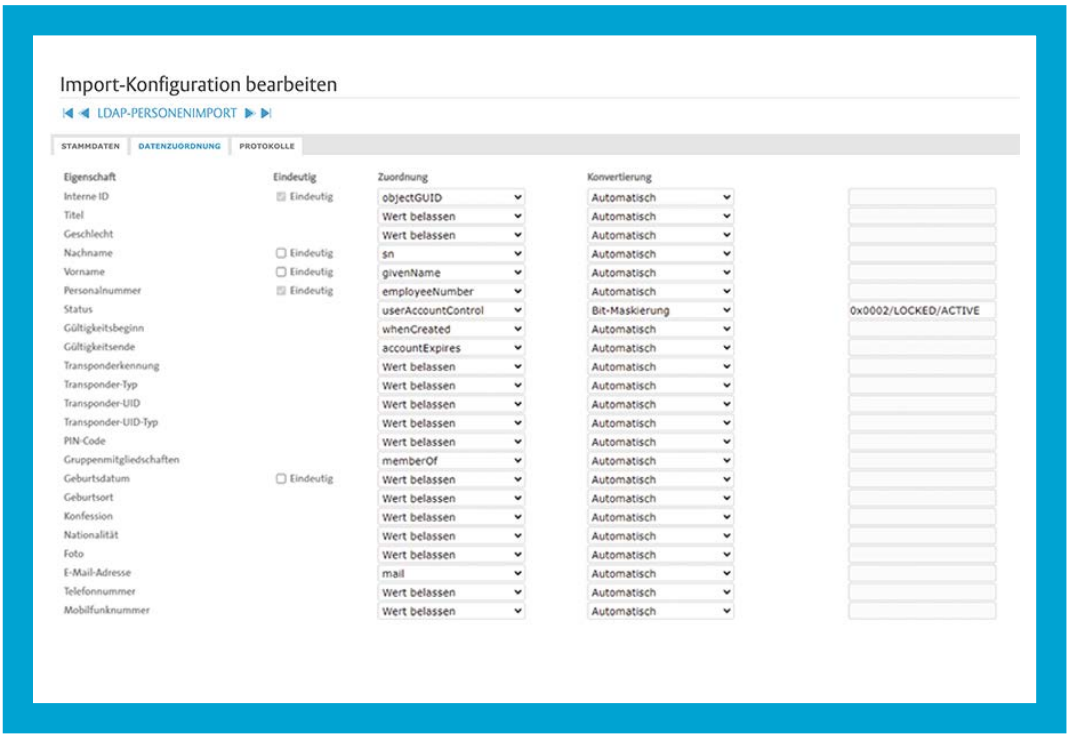


Abb. 38: Vorschlag von SCALA net für die Datenzuordnung für Microsoft Active Directory

Insbesondere das Attribut *employeeNumber*, das gemäß RFC 2798 die *Personalnummer* darstellt, wird häufig nicht gepflegt. Es ist daher wahrscheinlich, dass es beim Import zu Fehlern kommt, da dieser Wert in SCALA net ein Pflichtfeld darstellt, das nicht leer sein darf. Dies kann nur durch einen Testlauf herausgefunden werden.

Abb. 39: Testlauf mit Fehlern

Bei einem solchen Testlauf fällt auf, wenn etwas nicht wie erwartet funktioniert. Entsprechende Fehler werden im Importprotokoll ausgegeben. Abb. 39 zeigt beispielsweise den Fall, dass das Attribut *employeeNumber* auf die SCALA net *Personalnummer* gemappt wurde, aber seitens des LDAP-Servers nicht gefüllt ist. Da die *Personalnummer* aber eine Eigenschaft in SCALA net ist, die nicht leer sein darf, wird beim Speichern des Datensatzes in der Datenbank ein entsprechender Fehler erzeugt (SQLServerException: Cannot insert the value NULL into column ‚personnelNumber').

Hinweise!

Ermittlung des Importdeltas: Von besonderem Wert ist beim Importieren von Datendeltas, dass das Attribut *modifyTimestamp* durch RFC 2251 [1] für alle Datensätze vorgesehen ist:

The time this entry was last modified.

Dieser Wert zeigt an, wann ein Datensatz zuletzt geändert wurde. Daher kann über ihn das Delta seit dem letzten Import ermittelt werden. Dadurch gibt es die Möglichkeit, nur diese Daten zu importieren. Hierbei wird das Datum des letzten erfolgreichen Imports gespeichert. Erfolgreich bedeutet in diesem Zusammenhang, dass der Verbindungsaufbau zum LDAP-Server funktioniert hat und die Anfrage beantwortet werden konnte. Es bedeutet nicht, dass alle Datensätze bereits importiert wurden. Speziell zu Beginn, wenn noch mit der Datenzuordnung experimentiert wird, kann es möglich sein, dass der Import zwar nach dieser Definition erfolgreich war und dennoch keine Daten importiert wurden.

Im Importprotokoll zeigt SCALA net daher an, mit welchem Zeitstempel Daten beim LDAP-Verzeichnis angefragt werden:

Import timestamp set to 19700101T00:00:00.000+0000 for this run.

Der Zeitpunkt 01.01.1970 00:00 Uhr ist der Standardwert für den allerersten Durchlauf. Ein erneuter Durchlauf mit angepasster Datenzuordnung (*employeeNumber* wird nicht verwendet) führt im zuvor beschriebenen Szenario also zu folgendem Ergebnis.

2023-03-30 08:48:14 - INFO - Initializing import

2023-03-30 08:48:14 - INFO - Preparing import from ldap://WIN-2PFVFJIFD1G:389.

2023-03-30 08:48:14 - INFO - Analysing LDAP schema

2023-03-30 08:48:14 - INFO - Import timestamp set to ***20230330T06:29:41****.790+0000 for this run.*

2023-03-30 08:48:14 - INFO - Starting search for objects under dc=inform,dc=test matching (&(objectClass=inetOrgPerson)(modifyTimeStamp>=20230330062941.7Z))

2023-03-30 08:48:14 - INFO - ***0 objects imported*** from ldap://WIN-2PFVFJIFD1G:389.

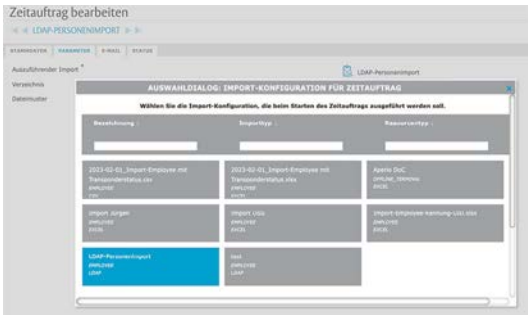
2023-03-30 08:48:14 - INFO - Updated import timestamp to 20230330T06:48:14.034+0000 for the next run.

2023-03-30 08:48:14 - INFO - Import finished

Wie man sieht, verwendet SCALA net das Datum des letzten Durchlaufs (im Protokoll 30.03.2023 06:29:41) als Startzeit für geänderte Datensätze. Da aber im Verzeichnis keine Daten geändert wurden, führt dies dazu, dass keine Datensätze aus dem LDAP-Verzeichnis gemeldet werden und somit auch nichts importiert wird.

Zeitgesteuerter LDAP-Personenimport anlegen

1 Klicken Sie auf **SYSTEM** und dann auf **Zeitauftrag**.
⇨ Die Zeitauftragsliste wird angezeigt.
2 Erfassen Sie einen Zeitauftrag („Zeitaufträge“, Seite 98).
3 Klicken Sie auf PARAMETER.
4 Klicken Sie bei *Auszuführender Import* auf .
5 Wählen Sie den gewünschten LDAP-Personenimport aus, der zu dem im Zeitauftrag definierten Zeiten ausgeführt werden soll.



Hinweis!

Notwendige Angaben für den Zeitauftrag LDAP-Personenimport: Bei der Definition eines Zeitauftrags für den LDAP-Personenimport entfallen die Angaben zu *Verzeichnis* und *Dateimuster*, da diese nur für dateibasierte Importe benötigt werden.

6 Klicken Sie auf Speichern.
⇨ Sie haben einen zeitgesteuerten LDAP-Personenimport angelegt, welcher sofort wirksam ist.

Systemeinstellungen

Für den Import aus einem LDAP-Verzeichnis wird der im OpenJDK enthaltene LDAP/JNDI-Client verwendet. Für die Parametrisierung wird an einigen Stellen auf sinnvolle Default-Einstellungen zurückgegriffen, die jedoch manchmal nicht passen.

Eigenschaft	Default-Wert
eu.inform.ldap.initialContextFactory	com.sun.jndi.ldap.LdapCtxFactory
eu.inform.ldap.referral	follow
eu.inform.ldap.personClasses	inetOrgPerson,organizationalPerson,person
eu.inform.ldap.incrementalImport	true
eu.inform.ldap.incrementalImportAttribute	modifyTimestamp

Hier folgen nun Erläuterungen zu den möglichen Systemparametern aus Tabelle 1.

eu.inform.ldap.initialContextFactory

Dies ist der vollqualifizierte Name einer Java-Klasse, die verwendet wird, um den initialen LDAP-Kontext zu erstellen. Dieser Wert sollte nur verwendet werden, wenn der Standardwert (com.sun.jndi.ldap.LdapCtxFactory) zu einem Fehler führt, so dass die Klasse nicht gefunden wird. Dies kann z.B. bei anderen Implementierungen des JDK der Fall sein.

