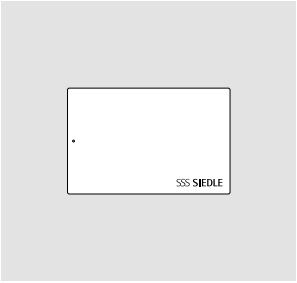
SSS SIEDLE

Inbetriebnahmeanleitung
Secure Controller



SC 600-0 (V. 2.12.7)

Inhalt

Allgemeine Hinweise 3
Service 3
Sicherheitshinweise 3
Netzwerksicherheit 3
Sabotageüberwachung 3
Secure Controller im Netzwerk 3
Benutzerkonten/Kennwörter 3
Automatische Abmeldung 3
Systemaktualisierung 3
Übersicht
Anwendung 4
Controller-Erweiterung 4
Systemgrenzen 4
Bestimmungsgemäße Verwendung 4
Auslieferungszustand 4
Inbetriebnahme 4
Controller-Eigenschaften 4
Systemübersicht
Lese-/Eingabeeinheiten (Siedle) 5
Betriebsformen 6
Einzelbetrieb 6
Betrieb mit Controller-Erweiterung 6
Betrieb im Geräteverbund 6
Konfigurationsmöglichkeiten 7
Inbetriebnahme-Wizard oder manuelle Konfiguration 7
Wochenprogramme 7
Vorrangregelung 7
Benutzer 7
Geräteübersicht
Anzeige-, Bedien- und Anschlusselemente 8
Anschlussklemmen 9
Steckbrücken (Jumper) 10
Betriebsdaten 12
Erste Schritte
Controller und Laptop verbinden 13
IP-Adresse des Controllers ermitteln 14
Kennwort neu vergeben 15
Sprache 15
Datum/Uhrzeit 16
Netzwerk 18
Optional: Secure Extension
Controller-Erweiterung(en) konfigurieren 21
Allgemeine Informationen 21
Voraussetzungen 21
Konfiguration 21
Vereinfachte Inbetriebnahme eines Controllers
Empfohlener Ablauf 23
Inbetriebnahme-Wizard 24
Erweiterte Inbetriebnahme von einem oder mehreren Controllern
Empfohlener Ablauf 25
Mehrere Controller vernetzen 26
Inbetriebnahme-Wizard 27
Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln 41
Optional: Wochenprogramm Allgemein 44
Optional: Konfiguration der Eingänge/Ausgänge
Eingänge 45
Ausgänge 51
Logik 54
Abschlussarbeiten
Funktionsprüfung 58
Daten/Konfiguration sichern 58
Übergabe/Kennwörter 58
Benutzerverwaltung durch Kunde/Betreiber
Planung der Benutzerverwaltung 59
Zutrittsparameter 60
Sondertag (Wochenprogramm) 63
Login 64
Kennwort neu vergeben 64
Benutzerverwaltung 64
Optional: Feiertage 65
Optional: Benutzer-Wochenprogramm 66
Optional: Zutrittsgruppen 67
Benutzer und Identifikationsmittel anlegen 69
Daten/Konfiguration sichern 74
Optional: Konten
Konto anlegen 75
Kennwort ändern 77
Optional: Türverwaltung
Manuelle Türsteuerung (Status) 78
Optional: Systemüberwachung 79
Optional: Protokoll/Report
Ereignisse 80
Berichte 81
Zutrittsprotokoll 86
Optional: Administration
Controller neu starten 87
Sabotageüberwachung konfigurieren 87
Daten löschen 88
Werkseinstellungen wiederherstellen 88
Netzwerkeinstellungen zurücksetzen 89
Optional: Benutzerverwaltung
Import/Export Benutzer 90
Export einer Datendatei 90
Aufbereitung von Datensätzen aus anderen Systemen 90
Erster Datenimport 91
Vorlagendatei für den ersten Datenimport 91
Import einer Datendatei 91
Optional: Service
Controller ersetzen 92
Einzelnen Controller ersetzen 92
Sekundären Controller ersetzen 93
Primären Controller ersetzen 94
Sekundären Controller aus dem Geräteverbund löschen 95
Servicemodus aktivieren 96
Systemaktualisierung 97
Firmware-Stand prüfen (Geräteverbund) 97
Index 98

Änderungen/Ergänzungen, Irrtümer und Druckfehler vorbehalten.

Allgemeine Hinweise

Diese Inbetriebnahmeanleitung beschreibt die Inbetriebnahme des Siedle Secure Controllers SC 600-0 mit dem Betrieb von Siedle-Lese-/ Eingabeeinheiten im Vario-Bus-Protokoll.

Dieses Dokument wird ergänzt durch:
• die Produktinformation Secure Controller SC 600-…
• das Planungs- und Systemhandbuch für Zutrittskontrolle
Die jeweils aktuelle Ausgabe finden Sie im Downloadbereich unter www.siedle.com
• den FAQ-Hilfebereich mit produktspezifischen Fragestellungen und Antworten auf der Siedle-Homepage unter www.siedle.de/faq_secure

Service
Für die Gewährleistung gelten die gesetzlichen Bestimmungen. Kontaktieren Sie im Servicefall Ihren Fachpartner oder Elektroinstallateur.

Ansprechpartner
Qualifizierte Ansprechpartner helfen Ihnen schnell und kompetent weiter. Telefonisch oder auch gerne vor Ort.

• **Kundenservice**
Kundenservice im Werk Furtwangen
+49 7723 63-375

• **Siedle Engineering**
Bei kundenspezifischen Anforderungen oder Lösungen außerhalb des Standards, wenden Sie sich bitte an Siedle Engineering im Werk Furtwangen
Telefon +49 7723 63-378
engineering@siedle.de

Sicherheitshinweise

Netzwerksicherheit
Verwenden Sie in Ihrem Netzwerk ausschließlich Komponenten und Geräte, die sich auf dem aktuellen Stand der Technik befinden. Aktualisieren Sie regelmäßig die Betriebssysteme aller Komponenten und Geräte. Tauschen Sie veraltete Komponenten und Geräte durch aktuelle Komponenten und Geräte aus. Verwenden Sie professionelle Schutzsoftware auf allen Geräten. Vergeben Sie sichere Passwörter. Sichern Sie Ihr Netzwerk mit den höchsten im Netzwerk verfügbaren Sicherheitsstandards ab. Schützen Sie Ihr Netzwerk gegen unbefugte Zugriffe von Innen und Außen!

Sabotageüberwachung
Der Secure Controller wird ab Werk mit einer aktiven Sabotageüberwachung ausgeliefert. Diese ist mit der Betriebsbereitschaft des Geräts sofort aktiv und überwacht das Gehäuse.
Wird das Gehäuse geöffnet, werden in regelmäßigen Zeitabständen Alarmmeldungen auf der Administrationsoberfläche ausgegeben. Informationen über die Sabotageüberwachung finden Sie auf Seite 87.

Secure Controller im Netzwerk
Für den regulären Betrieb des Secure Controllers ist keine Verbindung ins Internet erforderlich. Siedle empfiehlt den Secure Controller ausschließlich im lokalen Netzwerk zu betreiben und nicht über das Internet erreichbar zu machen.
Zugriff auf den Secure Controller sollten darüber hinaus ausschließlich Personen erhalten, die aufgrund ihrer Tätigkeit auf das Zutrittskontrollsystem zugreifen müssen (z. B. Pflege von Benutzern).

Benutzerkonten/Kennwörter
Sämtliche Benutzerkonten und deren Kennwörter liegen nach der Übergabe des Systems im Verantwortungsbereich des Kunden/ Betreibers. Mit der finalen Übergabe sollten alle Kennwörter durch den Kunden/Betreiber geändert sein!

Automatische Abmeldung
Der Secure Controller meldet aus Sicherheitsgründen jede Sitzung eines angemeldeten Benutzers ab, der 5 Minuten lang keine Eingabe in der Administrationsoberfläche vorgenommen hat. Um die Sitzungszeit nicht durch Änderung der Zeiteinstellungen künstlich verlängern zu können, erfolgt nach jeder Änderung der Zeiteinstellungen eine automatische Systemabmeldung.

Systemaktualisierung
Während des Updateprozesses darf die Stromversorgung der Siedle-Geräte nicht unterbrochen werden, da es sonst zu Schäden an den Geräten kommen kann. Ein erneutes Update ist dann nicht mehr möglich und die Geräte müssen zur Reparatur eingeschickt werden. Informationen über die Systemaktualisierung finden Sie auf Seite 97.

Übersicht

Anwendung
Secure Controller als zentrale Steuereinheit zur Verwaltung von Zutrittsberechtigungen in Privathäusern und gewerblichen Objekten.

Leistungsmerkmale:
• 2 RS485 Schnittstellen
• 4 Türen pro Controller
• Protokolle OSDP / Vario-Bus
• max. 500.000 Benutzer
• max. 16 Module pro Controller
• max. 64 Controller vernetzbar
• Log für 1.000.000 Ereignisse
• Programmierung via Web-Interface
• Wizard für einfache Inbetriebnahme

Controller-Erweiterung
Jeder Siedle Secure Controller ist mit bis zu 4 Siedle Secure Extensions (SE 600-…) erweiterbar.
Die Anbindung erfolgt über die RS485-Schnittstelle (Betriebsart: OSDP-Protokoll) und erfordert für den Siedle Secure Controller eine Firmware ab Version 2.12.7.

Leistungsmerkmale:
• RS485 Schnittstelle
• 4 Relais pro Extension
• pro Tür je 2 Eingänge (Status/Taster)
• Protokoll OSDP
• max. 4 Extensions pro Controller (2 pro RS485 Schnittstelle)
• LED-Statusanzeige

Systemgrenzen
• Mit 1 Controller und 4 Erweiterungen sind 20 Ausgänge (Relais) und 40 Eingänge (2 je Ausgang) und 3 Steuerausgänge nutzbar.
• Für die Zutrittskontrolle sind max. 12 Zutrittspunkte (Türen) an 1 Controller und 2 Erweiterungen konfigurierbar.
• Für andere Funktionen (z. B. Aufzugssteuerung) sind alle Aus-/Eingänge nutzbar.

Bestimmungsgemäße Verwendung
• Dieses Gerät ist für den Betrieb mit Siedle-Komponenten (Lese- und Eingabeeinheiten) für die Zutrittskontrolle vorgesehen.
• Die am Secure Controllers angeschlossenen Komponenten (Module, beschaltete Ausgänge, …) dürfen insgesamt im Verbrauch die Versorgungsleistung des Controllers (max. 20 Watt – abhängig von der Versorgung des Controllers) nicht überschreiten.
• Der reguläre Betrieb ist nur in lokalen Netzwerken (LAN) zulässig. Achten Sie darauf, dass der Secure Controller ausreichend gegen Zugriffe aus dem Internet geschützt ist (z. B. direkter Zugriff auf die Administrationsoberfläche aus dem Internet).
• Alle zulässigen Betriebsarten und für den Betrieb zulässige Siedle-Komponenten sind in diesem Dokument beschrieben.
• Für die Inbetriebnahme des Geräts ist ausschließlich das Benutzerkonto „Service“ zu verwenden.
• Das Benutzerkonto „root“ ist ausschließlich für den Siedle-Werksservice für Service-Zwecke vorgesehen.
• Jede darüber hinausgehende Verwendung gilt als nicht bestimmungsgemäß, für die Siedle keinen Support leistet.
• Siedle übernimmt keinerlei Haftung für Schäden, die aus einer nicht bestimmungsgemäßen Verwendung resultieren.

Auslieferungszustand
Im Auslieferungszustand sind folgende Konten (Benutzerkonten der Bedienoberfläche des Controllers) mit vorkonfigurierten Zugangsdaten angelegt:
• **root**: Konto mit allen Berechtigungen. Dieses Konto ist nur für Servicezwecke vorgesehen.
• **Service**: Konto mit umfangreicher Berechtigung für die Inbetriebnahme des Zutrittskontrollsystems und für die Verwaltung der Benutzer des Zutrittskontrollsystems.
• **Facility**: Konto mit eingeschränkter Berechtigung für die Verwaltung der Benutzer des Zutrittskontrollsystems.

Zugangsdaten (bei Auslieferung)

Konto/ Benutzername	**Kennwort**
root	78120Furtwangen!
Service	Siedle1234
Facility	Facility1234

Die Konten „root“, „Service“ und „Facility“ können nicht gelöscht werden. Weitere Konten sollen ausschließlich über das Konto „Service“ angelegt werden.

Inbetriebnahme
Die Inbetriebnahme erfolgt über einen Laptop per Webbrowser. Laptop und Controller müssen im gleichen Netzwerk miteinander verbunden sein.

Controller-Eigenschaften
• Der Controller ist ca. 1 Minute nach dem Einschalten der Spannungsversorgung betriebsbereit.
• Erfolgt in der geöffneten Menüoberfläche länger als 5 Minuten keine Eingabe, erfolgt eine automatische Abmeldung und der Wechsel zur Anmeldeseite. Nicht gespeicherte Eingaben gehen verloren.

Lese-/Eingabeeinheiten (Siedle)
Im Betrieb mit dem Siedle Vario-Bus-Protokoll können je RS485-Schnittstelle bis zu 8 Lese-/Eingabeeinheiten vom gleichen Typ betrieben werden (max. 16 Lese-/Eingabeeinheiten: 8 x ELM… + 8 x COM… je RS485-Schnittstelle = 32 Lese-/Eingabeeinheiten je Controller). Für den Betrieb des Zutrittskontrollsystems mit Lese-/Eingabeeinheiten von Siedle sind folgende Lese-/Eingabeeinheiten zulässig:

Lese-/Eingabeeinheiten	Max. Anzahl je Schnittstelle
Electronic-Key-Leser (berührungsloser Kartenleser) ELM 600-…	max. 8
Codeschloss COM 611-…	max. 8

Für jede Lese-/Eingabeeinheit vom gleichen Typ muss eine eigenen Bus-Adresse (1–8) eingestellt werden. Verschiedene Typen von Lese-/Eingabeeinheiten (z. B. ELM… und COM…) können mit der gleichen Busadresse betrieben werden. Dies ermöglicht dem Controller die beiden Lese-/Eingabeeinheiten zusätzlich als Kombi-Modul zu betreiben.
Die Einstellung erfolgt immer direkt an der Lese-/Eingabeeinheit über einen Drehschalter der sich unter dem rückseitigen Deckel neben dem Flachbandkabelanschluss befindet.

- Die Variobus-Adresseinstellung „0“ und „9“ ist nicht zulässig.
- Gleiche Typen von Lese-/Eingabeeinheiten (z. B. COM…) müssen an der gleichen RS485-Schnittstelle mit unterschiedlichen Busadressen betrieben werden.

Kombinationsbetrieb (Lese-/Eingabeeinheit)
Im Kombinationsbetrieb werden an einer RS485-Schnittstelle eine Leseeinheit und eine Eingabeeinheit mit der gleichen Vario-Bus-Adresse konfiguriert.
Der Kombinationsbetrieb ist nur im Siedle Vario-Bus möglich. Für diese Betriebsart müssen sowohl an der Leseeinheit als auch an der Eingabeeinheit die Option „Mit Tastenfeld“ konfiguriert sein. Die Identifikation ist dann abhängig von der Konfiguration wahlweise einfach (Karte oder Code) oder zweifach (Karte mit PIN) möglich.

Zutrittspunkte (Türen)
Am Secure Controller sind an vier möglichen Zutrittspunkten folgende Anschlussmöglichkeiten konfigurierbar:

Anschluss	Anzahl
Ausgang für die Ansteuerung eines Türöffnerkontakts (Wechselkontakt potentialfrei oder Spannungsausgang) je Zutrittspunkt. Details siehe Seite 10.	4
Eingang für die Zustandsüberwachung eines Zutrittspunkts per potentialfreien Rückmeldekontakt (Eingangskontakt 2-pol.).	4
Eingang für den Betrieb eines (bauseitigen) potentialfreien Türöffnertasters (Eingangskontakt 2-pol.)	4
Steuerausgang	3

Identifikationsmittel
Für den Betrieb des Zutrittskontrollsystems mit Lese-/Eingabeeinheiten von Siedle sind folgende Siedle-Identifikationsmittel konfigurierbar:

Lese-/Eingabeeinheiten	Identifikationsmittel
Leseeinheit ELM 600-…	Electronic-Key (EK 600-…)
	Electronic-Key-Card (EKC 600-…)
Eingabeeinheit COM 611-…	Numerischer Zugangscode
Kombi-Betrieb mit Leseeinheit + Eingabeeinheit (ELM 600-… + COM 611-…)	Electronic-Key / Elektronic-Key-Card + numerische PIN

Mit dem Secure Controller sind folgende Betriebsformen im Netzwerk möglich:

Einzelbetrieb
Betrieb eines einzelnen Controllers.

Für den Einzelbetrieb eines Controllers im Netzwerk gilt: Der Controller arbeitet im Auslieferungszustand bereits im Einzelbetrieb und kann sofort in Betrieb genommen werden.

Autonomer Einzelbetrieb (mehrerer Controller im gleichen Netzwerk)
Betrieb mehrerer Controller voneinander unabhängig, auch im gleichen Netzwerksegment.

Für den autonomen Einzelbetrieb mehrerer Controller im gleichen Netzwerksegment gilt:
• Der Ausfall eines Controllers hat auf die Betriebsbereitschaft und den Funktionsumfang der anderen Controller keine Auswirkung.
• Jeder Controller arbeitet im Auslieferungszustand bereits im Einzelbetrieb und kann jeweils unabhängig von den anderen Controllern in Betrieb genommen werden.
• Jeder Controller muss eigenständig und unabhängig von den anderen Controllern konfiguriert werden!

Betrieb mit Controller-Erweiterung
Controller mit bis zu 4 Controller-Erweiterungen je Controller (alle Betriebsformen).

Für den Betrieb mit Controller-Erweiterung gilt:
• Max. 4 Erweiterungen je Controller.
• Max. 2 Erweiterungen je RS485-Schnittstelle (OSDP) eines Controllers.
• Max. 12 Türen konfigurierbar (je Controller mit 4 Erweiterungen).
• Bei mehreren Controllern im Geräteverbund erfolgt die Einbindung und die Konfiguration der Erweiterungen zentral über den primären Controller.
• Beim Ausfall eines Controllers mit Erweiterungen sind alle daran betriebenen Komponenten des Zutrittskontrollsystems nicht nutzbar.

Betrieb im Geräteverbund
Betrieb mehrerer Controller in einem Geräteverbund.

Für den Betrieb mehrerer Controller im Verbund innerhalb eines Netzwerks (LAN) gilt:
• Max. 64 Controller sind miteinander vernetzbar (1 primäres Gerät, 63 sekundäre Geräte)
• Max. 1 primärer Controller je Verbund.
• Die Konfiguration erfolgt im Verbund zentral über den primären Controller.
• Der Datenaustausch (Synchronisation) im Verbund erfolgt im Betrieb gesichert und voll automatisch. Muss aber für die Synchronisation der Inbetriebnahme-Konfiguration einmalig manuell ausgeführt werden.
• Jeder Controller im Verbund kann als primäres Gerät ausgewählt werden. Ein Wechsel im laufenden Betrieb ist ebenfalls möglich. Der als primäres Gerät ausgewählte Controller führt einen Neustart durch und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.
• Alle Controller im Verbund müssen sich im gleichen Netzwerk-Segment befinden. Im Betrieb über mehrere Netzwerk-Segmente hinweg, muss das Routing im Netzwerk für die Controller entsprechend konfiguriert sein.
• Beim Ausfall eines Controllers im Verbund (auch das primäre Gerät), ist das Zutrittskontrollsystem (bis auf die Ein- und Ausgänge des ausgefallenen Controllers) weiterhin voll nutzbar.
• Bei Austausch eines Controllers innerhalb des Verbunds, erfolgt die Wiederherstellung der Controller-Konfiguration über die Daten-Nachbildung (Replikation) aus dem Controller-Verbund.

Inbetriebnahme-Wizard oder manuelle Konfiguration
Nach der Konfiguration von Sprache der Benutzeroberfläche, Datum/Uhrzeit sowie den Netzwerkeinstellungen, erfolgt die eigentliche Konfiguration des Zutrittskontrollsystems. Hierfür verfügt der Controller über zwei Möglichkeiten zur Inbetriebnahme:
• Inbetriebnahme-Wizard: Mit dem Inbetriebnahme-Wizard erfolgt die Gerätekonfiguration (Zutrittspunkte und Lese-/Eingabeeinheiten inklusive aller notwendigen Voreinstellungen) geführt in wenigen Schritten. Mit den optionalen Detaileinstellungen können bei Bedarf punktuell weitere spezifische Einstellungen manuell vorgenommen werden.
• Voll manuelle Inbetriebnahme: Bei dieser Form der Inbetriebnahme erfolgen alle notwendigen Konfigurationsschritte ungeführt und müssen manuell durchlaufen werden.

Die Konfiguration der Benutzer des Zutrittskontrollsystems erfolgt in beiden Fällen manuell. Es besteht die Möglichkeit zum Datenimport per Datei (im Format: *.Json, *.csv).

Wochenprogramme
Im Controller sind drei Arten von Wochenprogrammen konfigurierbar:
• Wochenprogramm Tür: Zeitgesteuerte Zutrittskontrolle eines Zutrittspunkt unabhängig von Benutzern.
• Wochenprogramm Benutzer: Zeitgesteuerte Zutrittskontrolle eines Benutzers an einem oder mehreren Zutrittspunkten (Türen).
• Wochenprogramm Allgemein: Zeitsteuerung von Ausgängen (Schaltkontakten) und konfigurierten Logik-Operationen aus Ausgängen / Eingängen und Ausgängen.

Je Controller bzw. je System mit mehreren Controllern (Geräteverbund) sind je Art des Wochenprogramms bis zu 1.000 Wochenprogramme konfigurierbar.

Wochenprogramm Tür
Bei einem neu angelegten Wochenprogramm befindet sich der Wochenplan immer vollständig im Modus „Normal“ (Öffnung eines Zutrittspunkts per Identifikationsmittel erforderlich). Andere Modi müssen hinzu konfiguriert werden (z. B. Gesperrt).

Wochenprogramm Benutzer
Bei einem neu angelegten Wochenprogramm befindet sich der Wochenplan immer vollständig im Modus „Kein Zutritt“ (Öffnung des Zutrittspunkts nicht erlaubt). Andere Modi müssen hinzu konfiguriert werden (z. B. Zutritt mit Karte oder Code).
Im Auslieferungszustand sind drei Benutzer-Wochenprogramme vorkonfiguriert:
• „Kein Zutritt“
• „Zutritt mit Karte oder Code und PIN“
• „Zutritt mit Karte oder Code“

Wochenprogramm Allgemein
Bei einem neu angelegten Allgemein-Wochenprogramm befindet sich der Wochenplan immer vollständig im Modus „Aus“. Der Modus „Ein“ muss hinzu konfiguriert werden.

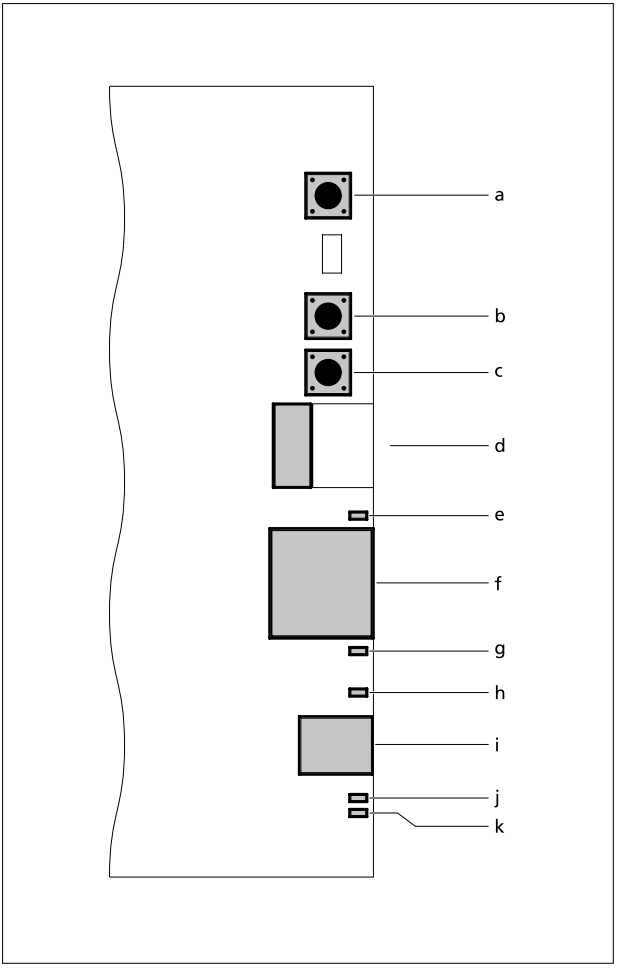
Vorrangregelung
Im Zutrittskontrollsystem gelten folgende Vorrang-Regelungen (Reihenfolge gemäß Vorrang):
1 Globale Türsteuerung
2 Wochenprogramm Tür
3 Wochenprogramm Benutzer
4 Wochenprogramm Allgemein
5 Kein Wochenprogramm

Benutzer
Benutzer die das Zutrittskontrollsystem nutzen, sind bei Anlage alle gleichberechtigt. Für Personen, für die erweiterte Zutrittsberechtigungen erforderlich sind, bestehen folgende Möglichkeiten:
• Individuell konfigurierte Wochenprogramme
• Zusätzliche Benutzer-Optionen für erweiterte Berechtigungen

Geräteübersicht

Anzeige-, Bedien- und Anschlusselemente

Am Secure Controller befinden sich mehrere Anzeige-, Bedien- und Anschlusselemente für die Inbetriebnahme und/oder den Betrieb. Für die Sicht / den Zugriff auf die meisten Elemente muss das Gehäuse des Secure-Controllers geöffnet sein. Alle Elemente befinden sich auf der Seite des Controllers an der der RJ45-Anschluss angebracht ist.



Übersicht

a Funktionstaste SD-Boot: Systemstart über SD-Karte auslösen

b Funktionstaste RESET: Neustart des Controllers

c Benutzertaste:
- Konfigurierbare Funktion für den geschützten Zugriff auf die Administrationsoberfläche (Web-Control) nur bei Tastendruck.
- Hardware-seitige Wiederherstellung der Werkseinstellungen.
- Hardware-seitige Rücksetzung der Netzwerkeinstellungen / Aktivierung einer vorkonfigurierten Netzwerkeinstellung.

d Steckplatz für Micro-SD-Karte

e LED (grün): Status-LED für die Anzeige der Datenübertragung. Blinkt/flackert die LED werden Daten übertragen.

f RJ45-Anschluss: Netzwerkanschluss (LAN)

g LED (gelb): Anzeige ist aktiv, wenn eine funktionsfähige hardwareseitige Verbindung zum Netzwerk besteht.

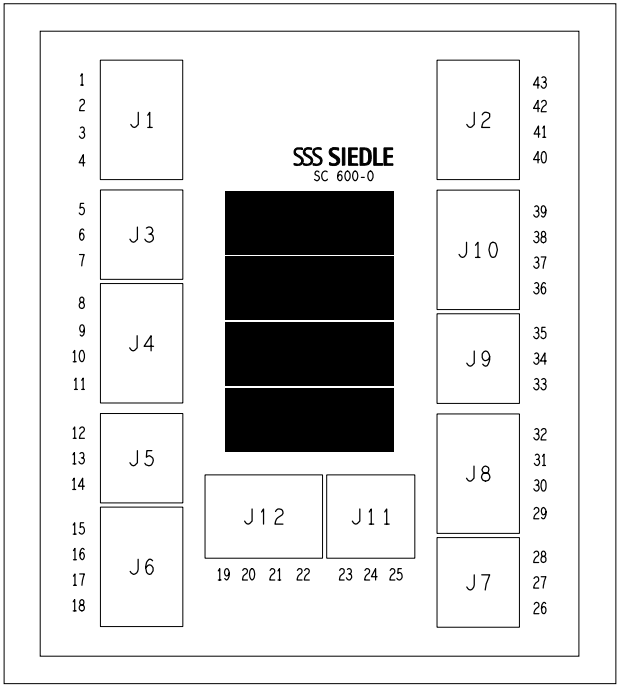
h LED (grün): Anzeige des Betriebszustands des Controllers:
- Normalbetrieb: blinkt (1 s)
- Firmware-Update: blinkt (0,1 s)
- DHCP-Abfrage: Aus
- Fehler (System): blinkt (1 s)
- Fehler (Controller): Aus

i Mini-USB-Port (USB 2.0): Anschluss für Service-Zwecke

j LED (rot): Anzeige Systemstatus des Controllers:
- Normalbetrieb: aus
- Firmware-Update: blinkt (0,5 s)
- DHCP-Abfrage: Ein (0,1 s blinkend); Aus (2 s)
- Fehler (System): blinkt (1 s)
- Fehler (Controller): blinkt (0,5 s) / Pause (2 s)

k LED (grün): Betriebsspannungsanzeige 12 V DC

Am Secure Controller befinden sich mehrere Anschlussklemmen. Für die Sicht / den Zugriff muss das Gehäuse des Secure-Controllers geöffnet sein.



Übersicht Anschlussklemmen	
J1	Lese-/Eingabeeinheiten (Schnittstelle RS485-A)
J2	Lese-/Eingabeeinheiten (Schnittstelle RS485-B)
J3	Eingang Tür 1 (Rückmeldekontakt und Türöffnertaster)
J4	Ausgang Tür 1 (Tür-Relais 1: Potentialfreier Relaiskontakt)
J5	Eingang Tür 2 (Rückmeldekontakt und Türöffnertaster)
J6	Ausgang Tür 2 (Tür-Relais 2: Potentialfreier Relaiskontakt)
J7	Eingang Tür 3 (Rückmeldekontakt und Türöffnertaster)
J8	Ausgang Tür 3 (Tür-Relais 3: Potentialfreier Relaiskontakt)
J9	Eingang Tür 4 (Rückmeldekontakt und Türöffnertaster)
J10	Ausgang Tür 4 (Tür-Relais 4: Potentialfreier Relaiskontakt)
J11	Ausgang 1–3 (Steuerausgänge für Kleinverbraucher)
J12	Spannungsversorgung (externe Versorgung des Controllers) und Spannungsausgang (Versorgung von Zusatzgeräten)

Anschlussbelegung

Leiste	Anschluss	Beschriftung	Erläuterung
J1	1	D–	Datenleitung
	2	D+	RS485-A
	3	GND	Versorgung von
	4	OUT+12…	OSDP-Modulen
J2	40	D–	Datenleitung
	41	D+	RS485-B
	42	GND	Versorgung für
	43	OUT+12…	OSDP-Module
J3	5	EXIT	Taster (TÖ)
	6	GND	Gemein. Ansch.
	7	CONTACT	Meldekontakt
J4	8	NO	Tür-Relais 1
	9	COM	mit Wechsler
	10	NC	(NO/COM/NC)
	11	GND	–
J5	12	EXIT	Taster (TÖ)
	13	GND	Gemein. Ansch.
	14	CONTACT	Meldekontakt
J6	15	NO	Tür-Relais 2
	16	COM	mit Wechsler
	17	NC	(NO/COM/NC)
	18	GND	–
J7	26	EXIT	Taster (TÖ)
	27	GND	Gemein. Ansch.
	28	CONTACT	Meldekontakt
J8	29	NO	Tür-Relais 3
	30	COM	mit Wechsler
	31	NC	(NO/COM/NC)
	32	GND	–
J9	33	EXIT	Taster (TÖ)
	34	GND	Gemein. Ansch.
	35	CONTACT	Meldekontakt
J10	36	NO	Tür-Relais 4
	37	COM	mit Wechsler
	38	NC	(NO/COM/NC)
	39	GND	–
J11	23	OUT-3	Ausgang 3
	24	OUT-2	Ausgang 2
	25	OUT-1	Ausgang 1
J12	19	Vin+24V	Versorgung
	20	GND	14–30 V DC
	21	Vout+12V	Ausgang
	22	GND	12 V DC

Geräteübersicht
Steckbrücken (Jumper)

Auf den beiden Leiterplatten des Secure Controller befinden sich mehrere Stiftleisten mit Steckbrücken (Jumper) für die Aktivierung/Deaktivierung verschiedener Funktionen. Im Auslieferungszustand sind die Relais-Kontakte der Tür-Relais 1–4 potentialfrei und die Spannungsausgänge der Schnittstellen RS485-A/B deaktiviert.

Jede Steckbrücke befindet sich bereits an der entsprechenden Stiftleiste der Leiterplatte mit offener oder geschlossener Verbindung:

- offen (Steckbrücke nicht gesteckt): Die Steckbrücke ist nur einpolig bzw. nicht mit zwei Kontakten einer Stiftleiste verbunden (Funktion deaktiviert / Option festgelegt).
- geschlossen (Steckbrücke gesteckt): Die Steckbrücke ist zweipolig bzw. mit zwei Kontakten einer Stiftleiste verbunden (Funktion aktiviert / Option festgelegt).

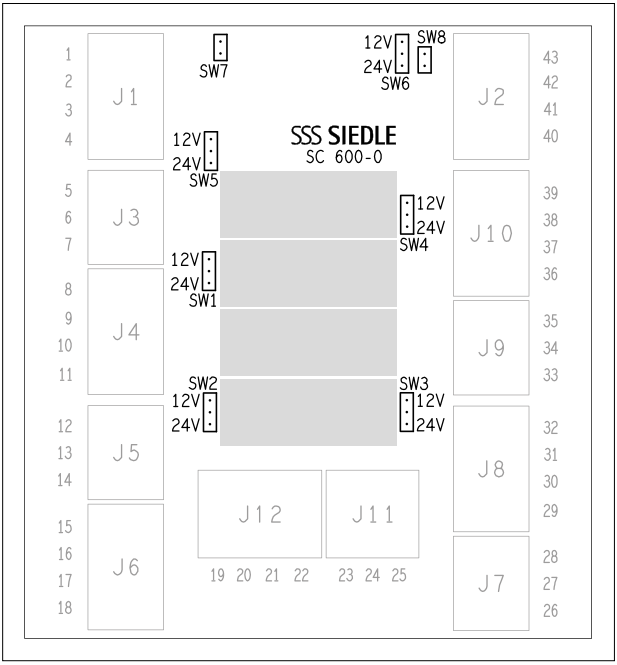
Übersicht – Obere Leiterplatte: E/A-Anschlusseinheit

Stiftleiste	Beschreibung	Verbindung (Auslieferungszustand)
SW1 (Stiftleiste: 3-polig)	Tür-Relais 1: Betrieb als Spannungsausgang – wahlweise mit 12 oder 24 V DC an Anschluss 9 (COM/+) und 11 (GND/–)	offen (deaktiviert: Relais-Kontakte potentialfrei)
SW2 (Stiftleiste: 3-polig)	Tür-Relais 2: Betrieb als Spannungsausgang – wahlweise mit 12 oder 24 V DC an Anschluss 16 (COM/+) und 18 (GND/–)	offen (deaktiviert: Relais-Kontakte potentialfrei)
SW3 (Stiftleiste: 3-polig)	Tür-Relais 3: Betrieb als Spannungsausgang – wahlweise mit 12 oder 24 V DC an Anschluss 16 (COM/+) und 18 (GND/–)	offen (deaktiviert: Relais-Kontakte potentialfrei)
SW4 (Stiftleiste: 3-polig)	Tür-Relais 4: Betrieb als Spannungsausgang – wahlweise mit 12 oder 24 V DC an Anschluss 37 (COM/+) und 39 (GND/–)	offen (deaktiviert: Relais-Kontakte potentialfrei)
SW5 (Stiftleiste: 3-polig)	Schnittstelle RS485-A: Betrieb mit Spannungsversorgung wahlweise mit 12 oder 24 V DC an Anschluss 4 (OUT/+) und 3 (GND/–)	offen (deaktiviert)
SW6 (Stiftleiste: 3-polig)	Schnittstelle RS485-B: Betrieb mit Spannungsversorgung wahlweise mit 12 oder 24 V DC an Anschluss 43 (OUT/+) und 42 (GND/–)	offen (deaktiviert)
SW7 (Stiftleiste: 2-polig)	Schnittstelle RS485-A: Betrieb der Datenleitung mit Abschlusswiderstand (240 Ohm)	offen (deaktiviert)
SW8 (Stiftleiste: 2-polig)	Schnittstelle RS485-B: Betrieb der Datenleitung mit Abschlusswiderstand (240 Ohm)	offen (deaktiviert)

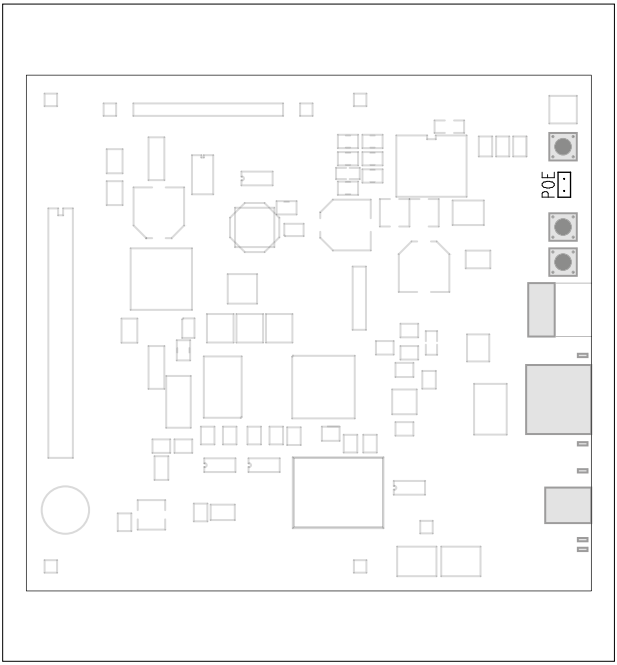
Übersicht – Untere Leiterplatte: Prozessoreinheit

Stiftleiste	Beschreibung	Verbindung (Auslieferungszustand)
POE (Stiftleiste: 2-polig)	Auswählbare PoE-Versorgungsstandard: • offen: Versorgung mit „PoE“ (max. 12,95 W) • geschlossen: Versorgung mit „PoE+“ (max. 25,5 W)	offen (PoE-Versorgung)

Ansicht Steckbrücken – Obere Leiterplatte: E/A-Anschlusseinheit



Ansicht Steckbrücken – Untere Leiterplatte: Prozessoreinheit



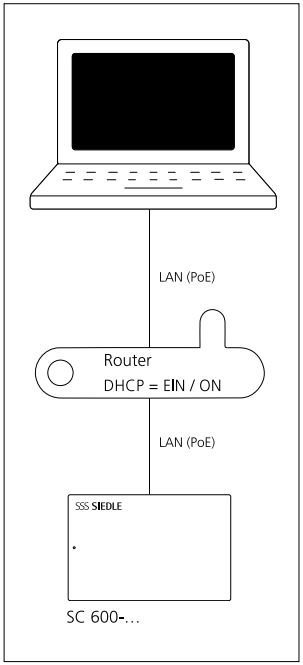
Versorgung	**Erläuterung**
Spannungsversorgung	• Externe Spannungsversorgung (14–28 V DC – über Anschlussklemmen (Vin / GND)) • PoE (IEEE 802.3af – Type 1, Klasse 3 , max. 12,95 W) **Wichtig!** • Der Secure Controller darf nicht gleichzeitig mit PoE/PoE+ versorgt werden, wenn die Versorgung bereits über eine externe Spannungsversorgung erfolgt (keine Redundanz/Doppelversorgung)! • Werden (mehrere) Secure Controller und Controller-Erweiterung(en) (Secure Extension) von verschiedenen Spannungsquellen (z. B. mehrere PSM… oder PSM… und PoE) versorgt, müssen die Bezugspotentiale (Masse) aller im Verbund betriebenen Controller und Erweiterungen miteinander verbunden sein (gemeinsames Masse-Potential aller Komponenten).
Versorgungsgrenzen	Die am Secure Controller verfügbare Versorgungsleistung für angeschlossene Komponenten ist abhängig von der verwendeten Spannungsversorgung:

Spannungsversorgung	**Max. Versorgungsleistung**
PoE (12,5 W)	10 W
Externe Spannungsversorgung mit PSM 1 12 24 (24 V DC, 0,5 A)	10 W
PoE+ (25,5 W)	20 W

Bei der Planung und Ausführung ist darauf zu achten, dass die verfügbare Versorgungsleistung des Secure Controllers zu keinem Zeitpunkt überschritten wird!

Eingänge	
Strombegrenzer (digitaler Eingang)	• Digitaler Eingang (wird systemintern innerhalb des Controllers verwendet)
Türkontakt 1–4 (symmetrischer Eingang) Türöffnertaste 1–2 (symmetrischer Eingang)	• Eingänge mit optional konfigurierbarer Leitungsüberwachung (Linienüberwachung) und konfigurierbarem Widerstandsnetzwerk gemäß Werteauswahl • Die Konfiguration erfolgt über die Administrationsoberfläche (siehe „Konfiguration der Eingänge/Ausgänge“ > „Leitungsüberwachung“) • Keine Zustandsänderung der Eingänge aufgrund einer anliegenden Fremdspannung (max. zulässige anliegende Fremdspannung aus angeschlossener Eingangsbeschaltung: 30 V DC)
Türöffnertaste 3–4 (digitaler Eingang)	• Eingänge ohne Leitungsüberwachung (Linienüberwachung) • Keine Zustandsänderung der Eingänge aufgrund einer anliegenden Fremdspannung (max. zulässige anliegende Fremdspannung aus angeschlossener Eingangsbeschaltung: 30 V DC) • Einzelne Merkmale nicht konfigurierbar.
Ausgänge	
Spannungsausgang	Abhängig von der Versorgung des Controllers, ist für den Anschluss und Betrieb von Zusatzgeräten folgende Versorgung durch den Controller möglich (max. 10 Watt): • Controller mit externer Spannungsversorgung: 12 V DC, max. 800 mA • Controller mit PoE-Versorgung: 24 V DC, max. 400 mA)
Tür-Relais 1–4	Potentialfreier Schaltkontakt (Wechsler: 30 V DC, 10 A) oder Spannungsausgang (Details siehe Seite 10)
Ausgang 1–3	Steuerausgang (Open-Drain-Ausgang, max. 750 mA je Ausgang) für die Steuerung von Kleinverbrauchern mit externer Spannungsversorgung mit max. 30 V DC

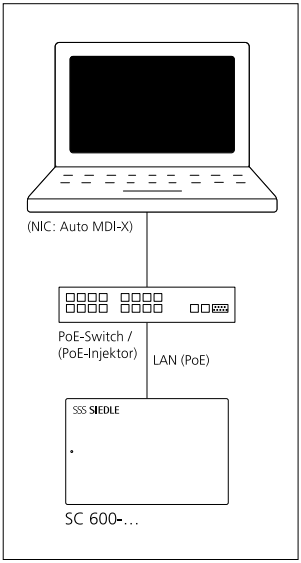
Verbindung über Netzwerk (LAN)
LAN-Verbindung über ein bestehendes Netzwerk (Router/Managed Switch/Server) mit aktivem DHCP-Server.



Voraussetzungen
• Controller und Laptop sind betriebsbereit.
• Das Netzwerk ist betriebsbereit.
• Controller und Laptop sind mit jeweils einem Netzwerkkabel über ein kabelgebundenes lokales Netzwerk (LAN – Router/Switch/Server) miteinander verbunden. Erfolgt die Spannungsversorgung des Controllers über Power over Ethernet (PoE) so ist zusätzlich ein PoE-Injektor erforderlich.
• Die Netzwerkeinstellungen des Controllers befinden sich im Auslieferungszustand.
• An Ihrem Laptop ist der Netzwerkanschluss (RJ45/LAN) mit „IP-Adresse automatisch beziehen“ konfiguriert.

Vorgehensweise
1 IP-Adresse ermitteln, wie im folgenden Kapitel „IP-Adresse des Controllers ermitteln“ beschrieben.

Direkte Verbindung
Direkte Verbindung zwischen Controller und Laptop per Netzwerkkabel oder über einen PoE-Switch/Injektor.



Voraussetzungen
• Controller und Laptop sind betriebsbereit und miteinander verbunden per Netzwerkkabel direkt (bei externer Spannungsversorgung), oder über einen PoE-Switch/Injektor.
• Die Netzwerkeinstellungen des Secure Controllers befinden sich im Auslieferungszustand.
• An Ihrem Laptop ist der Netzwerkanschluss (RJ45/LAN) mit der festen IP-Adresse konfiguriert: IP-Adresse: 192.168.1.200, Subnetzmaske: 255.255.255.0.
• Verfügt der Netzwerkanschluss ihres Laptops über die Funktion „Auto-MDI-X“, ist eine direkte Verbindung mit dem Secure Controller per Netzwerkkabel oder PoE-Injektor möglich.

Vorgehensweise
1 IP-Adresse ermitteln, wie im folgenden Kapitel „IP-Adresse des Controllers ermitteln“ beschrieben.

Die Konfiguration des Secure Controllers erfolgt über dessen Administrationsoberfläche.
Für den Zugriff auf die Administrationsoberfläche und die Konfiguration benötigen Sie einen Laptop mit aktuellem Webbrowser, der über das lokale Netzwerk (LAN) mit dem Controller verbunden ist.
Der Zugriff auf den Controller ist wahlweise über das Netzwerk mit dem Programm „Tech-Tool" möglich oder bei direkter Verbindung zwischen Controller und Laptop per manuellem Aufruf der IP-Adresse.

Aufruf der IP-Adresse des Controllers
Der Controller ist über eine verschlüsselte Verbindung mit seiner IP-Adresse (https://<IP-Adresse>) erreichbar.
Wir empfehlen, den Controllers immer per „https" über eine verschlüsselte Verbindung aufzurufen.

Verbindung über Netzwerk – IP-Adresse mit dem „Tech-Tool" ermitteln
Das Tech-Tool erhalten Sie im Downloadbereich der Siedle-Webseite unter www.siedle.de > Suche: „Tech-Tool". Mit dem Tool auf ihrem Laptop können Sie die IP-Adresse des Controllers im Netzwerk ermitteln und bei Bedarf anpassen.

Wichtig!
• Das Tool kann den Controller nur dann im Netzwerk finden, wenn sich Laptop und Controller im selben Netzwerk-Segment (Subnetz) des Netzwerks befinden (d. h. die ersten drei Blöcke der lokalen IP-Adresse müssen bei Controller und Laptop gleich sein – z. B. 192.168.178.xxx).
• Ist ein Zugriff auf den Controller unter diesen Voraussetzungen nicht möglich, wird alternativ die Vorgehensweise „Direkte Verbindung – IP-Adresse des Controllers manuell ermitteln" empfohlen.

Vorgehensweise
1 Tech-Tool auf dem Laptop installieren.
2 Tech-Tool auf dem Laptop „als Administrator ausführen" (per Rechtsklick auf das Programm-Symbol).
3 Windows-Betriebssystem-Meldung mit „Ja" bestätigen. Diese Meldung erscheint ggf. in Abhängigkeit von den Einstellungen der Benutzerkontensteuerung.
4 Auf der Tech-Tool-Programmoberfläche „Manage" öffnen.
5 Im geöffneten Kontextmenü „Configuration" ausführen.
6 „Search" öffnen.
7 Im geöffneten Kontextmenü „All" ausführen, um die Controller-Suche anzustoßen.
8 Gefundene Controller werden tabellarisch aufgelistet.
9 Controller in der Liste auswählen.
10 „Web Config" ausführen, um die Administrationsoberfläche des Controllers zu öffnen.

Direkte Verbindung – Statische IP-Adresse konfigurieren
Durch Betätigung der „Benutzertaste" am Secure Controller können die Netzwerkeinstellungen von DHCP-Betrieb in den Betrieb mit der vorkonfigurierter IP-Adresse 192.168.1.100 geändert werden.
Für die Betätigung der „Benutzertaste" muss das Gehäuse des Secure-Controllers geöffnet sein.
Details zur „Benutzertaste" und LED-Signalisierung siehe Seite 8.

Vorgehensweise
1 Gehäuse des Secure Controllers öffnen
2 „Benutzertaste" innerhalb von fünf Sekunden fünf mal betätigen.
3 Die beiden LEDs für die Anzeige des Betriebszustands (grün) und des Systemstatus (rot) blinken.
4 Ein Signalton ertönt, der sich bis zu drei Mal wiederholen wird (Intervall: 3 s Signalton gefolgt von 3 s Pause).

Erfolgt bis zum letzten Signalton keine Tastenbetätigung, endet der Vorgang automatisch ohne eine Systemveränderung durchzuführen.

5 Benutzertaste beim dritten Signalton betätigen und halten, bis der Signalton endet.
6 Die Netzwerkeinstellungen werden auf den Betrieb mit statischer IP-Adresse geändert. Der Controller wird automatisch neu gestartet und ist nach ca. einer Minute wieder über die Anmeldeseite unter https://192.168.1.100 erreichbar.