1. *follow* löst diese Verweise automatisch auf und folgt ihnen

2. *ignore* ignoriert diese Verweise vollständig

3. *throw* führt zu einem Fehler, sobald ein Verweis gefunden wird

Der Standardwert dieser Eigenschaft steht auf follow.

eu.inform.ldap.personClasses

Diese Eigenschaft definiert die Objekttypen, die beim Import von Personen berücksichtigt werden. Wie bereits erläutert, wird hier standardmäßig nach Objekten des Typs inetOrgPerson, organizationalPerson, person gesucht. Es ist jedoch denkbar, dass in einem stark angepassten LDAP-Schema ein anderer Typ verwendet werden soll, der hier definiert werden kann. Es ist auch möglich, mehrere Objekttypen getrennt durch Komma (,) oder Semikolon (;) anzugeben, z.B:

-Deu.inform.ldap.personClasses=organizationalPerson;customEmployeeClass

eu.inform.ldap.incrementalImport

Im vorigen Abschnitt wurde auch auf die Vorteile des inkrementellen Imports mit Hilfe des Datums der letzten Änderung hingewiesen. Für den unwahrscheinlichen Fall, dass kein inkrementeller Import gewünscht wird, kann diese Funktion deaktiviert werden. Es handelt sich um einen booleschen Wert, der entweder true oder false sein kann. Letzteres würde den inkrementellen Import deaktivieren und jedes Mal alle Datensätze aus dem LDAP-Verzeichnis holen.

-Deu.inform.ldap.incrementalImport=false

eu.inform.ldap.incrementalImportAttribute

Beim inkrementellen Import kommt es häufiger vor, dass das LDAP-Attribut, in dem die Information über die letzte Änderung gespeichert ist, vom Standardwert (modifyTimestamp) abweicht. Mit Hilfe dieses Parameters kann dieses Attribut dann geändert werden.

Login gegen LDAP-Verzeichnis

SCALA net bietet ab der Version 13.1.0.0 die Möglichkeit, Systembenutzer statt gegen die lokale Benutzerdatenbank gegen ein angebundenes LDAP-Verzeichnis (Microsoft Active Directory) zu authentifizieren.

Nachfolgend werden die Funktionalitäten zur Einrichtung und Anwendung eines solchen LDAP-Logins in Verbindung mit einem Microsoft Active Directory auf Windows Server 2019 beschrieben.

LDAP-Login

SCALA net verfügt grundsätzlich über eine eigene Benutzerdatenbank. Dazu werden Passwort-Hashes mit sicheren Algorithmen in der Datenbank gespeichert.

Eine Authentifizierung erfolgt in der Regel gegen diese Datenbank.

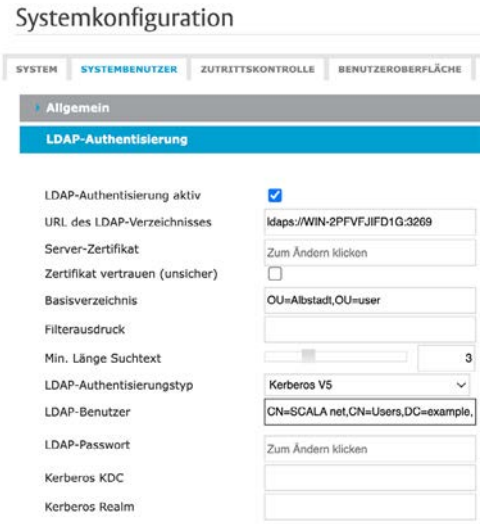
Ist die LDAP-Anbindung für einen Systembenutzer eingerichtet, wird dieser ausschließlich gegen das Active Directory authentifiziert.

LDAP-Login konfigurieren

Hinweise!

Aktivierte LDAP-Authentisierung: Solange die LDAP-Authentisierung aktiv ist, muss sich ein mit einem LDAP-Benutzer verknüpfter SCALA net Benutzer gegen das LDAP-Verzeichnis authentisieren. Eine lokale Authentisierung ist dann nicht möglich.
TCP-Port: In der Regel stellt ein LDAP-Verzeichnis seine Daten über Port 389 (unverschlüsselt) oder 636 (verschlüsselt) zur Verfügung. Aufgrund des Verhaltens des Global Catalogs Servers und der Implementierung in Java kann es hier nötig sein statt der genannten Ports die Ports 3268 bzw. 3269 zu verwenden, um Problemen bei sogenannten Referrals zu begegnen.
Gültigkeit des LDAP-Authentisierungstyps: Der festgelegte LDAP-Authentisierungstyp gilt sowohl für die Logins der SCALA net-Benutzer als auch für die Authentisierung im Zuge der Abfrage der existierenden LDAP-Benutzer während der Benutzerverknüpfung.
Angewendete Protokolle: Für Kerberos Authentisierung werden die Protokolle UDP und TCP jeweils auf Port 88 verwendet.
Verwendung von Zertifikatspinning: Wird kein Zertifikatspinning aber SSL/TLS verwendet, so muss das Server-Zertifikat ein vertrauenswürdiges Zertifikat aus Sicht der JVM sein. Dies kann außer mittels Zertifkatspinning auch mit dem manuellen Import des Zertifikats in den CA-Keystore der JVM erfolgen. Alternativ kann auch die Option *Zertifikat vertrauen* aktiviert werden. Diese Option bewirkt, dass jedem Zertifikat, das von der Gegenstelle gesendet wird, blind vertraut wird. Es findet in diesem Fall gar keine Zertifikatsprüfung statt. Dies ist deshalb äußerst unsicher und sollte nur in Szenarien und Umgebungen geschehen, wo nichts anderes möglich ist.
Basisverzeichnis: Das Basisverzeichnis kann leer bleiben. In diesem Fall wird ausgehend vom Domain Context der gesamte Verzeichnisbaum durchsucht, was potentiell langsam sein kann, wenn viele Objekte und Verzweigungen bestehen.
Login mit Kerberos: Beim Login mit Kerberos wird für den Kerberos Realm der Teil nach dem letzten @ Zeichen des sogenannten userPrincipalName verwendet. Dieser sieht in der Regel wie eine E-Mail-Adresse aus (z.B. Accountname@example.com). Manchmal kann es vorkommen, dass dies nicht für alle Benutzer eines LDAP-Verzeichnisses zutrifft, da es verschiedene UPN-Suffixe geben kann. In diesem Falle sollte hier die Login-Domäne explizit definiert werden. Diese gilt dann für alle Benutzer, unabhängig davon, wie ihr userPrincipalName definiert wurde.

1 Klicken Sie auf **SYSTEM** und dann auf **Systemkonfiguration**.
2 Klicken Sie auf **LDAP-Authentisierung**.
3 Geben Sie die Verbindungsparameter für das LDAP-Verzeichnis sowie den Authentisierungstyp ein.



Erläuterungen zur Konfiguration

Eigenschaft	Default-Wert	Bedeutung
LDAP-Authentisierung aktiv	false	Aktiviert den Login für alle Benutzer mit verknüpftem LDAP-Benutzer
URL des LDAP-Verzeichnisses		URL unter der das LDAP-Verzeichnis bereitgestellt wird (ldap:// für unverschlüsselte Kommunikation bzw. ldaps:// für TLS/SSL) z.B.: ldaps://WIN-2PFVFJIFD1G:3269
Server-Zertifikat		Falls ein self-signed Zertifikat verwendet wird, muss dieses hier mittels Zertifikatspinning eingestellt werden
Zertifikat vertrauen (unsicher)	false	Wird diese Option aktiviert, akzeptiert SCALA net **jedes** Zertifikat, das der LDAP-Server präsentiert. Dies eröffnet Sicherheitslücken und sollte nur in absoluten Ausnahmefällen verwendet werden.
Basisverzeichnis		DN des Basisverzeichnisses, von dem aus die Suche nach den zu verknüpfenden Benutzern gestartet werden soll (z. B. CN=Users,DC=exmple,DC=com)
Filterausdruck		Ein optionaler Suchfilter, der die Ergebnismenge für die Auswahl des LDAP-Objekts zu einem Systembenutzer einschränkt. Ein syntaktisch korrekter LDAP Filterausdruck (z.B. memberof=CN=ZK-Logins,OU=Service Users,OU=example,DC=com

Eigenschaft	Default-Wert	Bedeutung
Min. Länge Suchtext	3	Definiert die Anzahl der Zeichen, die ein Benutzer eingeben muss, bevor eine Suchanfrage an den LDAP-Server gesendet wird.
LDAP-Authentisierungstyp	Kerberos V5	Authentisierungsmethode beim Login der Benutzer
LDAP-Benutzer		DN des Benutzers, der für das Durchsuchen des LDAP-Verzeichnisses verwendet wird, um Systembenutzer zu verknüpfen (z.B. CN=SCALA net,CN=Users,DC=example,DC=com)
LDAP-Passwort		Passwort des LDAP-Benutzers, der für das Durchsuchen des LDAP-Verzeichnisses verwendet wird
Kerberos KDC		Key Distribution Center Server für die Kerberos-Authentisierung. Normalerweise wird als KDC der Host aus der LDAP-Url verwendet. Sollte dies für die konkrete Installation nicht passen, kann dieser hier explizit gesetzt werden.
Kerberos Realm		Der Realm entspricht sehr oft der Basisdomäne des LDAP-Verzeichnisses. Daher wird er auch aus dem distinguishedName des LDAP-Benutzers ermittelt. Sollte dies nicht passen, kann hier ein expliziter Realm angegeben werden (z.B. INTRA.EXAMPLE.COM).

5 Klicken Sie auf Speichern.

⇨ Sie haben die LDAP-Authentisierung (Login) konfiguriert.

Verknüpfen von Systembenutzern

LDAP-Benutzer verknüpfen

Hinweise!

Rechte für die Verknüpfung von LDAP-Benutzern: Jeder angemeldete Systembenutzer mit den entsprechenden Berechtigungen kann einen anderen Benutzer mit einem LDAP-Benutzer verknüpfen.
Voraussetzung für das Anlegen eines LDAP-Benutzers: Ist die LDAP-Anmeldung in SCALA net aktiv, kann in den Stammdaten des Benutzers eine Verknüpfung angelegt werden.
Erkennen von verknüpften Benutzern: Ist der Benutzer bereits verknüpft, wird der Prinzipalnamen sowie der Distinguished Name beim Menüpunkt „LDAP-Benutzer“ angezeigt.
Auswahl der LDAP-Benutzer: Im Auswahldialog der LDAP-Benutzer für Systembenutzer werden alle LDAP/AD-Benutzer angezeigt, die gewissen Kriterien genügen. So werden lediglich Elemente angezeigt, die den Objekttyp (objectClass) user haben und bei denen die drei Eigenschaften cn (commonName), distinguishedName und userPrincipalName einen Wert enthalten.
Verknüpfung von Administratoren: Der Systemadministrator (admin) kann nicht mit einem LDAP-Benutzer verknüpft werden, da dieser für die Benutzerverwaltung und Konfiguration verwendet wird. Um zu verhindern, dass sich ein Administrator aufgrund einer fehlerhaften LDAP-Konfiguration aus dem System aussperrt, kann sich der Systemadministrator nur lokal authentisieren.