Kennwort neu vergeben

Mit der ersten Anmeldung am Secure Controller öffnet sich bei jedem Benutzerkonto immer zuerst der Kennwort-Änderungsdialog. Bitte vergeben Sie zuerst ein neues Kennwort für das Konto „root“.

Zugangsdaten (bei Auslieferung)

Konto/ Benutzername	**Kennwort**
root	78120Furtwangen!

Vorgehensweise
1 Auf der Anmeldeseite des Controllers mit den Zugangsdaten des Konto „root“ anmelden.
2 Bei „Kennwort“ das bisherige Kennwort (Auslieferungszustand: „78120Furtwangen!“) eingeben.
3 „Neues Kennwort“ eingeben.
4 „Neues Kennwort wiederholen“.
5 „Speichern und Schließen“ ausführen.
6 „Ausloggen“ ausführen.
7 Kennwort für die Übergabe an den Betreiber notieren.

Neues Kennwort (root)

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Bitte vergeben Sie ein neues Kennwort für das Konto „Service“.

Zugangsdaten (bei Auslieferung)

Konto/ Benutzername	**Kennwort**
Service	Siedle1234

Vorgehensweise
8 Auf der Anmeldeseite des Controllers mit den Zugangsdaten des Kontos „Service“ anmelden.
9 Bei „Kennwort“ das bisherige Kennwort (Auslieferungszustand: „Siedle1234“) eingeben.
10 „Neues Kennwort“ eingeben.
11 „Neues Kennwort wiederholen“.
12 „Speichern und Schließen“ ausführen.
13 Kennwort für die Übergabe an den Betreiber notieren.

Neues Kennwort (Service)

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Für die Inbetriebnahme des Controllers ist die Anmeldung mit dem Konto „Service“ erforderlich.

Sprache

Die Administrationsoberfläche des Controllers kann in verschiedenen Sprachen bedient werden. Die Sprache kann jederzeit umgestellt werden. Mit der Umstellung der Sprache führt der Controller einen Neustart durch. Im Auslieferungszustand ist die Sprache „Deutsch“ voreingestellt.

Vorgehensweise
1 Auf der Startseite „System“ öffnen.
2 „Administration“ öffnen.
3 „Sprache“ öffnen.
4 Gewünschte Sprache auswählen.
5 „Ausgewählte Sprache aktivieren“ ausführen.
6 Der Controller führt einen Neustart durch und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.
7 Anmelden mit den neuen Zugangsdaten mit dem Konto „Service“.

Für den ordnungsgemäßen Betrieb des Controllers ist eine genaue Zeitangabe (Datum/Uhrzeit) erforderlich.
Abhängig von der Konfiguration kann der Controller seine Zeitangabe von einem Zeitserver (NTP-Server) aus dem lokalen Netzwerk oder aus dem Internet beziehen. Alternativ ist ein manueller Eintrag der Zeitangabe möglich (nicht empfohlen).

Vorgehensweise
1 Auf der Startseite „System“ öffnen.
2 „Administration“ öffnen.
3 „Datum/Uhrzeit“ öffnen.
4 Inhalte prüfen und ggf. anpassen (siehe „Konfigurationshilfe: Datum/Uhrzeit“).

Hinweis
Für den Betrieb mit einem oder mehrerer Zeitserver sind folgende Eigenschaften zu konfigurieren:
• Zeitzone
• Zeitserver 1, 2, …

Konfigurationshilfe: Datum/Uhrzeit

Datum/Uhrzeit	Erläuterung	Auslieferungszustand
Datumsformat	Optionsfeld wie das Datum in der Administrationsoberfläche des Controllers angezeigt werden soll. Beispiel: „dd/mm/yyyy“ => Tag/Monat/Jahr (z. B. 26/02/2021)	„dd/mm/yyyy“
Zeitformat	Optionsfeld wie die Uhrzeit in der Administrationsoberfläche des Controllers angezeigt werden soll. Beispiel: „hh:mm:ss“ => Stunde/Minute/Sekunde (z. B. 16:29:59)	„hh:mm:ss“
Datum	Feld, das automatisch mit den Angaben des Zeitservers befüllt wird. Alternativ kann das Datum manuell gesetzt werden.	–
Uhrzeit	Feld, das automatisch mit den Angaben des Zeitservers befüllt wird. Alternativ kann die Uhrzeit manuell gesetzt werden.	–
Zeitzone	Optionsfeld, für die Auswahl der regional gültigen Zeitzone (z. B. Deutschland => regional gültige Zeitzone: „Europa/Berlin“)	„Europe/Paris“
Zeitserverstatus	Nicht änderbares Informationsfeld über den Zeitserver-Status: • „Verbunden“: Der Controller bezieht seine Zeitangabe automatisch über den/die konfigurierten Zeitserver. Alle Zeitserver sind erreichbar. • „Verbunden (nicht alle)“: Der Controller bezieht seine Zeitangabe automatisch über den/die konfigurierten Zeitserver. Mindestens ein Zeitserver aus dem eingetragenen Pool ist nicht erreichbar. • „Nicht erreichbar“: Die Zeitserveradresse ist über das Netzwerk nicht erreichbar. Die Adresse ist entweder fehlerhaft oder der NTP-Server ist offline. • „Nicht verbunden“: Die konfigurierten Zeitserver sind über das Netzwerk nicht erreichbar oder offline. • „Nicht konfiguriert“: Es ist kein Zeitserver konfiguriert.	–

Konfigurationshilfe: Datum/Uhrzeit

Datum/Uhrzeit	Erläuterung	Auslieferungszustand
Zeitserver 1	IP-Adresse oder URL eines Zeitserver aus dem lokalen Netzwerk oder aus dem Internet (z. B. IP-Adresse eines Zeitservers im lokalen Netzwerk). Wir empfehlen die Konfiguration verschiedener interner/externer Zeitserver/ Zeitserver-Pools.	„uk.pool.ntp.org“
Zeitserver 2	Alternativ nutzbare IP-Adressen oder URL weiterer Zeitserver aus dem lokalen Netzwerk oder aus dem Internet.	–
Zeitserver 3		–
Zeitserver 4		–

Der Controller ist im Auslieferungszustand für den automatischen Bezug der Netzwerkkonfiguration per DHCP vorkonfiguriert (DHCP-Client ist aktiv).

Vorgehensweise
1 Auf der Startseite „System“ öffnen.
2 „Netzwerk“ öffnen.
3 Inhalte prüfen und ggf. anpassen (siehe „Konfigurationshilfe Netzwerk“):
- „IPv4-Verbindung“
- „Web“
- „Systemzugriff“

4 „Speichern“ ausführen.

Konfigurationshilfe: Netzwerk

IPv4-Verbindung	**Erläuterung**	**Auslieferungszustand**
Hostname	Bezeichnung des Controllers im Netzwerk. Der hier vergebene Name dient auch zur Identifikation verschiedener Controller im primären Controller bei Betrieb im Geräteverbund.	SC-600_…
DHCP	Option, ob der Controller seine Netzwerkkonfiguration aus dem Netzwerk zugewiesen bekommt (insofern das Netzwerk hierfür eingerichtet ist). Ist diese Option deaktiviert, muss die Netzwerkkonfiguration manuell durchgeführt werden.	aktiviert
IP-Adresse	IPv4-Adresse der Netzwerkschnittstelle des Controllers.	–
Subnetzmaske	Beschriebenes Netzwerksegment mit dem diese Netzwerkschnittstelle verbunden ist.	–
Standardgateway	IP-Adresse des Routers/Schnittstelle des Netzwerk (zu anderen Netzwerken oder dem Internet), mit dem diese Netzwerkschnittstelle verbunden ist.	–
Bevorzugter DNS-Server	Bevorzugt zu verwendende IP-Adresse des DNS-Servers des Netzwerk, mit dem diese Netzwerkschnittstelle verbunden ist.	–
Alternativer DNS-Server	Alternativ zu verwendende IP-Adresse des DNS-Servers des Netzwerk, mit dem diese Netzwerkschnittstelle verbunden ist.	–
MAC-Adresse	Eindeutige Hardware-Adresse des Controllers.	–
Manuell konfigurieren	Option, um die Einstellungen „Link-Geschwindigkeit“ und „Duplex“, manuell verändern zu können.	deaktiviert
Verbindungsgeschwindigkeit	Über das Netzwerk automatisch ausgehandelte Datenübertragungsrate zwischen Controller und Netzwerk. Es wird immer der bestmögliche nutzbare Wert im Netzwerk ausgewählt.	–

Konfigurationshilfe: Netzwerk

IPv4-Verbindung	Erläuterung	Auslieferungszustand
Duplex	Über das Netzwerk automatisch ausgehandelte Betriebsart der Datenübermittlung zwischen Controller und Netzwerk: • „Voll-Duplex“: Gleichzeitige Datenübertragung (Senden und Empfangen) • „Halb-Duplex“: Zeitlich wechselseitige Datenübertragung in jeweils eine Richtung (Senden oder Empfangen).	–
Web		
HTTP-Port (80)	Netzwerk-Port für den unverschlüsselten Aufruf des Controllers (http://[IP-Adresse des Controllers])	–
HTTPS-Port (443)	Netzwerk-Port für den verschlüsselten Aufruf des Controllers (https://[IP-Adresse des Controllers])	„443“
Zugriff auf die Systemverwaltung	Betriebsart über die Erreichbarkeit der Systemadministration des Controllers im Netzwerk: • „Immer“: Die Systemadministration des Controllers kann jederzeit aufgerufen werden. • „Nur bei offenem Gehäuse“: Der Zugriff auf die Systemadministration des Controllers ist nur mit geöffnetem Gehäuse möglich! Ansonsten ist der Controller per Browseraufruf nicht erreichbar. Der Controller muss sich für diese Funktion in einem ausreichend ausgeleuchteten Raum befinden. • „Nur bei gedrückter Benutzertaste“: Der Zugriff auf die Systemadministration des Controllers ist nur bei gedrückter Benutzer-Taste möglich! Ansonsten ist der Controller per Browseraufruf nicht erreichbar. Eine Übersicht der Bedienelemente des Controllers finden Sie im Kapitel „Anzeige- und Bedienelemente“ auf Seite 8.	„Immer“
SSL-Zertifikat	Der Controller verfügt über ein selbstsigniertes Zertifikat um einen verschlüsselten Zugriff per Browser zu ermöglichen. Aktuelle Browser kennen (akzeptieren) ein selbstsigniertes Zertifikat (Sicherheitszertifikat, das nicht von einer Zertifizierungsstelle signiert wurde) nicht. Dadurch erscheint einmalig oder ständig eine Fehlermeldung zur Browser-Sicherheit. Kunden/Betreiber des Controllers können für den sicheren Betrieb ihr/ein eigenes Zertifikat importieren.	–

Konfigurationshilfe: Netzwerk

Systemzugriff	Erläuterung	Auslieferungszustand
SSH-Zugriff	Betriebsart, um den Controller per SSH-Client aufzurufen. Ist die Option aktiviert, ist der Controller über eine gesicherte Verbindung mit einem SSH-Client erreichbar. Wir empfehlen diese Option nach erfolgreicher Inbetriebnahme zu deaktivieren.	aktiviert
Ping-Antwort	Option, ob der Controller auf Anfragen (Ping) über das Netzwerk antworten soll oder nicht. Ist die Option aktiviert, antwortet der Controller auf jede Anfrage aus dem Netzwerk. Wir empfehlen diese Option nach erfolgreicher Inbetriebnahme zu deaktivieren, damit der Controller auf keine Such-Anfragen aus dem Netzwerk mehr reagiert.	aktiviert

Optional: Secure Extension
Controller-Erweiterung(en) konfigurieren

Allgemeine Informationen
- Jeder Siedle Secure Controller ist mit bis zu 4 Siedle Secure Extensions (SE 600-…) erweiterbar.
- Die Anbindung erfolgt über die RS485-Schnittstelle und erfordert beim Siedle Secure Controller eine Firmware ab Version 2.12.7.
- Jede RS485-Schnittstelle am Secure Controller, an der eine Secure Extension betrieben werden soll (z. B. RS485 Strang A), muss sich in der Betriebsart „OSDP" befinden.
- Jede Adresseinstellung darf je RS485-Schnittstelle ein Mal verwendet werden.

Voraussetzungen
- Die Secure Extension kann nur über den Secure Controller mitversorgt werden, wenn an der verwendeten RS485-Schnittstelle des Secure Controllers (RS485-A oder B), die externe Spannungsversorgung mit 24 V DC aktiv ist (siehe Steckbrücke SW5 oder SW6).
- Die korrekte Adresseinstellung an jeder Secure Extension ist erfolgt.
- Die Secure Extension ist über die RS485-Schnittstelle mit dem Secure Controller verbunden und betriebsbereit.

Konfiguration
- Am Secure Controller können max. 2 Erweiterungen für den vollständigen Funktionsbedarf und max. 2 Erweiterungen für den eingeschränkten Funktionsbedarf konfiguriert werden:

Funktionsbedarf	Funktionsumfang
vollständig	Alle verfügbaren Funktionen der Zutrittskontrolle für bis zu jeweils 4 Zutrittspunkte (Türen) (z. B. reguläre Zutrittskontrolle) sowie alle verfügbaren Schalt- und Steuerungsfunktionen (z. B. Aufzugssteuerung)
eingeschränkt	Schalt- und Steuerungsfunktionen ohne Zutrittspunkte (Türen)

Für die Konfiguration von bis zu 12 Zutrittspunkten (Türen) an 1 Secure Controller, müssen mindestens 2 Erweiterungen für den vollständigen Funktionsbedarf konfiguriert werden.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Konfiguration" öffnen.
4 „Eingänge/Ausgänge" öffnen.
5 „Externes E/A-Modul" öffnen.
6 Mit „Neu anlegen" in der Liste entsprechende Option gemäß „Konfigurationstabelle: Funktionsbedarf" auswählen:

Konfigurationstabelle: Funktionsbedarf

RS485-Strang	Jumper-Position SE 600-…	OSDP-Bus-Adresse	Max. Anzahl	Funktionsbedarf	Option
A (oder B)	J1	30	1	vollständig	„Tür-E/A 5-8 – Secure Extension (OSDP)"
A (oder B)	J2	31	1	vollständig	„Tür-E/A 9-12 – Secure Extension (OSDP)"
B (oder A)	J1	30	1	eingeschränkt	„Schalt-E/A Secure Extension (OSDP)"
B (oder A)	J2	31	1	eingeschränkt	„Schalt-E/A Secure Extension (OSDP)"

7 Für jede Erweiterung die Inhalte prüfen und ggf. anpassen (siehe „Konfigurationshilfe: Erweiterung“).

Hinweis
• Erweiterungen für den vollständigen Funktionsbedarf werden automatisch erkannt und für die Konfiguration muss nur noch ein Name der Erweiterung vergeben werden.
• Bei Erweiterungen für den eingeschränkten Funktionsbedarf müssen neben dem Namen der Erweiterung, zusätzlich der für die Bus-Kommunikation verwendete Bus-Strang (z. B. „RS485 Strang B“) sowie die Bus-Adresse (z. B. „30“) im Menü „OSDP-Einstellungen“ konfiguriert werden.

8 „Speichern und Schließen“ ausführen.
9 Weitere Erweiterungen nach gleicher Vorgehensweise konfigurieren.

Konfigurationshilfe: Erweiterung

Allgemein	**Erläuterung**
Name	Eindeutige/aussagekräftige Bezeichnung für diese Erweiterung. Vergeben Sie die Bezeichnung so, dass auch bei mehreren Erweiterungen eine klare Unterscheidung möglich ist.
OSDP-Einstellungen	
Bus-Kommunikation	Zuordnung der Anbindung / des Anschlusses dieser Erweiterung: • „Nicht verwendet“: Diese Erweiterung ist noch nicht angeschlossen oder nicht in Betrieb. • „RS485 Strang A“: Diese Erweiterung ist am RS485-Busstrang A angeschlossen. • „RS485 Strang B“: Diese Erweiterung ist am RS485-Busstrang B angeschlossen.
Hersteller	Nicht änderbares Informationsfeld mit der Produktbezeichnung dieser Erweiterung.
Sicherer Kanal	Nicht änderbares Informationsfeld mit Informationen über die Geräteanbindung dieser Erweiterung.
Bus-Adresse	Reservierte OSDP-Bus-Adresse dieser Erweiterung, die gemäß Jumper-Position konfiguriert werden muss: „30“ oder „31“.
Einstellungen ändern	Option, um bereits konfigurierten Einstellungen ändern zu können. Soll z. B. die Bus-Adresse geändert werden, muss die neue Bus-Adresse eingetragen und diese Option gesetzt sein, damit Änderungen mit „Speichern“ übernommen werden.
Modell	Nicht änderbares Informationsfeld mit der Modellnummer dieser Erweiterung.
Version	Nicht änderbares Informationsfeld mit der Versionsnummer dieser Erweiterung.
Seriennummer	Nicht änderbares Informationsfeld mit der Seriennummer dieser Erweiterung.
Firmwareversion	Nicht änderbares Informationsfeld mit der Firmware-Version dieser Erweiterung.
Eingangsmodus	Nicht änderbares Informationsfeld mit dem Betriebsmodus dieser Erweiterung.

Vereinfachte Inbetriebnahme eines Controllers

Empfohlener Ablauf

Der Secure Controller bietet einen großen Funktionsumfang. Mit der vereinfachten Inbetriebnahme erreichen Sie in wenigen Schritten ein betriebsbereites Zutrittskontrollsystem mit einem Controller und einem auf das Wesentliche konzentrierten Funktionsumfang: Der Zutritt ist bei erfolgreicher Identifikation jederzeit möglich.

Erste Schritte
- Kennwort neu vergeben
- Sprache
- Datum/Uhrzeit
- Netzwerk

Seite 13

↓

Controller-Erweiterung(en) konfigurieren Seite 21

↓

Inbetriebnahme-Wizard: Konfiguration der Geräte (geführte Inbetriebnahme)
- Türen (Tür-Relais für Zutrittspunkte)
- Lese-/Eingabeeinheiten
- Optional: Wochenprogramm Türen

Seite 24

↓

Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln (Karte und Code)
- Benutzer
- Identifikationsmittel (Karte und Code)

Seite 41

↓

Funktionsprüfung Seite 58

↓

Daten/Konfiguration sichern Seite 58

↓

Einweisung/Übergabe Seite 58

↓

Kennwortänderung Seite 58

↓

Benutzerverwaltung durch Kunde/Betreiber
- Planung der Benutzerverwaltung
- Optional: Konfiguration der Feiertage
- Optional: Benutzer-Wochenprogramm
- Optional: Zutrittsgruppen
- Benutzer und Identifikationsmittel (Karten und Codes)

Seite 59

Vereinfachte Inbetriebnahme eines Controllers

Inbetriebnahme-Wizard

Mit dem Inbetriebnahme-Wizard bietet der Secure Controller eine geführte Inbetriebnahme für die Konfiguration der im Zutrittskontrollsystem angebundenen Zutrittspunkte und Lese-/Eingabeeinheiten.

Bedienelemente (Wizard)

- „Verwerfen“: Abbruch des Vorgangs und Beendigung des Wizards.
- „Wizard neu starten“: Abbruch des Vorgangs und Neustart des Wizards.
- „< Zurück“: Wechsel zum vorherigen Reiter (Schritt der Inbetriebnahme).
- „> Weiter“: Wechsel zum nächsten Reiter (Schritt der Inbetriebnahme).
- „Aktualisieren“: Wiederholung der Datenabfrage im System und Erneuerung der angezeigten Informationen.
- „Konfiguration löschen“: Bestehende Konfiguration löschen (nur aktiv, bei vorhandener Konfiguration).
- „Speichern“: Sichern und ablegen der Auswahl / Eingabe(n) im System.
- „Defaults“: Rücksetzen der Änderungen.

Vorgehensweise

1 Login mit Konto „Service“.
2 Menü „System“ öffnen.
3 „Inbetriebnahme-Wizard“ schrittweise ausführen:

1. Secure Controller auswählen

Keine Auswahl möglich, wenn nur ein einzelner Controller konfiguriert wird.
a „Weiter“ ausführen.

2. Vorbereiten

Nur zur Information:
- „Secure Controller“: Zeigt den Name des Controllers mit IP-Adresse an, der konfiguriert wird.
- „Bestehende Konfiguration“: Zeigt alle bisher konfigurierten Zutrittspunkte und Lese-/Eingabeeinheiten an. Bei Erstkonfiguration ohne Inhalt.

a „Weiter“ ausführen.

3. RS485-Kommunikation

Zuordnung des Protokolls für die Lese-/Eingabeeinheiten je RS485-Busstrang („Siedle Vario-Bus oder OSDP“).
a „Siedle Vario-Bus“ für einen oder beide RS485-Busstränge auswählen.
b „Speichern“ ausführen.
c „Weiter“ ausführen.

4. Türen

Konfiguration der Zutrittspunkte (Türen), die an den Schaltkontakten (z. B. Türöffner-Funktion) des Controllers angeschlossenen sind.
a Zu konfigurierenden Zutrittspunkt auswählen, der am Controller angeschlossen ist (z. B. „Tür 1“).
b Eindeutige/aussagekräftige Bezeichnung ins Eingabefeld daneben eingeben (z. B. Tür 1 Haupteingang Süd).
c Option „Rückmeldekontakt“ der Tür deaktivieren, wenn keine Zustandsüberwachung verwendet wird.
d „Speichern“ ausführen.
e Weitere Zutrittspunkte (Türen) nach gleicher Vorgehensweise konfigurieren.
f „Weiter“ ausführen.

5. Leser

Konfiguration der am Controller angeschlossenen Lese-/Eingabeeinheiten (Leser).
a „Neu anlegen“ ausführen.
b „Bus-Strang/Protokoll“ auswählen, an dem die Lese-/Eingabeeinheit angeschlossen ist (z. B. RS485 Strang A / Siedle Vario-Bus).
c „Zutrittspunkt“ auswählen, um dieser Lese-/Eingabeeinheit den dazugehörigen Zutrittspunkt (z. B. Leseeinheit bei „Tür 1“) zuzuordnen.
d Eindeutige/aussagekräftige Bezeichnung für „Name“ für die Lese-/Eingabeeinheit eingeben (z. B. Leser Tür 1 Haupteingang Süd ELM Adresse2 Strang A).
e „Bus-Adresse“ eingeben, die an der Lese-/Eingabeeinheit eingestellt wurde.
f „Typ“ (Gerätetyp) der Lese-/Eingabeeinheit auswählen.
g „Speichern“ ausführen.
h Weitere Lese-/Eingabeeinheiten nach gleicher Vorgehensweise konfigurieren.
i „Weiter“ ausführen.

6. Fertig

Die Konfiguration der Geräte (Zutrittspunkte und Lese-/Eingabeeinheiten) ist mit diesem Schritt abgeschlossen. Im Bericht ist eine kompakte Darstellung der durchgeführten Konfiguration zusammengefasst.
a „Fertig“ ausführen.

Erweiterte Inbetriebnahme von einem oder mehreren Controllern

Empfohlener Ablauf

Der Secure Controller bietet einen großen Funktionsumfang. Mit der erweiterten Inbetriebnahme ist die vollständige Konfiguration eines betriebsbereiten Zutrittskontrollsystems mit mehreren Controllern möglich.

Erste Schritte
- Kennwort neu vergeben
- Sprache
- Datum/Uhrzeit
- Netzwerk

Seite 13

↓

Mehrere Controller vernetzen (Geräteverbund) Seite 26

↓

Controller-Erweiterung(en) konfigurieren Seite 21

↓

Inbetriebnahme-Wizard: Konfiguration der Geräte (geführte Inbetriebnahme)
- Türen (Tür-Relais für Zutrittspunkte)
- Lese-/Eingabeeinheiten
- Optional: Wochenprogramm Türen

Seite 27

↓

Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln (Karte und Code)
- Benutzer
- Identifikationsmittel (Karte und Code)

Seite 41

↓

Optional: Wochenprogramm Allgemein Seite 44

↓

Optional: Konfiguration der Eingänge/Ausgänge
- Eingänge
- Ausgänge
- Logik

Seite 45

↓

Funktionsprüfung Seite 58

↓

Daten/Konfiguration sichern Seite 58

↓

Einweisung/Übergabe Seite 58

↓

Kennwortänderung Seite 58

↓

Benutzerverwaltung durch Kunde/Betreiber
- Planung der Benutzerverwaltung
- Optional: Konfiguration der Feiertage
- Optional: Benutzer-Wochenprogramm
- Optional: Zutrittsgruppen
- Benutzer und Identifikationsmittel (Karten und Codes)

Seite 59

Erweiterte Inbetriebnahme von einem oder mehreren Controllern

Mehrere Controller vernetzen

Für den Betrieb mehrerer Controller im Verbund innerhalb eines Netzwerks (LAN) gilt:

- Max. 64 Controller sind miteinander vernetzbar (1 primäres Gerät, 63 sekundäre Geräte)
- Max. 1 primärer Controller je Verbund.
- Die Konfiguration erfolgt im Verbund zentral über den primären Controller.
- Der Datenaustausch (Synchronisation) im Verbund erfolgt im Betrieb gesichert und voll automatisch. Muss aber für die Synchronisation der Inbetriebnahme-Konfiguration einmalig manuell ausgeführt werden.
- Jeder Controller im Verbund kann als primäres Gerät ausgewählt werden. Ein Wechsel im laufenden Betrieb ist ebenfalls möglich. Der als primäres Gerät ausgewählte Controller führt einen Neustart durch und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.
- Alle Controller im Verbund müssen sich im gleichen Netzwerk-Segment befinden. Im Betrieb über mehrere Netzwerk-Segmente hinweg, muss das Routing im Netzwerk für die Controller entsprechend konfiguriert sein.
- Beim Ausfall eines Controllers im Verbund (auch das primäre Gerät), ist das Zutrittskontrollsystem (bis auf die Ein- und Ausgänge des ausgefallenen Controllers) weiterhin voll nutzbar.
- Bei Austausch eines Controllers innerhalb des Verbunds, erfolgt die Wiederherstellung der Controller-Konfiguration über die Daten-Nachbildung (Replikation) aus dem Controller-Verbund.

Vorgehensweise

1 IP-Adresse des Controllers ermitteln, der als primäres Gerät vorgesehen ist.
2 Aufruf der Administrationsoberfläche per Webbrowser.
3 Login mit Konto „Service".
4 Menü „Secure Controller" öffnen (Pfad: System > Administration > Secure Controller).
5 „Neu anlegen" ausführen.
6 Es wird der Controller angezeigt, auf dem Sie sich angemeldet haben.
7 Angezeigten Inhalt (Name, Info) prüfen und ggf. anpassen oder ergänzen.
8 „Speichern" ausführen.
9 „Als primäres Gerät festlegen" ausführen.
10 Abfrage mit „Ja" bestätigen.
11 Der als primäres Gerät ausgewählte Controller führt einen Neustart durch und ist nach ca. einer Minute wieder mit der Anmeldeseite erreichbar.
12 Login mit Konto „Service".
13 Der Titel der Startseite lautet nun „Secure Controller (Primäres Gerät)".
14 Menü „Secure Controller" öffnen (Pfad: System > Administration > Secure Controller).
15 Der primäre Controller wird in der Auflistung angezeigt.
16 „Suche Siedle Secure Controller…" ausführen.
17 Gefundene Controller werden tabellarisch angezeigt.
18 Gefundene Controller die im Verbund mit dem primären Controller betrieben werden sollen, auswählen.
19 Ausgewählte Controller mit „Auswahl importieren" übernehmen.
20 Abfrage mit „Ja" bestätigen.
21 Bestätigungsmeldung mit „OK" bestätigen.
22 Importierte Controller werden in der Auflistung „Secure Controller" unterhalb vom primären Controller angezeigt.
23 Importierten Controller (zukünftiges sekundäres Gerät) auswählen.
24 „Bearbeitung von Secure Controller…" wird angezeigt.
25 Angezeigten Inhalt (Name, Info) prüfen und ggf. anpassen oder ergänzen.
26 Im Auswahlmenü „Aktionen" die Option „Als sekundäres Gerät festlegen" oder „Importiere als sekundäres Gerät" ausführen:

- „Als sekundäres Gerät festlegen": Der Controller wird ohne vorhandener/vorbereiteter Konfiguration übernommen.
- „Importiere als sekundäres Gerät": Der Controller wird mit vorhandener/vorbereiteter Konfiguration übernommen.

27 Abfrage mit „Ja" bestätigen.
28 Der sekundäre Controller führt einen Neustart durch und ist nach ca. einer Minute konfigurierbar.
29 „Speichern und Schließen" ausführen.
30 Vorgehensweise mit allen zukünftigen sekundären Controllern durchführen.

31 „Aktualisieren" ausführen.
32 In der Auflistung „Secure Controller" bei „Synchronisation" wird der primäre Controller mit „N/A" und alle sekundären Controller mit dem Status „Synchronisiert" angezeigt.

Hinweis

Die Controller arbeiten jetzt im Betrieb als Geräteverbund und sind vorbereitet für die nachfolgenden Inbetriebnahme-Schritte.
Die vollständige Inbetriebnahme aller im Geräteverbund befindlichen Controller ist ab jetzt nur noch über den primären Controller möglich.

Mit dem Inbetriebnahme-Wizard bietet der Secure Controller eine geführte Inbetriebnahme für die Konfiguration der im Zutrittskontrollsystem angebundenen Zutrittspunkte und Lese-/Eingabeeinheiten.
Im Betrieb als Geräteverbund erfolgt die Konfiguration aller Controller ausschließlich über den primären Controller.

Bedienelemente (Wizard)
- „Verwerfen": Abbruch des Vorgangs und Beendigung des Wizards.
- „Wizard neu starten": Abbruch des Vorgangs und Neustart des Wizards.
- „< Zurück": Wechsel zum vorherigen Reiter (Schritt der Inbetriebnahme).
- „> Weiter": Wechsel zum nächsten Reiter (Schritt der Inbetriebnahme).
- „Aktualisieren": Wiederholung der Datenabfrage im System und Erneuerung der angezeigten Informationen.
- „Konfiguration löschen": Bestehende Konfiguration löschen (nur aktiv, bei vorhandener Konfiguration).
- „Speichern": Sichern und ablegen der Auswahl / Eingabe(n) im System.
- „Defaults": Rücksetzen der Änderungen.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Inbetriebnahme-Wizard" schrittweise ausführen:

1. Secure Controller auswählen
a Controller auswählen (z. B. primären Controller), an dem die Konfiguration ausgeführt werden soll.
b „Weiter" ausführen.

2. Vorbereiten
Nur zur Information:
- „Secure Controller":
Zeigt den Name des Controllers mit IP-Adresse an, der konfiguriert wird.
- „Bestehende Konfiguration":
Zeigt alle bisher konfigurierten Zutrittspunkte und Lese-/Eingabeeinheiten an. Bei Erstkonfiguration ohne Inhalt.

a „Weiter" ausführen.

3. RS485-Kommunikation
Zuordnung des Protokolls für die Lese-/Eingabeeinheiten je RS485-Busstrang („Siedle Vario-Bus oder OSDP").
a „Siedle Vario-Bus" für einen oder beide RS485-Busstränge auswählen.
b „Speichern" ausführen.
c „Weiter" ausführen.

4. Türen
Konfiguration der Zutrittspunkte (Türen), die an den Schaltkontakten (z. B. Türöffner-Funktion) des Controllers angeschlossenen sind.
a Zu konfigurierenden Zutrittspunkt auswählen, der am Controller angeschlossen ist (z. B. „Tür 1").
b Eindeutige/aussagekräftige Bezeichnung ins Eingabefeld daneben eingeben (z. B. Tür 1 Haupteingang Süd).
c Option „Rückmeldekontakt" der Tür deaktivieren, wenn keine Zustandsüberwachung verwendet wird.
d „Speichern" ausführen.
e „Detaillierte Einstellungen" ausführen.
f Inhalte prüfen und ggf. anpassen (siehe Konfigurationshilfe auf den Folgeseiten 28–31):
- „Allgemein"
- „Eigenschaften"
- „Zeiten"
- „Sicherheit"
- „Logik"
- „Wochenprogramm Tür"
- „Aufzug"

g „Speichern und Schließen" ausführen.
h Weitere Zutrittspunkte nach gleicher Vorgehensweise konfigurieren.
i „Speichern" ausführen.
j „Weiter" ausführen.

Konfigurationshilfe: Türen (Zutrittspunkte)

Allgemein	Erläuterung	Auslieferungszustand
Name	Eindeutige/aussagekräftige Bezeichnung für den zu konfigurierenden Schaltkontakt.	–
Typ	Schaltkontakt des Controllers. Im Wizard ist dieses Feld bereits vorkonfiguriert (z. B. „Tür-E/A 1“ ist im Wizard der „Tür 1“ zugeordnet). In der manuellen Konfiguration gibt es diese Vorauswahl (z. B. „Tür 1“) nicht und daher kann hier ein noch nicht konfigurierter Schaltkontakt ausgewählt und dann konfiguriert werden.	–
Eigenschaften		
Auf globale Türsteuerung reagieren	Ist diese Option aktiviert, lässt der Controller eine übergeordnete (globale) Steuerung des jeweiligen Zutrittspunkts zu (z. B. durch eine Leitstelle). Die globale Steuerung hat Vorrang gegenüber dem Steuerung des Controllers.	deaktiviert
Rückmeldestatus unterdrücken	Ist diese Option aktiviert, werden an der dazugehörigen Eingabe-/Leseeinheit dieser Tür (Zutrittspunkt) keine Alarmmeldungen des Tür-Rückmeldekontakts ausgegeben, wenn die Tür nicht mit den vorgesehenen Methoden geöffnet wurde und dies dennoch nicht alarmiert werden soll (z. B. Tür wird von Mitarbeitern von innen nur mit dem Türdrücker geöffnet, um das Gebäude nach Arbeitsende zu verlassen). Dies betrifft auf die Funktionen innerhalb des Secure Controllers: „Manuelle Türsteuerung“ (Status) und „Ereignisprotokoll“. Andere Überwachungsfunktionen sind von dieser Funktion nicht betroffen (z. B. Überschreitung der maximalen Türöffnungszeit, …).	deaktiviert
Signalisierung unterdrücken	Ist diese Option aktiviert, wird die akustische Signalisierung der zu diesem Zutrittspunkt gehörenden Lese-/Eingabeeinheit vollständig deaktiviert (z. B. wenn diese störend sind). Diese Option setzt eine Lese-/Eingabeeinheit mit akustischer Signalisierung (z. B. Summer) voraus.	deaktiviert
Türgesteuerter Schaltkontakt	Ist die Option aktiviert, bleibt der zu diesem Zutrittspunkt gehörende Schaltkontakt solange in der Arbeitsstellung, bis der Zutrittspunkt wieder geschlossen ist. Diese Option setzt einen Rückmeldekontakt voraus und ist nur für Zutrittspunkte erforderlich, die für einen vollständigen Öffnungs- und Schließvorgang einen so konfigurierten Schaltkontakt benötigen.	deaktiviert

Konfigurationshilfe: Türen (Zutrittspunkte)

Eigenschaften	Erläuterung	Auslieferungszustand
Türrelais reagiert nicht auf Ausgangstaster	Ist diese Option aktiviert, wird der zu diesem Zutrittspunkt gehörende Schaltkontakt nicht aktiviert, wenn der in dem Zutrittspunkt integrierte Ausgangstaster (Türöffner-Taster) betätigt wird. Diese Option setzt einen Zutrittspunkt mit integriertem Ausgangstaster voraus.	deaktiviert
Rückmeldekontakt	Ist diese Option aktiviert, erfolgt der Betrieb des Zutrittspunkts mit einem Rückmeldekontakt. Diese Option setzt einen Rückmeldekontakt voraus.	deaktiviert
SAI-GUID	Ohne Funktion / Nicht nutzbar	deaktiviert
Schaltkontakt nachtriggern	Ist diese Option aktiviert, ist nach erfolgreicher Identifikation das erneute Öffnen eines Zutrittspunkts schon wieder möglich, obwohl dessen Schließvorgang noch nicht abgeschlossen ist (z. B. schließende Schranke, herunterfahrendes Rolltor, …). Diese Option ermöglicht an geeigneten Zutrittspunkten einen höheren Durchsatz an Zutritten und setzt beim Zutrittspunkt eine Steuerung mit diesem Leistungsmerkmal voraus.	deaktiviert
Auf Bedrohungslage reagieren	Ohne Funktion / Nicht nutzbar	deaktiviert
Protokolliere Türstatus	Ist diese Option aktiviert, erfolgt zusätzlich die Protokollierung der Zustände des Rückmeldekontakts („Geöffnet“ und „Geschlossen“) eines Zutrittspunkts. Die Protokollierung erfolgt im Bereich „Protokoll/Report“ und „Ereignisse“ und „Bericht“. Diese Option setzt einen Rückmeldekontakt voraus.	deaktiviert
Betriebsmodus	Auswählbarer Betriebsmodus dieses Zutrittspunkts: • „Normal“: Der Zutrittspunkt lässt sich mit allen berechtigten Identifikationsmitteln (Karten/Codes) öffnen und schließen. • „Schlüsselkasten“: Der Zutrittspunkt lässt sich nur mit dem Identifikationsmittel (Karte oder Code) öffnen, mit der er zuvor verschlossen wurde.	„Normal“
Öffnen bei fehlerhaftem Einbruchmeldestatus	Ohne Funktion / Nicht nutzbar	deaktiviert

Konfigurationshilfe: Türen (Zutrittspunkte)

Zeiten	Erläuterung	Auslieferungszustand
Türöffnungszeit (s)	Zeit in Sekunden, wie lange der Schaltkontakt (z. B. Türöffner) ausgelöst wird. Jedem Benutzer kann entweder die „Türöffnungszeit (s)“ oder die „Längere Türöffnungszeit (s)“ zugewiesen werden.	„3“
Längere Türöffnungszeit (s)	Zeit in Sekunden, wie lange der Schaltkontakt (z. B. Türöffner) ausgelöst wird. Diese Option ist für Benutzer gedacht die ggf. auf eine längere Türöffnungszeit angewiesen sind (z. B. Person in Rollstuhl). Jedem Benutzer kann entweder die „Türöffnungszeit (s)“ oder die „Längere Türöffnungszeit (s)“ zugewiesen werden.	„20“
Zulässige Öffnungszeit (s)	Zeit in Sekunden wie lange der Zutrittspunkt insgesamt geöffnet sein darf, bevor eine Warnmeldung ausgelöst wird. Diese Option setzt einen Rückmeldekontakt voraus.	„30“
Zulässige längere Öffnungszeit (s)	Verlängerte Zeit in Sekunden wie lange der Zutrittspunkt insgesamt geöffnet sein darf, bevor eine Warnmeldung ausgelöst wird. Diese Option setzt einen Rückmeldekontakt voraus.	„60“
Verzögerung Warnmeldung (s)	Zeit nach Überschreiten der zulässigen (verlängerten) Öffnungszeit, nach deren Ablauf eine Warnmeldung ausgegeben wird (verzögerte Warnmeldung). Diese Option setzt eine Lese-/Eingabeeinheit mit akustischer und/oder optischer Signalisierung (z. B. Summer und/oder blinkende Funktions-LED) voraus.	„10“
Verzögerung Türschließung (ms)	Zeit in Millisekunden bevor eine Schließung des Zutrittspunkts ausgelöst wird. Diese Funktion kann für den Betrieb von Hochsicherheitstüren mit Überwachungssystem erforderlich sein.	„0“
Verzögerung Türöffnung (ms)	Zeit in Millisekunden bevor eine Öffnung des Zutrittspunkts ausgelöst wird. Diese Funktion kann für den Betrieb von Hochsicherheitstüren mit Überwachungssystem erforderlich sein.	„0“
Sperrzeit bei PIN-Fehleingabe (s)	Zeit in Sekunden, die ein Zutrittspunkt für einen Benutzer mit zweifacher Identifikation (Karte oder Code und PIN) systemseitig nicht geöffnet wird, nachdem die maximal zulässige Anzahl an PIN-Fehleingaben erreicht wurde. Die Konfiguration der max. Anzahl an PIN-Fehleingaben erfolgt im Menü „Sicherheit“.	„60“
Retrigger-Dauer (ms)	Zeit in Millisekunden nach dem letzten Schaltimpuls, bis der Schaltkontakt für ein erneutes Öffnen eines Zutrittspunkts wieder einen Schaltimpuls auslöst (Kontakt in konfigurierter Arbeitsstellung). Dieses Feld ist nur konfigurierbar, wenn die Funktion „Schaltkontakt nachtriggern“ aktiviert ist.	„1000“

Konfigurationshilfe: Türen (Zutrittspunkte)

Sicherheit	Erläuterung	Auslieferungszustand
Protokolliere Zutritt nur bei geöffneter Tür	Ist diese Option aktiviert, erfolgt systemseitig die Protokollierung der Identifikation am Zutrittspunkt nur, wenn der Rückmeldekontakt einen offenen/geöffneten Zutrittspunkt meldet, und dadurch von einem Zutritt ins Gebäude ausgegangen werden kann. Diese Option setzt einen Rückmeldekontakt voraus.	deaktiviert
Schaltkontakt nur gesichert öffnen	Ist diese Option aktiviert, ist nach erfolgreicher Identifikation ein erneutes Öffnen eines Zutrittspunkts erst dann wieder möglich, wenn der Schließvorgang wieder beendet ist (z. B. Schleuse, …). Diese Option ermöglicht an geeigneten Zutrittspunkten einen sicheren Zutritt und setzt einen Rückmeldekontakt voraus.	deaktiviert
Max. Anzahl an PIN-Fehleingaben	Anzahl an zulässigen PIN-Fehleingaben, bis zur Aktivierung der zeitlichen Sperre des Zutrittspunkts. Die Sperrzeit wirkt dann nach jeder Fehleingabe erneut, um weitere Versuche durch zeitliche Verzögerung zu erschweren. Die Sperrzeit bei PIN-Fehleingabe ist im Menü „Zeiten“ konfigurierbar.	„10“

Logik
Im Bereich Logik sind mehrere Logik-Abläufe vorkonfiguriert, wie der betroffene Zutrittspunkt und das System auf bestimmte Ereignisse/ Auslöser reagieren soll. Die Verknüpfungen sind für die marktüblichen Anwendungsszenarien vorkonfiguriert. Ein Anpassung ist daher im Normalfall nicht notwendig.

Wochenprogramm Tür
Ein Wochenprogramm für einen Zutrittspunkt wird benötigt, wenn die Verwendung des Zutrittskontrollsystem unabhängig von Benutzern zeitlich unterschiedlich ausfallen soll (z. B. Zutritt zum Objekt an diesen oder allen Zutrittspunkten nur von Montags bis Freitags und von jeweils 08:00 bis 18:00 Uhr).

Neues Wochenprogramm konfigurieren
In einem neu erstellten Wochenprogramm ist die gesamte Woche mit „Normal" vorbelegt. In diesem Betriebsmodus funktioniert das Zutrittskontrollsystem zu jeder Zeit.

Vorgehensweise
1 „Neu anlegen" ausführen.
2 Eindeutige / aussagekräftige Bezeichnung für „Name" für das Wochenprogramm eingeben.
3 „Wochenprogramm" auswählen.
4 „Bearbeiten" öffnen.
5 „Tag" auswählen (z. B. „Montag")
6 Funktion auswählen (z. B. „Gesperrt"). Weitere Informationen siehe Tabelle „Konfigurationshilfe Wochenprogramm".
7 Startzeit auswählen.
8 Endzeit auswählen.
9 „Übernehmen" ausführen.
10 Weitere Funktionen nach gleicher Vorgehensweise konfigurieren.
11 Der konfigurierte Tag wird angezeigt.
12 Um die gleiche Konfiguration auf weitere Wochentage zu übertragen, „Kopieren nach" öffnen und einen Wochentag oder Sonderprogramm auswählen. Alternativ, andere Wochentage nach gleicher Vorgehensweise konfigurieren, bis das Wochenprogramm konfiguriert ist.
13 „Speichern" ausführen.
14 „Zuordnung zu Türen" auswählen.
15 Zutrittspunkte auswählen die mit diesem Wochenprogramm gesteuert werden.
16 „Speichern und Schließen" zweimal ausführen.

Konfigurationshilfe: Wochenprogramm

Funktion	Erläuterung
Dauerhaft geöffnet	Der Zutrittspunkt ist dauerhaft geöffnet und kann ohne Identifikationsmittel betreten und wieder verlassen werden.
Gesperrt	Der Zutrittspunkt ist geschlossen und kann durch reguläre Nutzer nicht geöffnet werden. Ausschließlich Nutzer mit erweiterter Berechtigung oder Sonderberechtigung können diesen Zutrittspunkt öffnen – insofern konfiguriert (z. B. Feuerwehr, VIP)
Normal	Der Zutrittspunkt kann nur durch Einsatz eines Identifikationsmittels (Karte/Code) geöffnet werden. Die Identifikation erfolgt immer einfach (entweder Karte oder Code).
Immer mit PIN	Am Zutrittspunkt ist eine zweifache Identifikation (Karte oder Code + PIN) erforderlich.
Dauerhaft geöffnet nach Karte oder Code	Der Zutrittspunkt wird erst nach erfolgreicher Identifikation durch Karte oder Code des ersten Nutzers dauerhaft geöffnet.
Umschalten	Im Betriebsmodus „Umschalten“ können Benutzer mit ihren Identifikationsmitteln (Karte oder Code) den Betriebsmodus des Zutrittspunkts wechseln. Der Wechsel ist zwischen den beiden Modi „Dauerhaft geöffnet“ und „Normal“ möglich.

Aufzug (Aufzugsteuerung in Zutrittskontrollanlagen)

Soll der Zutritt in Gebäuden zu bestimmten Stockwerken auch bei Aufzügen gesichert werden, ist dies mit dem Secure Controller und einer entsprechenden Erweiterung möglich.
Beispielsweise dürfen dann nur berechtigte Personen diese Stockwerke mit dem Aufzug anfahren.
Für die Integration einer Aufzugssteuerung wenden Sie sich bitte an das Siedle Engineering im Werk Furtwangen.
Telefon +49 7723 63-378
engineering@siedle.de

5. Leser
Konfiguration der am Controller angeschlossenen Lese-/Eingabeeinheiten (Leser).
a „Neu anlegen“ ausführen.
b „Bus-Strang/Protokoll“ auswählen, an dem die Lese-/Eingabeeinheit angeschlossen ist (z. B. RS485 Strang A / Siedle Vario-Bus).
c „Zutrittspunkt“ auswählen, um dieser Lese-/Eingabeeinheit den dazugehörigen Zutrittspunkt (z. B. Leseeinheit bei „Tür 1“) zuzuordnen.
d Eindeutige/aussagekräftige Bezeichnung für „Name“ für die Lese-/Eingabeeinheit eingeben (z. B. Leser Tür 1 Haupteingang Süd ELM Adresse2 Strang A).
e „Bus-Adresse“ eingeben, die an der Lese-/Eingabeeinheit eingestellt wurde.
f „Typ“ (Gerätetyp) der Lese-/Eingabeeinheit auswählen.
g „Speichern“ ausführen.
h „Detaillierte Einstellungen“ ausführen.
i Inhalte prüfen und ggf. anpassen (siehe Konfigurationshilfe auf den Folgeseiten
- „Allgemein“
- „Protokoll“
- „Zutrittsparameter“
- „Sofortzugang“
- „Türbefehle“
- „Einbruchserkennung“
- „Datenträger“
- „Siedle Vario-Bus“

j „Speichern und Schließen“ ausführen.
k Weitere Lese-/Eingabeeinheiten nach gleicher Vorgehensweise konfigurieren.
l „Speichern“ ausführen.
m „Weiter“ ausführen.