Falls die Verknüpfung nicht korrekt oder nicht vorhanden ist:

1 Klicken Sie auf **SYSTEM** und dann auf **Benutzer**.
2 Die *Benutzerliste* wird angezeigt, in der alle angelegten Benutzer aufgeführt sind.
3 Klicken Sie in der Benutzerliste auf den zu verknüpfenden Benutzer.
4 Klicken Sie in den STAMMDATEN bei *LDAP-Benutzer* auf .

⇨ Es wird der Auswahldialog *LDAP-Benutzerliste für Systembenutzer* angezeigt.

5 Wählen Sie einen der Benutzer aus dem in den Systemeinstellungen verknüpften Active Directory, den Sie mit diesem Systembenutzer verknüpfen wollen.
   5.1 Falls notwendig filtern Sie nach den drei möglichen Eigenschaften cn (commonName), distinguishedName oder bzw. und userPrincipalName
   5.2 Klicken Sie zur Auswahl auf den gewünschten LDAP-Benutzer

⇨ Es wird eine Bestätigung erforderlich, ob die Attribute des LDAP-Benutzers nach SCALA net übernommen werden sollen.

6 Klicken Sie auf *Ja*, um den Datensatz aus dem LDAP-Verzeichnis abzurufen und die Parameter *Benutzername*, *E-Mail-Adresse* und *Vollständiger Name* aus dem Active Directory zu übernehmen.
   6.1 Klicken Sie auf *Nein*, wenn Sie die Daten nicht übernehmen möchten.

7 Klicken Sie auf Speichern.

⇨ Sie haben einen Systembenutzer mit einem LDAP-Benutzer verknüpft.

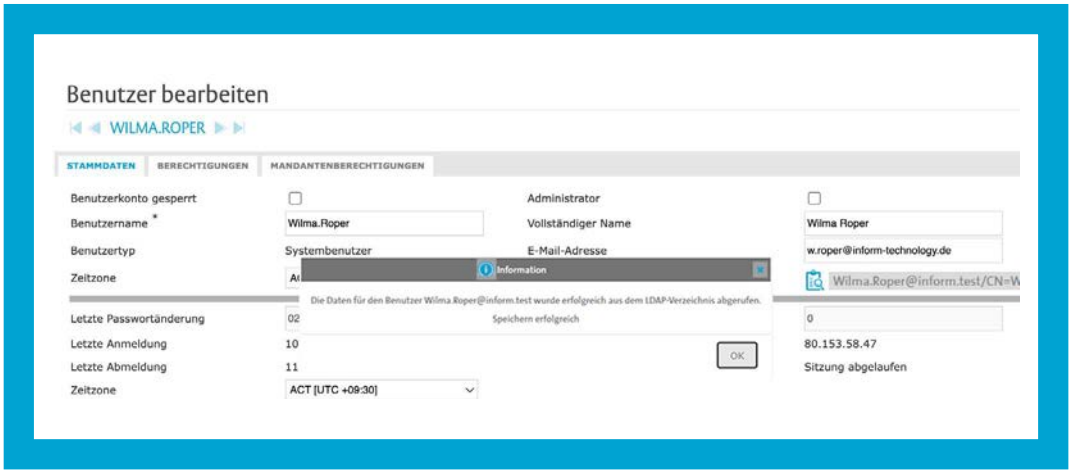


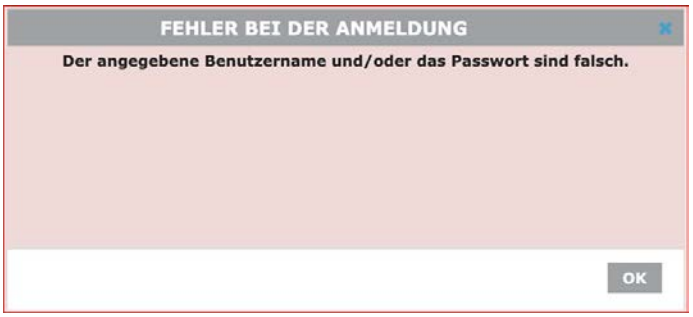
Abb. 40: Testlauf mit Fehlern

Hinweis!

Passwort: Ein so verknüpfter Datensatz benötigt ein lokales Passwort. Dieses Passwort wird immer dann wirksam, wenn die LDAP-Verknüpfung wieder entfernt oder die LDAP-Authentisierung in der Systemsteuerung deaktiviert wird. Solange dies nicht der Fall ist, muss sich der Systembenutzer gegen das LDAP-Verzeichnis authentisieren. Sind z.B. die beiden Passwörter (SCALA net und AD) unterschiedlich, muss der Benutzer das LDAP-Passwort eingeben. Ist die LDAP-Authentisierung hingegen deaktiviert, muss das SCALA net-Passwort eingegeben werden.

Login eines Systembenutzers

Der Login-Dialog unterscheidet sich bei aktiviertem LDAP-Login nicht vom Standard. Das SCALA net Login-Modul unterscheidet anhand des Systembenutzers, ob ein Login über LDAP oder lokal erfolgt und führt die entsprechende Authentisierung durch. Aus Sicherheitsgründen werden keine detaillierten Informationen über Fehlerzustände an das Frontend übertragen. Die allgemeine Informationsmeldung im Fehlerfall lautet:



Darüber hinaus führt SCALA net unabhängig von der Authentisierungsmethode ein Logbuch über die Anmeldeversuche und sperrt einen Benutzer nach einer einstellbaren Anzahl von fehlgeschlagenen Anmeldeversuchen. Diese Sperre muss in SCALA net aufgehoben werden und wird nicht mit dem LDAP-Verzeichnis synchronisiert.

Der Benutzername wird in SCALA net definiert und muss dort eindeutig sein. Soll dieser mit dem Benutzernamen des Domänenbenutzers übereinstimmen, muss diese Synchronisation manuell erfolgen, d.h. der gleiche Benutzername muss in SCALA net eingetragen werden.

Systemeinstellungen

Für die Durchführung des Logins sowie das Abrufen der vorhandenen Benutzer aus einem LDAP-Verzeichnis wird der im OpenJDK enthaltene LDAP/JNDI-Client verwendet. Für die Parametrierung wird an einigen Stellen auf sinnvolle Default-Einstellungen zurückgegriffen, die manchmal nicht passen könnten.

Systemparameter

Eigenschaft	Default-Wert
eu.inform.ldap.initialContextFactory	com.sun.jndi.ldap.LdapCtxFactory
eu.inform.ldap.referral	follow
eu.inform.ldap.userClasses	user
eu.inform.ldap.krb5.resolveKDC	false
eu.inform.ldap.krb5.resolveLDAPServer	true
eu.inform.ldap.searchPageSize	1000
eu.inform.ldap.referral.ignorePartialResultException	true
eu.inform.ldap.krb5.storeKey	false
eu.inform.ldap.krb5.useTicketCache	false

eu.inform.ldap.initialContextFactory

Dies ist der vollqualifizierte Name einer Java-Klasse, die verwendet wird, um den initialen LDAP-Kontext zu erstellen. Dieser Wert sollte nur verwendet werden, wenn der Standardwert (com.sun.jndi.ldap.LdapCtxFactory) zu einem Fehler führt, so dass die Klasse nicht gefunden wird. Dies kann z.B. bei anderen Implementierungen des JDK der Fall sein.

eu.inform.ldap.referral

Dieser Parameter beeinflusst das Verhalten des LDAP-Clients in Bezug auf sogenannte Referrals. Je nach Verzeichnisstruktur kann der LDAP-Server zu dem Schluss kommen, dass Daten im Verzeichnis, aber nicht auf dem angefragten LDAP-Server vorhanden sind. Dies erzeugt in der Antwort auf eine LDAP-Suchanfrage einen solchen Verweis. Der LDAP-Client kann auf diese Verweise auf drei Arten reagieren:

- *follow* löst diese Verweise automatisch auf und folgt ihnen (Standardwert)
- *ignore* ignoriert diese Verweise vollständig
- *throw* führt zu einem Fehler, sobald ein Verweis gefunden wird.

eu.inform.ldap.userClasses

Diese Eigenschaft definiert die Objekttypen, die bei der Auswahl der LDAP-Einträge berücksichtigt werden. Wie bereits erläutert, wird hier standardmäßig nach Objekten des Typs user gesucht. Es ist jedoch denkbar, dass in einem stark angepassten LDAP-Schema ein anderer Typ verwendet werden soll, der hier definiert werden kann. Es ist auch möglich, mehrere Objekttypen getrennt durch Komma (,) oder Semikolon (;) anzugeben, z.B.:-

Deu.inform.ldap.userClasses=organizationalPerson;customEmployeeClass

Diese Liste wird dann für die Suche verwendet oder-verknüpft, also in LDAP-Notation:

(|(objectClass=organizationalPerson)(objectClass=customEmployeeClass)).

eu.inform.ldap.krb5.resolveKDC

In größeren Netzwerken ist es sehr wahrscheinlich, dass es mehr als ein Key Distribution Center gibt. In der Regel wird dies über das DNS-System gehandhabt, wobei der angegebene Hostname in mehrere IP-Adressen aufgelöst wird. In diesem Zusammenhang kann es erforderlich sein, dass SCALA net vor der Authentisierung das konkrete KDC auflöst. Standardmäßig ist dies jedoch deaktiviert.