Konfigurationshilfe: Lese-/Eingabeeinheit

Allgemein	Erläuterung	Auslieferungszustand
Name	Zu vergebende eindeutige/aussagekräftige Bezeichnung der Lese-/Eingabeeinheit	–
Typ	Betriebsform der Lese-/Eingabeeinheit: • „Standard“: Lese-/Eingabeeinheit ist im Betrieb mit einem Zutrittspunkt) • „Leser für mehrere Türen“: Lese-/Eingabeeinheit im Betrieb mit mehreren Zutrittspunkten)	„Standard“
Zutrittspunkt	Schaltkontakt (Tür-Relais) der einer oder mehreren Lese-/Eingabeeinheiten zugeordnet werden kann. Unter „Türen“ werden alle Schaltkontakte (Tür-Relais) angezeigt, die unter „Türen“ angelegt wurden.	–
Protokoll		
Bus-Kommunikation	Zuordnung der Anbindung / des Anschlusses der Lese-/Eingabeeinheit: • „Nicht verwendet“: Die Lese-/Eingabeeinheit ist noch nicht angeschlossen oder nicht in Betrieb. • „RS485 Strang A“: Die Lese-/Eingabeeinheit ist am RS485-Busstrang A angeschlossen. • „RS485 Strang B“: Die Lese-/Eingabeeinheit ist am RS485-Busstrang B angeschlossen. • „TCP-IP“: Ohne Funktion / Nicht nutzbar.	–
Protokoll	Zuordnung des Betriebsprotokolls für die Datenübertragung der Lese-/Eingabeeinheit: • „Nicht verwendet“: Die Lese-/Eingabeeinheit ist noch nicht angeschlossen oder nicht in Betrieb. • „OSDP“: Protokoll für die Kommunikation zwischen Controller und ODSP-fähigen Lese-/Eingabeeinheiten von Siedle oder anderen Herstellern. • „Siedle Vario-Bus“: Protokoll für die Kommunikation zwischen Controller und Vario-Bus-fähigen Lese-/Eingabeeinheiten von Siedle. • Die Protokolle „Deister deBus“, „Aperio“, “Serielle Barcode-Leser“, „Smart Intego IP“, „Wiegand“ sind für die Konfiguration am Secure Controller nicht vorgesehen.	–

Konfigurationshilfe: Lese-/Eingabeeinheit

Zutrittsparameter	Erläuterung	Auslieferungszustand
Quittierton bei gelesenem Identifikationsmittel	Ist die Option aktiviert, erfolgt eine akustische Rückmeldung durch die Leseeinheit, wenn das Identifikationsmittel (Electronic-Key / Elektronic-Key-Card) erfolgreich eingelesen wurde. Diese Option setzt eine Leseeinheit mit akustischer Signalisierung (z. B. Summer) voraus.	deaktiviert
Quittierton bei akzeptiertem Identifikationsmittel	Ist die Option aktiviert, erfolgt eine akustische Rückmeldung durch die Leseeinheit, wenn das Identifikationsmittel (Electronic-Key / Elektronic-Key-Card) vom Zutrittskontrollsystem akzeptiert wurde. Diese Option setzt eine Leseeinheit mit akustischer Signalisierung (z. B. Summer) voraus.	deaktiviert
Zeitlimit Code / PIN (s)	Zeit in Sekunden, innerhalb der der Code / die PIN vollständig eingegeben und bestätigt sein muss, bevor das System den Eingabevorgang abbricht. Bei Abbruch muss mit dem Eingabevorgang erneut begonnen werden.	„10“
Zeitlimit Zifferneingabe (ms)	Zeit in Millisekunden, die zwischen den einzelnen Eingabeschritten der Ziffern eines Codes / einer PIN sowie der Bestätigung der Eingabe jeweils verstreichen darf, bevor das System den Eingabevorgang abbricht. Bei Abbruch muss mit dem Eingabevorgang erneut begonnen werden.	„2000“
Zeitüberschreitung bei Ziffern-eingabe signalisieren	Ist diese Option aktiviert, erfolgt bei Zeitüberschreitung der Einstellung „Zeitlimit Ziffern-eingabe (ms)“ eine akustische Rückmeldung durch die Eingabeeinheit. Diese Option setzt eine Eingabeeinheit mit akustischer Signalisierung (z. B. Summer) voraus.	deaktiviert
Zeitlimit Office-Modus (s)	Ohne Funktion / Nicht nutzbar	–
Mit Tastenfeld	Diese Option wird während der Konfiguration mit dem Inbetriebnahmen-Wizard automatisch gesetzt, wenn eine Eingabeeinheit ausgewählt wird (z. B. COM 611-…). Eine entsprechende Option muss sowohl bei der Eingabeeinheit als auch beim Controller gesetzt sein. Sollen je eine Lese- und Eingabeeinheit im Kombinationsbetrieb zusammen verwendet werden (nur Siedle-Vario-Bus), muss diese Option auch bei der dazugehörigen Leseeinheit (z. B. ELM 600-…) gesetzt werden und die Vario-Bus-Adresse an beiden Geräten gleich eingestellt sein. Die Identifikation ist dann abhängig von der Konfiguration wahlweise einfach (Karte oder Code) oder zweifach (Karte oder Code mit PIN) möglich. Für den Betrieb mit einer Eingabeeinheit müssen weitere Optionen gesetzt sein. Details siehe Seite 39, 60	aktiviert

Konfigurationshilfe: Lese-/Eingabeeinheit

Zutrittsparameter	Erläuterung	Auslieferungszustand
Codeeingabe nach Kartenlesung ignorieren (ms)	Zeit nach Identifikation mit Electronic-Key / Elektronic-Key-Card, in der alle Eingaben an der Eingabeeinheit ignoriert werden. Erst nach Ablauf der konfigurierten Zeit kann ein Zugangscode oder PIN eingegeben werden. Diese Funktion ist für Kombigeräte (Leseeinheit mit integrierter Eingabeeinheit) vorgesehen, bei denen eine unbeabsichtigte Handberührung mit der Tastatur der Eingabeeinheit während der Identifikation mit Electronic-Key / Electronic-Key-Card, zu einer versehentlichen Eingabe an der Eingabeeinheit führen könnte (z. B. bei einer kapazitiven Eingabeeinheit).	„0“
Einlern-Leseeinheit	Ist diese Option aktiviert, kann die Leseeinheit für das Einlernen neuer Electronic-Keys / Elektronic-Key-Cards verwendet werden.	deaktiviert
PIN-Änderung zulassen	Ist diese Option aktiviert, kann die Lese-/ Eingabeeinheit für das Ändern einer PIN (Code für die Doppel-Identifikation eines Benutzers nach Verwendung eines Electronic-Keys / einer Elektronic-Key-Card) verwendet werden.	aktiviert
Zeitlimit Leseeinheit (ms)	Zeit in Millisekunden, in der der Controller nur eine Meldung/Nachricht einer Leseeinheit akzeptiert, wenn ein Identifikationsmittel Electronic-Key / Elektronic-Key-Card) eingelesen wird. Diese Option dient zur Korrektur/ Verhinderung möglicher Fehlinterpretationen im Zutrittskontrollsystem, wenn eine Leseeinheit mehrfach Meldungen/Nachrichten je eingelesenem Identifikationsmittel versendet.	„0“
Exit-Push-Signalisierung unterdrücken	Ist diese Option aktiviert, erfolgt bei Betätigung eines Ausgangstasters (Exit-Push-Button) keine optische Rückmeldung durch die Lese-/Eingabeeinheit.	deaktiviert
Zwei-Personen-Regel	Bei aktiver „Zwei-Personen-Regel“ verlangt der Controller vor Freigabe eine Identifikation durch zwei Personen (Identifikationsmittel die zwei unterschiedlichen Benutzern zugeordnet sind): • „Kontrolle durch Wochenprogramm“: Die Regel an dieser Lese-/Eingabeeinheit wird über das konfigurierte Wochenprogramm gesteuert. • „Immer Zwei-Personen-Regel“: Die Regel an dieser Lese-/Eingabeeinheit ist immer aktiv. • „Wochenprogramm aussetzen“: Die Regel an diesem Lese-/Eingabeeinheit ist deaktiviert.	„Kontrolle durch Wochenprogramm“
Sofortzugang	Ohne Funktion / Nicht nutzbar	–
Türbefehle	Ohne Funktion / Nicht nutzbar	–
Einbruchserkennung	Ohne Funktion / Nicht nutzbar	–

Konfigurationshilfe: Lese-/Eingabeeinheit

Datenträger	Erläuterung	Auslieferungszustand
	Im Bereich „Datenträger“ werden Eigenschaften der verwendeten Identifikationsmittel mit (Electronic-Key / Elektronic-Key-Card) konfiguriert.	
Hersteller	Hersteller des Identifikationsmittels: • Allgemein: Siedle-Identifikationsmittel Ohne Funktion / Nicht nutzbar: • „HISEC“ • „TechSolutions“	„Allgemein“
Datenformat	Datenformat des Identifikationsmittels: • „Siedle Prox“: Siedle-Identifikationsmittel • „UTF8-Daten“: QR-Code-Leseeinheit (z. B. Messe-Zutrittsbereiche mit optischen Scannern/ Leseeinheiten Ohne Funktion / Nicht nutzbar: • „Chip ID“: • „HIKvision LPR Wiegand (72bit)“ • „Rohdaten (binär)“ • „Nokas DESFire (NO)“ • „HID SEOS“ • „Verschlüsseltes Magnetstreifen Format (1)“ • „Cotag/Deister prox./Hands-Free Format (3)“ • „HISEC Hughes-Prox/Hands-Free Format (4)“ • „Standard BCD Magstripe Format (13)“ • „Free·Programmable·Bit·Format (Wiegand) (14)“ • „MIFARE Chip ID-Nummer entschlüsselt (30)“ • „MIFARE Format mit 3-Byte Kartennum… (31)“ • „MIFARE Chip ID-Nummer nicht entschl… (32)“ • „Reichpass (NL)“ • „MIFARE Chip ID-Nummer nicht entschl…(34)“ • „KMD Sektor wird gelesen (35)“ • „G4S Sektor lesen (36)“	„Siedle Prox“
Datenträgertyp	Datenträgertyp des Identifikationsmittels (nur relevant für den Betrieb mit Offline-Leseeinheiten): • „Nativer Typ“ • „MIFARE classic 1K“ • „MIFARE classic 4K“ • „MIFARE DESFire“ • „Wiegand-Format“ • „HID UHF“	„MIFARE DESFire“

Konfigurationshilfe: Lese-/Eingabeeinheit

Datenträger	Erläuterung	Auslieferungszustand
Aktiviere kartenlosen Zugang für dieses Gerät	Diese Option wird während der Konfiguration mit dem Inbetriebnahmen-Wizard automatisch gesetzt, wenn eine Eingabeeinheit ausgewählt wird (z. B. COM 611-…). Eine entsprechende Option muss sowohl bei der Eingabeeinheit als auch beim Controller gesetzt sein. Sollen je eine Lese- und Eingabeeinheit im Kombinationsbetrieb zusammen verwendet werden (nur Siedle-Vario-Bus), muss diese Option auch bei der dazugehörigen Leseeinheit (z. B. ELM 600-…) gesetzt werden und die Vario-Bus-Adresse an beiden Geräten gleich eingestellt sein. Die Identifikation ist dann abhängig von der Konfiguration wahlweise einfach (Karte oder Code) oder zweifach (Karte oder Code mit PIN) möglich. Für den Betrieb mit einer Eingabeeinheit müssen weitere Optionen gesetzt sein. Details siehe Seite 37, 60	aktiviert
CSN tauschen	Ist diese Option aktiviert, ist die Leserichtung getauscht und das Einlesen der Kartennummer (Chip Share Number) erfolgt in der anderen Richtung. Diese Option ist erforderlich, wenn das Einlernen der Identifikationsmittel durch die Einlern-Leseeinheit in einer anderen Richtung erfolgt als die Identifikation am Zutrittspunkt.	deaktiviert
CSN tauschen (Nibbles)	Ist diese Option aktiviert, ist die Leserichtung auch zusätzlich paarweise getauscht (Nibbles) und das Einlesen der Kartennummer (Chip Share Number) erfolgt paarweise getauscht in der anderen Richtung. Diese Option ist erforderlich, wenn das Einlernen der Identifikationsmittel durch die Einlern-Leseeinheit paarweise getauscht in einer anderen Richtung erfolgt als die Identifikation am Zutrittspunkt.	deaktiviert
Siedle Vario-Bus	Dieser Bereich ist im Wizard immer konfigurierbar. Bei manueller Konfiguration ist zuvor für „Protokoll" die Option „Siedle Vario-Bus" auszuwählen.	
Typ	Auswahl der Siedle-Lese-/Eingabeeinheit: • COM 611-…: Eingabeeinheit • ELM 600-…: Leseeinheit	–
Bus-Adresse	Busadresse (Vario-Bus) der Siedle-Lese-/Eingabeeinheit. Für weitere Informationen siehe Seite 5	–
Version	Nicht änderbares Informationsfeld mit dem Datum der Firmware der Lese-/Eingabeeinheit.	–

6. Fertig
Die Konfiguration der Geräte (Zutrittspunkte, Lese-/Eingabeeinheiten) sowie der Systemkonfiguration (Wochenprogramm ist mit diesem Schritt abgeschlossen.
Im Bericht ist eine kompakte Darstellung der durchgeführten Konfiguration zusammengefasst.
a „Fertig“ ausführen.

Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln

Für die Inbetriebnahme und zur Funktionsprüfung des Zutrittskontrollsystems ist mindestens ein angelegter Benutzer, und sind abhängig von den installierten Lese-/Eingabeeinheiten und den vorgegebenen Identifikationsformen (z. B. Karte oder Karte und PIN) ggf. mehrere Identifikationsmittel (z. B. Karte, Code, PIN) erforderlich.

Benutzerverwaltung
In der Benutzerverwaltung erfolgt die vollständige Konfiguration neuer und bestehender Benutzer (natürliche Personen) des Zutrittskontrollsystems sowie deren Identifikationsmittel. Darüber hinaus erfolgt hier bei Bedarf die Konfiguration von Benutzergruppen sowie der Wochenprogramme für Benutzer.

Benutzer
In „Benutzer" erfolgt die Konfiguration neuer und bestehender Benutzer sowie neuer und bestehender Identifikationsmittel.

Bedienelemente (Benutzer)
• „Aktualisieren": Wiederholung der Datenabfrage im System und Erneuerung der angezeigten Informationen.
• „Neuen Benutzer anlegen": Funktion um einen neuen Benutzer anzulegen.
• „Suchen": Funktion für die Suche bzw. Eingrenzung der Suche von Benutzern.
• „Kartennummer von Einlern-Leseeinheit empfangen": Funktion für das Einlernen eines neuen physischen Identifikationsmittels (Electronic-Key / einer Elektronic-Key-Card)
• „Neue Kopie": Erstellung eines neuen Benutzers mit gleicher Konfiguration der Zutrittsgruppen, Zutrittsberechtigungen und Optionen. Geeignet für das Anlagen mehrerer ähnlicher Benutzer.
• „Speichern": Sichern und ablegen der Auswahl / Eingabe(n) im System.
• „Löschen": Ausgewählten Benutzer löschen
• „Speichern und Schließen": Sichern und ablegen der Auswahl / Eingabe(n) im System und Rückkehr zum vorherigen Menü.
• „Schließen": Rückkehr zum vorherigen Menü ohne automatisches Speichern. Bei ungespeicherten Änderungen erfolgt immer ein Abfrage.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „Benutzerverwaltung" öffnen.
3 Menü „Benutzer" öffnen.
4 „Neuen Benutzer anlegen" ausführen.
5 Im Bereich „Allgemein" und „Karten/Codes" fehlende Angaben vervollständigen (siehe nachfolgende Konfigurationshilfe).

Für die Inbetriebnahme der Lese- und Eingabeeinheiten empfehlen wir die Anlage eines Benutzers mit mehreren Identifikationsmitteln (Karte und Code sowie PIN) und der Zutrittsberechtigung für alle Zutrittspunkte.
6 „Speichern und Schließen" ausführen.
7 Weitere Benutzer konfigurieren, wahlweise:
• nach gleicher Vorgehensweise (empfohlen, wenn sich die Benutzerkonfiguration in allen Bereichen unterscheidet)
• mit Funktion „Neue Kopie" (empfohlen bei gleichbleibender Konfiguration der Zutrittsgruppen, Zutrittsberechtigungen und Optionen)

Konfigurationshilfe: Neuen Benutzer anlegen

Allgemein	Erläuterung
Typ	Nicht änderbares Informationsfeld mit der Anzeige „Standard".
Vorname	Vorname des Benutzers
Zweitname	Zweiter Vorname des Benutzers
Nachname	Nachname des Benutzers
Firma/Abteilung	Firmenzugehörigkeit des Benutzers
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu diesem Benutzer.
Gültig ab	Zeitpunkt, ab dem der Benutzer mit seinen Identifikationsmitteln im Zutrittskontrollsystem agieren darf.
Unendlich gültig	Ist diese Option aktiviert, darf der Benutzer mit seinen Identifikationsmitteln dauerhaft im Zutrittskontrollsystem agieren.
Gültig bis	Zeitpunkt, bis zu dem der Benutzer mit seinen Identifikationsmitteln im Zutrittskontrollsystem agieren darf. Dieses Feld ist nur aktiv, wenn die Option "Unendlich gültig" deaktiviert wurde.

Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln

Konfigurationshilfe: Neuen Benutzer anlegen

Karten/Codes	Erläuterung	Auslieferungszustand
Modus	Mit dieser Auswahl kann einem Benutzer die Anzahl an dessen verfügbaren Identifikationsmitteln zugeordnet werden: • „Kein Identifikationsmittel“: Dem Benutzer sind keine Identifikationsmittel zugeordnet. In diesem Fall werden sämtliche Konfigurationsmöglichkeiten in der Administrationsoberfläche ausgeblendet. • „Einzelnes Identifikationsmittel“: Dem Benutzer ist ein Identifikationsmittel zugeordnet. • „Mehrere Identifikationsmittel“: Dem Benutzer sind mindestens zwei Identifikationsmittel zugeordnet.	„Einzelnes Identifikationsmittel“
Karte/Code		
Kartennummer/Code	Identifikationskennung: • einer manuell eingegebenen Ziffernfolge (Zutritts-Code) oder • eines eingelernten physischen Identifikationsmittels (Electronic-Key / Elektronic-Key-Card). Jede Identifikationskennung darf nur einmal im System vergeben werden!	–
Kartennummer von Einlern-Leseeinheit empfangen	Funktions-Button: Einsatzbereite Funktion zum Einlernen von physikalischen Identifikationsmitteln, insofern im System eine Einlern-Leseeinheit konfiguriert wurde. Die Einlern-Leseeinheit kann eine beliebig im Objekt installierte und am Zutrittskontrollsystem angebundene Leseeinheit sein (z. B. ELM 600-…). Alternativ ist der Einsatz einer portablen Leseeinheit für den direkten Anschluss an einem Laptop/PC möglich (z. B. Siedle USB-Reader „readID One SE 1220 MNP“).	–

Konfigurationshilfe: Neuer Benutzer anlegen

Karte/Code	Erläuterung	Auslieferungszustand
PIN (Ziffern)	Eingabefeld, um einem Benutzer eine PIN zuzuweisen. Die PIN ist nur dann erforderlich, wenn eine Doppel-Identifikation für ein höheres Maß an Sicherheit gewünscht wird (z. B. Identifikation mit Karte oder Zutritts-Code und zusätzlicher PIN). Jedem Benutzer kann ein beliebige PIN (Standard: vierstellig) zugewiesen werden. **Wichtig!** Sollen Benutzer bei einer vom System vorkonfigurierten Doppel-Identifikation ihren PIN selbst vergeben, darf kein Wert vorkonfiguriert werden. Der Benutzer muss dann seine PIN selbst vergeben, indem er ihn bei seiner ersten Identifikation an diesem Zutrittskontrollsystem an der entsprechenden Eingabeeinheit eingibt und bestätigt.	–
PIN wiederholen	Eingabefeld zur Bestätigung des bereits in Feld „PIN (Ziffern)“ eingegebenen PIN.	–
Zutrittsberechtigungen		
Auswahlmenü	Auswahlmenü für die Filterung der angezeigten Zutrittsberechtigungen: • „Alle Türen anzeigen“: Es werden alle bereits konfigurierten (verfügbaren) Zutrittspunkte angezeigt. • „Ausgewählte Türen anzeigen“: Es werden die Zutrittspunkte angezeigt, die dem Benutzer zugeordnet sind. Zutrittspunkte aus der Zutrittsgruppe werden als bereits ausgewählt und nicht änderbar angezeigt, und können unter „Zutrittsberechtigungen“ nicht als einzelne Zutrittsberechtigung ausgewählt und konfiguriert werden. **Für jeden Benutzer muss entweder mindestens eine Zutrittsgruppe oder eine Zutrittsberechtigung konfiguriert sein.** **In beiden Fällen ist eine Mehrfachauswahl möglich.**	–

Optional: Wochenprogramm Allgemein

Wochenprogramm Allgemein
Ein Allgemein-Wochenprogramm ist erforderlich, wenn im Zutrittskontrollsystem Ausgänge (Schaltkontakte) und konfigurierte Logik-Operationen aus Ausgängen / Eingängen und Ausgängen vorhanden sind und auch in Abhängigkeit von der Zeit mit gesteuert werden sollen.

Neues Wochenprogramm konfigurieren
Bei einem neu angelegten Allgemein-Wochenprogramm befindet sich der Wochenplan immer vollständig im Modus „Aus". Der Modus „Ein" muss hinzu konfiguriert werden.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Konfiguration" öffnen.
4 „Wochenprogramme" öffnen.
5 „Wochenprogramm Allgemein" öffnen.
6 „Neu anlegen" ausführen.
7 Bei „Allgemein" eindeutige / aussagekräftige Bezeichnung für „Name" des Wochenprogramms eingeben.
8 „Wochenprogramm" auswählen.
9 „Bearbeiten" öffnen.
10 „Tag" auswählen (z. B. „Montag")
11 Funktion auswählen (z. B. „Ein"). Weitere Informationen siehe Tabelle „Konfigurationshilfe Wochenprogramm".
12 Startzeit auswählen.
13 Endzeit auswählen.
14 „Übernehmen" ausführen.
15 Weitere Funktionen nach gleicher Vorgehensweise konfigurieren.
16 Die Tageskonfiguration wird tabellarisch angezeigt.
17 Um die gleiche Tageskonfiguration auf weitere Wochentage zu übertragen, „Kopieren nach" öffnen und einen Wochentag oder Sonderprogramm auswählen. Alternativ, andere Wochentage nach gleicher Vorgehensweise konfigurieren, bis das Wochenprogramm konfiguriert ist.
18 „Speichern und Schließen" ausführen.

Konfigurationshilfe: Wochenprogramm

Modus	Erläuterung
Ein	Ausgänge (Schaltkontakte) und konfigurierte Logik-Operationen sind eingeschalten.
Aus	Ausgänge (Schaltkontakte) und konfigurierte Logik-Operationen sind ausgeschalten.

Optional: Konfiguration der Eingänge/Ausgänge

Eingänge/Ausgänge Eingänge

Bei der Inbetriebnahme mit dem Inbetriebnahme-Wizard werden nur ausgesuchte Ein- und Ausgänge zur Konfiguration bereitgestellt. In diesem Bereich ist die Konfiguration aller am Secure Controller befindlichen Ein- und Ausgänge möglich. Im Bereich „E/A" können Eingänge, Ausgänge (Schaltkontakte) und konfigurierte Logik-Operationen aus Ausgängen / Eingängen und Ausgängen konfiguriert werden. Die Steuerung der Ausgänge und Logik-Operationen erfolgt je nach Konfiguration ereignisbasiert (z. B. am Eingang liegt ein Signal an), per Wochenprogramm „Allgemein" (zeitlich gesteuert), oder kombiniert.

In diesem Bereich ist die Konfiguration aller am Secure Controller befindlichen Eingänge möglich. Am Secure Controller sind ein interner Meldeeingang (Strombegrenzer) und bis zu acht externe Eingänge (sechs symmetrisch, zwei digital) konfigurierbar:

Vorgehensweise

1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Konfiguration" öffnen.
4 „Eingänge/Ausgänge" öffnen.
5 „Eingänge" öffnen.
6 Alle konfigurierbaren Eingänge werden tabellarisch aufgelistet.
7 Gewünschten Eingang auswählen.
8 Bearbeitung von Eingang […] wird angezeigt.
9 Im Bereich „Eingangseinstellungen" fehlende Angaben vervollständigen (siehe Konfigurationshilfe Eingänge).
10 „Speichern und Schließen" ausführen.
11 Weitere Ausgänge nach gleicher Vorgehensweise konfigurieren.