eu.inform.ldap.krb5.resolveLDAPServer

Analog zum KDC kann auch der angegebene LDAP-Server in mehrere IP-Adressen aufgelöst werden. Um Schwierigkeiten beim Zugriff auf das LDAP-Verzeichnis zu vermeiden, löst SCALA net auch hier den Hostnamen auf und verwendet den ersten Eintrag aus dem DNS-System. Gleichzeitig wird eine einfache Verfügbarkeitsprüfung durchgeführt, indem eine Verbindung zum LDAP-Port aufgebaut wird. Der erste Server, der auch erreichbar ist, wird dann verwendet. Diese Option ist standardmäßig aktiv.

eu.inform.ldap.searchPageSize

Ein LDAP-Server wird nie alle möglichen Objekte als Antwort auf eine Suchanfrage liefern, sondern hat in der Regel eine Beschränkung der Datensätze, die er an den anfragenden Client übermittelt. Der Client muss daher ein sogenanntes Paging implementieren, um alle Objekte abrufen zu können. Um nicht mit dem serverseitigen Limit in Konflikt zu geraten, definiert SCALA net hier eine Seitengröße von 100 Objekten. Gängige Server arbeiten mit Limits in der Größenordnung von 1000 Objekten. Sollte ein Administrator dieses Limit unter 100 herabgesetzt haben, kann dies in SCALA net über diese Einstellung nachgepflegt werden.

eu.inform.ldap.referral.ignorePartialResultException

Insbesondere bei Microsoft Active Directory tritt häufig das Problem auf, dass sogenannte Referrals nicht korrekt aufgelöst werden können. Dies würde zu einem Abbruch der Verarbeitung aufgrund von Partial-Result-Fehlern führen. Daher ignoriert SCALA net diese Fehler standardmäßig. Mit dieser Option kann dies jedoch bei Bedarf deaktiviert werden.

eu.inform.ldap.krb5.storeKey

Diese Einstellung legt fest, ob das Login-Modul den Schlüssel nach dem Login zwischenspeichert.

eu.inform.ldap.krb5.useTicketCache

Diese Einstellung legt fest, ob der Ticket-Cache für die Authentisierung verwendet wird.

VII – CLIQ® Web Manager Integration

Dieses Kapitel beschreibt Funktionen bei der optionalen Integration von CLIQ-Produkten.

Bestimmungsgemäßer Gebrauch

Die Schlüssel und Zylinder der Produktserie *eCLIQ*® sind die neueste Generation von elektronischen Schließanlagen der Serie *CLIQ*® und bieten einen hohen Schutz gegen Manipulationen. Der *CLIQ*® *Web Manager* ist eine online zugängliche Software zur Verwaltung von *CLIQ*®-Schließanlagen (separate Anleitung D01290xx).

In dieser Anleitung ist die Integration des *CLIQ*® *Web Managers* in das Zutrittskontrollsystem *SCALA net* beschrieben. *SCALA net* und *CLIQ*® *Web Manager* sind für die Nutzung entsprechend dieser Anleitung geeignet.

Jede darüber hinausgehende Verwendung gilt als nicht bestimmungsgemäß.

Besondere Systemeigenschaften

initialer Datenimport

Folgende Daten werden initial vom *CLIQ*® *Web Manager* nach *SCALA net* importiert:

- Personendaten,
- Zylinder und Zylindergruppen,
- Schlüssel- und Zylinderereignisse,

Schlüssel
- Berechtigungen für einzelne Zylinder
- Berechtigungen für Zylindergruppen
- Zeitpläne
- Gültigkeiten der Schlüssel
- Revalidierungszeiten der Schlüssel
- Schlüsselstatus mit Ausgabedatum
- Zugangsprofile

zusätzliche Möglichkeiten in der Software *SCALA net*

Durch die Integration des *CLIQ*® *Web Managers* in *SCALA net* ergeben sich folgende zusätzliche Möglichkeiten in der Software *SCALA net*:

- Schlüsselausgabe bzw. Schlüsselrücknahme (inkl. Quittung) via Workflow:
  - Besitzer des Schlüssels auswählen
  - Optional Rückgabedatum definieren
  - Gültigkeit / Revalidierungszeit des Schlüssels festlegen
  - Zeitplanvorlagen zuweisen (zylinderbezogene Zeitpläne sind möglich)
  - Explizite Zylinder- und Zylindergruppenberechtigungen verwalten
  - Zugangsprofile zuweisen
- Personenstammsätze bearbeiten bzw. erstellen
- Zugangsprofile bearbeiten bzw. erstellen
- Zeitplanvorlagen erstellen
- Schlüsselstatus setzen (ausgegeben, verloren oder defekt)

muss in *SCALA net* gepflegt werden

Folgendes muss in *SCALA net* gepflegt werden:

- Schlüsselausgabe bzw. Schlüsselrücknahme
- Personenstammsätze bearbeiten bzw. erstellen
- Zugangsprofile bearbeiten bzw. erstellen
- Zeitplanvorlagen erstellen

muss im *CLIQ*® *Web Manager* gepflegt werden

Folgendes muss im *CLIQ*® *Web Manager* gepflegt werden:

- Hinzufügen neuer Schlüssel und neuer Zylinder
- Erstellen und Ändern von Zylindergruppen
- Allgemeine Systemeinstellungen, zum Beispiel zu Nutzern des *CLIQ*® *Web Managers*
- Abholung von Ereignislisten aus den Zylindern
- Reprogrammieren von Zylindern
- Einstellungen zu Remote-Programmiergeräten
- Firmware-Updates von Schlüsseln

Konfiguration – Vorbereitung

Zum Einrichten der Schnittstelle zum *CLIQ® Web Manager* benötigen Sie folgende Daten und Zertifikate.

Server-Pfad (URL) zum CLIQ® Web Manager und Server-Zertifikat

Server-Pfad zum *CLIQ® Web Manager*

Der Server-Pfad (URL) ist die URL, unter der Sie den *CLIQ® Web Manager* im Browser erreichen. Hier können Sie sich auch das Server-Zertifikat (CRT-Datei) über den Browser herunterladen, welches ebenfalls für die Schnittstelle benötigt wird. Mit diesem Zertifikat wird sichergestellt, dass der Kommunikationspartner von *SCALA net* auch tatsächlich das entsprechende *CLIQ® Web Manager* System ist.

Client-Zertifikat

Client-Zertifikat

Das Client-Zertifikat (inklusive Passwort) erhalten Sie bei Bestellung der *CLIQ® Web Manager* Erweiterung Web Services automatisch per E-Mail. Mit diesem Zertifikat authentisiert sich *SCALA net* gegenüber dem *CLIQ® Web Manager.* Ohne dieses Zertifikat kann keine Verbindung hergestellt werden.

Notwendige Erweiterungen und Einstellungen im *CLIQ® Web Manager*

Folgende Erweiterungen werden im *CLIQ® Web Manager* benötigt und müssen dort aktiviert sein:
- Remote *(XS26)* zur Revalidierung von Schlüsseln an Wandprogrammiergeräten.
- *Web Service (XS30)* zur Kommunikation zwischen *SCALA net* und dem *CLIQ® Web Manager.*

Verbindung von SCALA net und CLIQ® Web Manager konfigurieren und testen

Die Verbindungsdaten konfigurieren

Voraussetzung

Daten können nicht synchronisiert werden, wenn „Integrierung von Web Services“ im *CLIQ® Web Manager* inaktiv ist.

1 Aktivieren Sie „Integrierung von Web Services“ bevor Sie mit der Konfiguration der Schnittstelle in *SCALA net* beginnen

Konfigurieren

1 Klicken Sie auf **CLIQ** / **Konfiguration**.
⇨ *CLIQ®-Konfiguration bearbeiten* wird angezeigt.
2 Wechseln Sie auf die Registerkarte **STAMMDATEN**.
3 Wählen Sie eine Bezeichnung für die *CLIQ®*-Konfiguration.
Server-Pfad eintragen
4 Tragen Sie den *Server-Pfad (URL)* ein.
Zertifikate hochladen
5 Klicken Sie hinter Server-Zertifikat auf das leere Textfeld.
5.1 Laden Sie das Zertifikat hoch.
5.2 Geben Sie das Passwort ein, falls notwendig.

6 Klicken Sie hinter *Client-Zertifikat* auf das leere Textfeld.
6.1 Laden Sie das Zertifikat hoch.
6.2 Geben Sie das Passwort ein, falls notwendig.

⇨ Wurden die Zertifikate erfolgreich hochgeladen, dann wechselt das Symbol auf .
⇨ Die Daten von *CLIQ® Web Manager* und *SCALA net* müssen synchronisiert werden („Folgedatenimport (Synchronisieren)“, Seite 138).

Verbindung testen

1 Klicken Sie auf **CLIQ** / **Konfiguration**.
⇨ Die Konfiguration bearbeiten wird angezeigt.
2 Klicken Sie auf Verbindungstest.
⇨ Es wird angezeigt, dass ein Verbindungstest geplant ist.
⇨ Nach kurzer Wartezeit erscheint eine Erfolgsmeldung, wenn die Verbindung funktioniert.
⇨ Die Meldung wurde von *SCALA* protokolliert und kann eingesehen werden unter: **CLIQ** / **Konfiguration** auf der Registerkarte DATENÜBERTRAGUNG in der ersten Zeile
3 Schließen Sie die Dialoge.

Falls Sie keine Erfolgsmeldung erhalten haben:

1 Prüfen Sie
- die Kabelverbindungen,
- die Konfigurationsdaten („Konfiguration – Vorbereitung“, Seite 136),
- den Online-Status von *SCALA net*,
- den Online-Status des *CLIQ® Web Manager*,
- die Gültigkeit der Zertifikate und Lizenzen.

2 Wiederholen Sie den Test

Systemstatus anzeigen

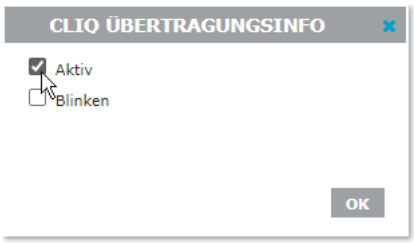
Abb. 41: Systemstatus dauerhaft anzeigen

Folgende Informationen werden oben rechts angezeigt:
- Synchronisationsmeldungen: Datenmenge, die aktuell an den *CLIQ® Web Manager* übertragen wird,
- Systemstatus
- Anzahl- der Erfolgs- und Fehlermeldungen zur Synchronisation der Systeme.

Systemstatus dauerhaft ein- / ausblenden

1 Klicken Sie auf das Symbol neben *CLIQ®-Übertragungsinfo.*

2 Aktivieren / Deaktivieren Sie die dauerhafte Anzeige, indem Sie das Häkchen setzen.



Initialer Datemimport

beim ersten Import von Daten

Der initiale Import wird ausschließlich beim ersten Import von Daten aus dem *CLIQ® Web Manager* nach *SCALA net* vorgesehen.

In allen nachfolgenden Fällen (nach dem einmaligen *initialen Datenimport*) werden neue Daten aus dem *CLIQ® Web Manager* über den Folgedatenimport synchronisiert („Folgedatenimport (Synchronisieren)“, Seite 138).

Daten initial importieren

1 Klicken Sie auf **CLIQ** / **Konfiguration**.
⇨ *CLIQ®*-Konfiguration bearbeiten wird angezeigt.
2 Klicken Sie auf Initialer Import.
⇨ Es wird ein Bestätigungsdialog angezeigt.
3 Klicken Sie auf OK, um den initialen Datenimport zu starten.

Folgedatenimport (Synchronisieren)

Ein Folgedatenimport muss regelmäßig durchgeführt werden. ASSA ABLOY empfiehlt dazu einen Zeitauftrag anzulegen („Konfiguration von Zeitaufträgen“, Seite 140). Bei Bedarf (on demand) kann aber auch jederzeit ein Folgedatenimport durchgeführt werden („Synchronisieren (on demand)“, Seite 139).

Beim Folgedatenimport werden Daten zu neuen, gelöschten und veränderten Zylindern, Zylindergruppen, Zugangsprofilen, Schlüsseln und optional auch Ereignisdaten synchronisiert.

Achtung!

Dateninkonsistenz nach Synchronisierung: Nach einer Synchronisierung der Systeme *CLIQ® Web Manager* und *SCALA net* dürfen folgende Daten nicht mehr im *CLIQ® Web Manager* bearbeitet werden:
- Schlüsselausgabe bzw. Schlüsselrücknahme,
- Personenstammsätze bearbeiten bzw. erstellen und
- Zugangsprofile bearbeiten bzw. erstellen

Werden diese Daten nach einer erfolgten Synchronisierung im *CLIQ® Web Manager* bearbeitet, sind Dateninkonsistenzen möglich, so dass alle Berechtigungen gelöscht und neu vergeben werden müssen.
- Bearbeiten Sie die genannten Daten nach einer erfolgten Synchronisierung ausschließlich über *SCALA net*.

Synchronisieren (on demand)

1 Klicken Sie auf **CLIQ** / **Konfiguration**.
⇨ *CLIQ®-Konfiguration* bearbeiten wird angezeigt.
2 Klicken Sie auf Folgedatenimport.
3 Markieren Sie im angezeigten Dialog, ob auch Ereignisdaten importiert werden sollen.

4 Klicken Sie auf OK, um den Datenimport zu starten.
⇨ Ein Dialog zeigt den Fortschritt des Datenimports an (Abb. 42).
5 Schließen Sie den Dialog, wenn der Datenimport beendet ist.
⇨ Der Folgedatenimport ist abgeschlossen und die Daten in *SCALA net* sind aktuell.

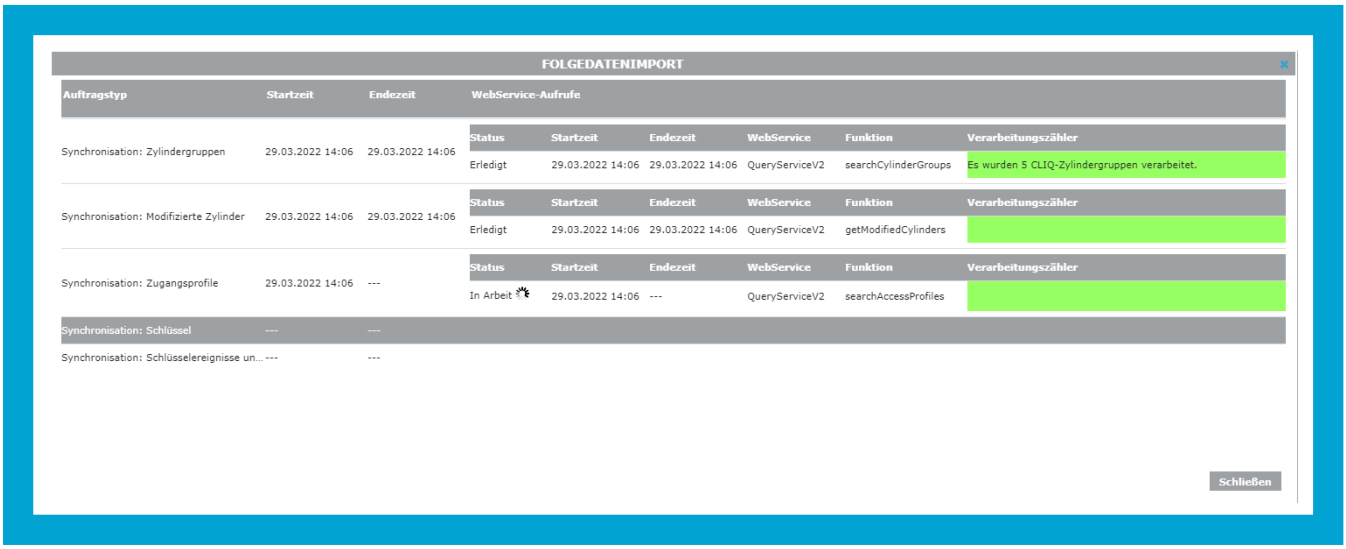


Abb. 42: Fortschrittsanzeige beim Folgedatenimport

Konfiguration von Zeitaufträgen

Damit Daten über Schlüssel, Zylinder und Zylindergruppen sowie Schlüssel- und Zylinderereignisse regelmäßig automatisch vom *CLIQ® Web Manager* System abgefragt werden können, muss dafür in *SCALA net* ein Zeitauftrag eingerichtet werden:

Einen Zeitauftrag einrichten

1 Klicken Sie auf **SYSTEM** / **Zeitauftrag** .
⇨ Die Zeitauftragsliste wird angezeigt.
2 Klicken Sie auf Erfassen .
3 Wählen Sie auf der Registerkarte STAMMDATEN den Typ *CLIQ®* Daten anwenden aus (Abb. 43).
4 Konfigurieren Sie alle weiteren Parameter zur Zeitauftragsausführung.
5 Klicken Sie auf Speichern .
⇨ Der Zeitauftrag ist angelegt. Es werden weitere Registerkarten angezeigt.
6 Wählen Sie die Registerkarte STATUS , um den Status des soeben angelegten Zeitauftrags abzufragen (Abb. 44).

Abb. 43: Zeitauftrag einrichten

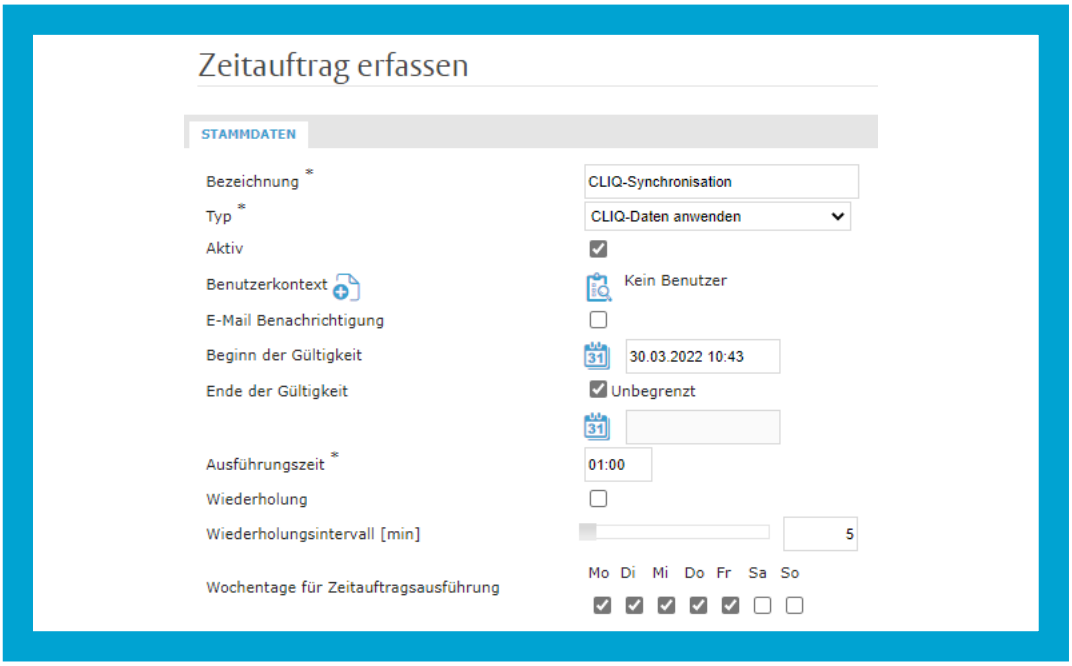


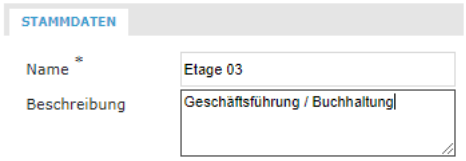
Abb. 44: Status Zeitauftrag abfragen

Zugangsprofile

In Zugangsprofil können Türen, Zylinder und Zutrittspunkte zusammengefasst werden. Zum Beispiel, um Mitarbeitern einer Abteilung oder Mitarbeitern mit besonderen Funktionen bei einer Schlüsselausgabe alle notwendigen Berechtigungen in einem Schritt zuzuweisen. Im Nachgang können diesen Mitarbeitern durch Änderungen am Zugangsprofil jederzeit Berechtigungen hinzugefügt oder genommen werden.