Typ	Erläuterung
Strombegrenzer (digitaler Eingang)	• Digitaler Eingang (wird systemintern innerhalb des Controllers verwendet), von extern nicht beschaltbar, keine Leitungsüberwachung erforderlich. • Einzelne Merkmale sind nicht konfigurierbar.
Türkontakt 1–4 (symmetrischer Eingang) Türöffnertaste 1–2 (symmetrischer Eingang)	• Eingänge mit optional konfigurierbarer Leitungsüberwachung (Linienüberwachung) und konfigurierbarem Widerstandsnetzwerk gemäß Werteauswahl • Die Konfiguration erfolgt über die Administrationsoberfläche (siehe „Konfiguration der Eingänge/Ausgänge" > „Leitungsüberwachung") • Keine Zustandsänderung der Eingänge aufgrund einer anliegenden Fremdspannung (max. zulässige anliegende Fremdspannung aus angeschlossener Eingangsbeschaltung: 30 V DC)
Türöffnertaste 3–4 (digitaler Eingang)	• Eingänge ohne Leitungsüberwachung (Linienüberwachung) • Keine Zustandsänderung der Eingänge aufgrund einer anliegenden Fremdspannung (max. zulässige anliegende Fremdspannung aus angeschlossener Eingangsbeschaltung: 30 V DC) • Einzelne Merkmale nicht konfigurierbar.

Optional: Konfiguration der Eingänge/Ausgänge

Eingänge

Konfigurationshilfe: Eingänge

Allgemein	Erläuterung	Auslieferungszustand
Name	Nicht änderbares Informationsfeld mit der Bezeichnung des Eingangs.	„[Name des Eingangs]“
Eigenschaften		
Leitungsüberwachung	Auswahl (nur bei symmetrischen Eingängen), ob am Eingangskontakt eine Beschaltung mit Leitungsüberwachung (Linienüberwachung) (per Widerstand) zur Überwachung des Leitungszustands eingesetzt ist: • „2 Zustände“: Keine Überwachung • „3 Zustände“: Einfache Überwachung • „4 Zustände“: Erweiterte Überwachung Details zum Thema Leitungsüberwachung finden Sie auf Seite 48	„2 Zustände“
Kontaktart	Auswahl, welche Kontaktart am Eingang angeschlossen ist: • Öffner-Kontakt: Am Eingang ist ein Öffner-Kontakt angeschlossen (Ruhestellung: geschlossen) • Schließer-Kontakt: Am Eingang ist ein Schließer-Kontakt angeschlossen (Ruhestellung: offen) Der Meldeeingang „Strombegrenzer“ ist ein Eingang innerhalb des Controllers. Mit der Auswahl der Kontaktart ist dessen Ansprechverhalten konfigurierbar (invertierbar).	„Öffner-Kontakt“
Endwiderstand	Auswahl des Widerstands der für die Linienüberwachung als „Endwiderstand“ (EOL-Widerstand (End of line)) eingesetzt wurde. Folgende Werte sind auswählbar (Ohm): • „1k“: (1000 Ohm) • „2k2“: (2200 Ohm) • „3k3“: (3300 Ohm) • „3k9“: (3900 Ohm) • „4k7“: (4700 Ohm) • „5k6“: (5600 Ohm) • „6k8“: (6800 Ohm) • „8k2“: (8200 Ohm) • „10k“: (10000 Ohm) • „12k“: (12000 Ohm) Endwiderstand und Alarmwiderstand sind unabhängig voneinander auswählbar.	„2k2“

Konfigurationshilfe: Eingänge

Eigenschaften	Erläuterung	Auslieferungszustand
Alarmwiderstand	Auswahl des Widerstands der für die Linienüberwachung als „Alarmwiderstand“ (AR: Alarm resistor) eingesetzt wurde. Folgende Werte sind auswählbar (Ohm): • „1k“: (1000 Ohm) • „2k2“: (2200 Ohm) • „3k3“: (3300 Ohm) • „3k9“: (3900 Ohm) • „4k7“: (4700 Ohm) • „5k6“: (5600 Ohm) • „6k8“: (6800 Ohm) • „8k2“: (8200 Ohm) • „10k“: (10000 Ohm) • „12k“: (12000 Ohm) Alarmwiderstand und Endwiderstand sind unabhängig voneinander auswählbar.	„2k2“
Auslöser folgen	Ist diese Option aktiviert, verbleibt der Eingang solange im Arbeitszustand, bis das auslösende Element (z. B. geschlossener Kontakt) wieder zurück in den Ruhezustand wechselt. Sobald das auslösende Element nicht mehr aktiv ist, wechselt der Eingang zurück in seinen Ruhezustand. Ist diese Option aktiviert, ist das Feld „Dauer (ms)“ nicht konfigurierbar.	
Verzögerung (ms)	Zeit in Millisekunden, bevor der Eingang in den Arbeitszustand wechselt.	„10“
Dauer (ms)	Zeit in Millisekunden die der Eingang im Arbeitszustand verbleibt, unabhängig vom Zustand des auslösenden Elements am Eingangskontakt. Dieses Feld ist nur konfigurierbar, wenn die Option „Auslöser folgen“ nicht aktiviert ist.	„0“
Verzögerung erneut auslösen	Ist diese Option aktiviert, erfolgt der Wechsel in den nächsten Arbeitszustand auch dann wieder verzögert, wenn die Auslösung durch das auslösende Element erfolgt ist, während sich der Eingang bereits in einem Arbeitszustand befunden hat.	deaktiviert
Ausführen, wenn Auslöser wieder in Ruhezustand	Ist diese Option aktiviert, wechselt der Eingang erst in den Arbeitszustand für die unter „Dauer“ angegebene Zeit, wenn das auslösende Element am Eingangskontakt nicht mehr aktiv ist (z. B. Kontakt ist nicht mehr geschlossen).	deaktiviert

Optional: Konfiguration der Eingänge/Ausgänge

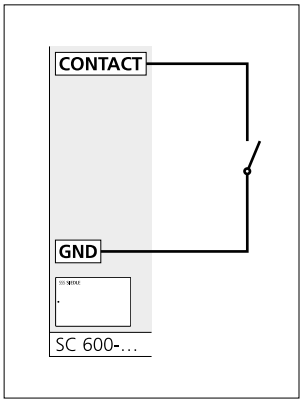
Exkurs: Leitungsüberwachung

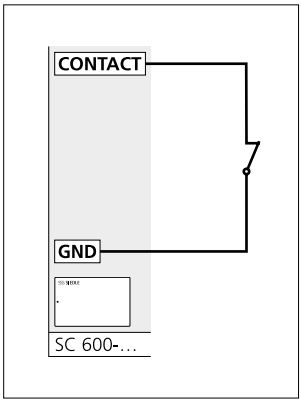
Eine Leitungsüberwachung (Linienüberwachung) dient der Überwachung des Zustands einer an einem Eingang angeschlossenen Beschaltung und deren Leitung. Am Secure Controller sind sechs symmetrische Eingänge die mit einer Überwachung betrieben werden können. Folgende Verdrahtungsvarianten sind möglich:

Verdrahtung für …	Beschaltung: Schließer-Kontakt (Ruhezustand: geöffnet)	Beschaltung: Öffner-Kontakt (Ruhezustand: geschlossen)
2 Zustände – (Keine Überwachung) Bei dieser Variante wird die Leitung nicht überwacht. Systemseitig können am Eingang folgende Zustände erfasst werden: • geöffnet • geschlossen Der Controller ist dadurch in der Lage einen „Normalzustand“ und einen „Alarmzustand“ zu erkennen. Diese sind abhängig von der eingesetzten Beschaltung und der Konfiguration des Eingangs.	**Eigenschaften** • Meldung nach dem Arbeitsstrom-Prinzip. • Sicherheit: Keine Überwachung, einfache Manipulation durch „Unterbrechung“ der Leitung möglich. • Manipulation durch Controller im laufenden Betrieb erkennbar: nein	**Eigenschaften** • Meldung nach dem Ruhestrom-Prinzip. • Sicherheit: Keine Überwachung, einfache Manipulation durch „Kurzschluss“ der Leitung möglich. • Manipulation durch Controller im laufenden Betrieb erkennbar: nein

Zustand	Meldung
Kontakt geöffnet	Normal
Kontakt geschlossen	Alarm

Zustand	Meldung
Kontakt geöffnet	Alarm
Kontakt geschlossen	Normal

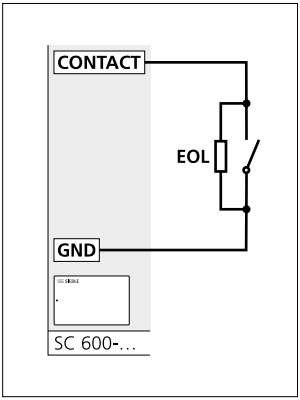




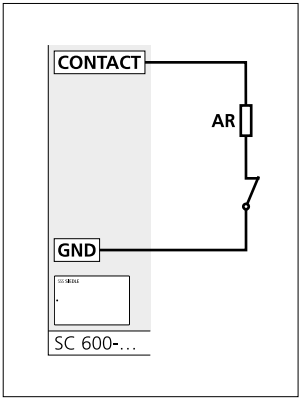
Verdrahtung für …	Beschaltung: Schließer-Kontakt (Ruhezustand: geöffnet)	Beschaltung: Öffner-Kontakt (Ruhezustand: geschlossen)
3 Zustände – (Einfache Überwachung) Bei dieser Variante ist jeder Zustand überwacht, kann aber nicht eindeutig erkannt werden. Je Beschaltung gibt es für je zwei Zustände die gleiche Meldung, da sie nicht unterscheidbar sind. Systemseitig können am Eingang folgende Zustände erfasst, aber abhängig von der Beschaltung nicht in jedem Fall eindeutig gemeldet werden: **Schließer-Kontakt** • geöffnet • geschlossen/kurzgeschlossen • unterbrochen **Öffner-Kontakt** • geöffnet/unterbrochen • geschlossen • kurzgeschlossen	**Eigenschaften** • Meldung nach dem Arbeitsstrom-Prinzip mit Widerstand. • Sicherheit: Einfache Überwachung: gegen Kurzschluss und Unterbrechung der Leitung. • Manipulation durch Controller im laufenden Betrieb erkennbar: ja • Ein Endwiderstand muss konfiguriert werden.	**Eigenschaften** • Meldung nach dem Ruhestrom-Prinzip mit Widerstand. • Sicherheit: Erweiterte Überwachung: gegen Kurzschluss und Unterbrechung der Leitung. • Manipulation durch Controller im laufenden Betrieb erkennbar: ja • Ein Alarmwiderstand muss konfiguriert werden.

Zustand	Meldung
Kontakt geöffnet	Normal
Kontakt geschlossen	Alarm
Leitung unterbrochen	Unterbrechung
Leitung kurzgeschlossen	Alarm

Zustand	Meldung
Kontakt geöffnet	Alarm
Kontakt geschlossen	Normal
Leitung unterbrochen	Alarm
Leitung kurzgeschlossen	Kurzschluss



Bei dieser Beschaltung befindet sich ein Endwiderstand parallel zum Kontakt des Auslösers.

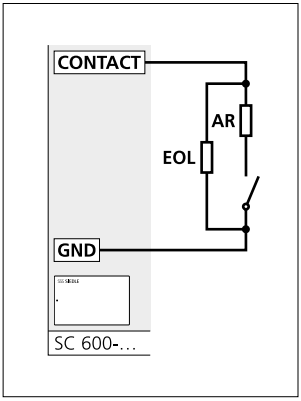


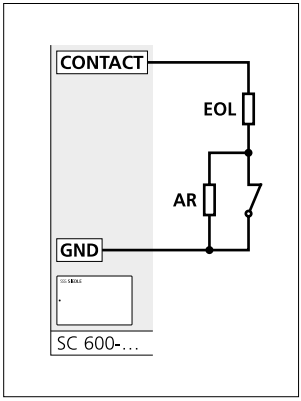
Bei dieser Beschaltung befindet sich ein Alarmwiderstand in Reihe zum Kontakt des Auslösers.

Verdrahtung für …	Beschaltung: Schließer-Kontakt (Ruhezustand: geöffnet)	Beschaltung: Öffner-Kontakt (Ruhezustand: geschlossen)
4 Zustände – (Erweiterte Überwachung) Bei dieser Variante ist jeder Zustand überwacht und wird eindeutig erkannt – unabhängig von der Art der Beschaltung. Systemseitig können am Eingang folgende Zustände eindeutig erfasst und über den Controller gemeldet werden: • geöffnet • geschlossen • unterbrochen • kurzgeschlossen	**Eigenschaften** • Meldung nach dem Arbeitsstrom-Prinzip mit Widerstandsnetzwerk • Sicherheit: Erweiterte Überwachung: gegen Kurzschluss und Unterbrechung der Leitung. • Höchster Manipulationsschutz, da für jeden Zustand ein anderer Widerstandswert entsteht. • Manipulation durch Controller im laufenden Betrieb erkennbar: ja • Ein Endwiderstand und ein Alarmwiderstand müssen konfiguriert werden.	**Eigenschaften** • Meldung nach dem Ruhestrom-Prinzip mit Widerstandsnetzwerk. • Sicherheit: Erweiterte Überwachung: gegen Unterbrechung der Leitung. • Höchster Manipulationsschutz, da für jeden Zustand ein anderer Widerstandswert entsteht. • Manipulation durch Controller im laufenden Betrieb erkennbar: ja • Ein Endwiderstand und ein Alarmwiderstand müssen konfiguriert werden.

Zustand	Meldung
Kontakt geöffnet	Normal
Kontakt geschlossen	Alarm
Leitung unterbrochen	Unterbrechung
Leitung kurzgeschlossen	Kurzschluss

Zustand	Meldung
Kontakt geöffnet	Alarm
Kontakt geschlossen	Normal
Leitung unterbrochen	Unterbrechung
Leitung kurzgeschlossen	Kurzschluss





Bei dieser Beschaltung werden je ein Endwiderstand und ein Alarmwiderstand benötigt: Alarmwiderstand und Kontakt bilden eine Reihenschaltung. Der Endwiderstand ist parallel zur Reihenschaltung.

Bei dieser Beschaltung werden je ein Endwiderstand und ein Alarmwiderstand benötigt: Alarmwiderstand und Kontakt bilden eine Parallelschaltung. Der Endwiderstand ist in Reihe zur Parallelschaltung.

In diesem Bereich ist die Konfiguration aller am Secure Controller befindlichen Ausgänge möglich. Am Secure Controller sind ein Summer und bis zu sieben Ausgänge konfigurierbar. Summer und Ausgänge können jeweils zeit-, ereignisgesteuert oder kombiniert (Logik: zeit- und ereignisgesteuert) ausgelöst werden. Folgende Ausgänge sind konfigurierbar:

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Konfiguration" öffnen.
4 „Eingänge/Ausgänge" öffnen.
5 „Ausgänge" öffnen.
6 Alle konfigurierbaren Ausgänge werden tabellarisch aufgelistet.
7 Gewünschten Ausgang auswählen.
8 Bearbeitung von Ausgang […] wird angezeigt.
9 Im Bereich „Eigenschaften" und „Steuerung" fehlende Angaben vervollständigen (siehe Konfigurationshilfe Ausgänge).
10 „Speichern und Schließen" ausführen.
11 Weitere Ausgänge nach gleicher Vorgehensweise konfigurieren.

Typ	Erläuterung
Summer	Konfigurierbar Summer innerhalb des Secure Controllers für akustische Rückmeldungen konfigurierter Ereignisse oder zur Suche/Lokalisierung eines Controller mit dem „Tech-Tool".
Tür-Relais 1–4	Potentialfreier Schaltkontakt (Wechsler: 30 V DC, 10 A) oder Spannungsausgang (Details siehe Seite 10)
Ausgang 1–3	Steuerausgang (Open-Drain-Ausgang, max. 750 mA je Ausgang) für die Steuerung von Kleinverbrauchern mit externer Spannungsversorgung mit max. 30 V DC

Optional: Konfiguration der Eingänge/Ausgänge

Ausgänge

Konfigurationshilfe: Ausgänge

Allgemein	Erläuterung	Auslieferungszustand
Name	Nicht änderbares Informationsfeld mit der Bezeichnung des Ausgangs.	„[Name des Ausgangs]“
Eigenschaften		
Normalerweise aus	Ist diese Option aktiviert, befindet sich der Ausgang im Ruhezustand, wenn er nicht ausgelöst ist. Ist diese Option deaktiviert, wechselt der Ausgang in den Arbeitszustand, wenn er nicht ausgelöst ist (invertiert).	aktiviert
Auslöser folgen	Ist diese Option aktiviert, verbleibt der Ausgang solange im Arbeitszustand, wie dies die Steuerung über das auslösende Element vorgibt (z. B. geschlossener Eingangskontakt). Sobald das auslösende Element nicht mehr aktiv ist, wechselt der Ausgang zurück in seinen Ruhezustand. Ist diese Option aktiviert, ist das Feld „Dauer (ms)“ nicht konfigurierbar.	aktiviert
Modus	Konfiguration des Verhaltens des Ausgangs im Arbeitszustand: • „Ein“ (statisch): Ausgang verbleibt statisch im ausgelösten/aktiven Zustand • „Toggle 250 ms“: Ausgang wechselt alle 250 Millisekunden seinen Zustand (Toggle-Betrieb), solange die auslösende Steuerung einen Arbeitszustand vorgibt. • „Toggle 500 ms“: Ausgang wechselt alle 500 Millisekunden seinen Zustand (Toggle-Betrieb), solange die auslösende Steuerung einen Arbeitszustand vorgibt.	„Statisch“
Verzögerung (ms)	Zeit in Millisekunden, bevor der Ausgang in den Arbeitszustand wechselt.	„0“
Dauer (ms)	Zeit in Millisekunden die der Ausgang im Arbeitszustand verbleibt, unabhängig vom Zustand der auslösenden Steuerung. Dieses Feld ist nur konfigurierbar, wenn die Option „Auslöser folgen“ nicht aktiviert ist.	„0“
Verzögerung erneut auslösen	Ist diese Option aktiviert, erfolgt der Wechsel in den nächsten Arbeitszustand auch dann wieder verzögert, wenn die Auslösung der Steuerung erfolgt ist, während sich der Ausgang bereits in einem Arbeitszustand befunden hat.	deaktiviert
Ausführen, wenn Auslöser wieder in Ruhezustand	Ist diese Option aktiviert, wechselt der Ausgang erst in den Arbeitszustand für die unter „Dauer“ angegebene Zeit, wenn die Steuerung zurück in den Ruhezustand wechselt bzw. das auslösende Element nicht mehr aktiv ist (Eingangskontakt ist nicht mehr geschlossen).	deaktiviert

Konfigurationshilfe: Ausgänge

Verknüpfung mit Eingang	Erläuterung	Auslieferungszustand
Secure Controller	Auswahl des Controllers über den die Ansteuerung des Ausgangs erfolgt. Diese Auswahl wird nur angezeigt, wenn mehrere Controller für den Betrieb im Geräteverbund konfiguriert sind.	„[Bezeichnung des primären Controllers]“
Auslöseelement	Auswahl, wie der Ausgang gesteuert wird: • „Keins“: Es gibt kein Auslöseelement das den Ausgang zeit- oder ereignisgesteuert auslöst. Mit dieser Auswahl ist der Ausgang und dessen Steuerung deaktiviert. • „Eingang“: Physikalischer Eingang (z. B. Türkontakt) oder systeminterner Statuspunkt / konfigurierte Logik (z. B. Netzwerk-Fehler) innerhalb des Controllers mit dem der Ausgang ausgelöst werden kann. • „Eingang von Objekt“: Ereignis eines konfigurierten Objekts (z. B. Lese-/Eingabeeinheit oder Wochenkalender), innerhalb des Controllers/ Zutrittskontrollsystems (z. B. Meldung einer Lese-/Eingabeeinheit an den Controller), mit dem der Ausgang ausgelöst werden kann.	„Ohne“
Objekttyp	Auswahlfilter für die Eingrenzung auswählbarer „Objekte“. Diese Auswahl ist nur aktiv, wenn bei „Auslöseelement“ „Objekt“ ausgewählt ist.	–
Objekt	Auswahlfilter für die Eingrenzung auswählbarer Ereignisse in Auswahl „Eingang“ für die Steuerung des Ausgangs. Diese Auswahl ist nur aktiv, wenn bei „Auslöseelement“ „Objekt“ ausgewählt ist. Die angezeigte Auswahl ist abhängig von der Auswahl in "Objekttyp".	–
Eingang	Physikalischer Eingang, systeminterner Statuspunkt / konfigurierter Logik, oder Ereignis eines Objekts für die Steuerung des Ausgangs. Die Auswahl ist abhängig vom ausgewählten Auslöseelement.	–

Optional: Konfiguration der Eingänge/Ausgänge

Logik

In diesem Bereich sind mehrere Logik-Abläufe vorkonfiguriert, wie der betroffene Zutrittspunkt und das System auf bestimmte Ereignisse/Auslöser reagieren soll. Die Logik ist für die marktüblichen Anwendungsszenarien vorkonfiguriert. Ein Anpassung ist daher im Normalfall nicht notwendig. Für die Anpassung der Logik sind erweiterte Kenntnisse über die Konfiguration von Zutrittskontrollsystemen erforderlich.

Bedienelemente

- „Hinzufügen“: Erstellen einer neuen Verknüpfung.
- „Entfernen“: Entfernen einer ausgewählten Verknüpfung.
- „Defaults“: Rücksetzen der Änderungen.
- „Einfügen“ (bei ausgewählter Verknüpfung): Ergänzung einer weiteren Verknüpfung an die ausgewählte Position.

Vorgehensweisen

Bestehende Logik prüfen und ggf. anpassen

1 Login mit Konto „Service“.
2 Menü „System“ öffnen.
3 „Konfiguration“ öffnen.
4 „Eingänge/Ausgänge“ öffnen.
5 „Logik“ öffnen.
6 Logik auswählen (z. B. Tür-Alarm).
7 „Name“ bei Reiter „Allgemein“ ggf. anpassen.
8 Reiter „Verknüpfung“ auswählen.
9 Konfigurationselemente prüfen und ggf. anpassen.
10 „Speichern“ ausführen.
11 Weitere Verknüpfungen nach gleicher Vorgehensweise bearbeiten.

Neue Logik hinzufügen

1 „Neu anlegen“ ausführen.
2 Eindeutige / aussagekräftige Bezeichnung für „Name“ bei Reiter „Allgemein“ eingeben.
3 Reiter „Verknüpfung“ auswählen.
4 „Hinzufügen“ ausführen.
5 Verknüpfungselemente (Betreiber, Verbindungstyp, Objekttyp, Gegenstand und Eingang) per Menüauswahl konfigurieren.
6 Bei Bedarf Vorgang für weitere Unterverknüpfungen wiederholen.
7 „Speichern“ ausführen.
8 Weitere Logik nach gleicher Vorgehensweise erstellen.

Bestehende Logik entfernen

1 Logik auswählen.
2 „Entfernen“ ausführen.
3 „Speichern“ bzw. „Speichern und Schließen“ ausführen.

Konfigurationshilfe: Logik

Allgemein	Erläuterung	Auslieferungszustand
Name	Zu vergebende eindeutige/aussagekräftige Bezeichnung der Logik.	–
Eigenschaften		
Auslöser folgen	Ist diese Option aktiviert, verbleibt der Logikstatus solange im Arbeitszustand, bis das auslösende Element (z. B. geschlossener Kontakt) wieder zurück in den Ruhezustand wechselt. Sobald das auslösende Element nicht mehr aktiv ist, wechselt der Logikstatus zurück in seinen Ruhezustand. Ist diese Option aktiviert, ist das Feld „Dauer (ms)“ nicht konfigurierbar.	aktiviert
Verzögerung (ms)	Zeit in Millisekunden, bevor der Logikstatus in den Arbeitszustand wechselt.	„0“
Dauer (ms)	Zeit in Millisekunden die der Logikstatus im Arbeitszustand verbleibt, unabhängig vom Zustand des auslösenden Elements. Dieses Feld ist nur konfigurierbar, wenn die Option „Auslöser folgen“ nicht aktiviert ist.	„0“
Verzögerung erneut auslösen	Ist diese Option aktiviert, erfolgt der Wechsel in den nächsten Arbeitszustand auch dann wieder verzögert, wenn die Auslösung durch das auslösende Element erfolgt ist, während sich der Logikstatus bereits in einem Arbeitszustand befunden hat.	deaktiviert
Ausführen, wenn Auslöser wieder in Ruhezustand	Ist diese Option aktiviert, wechselt der Logikstatus erst in den Arbeitszustand für die unter „Dauer“ angegebene Zeit, wenn das auslösende Element nicht mehr aktiv ist (z. B. Kontakt ist nicht mehr geschlossen).	deaktiviert
Ruhezustand bei Sabotage	Ist diese Option aktiviert, wechselt der Logikstatus aus Sicherheitsgründen in den Ruhezustand, wenn eine Sabotagemeldung vorliegt.	deaktiviert

Konfigurationshilfe: Logik

Logik	Erläuterung
Operator	Auswählbares Bindeglied zwischen Auslöseelementen (z. B. Eingänge oder Eingänge von Objekten): • „(„: geöffnete Klammer • „)“: geschlossene Klammer • „NICHT“: für negierende Operationen (gegenteilig: z. B. nicht Zustand A) • „UND“: für zusammenfassende Operationen (z. B. Zustand A und Zustand B) • „UND NICHT“: für zusammenfassende Operationen mit Negation (z. B. Zustand A und nicht Zustand B) • „ODER“: für unterscheidende Operationen (Zustand A oder Zustand B) • „ODER NICHT“: für unterscheidende Operationen mit Negation (z. B. Zustand A oder nicht Zustand B) **Hinweis** Operatoren können beliebig kombiniert werden. Die Kombination muss aber sinnvoll sein, da die Operation sonst kein Ergebnis bzw. keinen Zustandswechsel der Logik erzeugen kann. **Beispiel** Für eine Logik die den Status der lokalen Netzwerkanbindung überwachen soll, müssen mögliche Fehlerzustände miteinander verknüpft werden. Operation im Anzeigefeld: LAN-Adresse verloren ODER LAN-Adresskonflikt ODER LAN-LINK verloren Für die Signalisierung kann die Logik beispielsweise als Auslöser für einen Ausgang konfiguriert werden.