Ein Zugangsprofil anlegen

1 Klicken Sie auf **CLIQ** / **Zugangsprofil** .
⇨ Die Liste der *CLIQ*®-Zugangsprofile wird angezeigt
2 Klicken Sie auf Erfassen .
3 Geben Sie die Stammdaten zum Zugangsprofil ein.



⇨ Die Registerkarten ZUGANGSLISTE und PERSONEN werden zusätzlich angezeigt.
⇨ Auf der Registerkarte ZUGANGSLISTE können Zylinder und Zylindergruppen hinzugefügt und auch wieder gelöscht werden
⇨ Auf der Registerkarte PERSONEN können durch Hinzufügen oder Löschen von Personen Berechtigungen für die Zylinder und Zylindergruppen verwaltet werden.
4 Klicken Sie auf Speichern .
⇨ Das Zugangsprofil kann bei einer Schlüsselausgabe verwendet werden („Schlüsselausgabe – Berechtigung“, Seite 146).

Ein Zugangsprofil bearbeiten

1 Klicken Sie auf **CLIQ** / **Zugangsprofil** .
⇨ Die Liste der *CLIQ*®-Zugangsprofile wird angezeigt
2 Öffnen Sie das zu bearbeitende Zugangsprofil (Doppelklick)
3 Ergänzen oder Löschen Sie auf den Registerkarten ZUGANGSLISTE und PERSONEN Zylinder, Zylindergruppen und/oder Personen.
3.1 Klicken Sie auf das Symbol , um Zylinder, Zylindergruppen und /oder Personen dem Zugangsprofil hinzuzufügen.
3.2 Klicken Sie auf das Symbol , um Zylinder, Zylindergruppen und /oder Personen aus dem Zugangsprofil zu entfernen.
4 Klicken Sie auf Speichern .
⇨ Das Zugangsprofil kann bei einer Schlüsselausgabe verwendet werden („Schlüsselausgabe – Berechtigung“, Seite 146).

Stammdaten und Ereignisdaten

Die Stamm- und Ereignisdaten sind nach einer erfolgreichen Synchronisation in *SCALA net* vorhanden („Folgedatenimport (Synchronisieren)“, Seite 138). Daten zu Schlüsseln, Zylindern und Zylindergruppen können ausschließlich im *CLIQ® Web Manager* bearbeitet werden und werden anschließend in *SCALA net* importiert.

Schlüsselereignisse werden über die Nutzerschlüssel zurück ins *CLIQ®*-System gegeben.

Zylinderereignisse müssen über die *CLIQ®*-Programmierschlüssel aus den Zylindern abgefragt werden. Dies erfolgt ausschließlich über den *CLIQ® Web Manager*.

Danach können die Ereignisdaten über *SCALA net* abgerufen werden.

Stammdaten Schlüssel

Zu den Schlüsseln kann eine individuelle Zeitplanvorlage festgelegt werden. Die Gültigkeit der Schlüssel kann bearbeitet werden.

Die Schlüssel-Liste anzeigen lassen

1 Klicken Sie auf **CLIQ** / **Schlüssel**.
⇨ Die Liste Schlüssel wird angezeigt (Abb. 45).

Details zu einem Schlüssel anzeigen lassen

1 Klicken Sie auf einen Schlüssel in der Liste.
⇨ Auf den Registerkarten STAMMDATEN und EREIGNISSE werden die Daten zum ausgewählten Schlüssel angezeigt.
2 Wählen Sie bei Bedarf über den Navigator einen anderen Schlüssel.

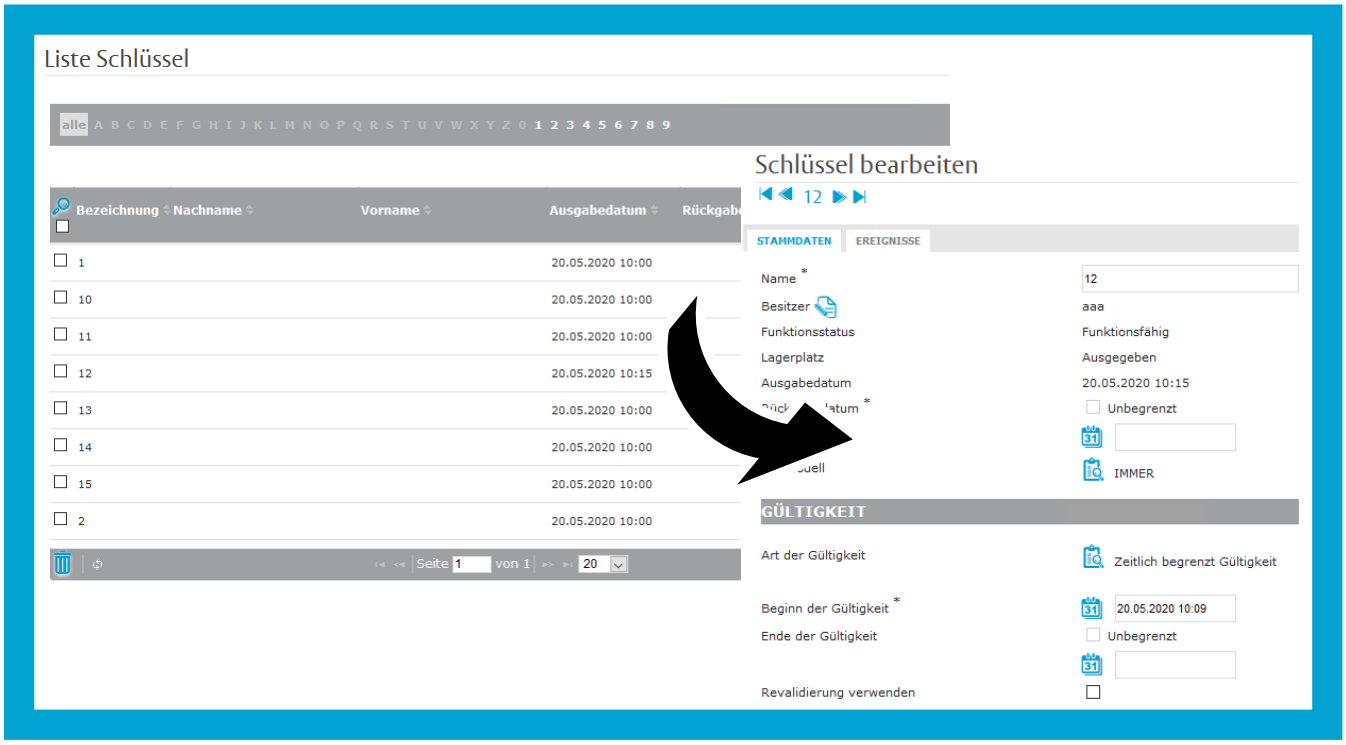


Abb. 45: Liste der Schlüssel und Ansicht der Stammdaten

Stammdaten Zylinder

Die Zylinder-Liste anzeigen lassen

1 Klicken Sie auf **CLIQ** / **Zylinder**.
⇨ Die Terminal-Liste wird angezeigt, in der die Zylinder aufgelistet sind (Abb. 46).

Details zu einem Zylinder anzeigen lassen

1 Klicken Sie auf einen Zylinder in der Liste.
⇨ Auf den Registerkarten STAMMDATEN und EREIGNISSE werden die Daten zum ausgewählten Zylinder angezeigt.
2 Wählen Sie über den Navigator einen anderen Zylinder .