Konfigurationshilfe: Logik

Logik	Erläuterung	Auslieferungszustand
Secure Controller	Auswahl des Controllers über den die Ansteuerung der Logik erfolgt. Diese Auswahl wird nur angezeigt, wenn mehrere Controller für den Betrieb als Geräteverbund konfiguriert sind.	–
Auslöseelement	Auswahl, wie der Ausgang gesteuert wird: • „Keins“: Es gibt kein Auslöseelement das den Ausgang zeit- oder ereignisgesteuert auslöst. Mit dieser Auswahl ist der Ausgang und dessen Steuerung deaktiviert. • „Eingang“: Physikalischer Eingang (z. B. Türkontakt) oder systeminterner Statuspunkt / konfigurierte Logik (z. B. Netzwerk-Fehler) innerhalb des Controllers mit dem der Ausgang ausgelöst werden kann. • „Eingang von Objekt“: Ereignis eines konfigurierten Objekts (z. B. Lese-/Eingabeeinheit oder Wochenkalender), innerhalb des Controllers/ Zutrittskontrollsystems (z. B. Meldung einer Lese-/Eingabeeinheit an den Controller), mit dem der Ausgang ausgelöst werden kann.	„Ohne“
Objekttyp	Auswahlfilter für die Eingrenzung auswählbarer „Objekte“. Diese Auswahl ist nur aktiv, wenn bei „Auslöseelement“ „Objekt“ ausgewählt ist.	–
Objekt	Auswahlfilter für die Eingrenzung auswählbarer Ereignisse in Auswahl „Eingang“ für die Steuerung des Ausgangs. Diese Auswahl ist nur aktiv, wenn bei „Auslöseelement“ „Objekt“ ausgewählt ist. Die angezeigte Auswahl ist abhängig von der Auswahl in "Objekttyp".	–
Eingang	Physikalischer Eingang, systeminterner Statuspunkt / konfigurierter Logik, oder Ereignis eines Objekts für die Steuerung des Ausgangs. Die Auswahl ist abhängig vom ausgewählten Auslöseelement.	–

Abschlussarbeiten

Funktionsprüfung

Führen Sie eine Funktionsprüfung des Zutrittskontrollsystems durch.

Vorgehensweise

1 Führen Sie eine vollständige Funktionsprüfung des Zutrittskontrollsystems durch.

2 Prüfen Sie die Funktionsfähigkeit aller Zutrittspunkte, Lese- und Eingabeeinheiten sowie konfigurierter Funktionen.

Daten/Konfiguration sichern

Führen Sie eine vollständige Daten- und Konfigurationssicherung durch.

Vorgehensweise

1 Login mit Konto „Service".

2 Menü „System" öffnen.

3 „Administration" öffnen.

4 „Systeminformationen/Datenbank/Lizenz" öffnen.

5 „Datenbank" öffnen.

6 „Datenbank sichern" ausführen.

7 Abfrage mit „Ja" bestätigen.

8 Abfrage des Browsers mit „OK" bestätigen, um die Sicherung auf dem Laptop zu speichern.

Übergabe/Kennwörter

Übergeben Sie das Zutrittskontrollsystem an den Kunden/Betreiber.

Vorgehensweise

1 Übergeben Sie alle Dokumente/Dateien die mit der Inbetriebnahme zusammenhängen an den Kunden/Betreiber:

- Diese Inbetriebnahmeanleitung mit den eingetragenen neu vergebenen Kennwörtern.
- Datei der Konfigurationssicherung.
- Anlagendokumentation

2 Löschen Sie nach erfolgreicher Übergabe alle Dateien der Inbetriebnahme von Ihrem Laptop.

3 Hinweis für Ihren Kunden (Eigentümer/Betreiber des Zutrittskontrollsystems)

Siedle empfiehlt zur Datensicherheit und für den sicheren Betrieb, nach der Übergabe neue und sichere Kennwörter für alle Benutzerkonten durch den Kunden/Betreiber selbst vergeben zu lassen. Die neu vergebenen Zugangsdaten sollten Dritten (z. B. Elektriker, Inbetriebnehmer) nicht mehr bekannt sein.

Bitte weisen Sie Ihren Kunden darauf hin.

Im Secure Controller gibt es die Möglichkeit die Konfiguration der Benutzerstrukturen nach unterschiedlichen Gesichtspunkten durchzuführen. Kunden/Betreiber eines Zutrittskontrollsystems sollte daher im Vorfeld abwägen, welches die beste Benutzerstruktur für sie ist.

Benutzerverwaltung	**Erläuterung**
Zutrittsparameter	Regeln die Konfigurationsmöglichkeiten zu den verschiedenen Identifikationsmitteln (Karte, Code, PIN) innerhalb der Benutzerverwaltung und erweitern oder reduzieren diese je nach Konfiguration der Zutrittsparameter.
Wochenprogramm Benutzer	Regeln den zeitlichen Zutritt von Benutzern an einem oder mehreren Zutrittspunkten (Türen). Sollten Wochenprogramme erforderlich sein, sollten diese vorab durch den Kunden/Betreiber konfiguriert werden, da diese bei der Konfiguration der Zutrittsgruppen und Benutzer hinterlegt werden müssen. Änderungen betreffen jeweils die Benutzer, bei denen das Wochenprogramm direkt (Zutrittsberechtigungen) oder indirekt (Zutrittsgruppen) hinterlegt ist. Alternativ können Wochenprogramme direkt für den Zutrittspunkt angelegt werden. In diesem Fall gelten an diesem Zutrittspunkt immer die gleichen Zutrittsregeln für alle Benutzer. Weitere Hinweise über die „Wochenprogramme“ und der im Secure Controller bestehenden „Vorrangregelung“ und „Wochenprogramme“ finden Sie auf der Seite 7
Zutrittsgruppen	Regeln den zeitlichen und örtlichen Zutritt eines oder mehrerer Zutrittspunkte. In Zutrittsgruppen können verschiedenen Benutzern die gleichen Zutrittsregeln einfach zugewiesen werden, um den Konfigurationsaufwand zu verringern. Einem Benutzer können mehrere Zutrittsgruppen zugewiesen werden. Änderungen wirken sich auf alle Benutzern aus, die dieser Zutrittsgruppe zugeordnet sind. Bei großen Strukturen mit vielen Benutzern und Zutrittsregeln sind der Einsatz von Zutrittsgruppen sinnvoll und erleichtern die Konfiguration. Sollten Zutrittsgruppen benötigt werden, so sollten diese vor den Benutzern selbst angelegt sein, da diese bei der Konfiguration der Benutzer hinterlegt werden müssen.
Benutzer und Identifikationsmittel	Identifikationsmittel sind immer an einen Benutzer gebunden. Je Benutzer können mehrere Identifikationsmittel konfiguriert werden. Zutrittsberechtigungen einzelner oder mehrerer Zutrittspunkte können auf Benutzerebene (Zutrittsberechtigungen), auf Ebene der Zutrittsgruppen oder kombiniert konfiguriert werden. Darüber hinaus sind Zutrittsoptionen jeweils auf Benutzerebene konfigurierbar. Änderungen wirken sich jeweils nur auf den einzelnen Benutzer aus. Die Konfiguration aus Benutzerebene ohne Zutrittsgruppen empfiehlt sich nur bei kleinen Zutrittskontrollsystemen mit wenigen Benutzern und wenigen Zutrittsregeln.

Benutzerverwaltung durch Kunde/Betreiber

Zutrittsparameter

In diesem Bereich ist die Konfiguration verschiedener Zutrittsparameter zu den verschiedenen Identifikationsmitteln (Karte, Code, PIN) möglich.

Vorgehensweise

1 Login mit Konto „Service“.
2 Menü „System“ öffnen.
3 „Administration“ öffnen.
4 „Benutzerverwaltung“ öffnen.
5 „Zutrittsparameter“ öffnen.
6 Inhalte prüfen und ggf. anpassen (siehe Konfigurationshilfe: Zutrittsparameter).

Konfigurationshilfe: Zutrittsparameter

Allgemein	Erläuterung	Auslieferungszustand
Zutrittskonfiguration (Benutzer)	Auswahl, welche Berechtigungen für die Zutrittskonfiguration der einzelnen Benutzer konfigurierbar sind: • Alle Türen + Wochenprogramme: Jedem Benutzer können mehrere Zutrittsbereiche und unterschiedliche Wochenprogramme zugeordnet werden. Für jeden Zutrittsbereich kann wahlweise ein anderes Wochenprogramm ausgewählt werden. • Alle Türen, ein Wochenprogramm: Jedem Benutzer können mehrere Zutrittsbereiche aber insgesamt nur ein Wochenprogramm zugeordnet werden. Dieses Wochenprogramm gilt für alle zugeordneten Zutrittsbereiche. • Alle Zutrittsgruppen: Jedem Benutzer können mindestens eine oder mehrere Zutrittsgruppen zugeordnet werden, in denen ein oder mehrere Zutrittsbereiche und zugehörige Wochenprogramme vordefiniert sind. • Alle Zutrittsgruppen + Türen + Wochenprogramme: Jedem Benutzer können einzelne oder mehrere Zutrittsgruppen (in denen ein oder mehrere Zutrittsbereiche und zugehörige Wochenprogramme vordefiniert sind), Zutrittsbereiche und Wochenprogramme frei zugeordnet werden.	„Alle Zutrittsgruppen + Türen + Wochenprogramme“
Gültigkeitsdauer mit Datum/Uhrzeit	Ist diese Option aktiviert, kann für den Zeitpunkt, ab dem ein Identifikationsmittel (Karte/Code) im Zutrittskontrollsystem eingesetzt werden darf (kann), ein Datum mit Uhrzeit angegeben werden. Ist die Option deaktiviert, ist nur die Eingabe eines Datums möglich.	aktiviert

Konfigurationshilfe: Zutrittsparameter

Allgemein	Erläuterung	Auslieferungszustand
Codelänge für kartenlosen Zutritt	Auswahl, die den Betrieb von Eingabeeinheiten an Zutrittspunkten für den Zutrittsversuch / die Identifikation mit Code ermöglicht: • „– (nicht erlaubt)“: Der Betrieb von Eingabeeinheiten für den Zutrittsversuch / die Identifikation mit Code ist systemseitig nicht möglich. • „4 Ziffern“: Der Betrieb von Eingabeeinheiten für den Zutrittsversuch / die Identifikation mit Code ist systemseitig möglich. Die Eingabe ist auf max. vier Ziffern begrenzt bzw. es werden nur die ersten vier eingegebenen Ziffern ausgewertet. • „5 Ziffern“: gleiche Funktion wie bei „4 Ziffern“, nur mit fünf Ziffern • „6 Ziffern“: gleiche Funktion wie bei „4 Ziffern“, nur mit sechs Ziffern • „Variable Länge“: gleiche Funktion wie bei „4 Ziffern“, nur mit einer beliebigen Anzahl an Ziffern. **Wichtig!** Für den Betrieb der Siedle-Eingabeeinheit COM 611-… ist die Einstellung „Beliebige Länge“ erforderlich, da die Eingabe eines Codes immer mit der Funktionstaste „F“ für die Übertragung an den Secure Controller bestätigt werden muss!	„Variable Länge“
Codeeingabe mit führenden Nullen	Ist diese Option aktiviert, sind führende Nullen für Codes erlaubt (z. B. Code: „0015“). Ist diese Option deaktiviert, können kein Codes mit führenden Nullen verwendet werden.	aktiviert
PIN		
Länge der PIN	Auswahl für die Länge der PIN die Benutzern zugewiesen werden sollen: • „4“: PIN muss immer vierstellig sein. • „5“: PIN muss immer fünfstellig sein. • „6“: PIN muss immer sechsstellig sein.	„4“
Protokolliere nur Ereignisse bei Karte/Code + PIN	Ist diese Option aktiviert, werden nur Ereignisse von Zutrittsversuchen mit zweifacher Identifikation (Karte + PIN oder Code + PIN) aufgezeichnet. Ist diese Option deaktiviert, werden auch die einzelnen Identifikationsschritte protokolliert.	deaktiviert

Konfigurationshilfe: Zutrittsparameter

PIN	Erläuterung	Auslieferungszustand
PIN verfällt nie	Ist diese Option aktiviert, bleiben alle vergebenen PINs dauerhaft gültig. Ist diese Option deaktiviert, enden alle PINs gemäß Eintragung in Feld „PIN verfällt nach [x] Tagen“, abhängig vom Gültigkeiteszeitpunkts der Identifikationsmittel eines Benutzers.	aktiviert
PIN verfällt nach [x] Tagen	Eingabefeld für die Anzahl an Tagen, nach denen die PIN nicht mehr verwendet werden kann. Der Zeitraum beginnt ab dem Moment, ab dem die PIN einem Benutzer zugewiesen und gespeichert wurde. Nach Ablauf des Gültigkeitszeitraums kann dieser beim betroffenen Benutzer in der Benutzerverwaltung verlängert/erneuert werden.	„90“
Sperre Karte/Code bei PIN-Missbrauch	Ist diese Option aktiviert, wird ab Erreichen der maximalen Anzahl an PIN-Fehleingaben das dazugehörige Identifikationsmittel (Karte/Code) dauerhaft gesperrt. Details zur maximalen Anzahl an PIN-Fehleingaben siehe Seite 31.	deaktiviert
Überfall-PIN	PIN, die im Falle eines Überfalls (Zwang durch eine andere Person den Zutrittsbereich zu öffnen) dem Benutzer die Möglichkeit bietet, den Zutrittsbereich augenscheinlich normal zu öffnen und gleichzeitig einen (stillen) Alarm auszulösen. Der Benutzer gibt nach Identifikation per Karte oder Code anstatt seiner regulären PIN, die Überfall-PIN ein. PIN und Überfall-PIN müssen gleich lang sein. Für diese Funktion muss ein Ausgangskontakt konfiguriert werden, der an ein Gefahrenmeldesystem / eine Alarmanlage angebunden ist.	„1234“
Überfall-Code	Code-Anhängsel, das dem regulären Code angehängt wird, um im Falle eines Überfalls (Zwang durch eine andere Person den Zutrittsbereich zu öffnen) dem Benutzer die Möglichkeit bietet, den Zutrittsbereich augenscheinlich normal zu öffnen und gleichzeitig einen (stillen) Alarm auszulösen. Der Benutzer gibt den Code und den Überfall-Code aufeinanderfolgend ein und bestätigt erst dann die Eingabe an seiner Eingabeeinheit. Code und Überfall-Code können unterschiedlich lang sein. Für diese Funktion muss ein Ausgangskontakt konfiguriert werden, der an ein Gefahrenmeldesystem / eine Alarmanlage angebunden ist.	–

Für die Konfiguration von speziellen Zeitpunkten oder Zeiträumen (z. B. Feiertage) sind im Secure Controller sieben Sonderprogramme verfügbar. In diesem Bereich ändern Sie die Benennung der Sonderprogramme.

Beispiele

Benennung bei Auslieferung	Benennung des Kunden
Sonder-programm I	Gesetzlicher Feiertag
Sonder-programm II	Inventur
Sonder-programm III	Weihnachten

Bedienelemente

„Aktualisieren“: Wiederholung der Datenabfrage im System und Erneuerung der angezeigten Informationen.

Vorgehensweise

1 Login mit Konto „Service“.
2 Menü „System“ öffnen.
3 „Administration“ öffnen.
4 „Benutzerverwaltung“ öffnen.
5 „Sondertage (Wochenprogramm)“ öffnen.
6 Gewünschtes Sonderprogramm per Mausklick öffnen.
7 Inhalt anpassen (siehe Konfigurationshilfe: Sondertag (Wochenprogramm)).

Konfigurationshilfe: Sondertag (Wochenprogramm)

Allgemein	Erläuterung	Auslieferungszustand
Name	Zu vergebende eindeutige/aussagekräftige Benennung des Sonderprogramms (z. B. Gesetzlicher Feiertag). Soll stattdessen die Benennung bei Auslieferungszustand (z. B. Sonderprogramm I) wieder angezeigt werden, ist der Eintrag im Namensfeld zu löschen und die Änderung zu speichern.	–

Benutzerverwaltung durch Kunde/Betreiber

Login

Für die Benutzerverwaltung durch den Kunden/Betreiber ist der Login mit dem Konto „Facility“ vorgesehen. In diesem Konto besteht kein Zugriff auf die eigentliche System- und Gerätekonfiguration.

Zugangsdaten (bei Auslieferung)

Konto/ Benutzername	**Kennwort**
Facility	Facility1234

Vorgehensweise
1 Auf der Anmeldeseite des Controllers mit den Zugangsdaten des Kontos „Facility“ anmelden.

Kennwort neu vergeben

Mit der ersten Anmeldung mit diesem Konto öffnet sich der Kennwort-Änderungsdialog.

Vorgehensweise
1 Bei „Kennwort“ das bisherige Kennwort (Auslieferungszustand: „Facility1234“) eingeben.
2 „Neues Kennwort“ eingeben.
3 „Neues Kennwort wiederholen“.
4 „Speichern und Schließen“ ausführen.
5 Kennwort für die Übergabe an den Betreiber notieren.

Neues Kennwort (Facility)

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Benutzerverwaltung

In diesem Bereich erfolgt die vollständige Konfiguration neuer und bestehender Benutzer (natürliche Personen) des Zutrittskontrollsystems sowie deren Identifikationsmittel. Darüber hinaus erfolgt hier bei Bedarf die Konfiguration von Benutzergruppen sowie der Wochenprogramme für Benutzer. Der Import/Export von Benutzern ist ebenfalls möglich.

Vorgehensweise
1 Login mit Konto „Facility“.
2 Menü „Benutzerverwaltung“ öffnen.

Optional: Feiertage

In diesem Bereich werden einzelne Zeitpunkte oder Zeiträume konfiguriert, die über ein Wochenprogramm nicht abgebildet werden können. Im Auslieferungszustand sind keine „Feiertage“ vorkonfiguriert und müssen bei Bedarf durch den Kunden/Betreiber konfiguriert werden. Die Konfiguration der Feiertage ist über das Benutzerkonto „Service“ und „Facility“ möglich. Feiertage (z. B. Regionale Feiertage, Betriebsurlaube und andere Schließungstage) können kategorisiert in verschiedenen Sonderprogrammen gebündelt und für die Abbildung unregelmäßiger Ausnahmen in Wochenprogrammen verwendet werden. Hierfür können bis zu sieben Sonderprogramme befüllt werden (z. B. Sonderprogramm I = Betriebsurlaub, Sonderprogramm II = Regionale Feiertage, etc.). Mit verschiedenen Wochenprogrammen (z. B. mit und ohne Feiertage) können unterschiedlichen Benutzern/Benutzergruppen unterschiedliche Zutrittsrechte zugewiesen werden.

Vorgehensweise

1 Login mit dem Benutzerkonto „Facility“.
2 Menü „Benutzerverwaltung“ öffnen.
3 „Feiertage“ öffnen.
4 Bereits konfigurierte Feiertage werden tabellarisch in der Ansicht angezeigt und können per direkte Auswahl geändert werden.
5 „Neu anlegen" ausführen.
6 Bei „Allgemein“ eindeutige/aussagekräftige Bezeichnung für „Name“ des Feiertags eingeben.
7 Option „Jährlich wiederholen“ bei Bedarf aktivieren.
8 „Zeitraum“ öffnen.
9 „Hinzufügen“ ausführen.
10 Für „Anfang“ einen Startzeitpunkt im Kalender auswählen.
11 Für „Ende“ einen Endzeitpunkt im Kalender auswählen.
12 Für „Angenommener Wochentag“ ein Sonderprogramm auswählen. Für die einfache Verwendung in Wochenprogrammen empfiehlt Siedle, die Zeitpunkte/Zeiträume sämtlicher Feiertage in Sonderprogrammen zu übernehmen.
13 Weitere Zeitpunkte/Zeiträume für diesen Feiertag nach gleicher Vorgehensweise konfigurieren.
14 „Speichern und Schließen“ ausführen.
15 Weitere Feiertage nach gleicher Vorgehensweise konfigurieren.

Ein Benutzer-Wochenprogramm ist erforderlich, wenn die Verwendung des Zutrittskontrollsystems bei Zutrittsgruppen und/oder Benutzern zeitlich unterschiedlich ausfallen soll (z. B. Zutritt zum Objekt an diesem oder allen Zutrittspunkten (Türen) nur von Montag – Freitags und von 08:00 – 18:00 Uhr täglich).

Neues Wochenprogramm konfigurieren
In einem neuen Benutzer-Wochenprogramm ist der gesamte Wochenplan mit dem Modus „Zutritt mit Karte oder Code„ vorbelegt. In diesem Betriebsmodus funktioniert das Zutrittskontrollsystem zu jeder Zeit für den Zutritt mit Karte oder Code.

Vorgehensweise
1 Login mit dem Benutzerkonto „Facility".
2 Menü „Benutzerverwaltung" öffnen.
3 „Wochenprogramm Benutzer" öffnen.
4 „Neu anlegen" ausführen.
5 Bei „Allgemein" eindeutige / aussagekräftige Bezeichnung für „Name" des Wochenprogramms eingeben.
6 „Wochenprogramm" auswählen.
7 „Bearbeiten" öffnen.
8 „Tag" auswählen (z. B. „Montag")
9 Funktion auswählen (z. B. „Zutritt mit Karte oder Code"). Weitere Informationen siehe Tabelle „Konfigurationshilfe: Wochenprogramm Benutzer".
10 Startzeit auswählen.
11 Endzeit auswählen.
12 „Übernehmen" ausführen.
13 Weitere Funktionen nach gleicher Vorgehensweise konfigurieren.
14 Die Tageskonfiguration wird tabellarisch angezeigt.
15 Um die gleiche Tageskonfiguration auf weitere Wochentage zu übertragen, „Kopieren nach" öffnen und einen Wochentag oder Sonderprogramm auswählen.
Alternativ, andere Wochentage nach gleicher Vorgehensweise konfigurieren, bis das Wochenprogramm konfiguriert ist.
16 „Speichern und Schließen" ausführen.

Konfigurationshilfe: Wochenprogramm Benutzer

Modus	Erläuterung
Kein Zutritt	Kein Zutritt möglich.
Zutritt mit Karte oder Code	Ein Zutritt ist entweder mit Karte oder Code möglich.
Zutritt mit Karte oder Code und PIN	Ein Zutritt ist nur mit Karte oder Code und PIN möglich.
Umschalten mit Karte oder Code	Ein Wechsel zwischen den Betriebsmodi „Zutritt mit Karte oder Code" und „Dauerhaft geöffnet" ist mit Karte oder Code immer möglich.
Umschalten mit Karte oder Code und PIN	Ein Wechsel zwischen den Betriebsmodi „Zutritt mit Karte oder Code" und „Dauerhaft geöffnet" ist mit Karte oder Code und PIN immer möglich.
Zwei-Personen-Regel mit Karte oder Code	Ein Zutritt ist nur mit Karte oder Code von je zwei Benutzern möglich.
Zwei-Personen-Regel mit Karte oder Code und PIN	Ein Zutritt ist nur mit Karte oder Code und PIN von je zwei Benutzern möglich.
Dauerhaft geöffnet bis mit Karte oder Code geschlossen wird	Ein Wechsel zwischen den Betriebsmodi „Dauerhaft geöffnet" und „Zutritt mit Karte oder Code" ist einmalig mit Karte oder Code möglich.
Dauerhaft geöffnet bis mit Karte oder Code und PIN geschlossen wird	Ein Wechsel zwischen den Betriebsmodi „Dauerhaft geöffnet" und „Zutritt mit Karte oder Code" ist einmalig mit Karte oder Code und PIN möglich.
Office-Modus mit Karte	Ohne Funktion / Nicht nutzbar
Office Modus mit Karte und PIN	Ohne Funktion / Nicht nutzbar

Eine Zutrittsgruppe enthält zeitliche und örtliche Zutrittsregeln eines oder mehrerer Zutrittspunkte die mehreren Benutzer zugewiesen werden können. Dadurch kann diese Konfiguration bei jedem einzelnen Benutzer entfallen und sich der Konfigurationsaufwand verringern. Dies gilt auch für nachträgliche Änderungen.