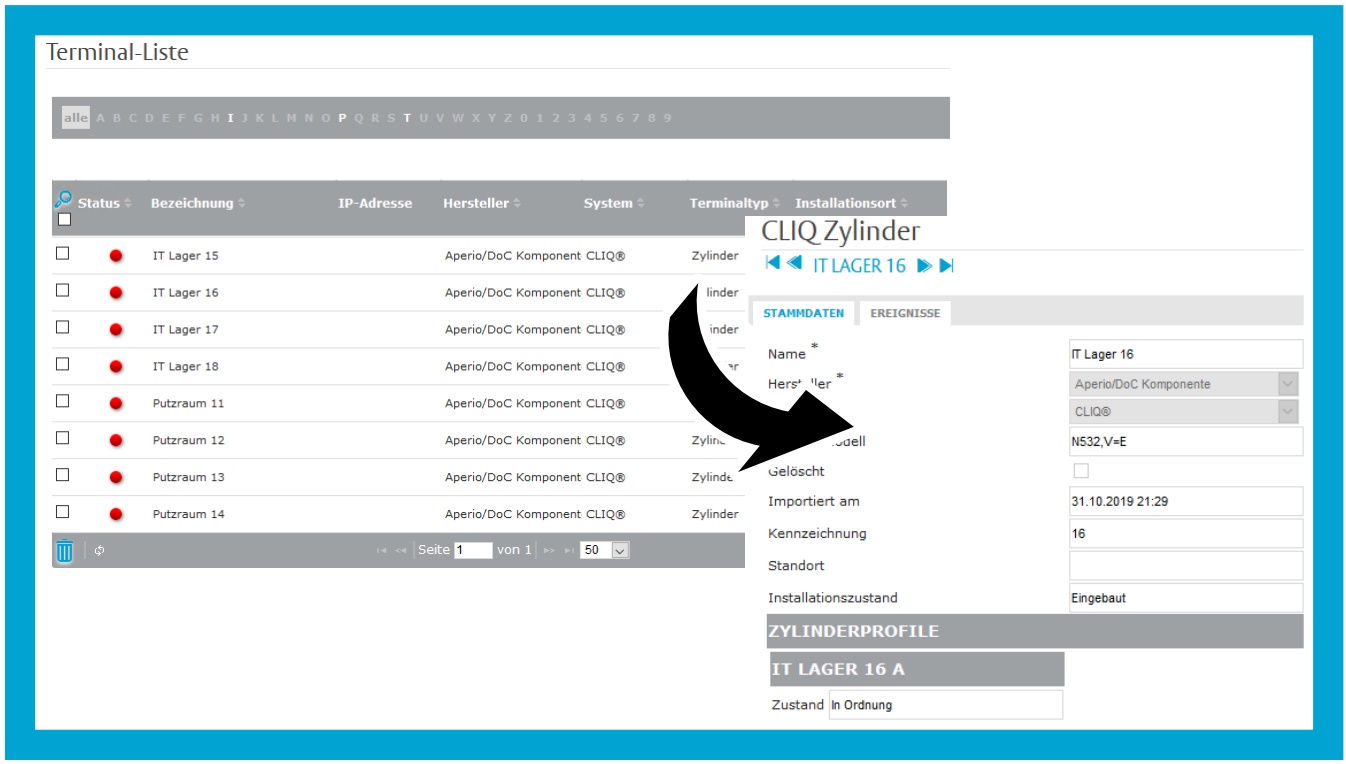


Abb. 46: Liste der Zylinder und Ansicht der Stammdaten

Schlüsselausgabe – Gültigkeit von Schlüsseln / Revalidierung erzwingen

Gültigkeit

Die Gültigkeit eines Schlüssels kann grundsätzlich befristet werden, indem ein Ablaufdatum gesetzt wird. Nach Ablauf des Gültigkeitsdatums ist der Schlüssel dauerhaft ungültig. Sobald eine Person in *SCALA net* gesperrt wird, wird auch der zugehörige Schlüssel inaktiv.

Die Gültigkeit eines Schlüssels darf die Gültigkeit einer Person nicht übersteigen. Wird die Gültigkeit einer Person nach der Schlüsselausgabe verringert, so wird auch die Schlüsselgültigkeit angepasst.

Revalidierung

Zudem kann eine Revalidierung erzwungen werden, so dass der Schlüssel in vorgegebenen Intervallen an einem *CLIQ*®-Programmiergerät seine Berechtigung neu bestätigt bekommt und aktuelle Berechtigungen erhält.

Hinweis!

Berechtigungen grundsätzlich befristen und Revalidieren erzwingen: Damit jeder Schlüssel mindestens einmal täglich aktualisiert wird, ist es sinnvoll, die Berechtigung der Schlüssel zeitlich zu begrenzen, zum Beispiel auf 18 Stunden. So muss jeder Schlüsselbesitzer mindestens einmal täglich zum Revalidieren an einem *CLIQ*®-Programmiergerät vorbei, zum Beispiel am Haupteingang. Selbstverständlich können abweichend vom Grundsatz einige Schlüssel unbefristet berechtigt sein.

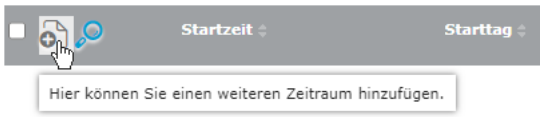
Schlüsselausgabe – Zeitplanvorlagen

Über Zeitplanvorlagen können Zutrittsberechtigungen zeitlich eingeschränkt werden. In *SCALA net* ist standardmäßig die Zeitplanvorlage *IMMER* für *CLIQ*®-Schlüssel hinterlegt. Weitere Zeitplanvorlagen können zusätzlich angelegt werden. Bei der Schlüsselausgabe wird jedem Schlüssel eine Zeitplanvorlage zugeordnet („Schlüsselausgabe – Berechtigung“, Seite 146).

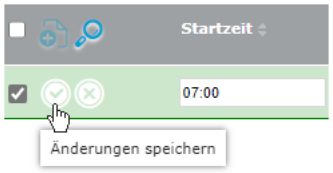
Es ist bei der Schlüsselausgabe möglich, die Vorgaben aus der zugewiesenen Zeitplanvorlage nachträglich individuell zu bearbeiten. So kann bei Bedarf einem einzelnen Mitarbeiter mit etwas abweichenden Arbeitszeiten grundsätzlich eine vorbereitete Zeitplanvorlage zugewiesen werden, die dann nachträglich geändert wird.

Eine Zeitplanvorlage erstellen

1 Klicken Sie auf **CLIQ** / **Zeitplanvorlagen**.
⇨ Die Liste der *CLIQ*®*-Zeitplanvorlagen* wird angezeigt (Abb. 47).
2 Klicken Sie auf Erfassen.
3 Klicken Sie das Symbol *Hinzufügen* .



4 Legen Sie die Berechtigungszeiten fest und geben Sie einen eindeutigen Namen ein.
⇨ Klicken Sie auf das Symbol *Änderungen speichern*.



5 Wiederholen Sie die Schritte 3 und 4 bis Sie alle betroffenen Wochentage erfasst haben.
6 Klicken Sie auf Speichern.
⇨ Die Zeitplanvorlage kann nun in der Schlüsselausgabe verwendet werden.

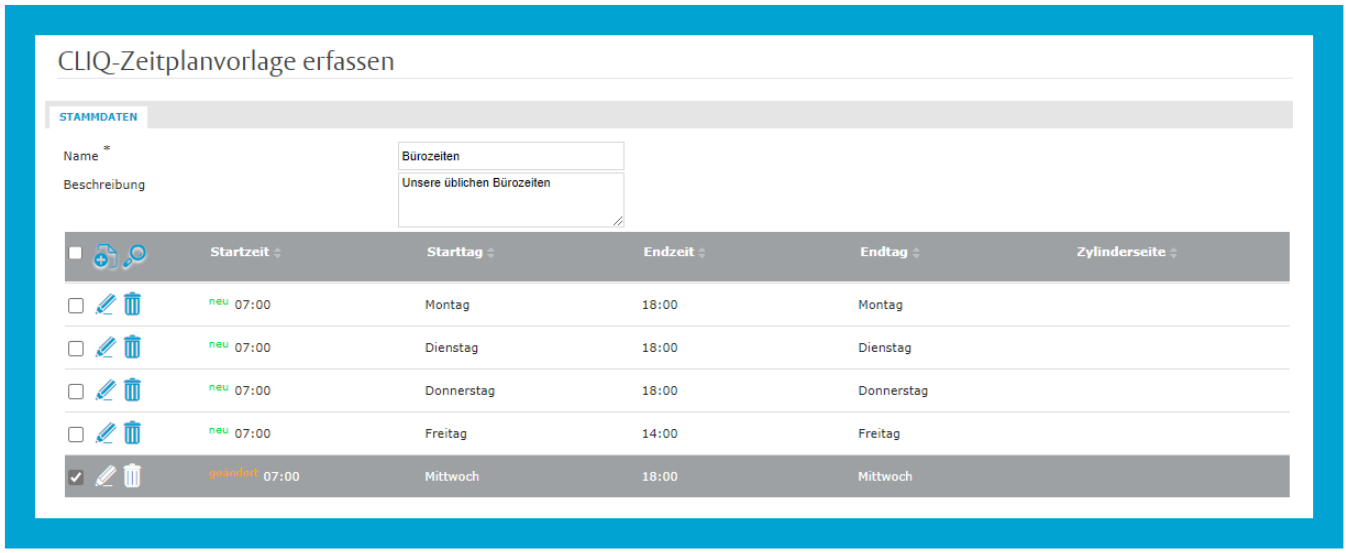


Abb. 47: Zeitplanvorlagen für zeitlich begrenzte Berechtigungen erstellen

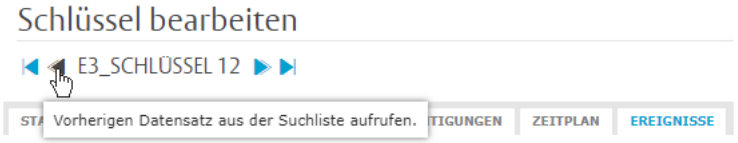
Schlüsselausgabe – Berechtigung

Die Vergabe von Zugangsberechtigungen erfolgt gleichzeitig mit der Schlüsselausgabe.

Ein Schlüssel kann explizit für Zylinder und/oder Zylindergruppen, aber auch zusätzlich oder alternativ über Zugangsprofile berechtigt werden.

Einen Schlüssel ausgeben

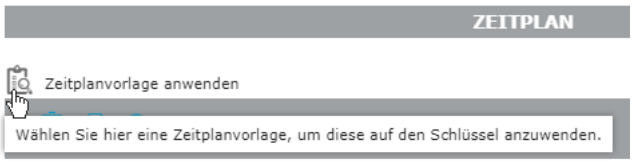
1 Klicken Sie auf **CLIQ** / **Schlüssel**.
⇨ Die *Liste Schlüssel* wird angezeigt (Abb. 45).
2 Klicken Sie auf den zu vergebenden Schlüssel in der Liste.
⇨ Es werden die Daten zum ausgewählten Schlüssel angezeigt.
3 Wählen Sie bei Bedarf über den Navigator einen anderen Schlüssel.



4 Klicken Sie auf Schlüsselausgabe.
⇨ Es wird eine Abfolge von Dialogen angezeigt, beginnend mit Schritt 2 (Abb. 48).
5 Folgen Sie den angezeigten Dialogen und geben Sie die angefragten Daten ein.
5.1 Schritt 1: Schlüssel auswählen - bereits vorher erledigt
5.2 Schritt 2: Schlüsselempfänger (Besitzer) auswählen
5.3 Schritt 3: Geplantes Rückgabedatum
5.4 Schritt 4: Gültigkeit und Revalidierung
(„Schlüsselausgabe – Gültigkeit von Schlüsseln / Revalidierung erzwingen“, Seite 144)

Zeitliche Berechtigung über Zeitplanvorlage

5.5 Schritt 5: Zeitplanvorlage auswählen („Schlüsselausgabe – Zeitplanvorlagen“, Seite 145)



Die Zeitplanvorlage *IMMER* wird automatisch zugewiesen, falls in diesem Schritt keine Zeitplanvorlage ausgewählt wird.
Die Vorgaben aus der Zeitplanvorlage können hier nachträglich bearbeitet werden.

Explizite Berechtigung für Zylinder

5.6 Schritt 6: Explizite Berechtigungen für Zylinder vergeben.

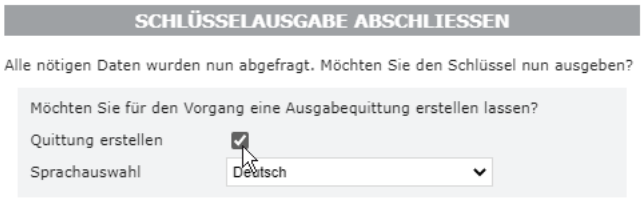
Explizite Berechtigung für Zylindergruppen

5.7 Schritt 7: Explizite Berechtigungen für Zylindergruppen vergeben.

Berechtigung über ein Zugangsprofil

5.8 Schritt 8: Wählen Sie ein Zugangsprofil aus

5.9 Schritt 9: Ausdruck einer Quittung

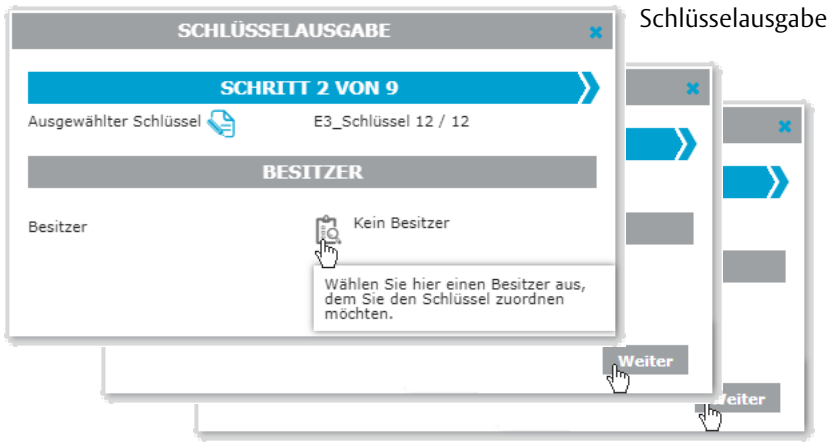


⇨ Die Schlüsselausgabe wurde in *SCALA net* erfasst. Der Schlüssel kann dem Empfänger übergeben werden.

⇨ Falls eine Quittung erstellt wurde, liegt diese als PDF-Datei im Download-Ordner des Browsers, zum Beispiel: C:/Users/admin/Downloads/IdentifierHandOutHandIn.pdf

Abb. 48: Die Schlüsselausgabe erfolgt in neun Dialogschritten

Schlüsselausgabe in 9 Schritten



Ausdruck der Empfangsbestätigung

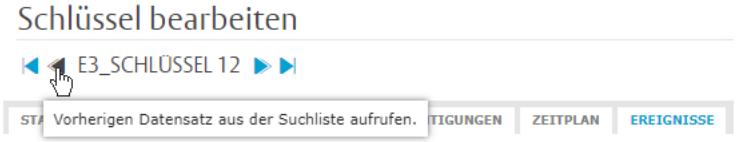
Schlüsselrücknahme

Wird ein Schlüssel zurückgegeben, dann muss der Schlüssel in *SCALA net* zurückgenommen werden. Damit verliert der Schlüssel alle zugeordneten Berechtigungen.

Bei defekten oder verlorenen Schlüsseln muss nach einer Schlüsselrücknahme zusätzlich der Funktionsstatus geändert werden („Funktionsstatus / Funktionierende, verlorene oder defekte Schlüssel“, Seite 149).

Einen Schlüssel zurücknehmen

1 Klicken Sie auf **CLIQ** / **Schlüssel**.
⇨ Die *Liste Schlüssel* wird angezeigt (Abb. 45).
2 Klicken Sie auf den zu vergebenden Schlüssel in der Liste.
⇨ Es werden die Daten zum ausgewählten Schlüssel angezeigt.
3 Wählen Sie bei Bedarf über den Navigator einen anderen Schlüssel.



4 Klicken Sie auf Schlüsselrücknahme.
⇨ Es wird ein Dialog zur Bestätigung angezeigt.
Es folgt die Abfrage, ob eine Quittung erzeugt werden soll (Abb. 49).
⇨ Falls eine Quittung erstellt wurde, liegt diese als PDF-Datei im Download-Ordner des Browsers, zum Beispiel: C:/Users/admin/Downloads/IdentifierHandOutHandIn.pdf

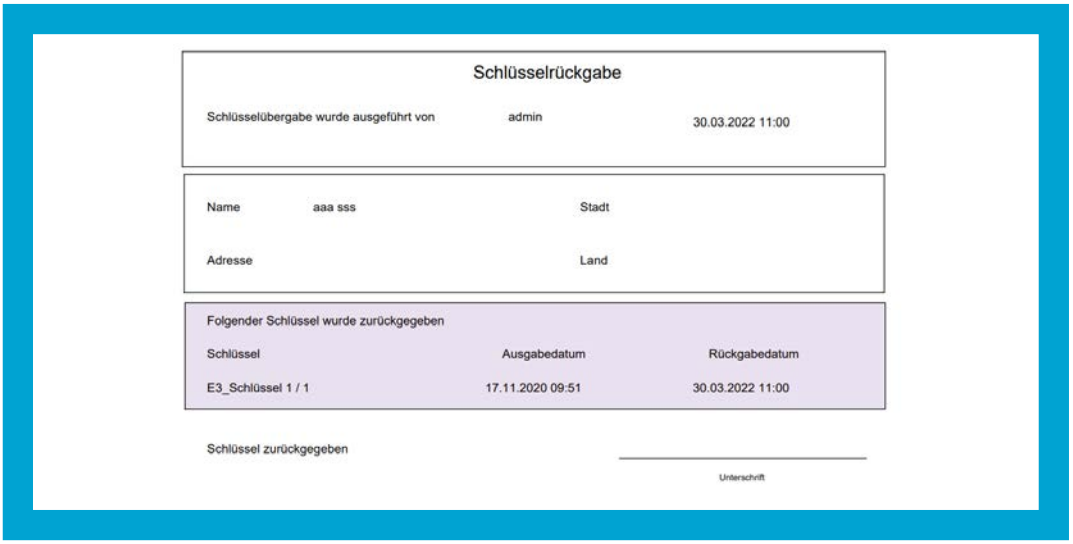


Abb. 49: Ausdruck der Rücknahmebestätigung

Funktionsstatus / Funktionierende, verlorene oder defekte Schlüssel

Der Funktionsstatus kennzeichnet einen Schlüssel als
- funktionsfähig,
- verloren oder
- defekt.

Schlüssel verloren

Wurde ein Schlüssel verloren, muss das in *SCALA net* im Schlüssel eingetragen werden. Damit verliert der Schlüssel alle zugeordneten Berechtigungen.

Achtung!

Verlorener Schlüssel bleibt zunächst gültig: Erst wenn die vorgegebene Gültigkeitsdauer oder die Berechtigungsdauer abgelaufen ist, wird der Schlüssel ungültig. Der Schlüssel wird sofort ungültig, wenn der Schlüssel an einem *CLIQ*®-Programmiergerät benutzt wird.

Den Funktionsstatus eines Schlüssels ändern

1 Klicken Sie auf **CLIQ** / **Schlüssel**.
⇨ Die *Liste Schlüssel* wird angezeigt.
2 Klicken Sie auf den zu bearbeitenden Schlüssel.
⇨ Die Eingabemaske *Schlüssel bearbeiten* wird angezeigt.
3 Wechseln Sie auf die Registerkarte STAMMDATEN.
4 Klicken Sie je nach Statusänderung
- auf Defekt melden, bzw. zum wieder rückgängig machen auf Funktionsfähig melden
- auf Verloren melden, bzw. zum wieder rückgängig machen auf Gefunden melden

⇨ Ein Schlüssel mit Funktionsstatus *Funktionsfähig* kann an eine Person ausgegeben werden.

Rückgabedatum / Überfällige Schlüssel

Steht fest, dass ein Schlüssel zu einem bestimmten Datum zurückgegeben werden muss, dann kann dem Schlüssel bei der Ausgabe oder auch später ein Rückgabedatum zugewiesen werden.

Damit eine betroffene Person vor Ablauf des Rückgabedatums eine Erinnerung per E-Mail erhält,
- muss eine E-Mail-Verbindung konfiguriert sein,
- muss für Ihren *SCALA net* Systembenutzer eine E-Mail-Adresse hinterlegt sein,
- muss ein Zeitauftrag des Typs *CLIQ*®*-Schlüsselrückgabe* definiert sein,
- muss eine E-Mail-Adresse in den Stammdaten der betroffenen Person eingetragen sein.

Ereignisdaten

Um Ereignisdaten zu Schlüsseln und Zylindern aus dem *CLIQ*® *Web Manager* abrufen zu können, müssen sie im *CLIQ*® *Web Manager* vorhanden sein. Die Synchronisierung in *SCALA net* erfolgt dann entweder über einen *Zeitauftrag* („Konfiguration von Zeitaufträgen“, Seite 140) oder manuell über einen *Folgedatenimport* („Folgedatenimport (Synchronisieren)“, Seite 138).

Die ASSA ABLOY Gruppe ist der Weltmarktführer in Zugangslösungen. Jeden Tag helfen wir Menschen sich sicherer und geborgener zu fühlen und eine offenere Welt zu erleben.

ASSA ABLOY
Opening Solutions

Technische Änderungen vorbehalten.

ASSA ABLOY
Sicherheitstechnik GmbH
Bildstockstraße 20
72458 Albstadt
DEUTSCHLAND
Tel. +49 7431 123-0
albstadt@assaabloy.com
www.assaabloy.com/de