Neue Zutrittsgruppe konfigurieren

In einer Zutrittsgruppe werden zeitliche und örtliche Zutrittsregeln zusammengestellt. Die Zuweisung erfolgt zu Benutzern erfolgt in der Benutzerkonfiguration.

Vorgehensweise

1 Login mit dem Benutzerkonto „Service".
2 Menü „Benutzerverwaltung" öffnen.
3 „Alle Zutrittsgruppen" öffnen.
4 „Neu anlegen" ausführen.
5 Im Bereich „Allgemein" fehlende Angaben vervollständigen (siehe „Konfigurationshilfe: Zutrittsgruppe").
6 Im Bereich „Zutrittsberechtigungen" den gewünschten Zutrittspunkt auswählen.
7 Bei „Wochenprogramm" das gewünschte Wochenprogramm des ausgewählten Zutrittspunkts auswählen.
8 Weitere Zutrittspunkte für diese Zutrittsgruppe nach gleicher Vorgehensweise auswählen und konfigurieren.
9 „Speichern und Schließen" ausführen.
10 Weitere Zutrittsgruppen nach gleicher Vorgehensweise anlegen.

Konfigurationshilfe: Zutrittsgruppe

Allgemein	**Erläuterung**	**Auslieferungszustand**
Name	Zu vergebende eindeutige/aussagekräftige Bezeichnung der Zutrittsgruppe (z. B. Mitarbeiter Produktion)	–
Priorität (niedriger Wert hat höhere Priorität)	Die Priorität regelt den Vorrang zwischen Zutrittsgruppen, wenn diese miteinander kollidieren (z. B. wenn einem Benutzer mehrere Zutrittsgruppen zugewiesen wurden). Systemseitig erfolgt folgende Vorrangregelung: • Die Zutrittsgruppe mit dem niedrigsten Wert hat die höchsten Priorität (Vorrang vor allen anderen Zutrittsgruppen). • Bei Kollision von Zutrittsgruppen mit gleicher Priorität wird die Zutrittsgruppe mit den strengeren Zutrittsregeln (z. B. Zutritt mit Karte oder Code und PIN anstatt Zutritt mit Karte oder Code) angewendet.	„50“
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu dieser Zutrittsgruppe	–
Zutrittsberechtigungen		
Auswahlmenü	Auswahlmenü für die Filterung der angezeigten Zutrittspunkte: • „Alle Türen anzeigen“: Es werden alle bereits konfigurierten (verfügbaren) Zutrittspunkte angezeigt. • „Ausgewählte Türen anzeigen“: Es werden die Zutrittspunkte angezeigt, die der Zutrittsgruppe zugeordnet sind.	
Wochenprogramm	Auswahlmenü für die Zuordnung eines Wochenprogramms für den Zutrittspunkt in dieser Zutrittsgruppe. Das Wochenprogramm muss für jeden Zutrittspunkt einzeln ausgewählt werden. Die Auswahl gilt nur für diese Zutrittsgruppe.	

Benutzer
In diesem Bereich erfolgt die Konfiguration neuer und bestehender Benutzer sowie neuer und bestehender Identifikationsmittel.

Bedienelemente (Benutzer)
- „Aktualisieren“: Wiederholung der Datenabfrage im System und Erneuerung der angezeigten Informationen.
- „Neuen Benutzer anlegen“: Funktion um einen neuen Benutzer anzulegen.
- „Suchen“: Funktion für die Suche bzw. Eingrenzung der Suche von Benutzern.
- „Kartennummer von Einlern-Leseeinheit empfangen“: Funktion für das Einlernen eines neuen physischen Identifikationsmittels (Electronic-Key / einer Elektronic-Key-Card)

Vorgehensweise
1 Login mit Konto „Facility“.
2 Menü „Benutzerverwaltung“ öffnen.
3 Menü „Benutzer“ öffnen.
4 „Neuen Benutzer anlegen“ ausführen.
5 Im Bereich „Allgemein“ und „Karten/Codes“ fehlende Angaben vervollständigen und Zutrittsoptionen zuweisen (siehe nachfolgende Konfigurationshilfe).
6 „Speichern und Schließen“ ausführen.
7 Weitere Benutzer und Identifikationsmittel nach gleicher Vorgehensweise anlegen.

Konfigurationshilfe: Neuer Benutzer anlegen

Allgemein	**Erläuterung**
Typ	Nicht änderbares Informationsfeld mit der Anzeige „Standard“.
Vorname	Vorname des Benutzers
Zweitname	Zweiter Vorname des Benutzers
Nachname	Nachname des Benutzers
Firma/Abteilung	Firmenzugehörigkeit des Benutzers
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu diesem Benutzer.
Gültig ab	Zeitpunkt, ab dem der Benutzer mit seinen Identifikationsmitteln im Zutrittskontrollsystem agieren darf.
Unendlich gültig	Ist diese Option aktiviert, darf der Benutzer mit seinen Identifikationsmitteln dauerhaft im Zutrittskontrollsystem agieren.
Gültig bis	Zeitpunkt, bis zu dem der Benutzer mit seinen Identifikationsmitteln im Zutrittskontrollsystem agieren darf. Dieses Feld ist nur aktiv, wenn die Option "Unendlich gültig" deaktiviert wurde.

Konfigurationshilfe: Neuer Benutzer anlegen

Karten/Codes	**Erläuterung**	**Auslieferungszustand**
Modus	Mit dieser Auswahl kann einem Benutzer die Anzahl an dessen verfügbaren Identifikationsmitteln zugeordnet werden: • „Kein Identifikationsmittel“: Dem Benutzer sind keine Identifikationsmittel zugeordnet. In diesem Fall werden sämtliche Konfigurationsmöglichkeiten in der Administrationsoberfläche ausgeblendet. • „Einzelnes Identifikationsmittel“: Dem Benutzer ist ein Identifikationsmittel zugeordnet. • „Mehrere Identifikationsmittel“: Dem Benutzer sind mindestens zwei Identifikationsmittel zugeordnet.	„Einzelnes Identifikationsmittel“
Karte/Code		
Kartennummer/Code	Identifikationskennung eines eingelernten physischen Identifikationsmittels (Electronic-Key / Elektronic-Key-Card)) bzw. einer manuell eingegebenen Ziffernfolge (Code).	–
Kartennummer von Einlern-Leseeinheit empfangen	Funktions-Button: Einsatzbereite Funktion zum Einlernen von physikalischen Identifikationsmitteln, insofern im System eine Einlern-Leseeinheit konfiguriert wurde. Die Einlern-Leseeinheit kann eine beliebig im Objekt installierte und am Zutrittskontrollsystem angebundene Leseeinheit sein (z. B. ELM 600-…). Alternativ ist der Einsatz einer portablen Leseeinheit für den direkten Anschluss an einem Laptop/PC möglich (z. B. Siedle USB-Reader „readID One SE 1220 MNP“).	–
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu diesem Identifikationsmittel.	–
Gesperrt	Ist diese Option aktiviert, kann das Identifikationsmittel im Zutrittskontrollsystem nicht verwendet werden.	deaktiviert

Konfigurationshilfe: Neuer Benutzer anlegen

Karte/Code	Erläuterung	Auslieferungszustand
PIN (Ziffern)	Eingabefeld, um einem Benutzer eine PIN zuzuweisen. Die PIN ist nur dann erforderlich, wenn eine Doppel-Identifikation für ein höheres Maß an Sicherheit gewünscht wird (z. B. Identifikation mit Karte oder Zutritts-Code und zusätzlicher PIN). Jedem Benutzer kann ein beliebige PIN (Standard: vierstellig) zugewiesen werden.	–
PIN wiederholen	Eingabefeld zur Bestätigung des bereits in Feld „PIN (Ziffern)“ eingegebenen PIN.	–
Nutzungsanzahl	Anzahl, wie oft dieses Identifikationsmerkmal (Karte oder Code) in Abhängigkeit von der Wiederaufladezeit benutzt werden darf.	–
Wiederaufladezeit (min)	Zeit in Minuten, nach der die Restnutzungsanzahl wieder auf den Wert der Nutzungsanzahl gesetzt wird, um eine sich regelmäßig wiederholende Nutzung zu ermöglichen: • „0“: Das Identifikationsmittel ist gemäß der konfigurierten Nutzungsanzahl einmalig für die entsprechende Anzahl nutzbar. • „[Zahlenwert]“ (z. B. „600“): Die Nutzung des Identifikationsmittels ist für die entsprechende Anzahl mehrfach möglich. Beispiel „600“: Alle 600 Minuten ist gemäß der konfigurierten Nutzungsanzahl wieder die entsprechende Anzahl an Nutzungen möglich.	–
Restnutzungsanzahl	Zähler, wie viele Nutzungen mit diesem Identifikationsmerkmal (Karte oder Code) noch möglich sind.	–

Konfigurationshilfe: Neuer Benutzer anlegen

Alle Zutrittsgruppen	**Erläuterung**	**Auslieferungszustand**
Alle Zutrittsgruppen	Auswählbare Zutrittsgruppe(n) die für diesen Benutzer gelten sollen. Es müssen entweder mindestens eine Zutrittsgruppe oder eine Zutrittsberechtigung konfiguriert sein, da der Benutzer ansonsten keinen Zutritt erhält. In beiden Fällen ist eine Mehrfachauswahl möglich.	–
Gültig ab	Ist diese Option aktiviert, kann für diesen Benutzer einen Zeitpunkt konfiguriert werden, ab dem die Zutrittsregeln der ausgewählten Zutrittsgruppe gelten.	–
Gültig bis	Ist diese Option aktiviert, kann für diesen Benutzer einen Zeitpunkt konfiguriert werden, ab dem die Zutrittsregeln der ausgewählten Zutrittsgruppe nicht mehr gelten.	
Zutrittsberechtigungen		
Auswahlmenü	Auswahlmenü für die Filterung der angezeigten Zutrittsberechtigungen: • „Alle Türen anzeigen“: Es werden alle bereits konfigurierten (verfügbaren) Zutrittspunkte angezeigt. • „Ausgewählte Türen anzeigen“: Es werden die Zutrittspunkte angezeigt, die dem Benutzer zugeordnet sind. Zutrittspunkte aus der Zutrittsgruppe werden als bereits ausgewählt und nicht änderbar angezeigt, und können unter „Zutrittsberechtigungen“ nicht als einzelne Zutrittsberechtigung ausgewählt und konfiguriert werden. **Für jeden Benutzer muss entweder mindestens eine Zutrittsgruppe oder eine Zutrittsberechtigung konfiguriert sein. In beiden Fällen ist eine Mehrfachauswahl möglich.**	–

Konfigurationshilfe: Neuer Benutzer anlegen

Optionen	Erläuterung	Auslieferungszustand
Whitelist-Karte	Ohne Funktion / Nicht nutzbar	deaktiviert
Öffnen gesperrter Türen	Ist diese Option aktiviert, dürfen berechtigte Benutzer auch im Modus „Kein Zutritt“ den Zutrittspunkt mit ihrem Identifikationsmittel öffnen.	deaktiviert
Karte nachverfolgen	Ohne Funktion / Nicht nutzbar	deaktiviert
Berechtigung für Einbruchserkennung	Ohne Funktion / Nicht nutzbar	deaktiviert
Genehmiger (Zwei-Personen-Regel)	Ist diese Option aktiviert, darf ein hierfür berechtigter Benutzer den Zutritt an einem Zutrittspunkt als zweite Person freigeben, wenn dieser durch eine Zwei-Mann-Regel gesichert ist.	deaktiviert
Feuerwehr-Zutrittskarte	Ist diese Option aktiviert, erhält ein berechtigter Benutzer mit diesem Identifikationsmittel eine uneingeschränkte Zutrittsberechtigung an allen Zutrittspunkten.	deaktiviert
Längere Türöffnungszeit	Ist diese Option aktiviert, gelten für diesen Benutzer eine verlängerte Öffnungszeit an allen zugewiesenen Zutrittspunkten (z. B. Person im Rollstuhl).	deaktiviert
Einbruchsmelderegeln außer Kraft setzen	Ohne Funktion / Nicht nutzbar	deaktiviert
Befehle von Eingabeeinheiten erlauben	Ist diese Option aktiviert, darf ein berechtigter Benutzer den Zutrittspunkt manuell über die Eingabeeinheit des Zutrittspunkts steuern, wenn an der Eingabeeinheit die Türbefehle konfiguriert wurden (siehe Leser-Konfiguration „Türbefehle“ auf Seite 37).	deaktiviert
Sekundären Gültigkeitszeitraum nutzen	Ohne Funktion / Nicht nutzbar	deaktiviert
Allgemeine Offline-Karte	Ohne Funktion / Nicht nutzbar	deaktiviert
Offline-Alarme auslesen	Ohne Funktion / Nicht nutzbar	deaktiviert

Benutzerverwaltung durch Kunde/Betreiber

Daten/Konfiguration sichern

Führen Sie eine vollständige Daten- und Konfigurationssicherung durch.

Vorgehensweise

1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Administration" öffnen.
4 „Systeminformationen/Datenbank/Lizenz" öffnen.
5 „Datenbank" öffnen.
6 „Datenbank sichern" ausführen.
7 Abfrage mit „Ja" bestätigen.
8 Abfrage des Browsers mit „OK" bestätigen, um die Sicherung auf dem Laptop zu speichern.

Führen Sie eine Sicherung (Export) der Benutzerdaten und Zutrittsberechtigungen durch.

Hinweis

Ein Export vorhandener Benutzerdaten und deren Zutrittsberechtigungen ist ausschließlich mit dem Json-Dateiformat (*Json) möglich.

Vorgehensweise

1 Login mit Konto „Service".
2 Menü „Benutzerverwaltung" öffnen.
3 „Benutzer-Import/Export" öffnen.
4 „Exportiere…" ausführen.
5 Dateiformat „JSON-Dateiexport" auswählen.
6 Abfrage mit „Ja" bestätigen.
7 Im Dialog die Datentatei auf dem Laptop speichern.

Optional: Konten
Konto anlegen

Im Auslieferungszustand sind zwei Konto (Benutzerkonten der Bedienoberfläche des Controllers) mit vorkonfigurierten Zugangsdaten angelegt:
• Service: Konto mit umfangreicher Berechtigung für die Inbetriebnahme und Verwaltung des Zutrittskontrollsystems.
• Facility: Konto mit eingeschränkter Berechtigung für die Verwaltung der Benutzer des Zutrittskontrollsystems.

Weitere Konten können ausschließlich im Konto „Service“ angelegt werden.

Vorgehensweise
1 Login mit Konto „Service“.
2 Menü „Konten“ öffnen.
3 „Konten“ öffnen.
4 Bestehende Konten sind tabellarisch aufgelistet.
5 „Neu anlegen“ ausführen, wenn ein neues Konto angelegt werden soll oder bestehendes Konto zur Bearbeitung oder Neuerstellung (Neue Kopie)auswählen.
6 Im Bereich „Allgemein“ fehlende Angaben vervollständigen (siehe nachfolgende Konfigurationshilfe).
7 „Speichern und Schließen“ ausführen.
8 Weitere Konten neu anlegen / bearbeiten, wahlweise:
• nach gleicher Vorgehensweise (empfohlen, wenn sich beim Konto die Rolle und die Menürechte im Detail sehr unterscheiden)
• mit Funktion „Neue Kopie“ (empfohlen, wenn beim Konto die Rolle und die Menürechte gleich bleiben)

Konfigurationshilfe: Konto anlegen/bearbeiten

Allgemein	Erläuterung	Auslieferungszustand
Benutzername	Zu vergebende eindeutige/aussagekräftige Bezeichnung des Benutzerkontos. Der Benutzername ist ein Teil für die Anmeldung am Controller.	–
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu diesem Benutzerkonto.	–
Kennwort	Zu vergebendes Kennwort für die Anmeldung am Controller. Das Kennwort muss mindestens sechs Zeichen (Buchstaben, Ziffern, Sonderzeichen) enthalten.	–
Kennwort wiederholen	Bestätigung des eingegebenen „Kennworts“.	–
Kennwort muss geändert werden	Ist diese Option aktiviert, muss bei Erstanmeldung das Kennwort neu vergeben werden.	deaktiviert
Benutzer	Optional Auswahl eines Benutzers (verantwortliche natürliche Person des Benutzerkontos) des Zutrittskontrollsystem, dass einem Benutzerkonto zugewiesen werden kann.	–
Rolle	Rolle mit entsprechenden Rechten für die Zuordnung bei dem Benutzerkonto: • Regulärer Benutzer: Konfigurierbare Rolle mit umfangreichen Berechtigungen für die Inbetriebnahme und Verwaltung des Zutrittskontrollsystems. Über ein Benutzerkonto mit diesen Rollen können weitere Benutzerkonten angelegt werden. • Sitzung aufrecht erhalten: Option für die Rolle „Regulärer Benutzer“, zur Erstellung von Benutzerkonto ohne automatische Abmeldung von der Administrationsoberfläche wenn 10 Minuten lang keine Eingabe erfolgt ist.	–
Menürechte	Der Bereich „Menürechte“ wird nur angezeigt und ist konfigurierbar, wenn als Rolle „Regulärer Benutzer“ ausgewählt ist. Hier sind erlaubte Menüzugriffe für das Benutzerkonto detailliert konfigurierbar.	

Kennwort ändern

In diesem Bereich kann ausschließlich das Kennwort für das Benutzerkonto geändert werden, mit dem man am Controller angemeldet ist.
Kennworte für andere Benutzerkonten können nur über das Benutzerkonto „Service“ im Bereich „Konten“ direkt am ausgewählten Benutzerkonto geändert werden.

Vorgehensweise
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Konten“ öffnen.
3 „Kennwort“ öffnen.
4 Im Bereich „Allgemein“ wird der Benutzername des Benutzerkontos angezeigt.
5 „Kennwort ändern“ öffnen.
6 In Feld „Kennwort“ bisheriges Kennwort eingeben.
7 In Feld „Neues Kennwort“ neues und sicheres Kennwort eingeben.
8 In Feld „Neues Kennwort wiederholen“ die Kennworteingabe mit dem neuen Kennwort wiederholen.
9 „Speichern und Schließen“ ausführen.

Optional: Türverwaltung
Manuelle Türsteuerung (Status)

In diesem Bereich können alle konfigurierten Zutrittspunkte manuell über die Administrationsoberfläche des Secure Controllers bedient (ferngesteuert) werden. Es sind fünf Funktionen für die Zutrittspunkte auswählbar. Der Zugriff ist über das Benutzerkonto „Service“ und „Facility“ möglich.

Vorgehensweise
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Benutzerverwaltung“ öffnen.
3 „Türverwaltung“ öffnen.
4 „Manuelle Türsteuerung (Status)“ öffnen.
5 Alle konfigurierten Zutrittspunkte werden mit Zustands- und Statusinformationen tabellarisch aufgelistet.
6 Gewünschten Zutrittspunkt auswählen.
7 Gewünschte Funktion ausführen. Am entsprechenden Zutrittspunkt ändert sich der Status entsprechend der ausgeführten Funktion (siehe Tabelle „Manuelle Türsteuerung“).

Funktionsübersicht – Manuelle Türsteuerung

Funktion	Erläuterung	Zustandsanzeige des Zutrittspunkts	Statusanzeige des Zutrittspunkts
„Öffnen“	Der Zutrittspunkt wird geöffnet. Die Zeit der Öffnungsdauer ist abhängig von der Konfiguration des Zutrittspunkts.	„Geöffnet“ (Anzeige nur während der Öffnungsdauer)	–
„Schließen“	Der Zutrittspunkt wird wieder geschlossen. Diese Funktion ist bei dauerhaft geöffneten Zutrittspunkten erforderlich. Der Zutrittspunkt befindet sich dann wieder im Zustand „Normal“.	„Gesichert“	–
„Dauerhaft öffnen“	Der Zutrittspunkt wird dauerhaft geöffnet. Dieser Zustand besteht so lange, bis der Zutrittspunkt wieder geschlossen wird (manuell oder per Wochenprogramm).	„Geöffnet“	„Dauer-Auf“
„Normal“	Der Zutrittspunkt kann nur durch Einsatz eines Identifikationsmittels (Karte/Code) geöffnet werden.	„Gesichert“	–
„Sperren“	Der Zutrittspunkt ist geschlossen und kann durch reguläre Nutzer nicht geöffnet werden. Ausschließlich Nutzer mit erweiterter Berechtigung oder Sonderberechtigung können diesen Zutrittspunkt öffnen – insofern konfiguriert (z. B. Feuerwehr, VIP)	„Gesichert“	„Gesperrt“

Optional: Systemüberwachung

In diesem Bereich ist es möglich, den aktuellen Status der Schnittstellen, Ein- und Ausgänge, Verbindungen zu anderen Controllern (Geräteverbund) sowie deren Synchronisationsstatus einzusehen. In diesem Bereich ist keine Konfiguration des Systems möglich. Die Systemüberwachung ist ausschließlich über ein Benutzerkonto mit der zugeordneten Rolle „Service“ einsehbar.

Vorgehensweise

1 Login mit dem Benutzerkonto „Service“.
2 Menü „System“ öffnen.
3 „Systemüberwachung“ öffnen.
4 Gewünschten Bereich (z. B. Eingänge/Ausgänge) auswählen.
5 Sind weitere Unterbereiche auswählbar, durch die gewünschten Unterbereiche navigieren, bis die gewünschten Informationen angezeigt werden.

Optional: Protokoll/Report

Ereignisse

In diesem Bereich sind alle Systemereignisse protokolliert. Die Einträge werden nach Uhrzeit sortiert tabellarisch angezeigt. Jedem Ereignis ist eine Kategorie (Info, Achtung, Alarm) zugeordnet. Die angezeigten Ereignisse können wahlweise nach Zeit („Zeitspanne“) oder Kategorie („Tags/Typen“) gefiltert und sortiert angezeigt werden. Der Bereich „Ereignisse“ ist über das Benutzerkonto „Service“ und „Facility“ aufrufbar.

Vorgehensweise

1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Protokoll/Report“ öffnen.
3 „Ereignisse“ wird angezeigt.
4 Protokollierte Ereignisse werden nach Uhrzeit sortiert tabellarisch angezeigt.
5 Bei Bedarf, „Filter“ auswählen und Filterdetails zu „Kategorien“ anpassen, um nur gewünschte Ereignisse angezeigt zu bekommen.

In diesem Bereich können Berichte konfiguriert werden. Ein Bericht enthält ausgesuchte Ereignisse die systemseitig protokolliert sind (z. B. „Anzahl gewährter Zutritte je Tag“) und kann diese für einen konfigurierten Zeitraum anzeigen. Jeder Bericht muss individuell konfiguriert werden. Jeder Bericht kann nach dem Speichern jederzeit umkonfiguriert werden. Mit jedem Bericht können bis zu 1000 Zeilen (Ereignisse) angezeigt werden. Größere Berichte (mit konfigurierter Anzahl „Unbegrenzt“) sind ausschließlich direkt über den Dateiexport im CSV-Dateiformat (*.csv) möglich.
Die Datenbank speichert bis zu eine Millionen Ereignisse. Folgen weitere Ereignisse, werden immer die ältesten Ereignisse gelöscht.

Hinweis
Beim Betrieb mehrerer Controller in einem Geräteverbund, ist der zentrale Zugriff auf die Ereignisse und Berichte aller Controller und Controller-Erweiterungen ausschließlich über den primären Controller möglich. Bei den sekundären Controllern sind aber weiterhin der Zugriff auf die jeweils eigenen Ereignisse und Berichte möglich.

Neuen Bericht konfigurieren
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Protokoll/Report“ öffnen.
3 „Berichte“ öffnen.
4 Konfigurierte Berichte werden im Bereich „Berichte“ nach Reihenfolge der Erstellung tabellarisch angezeigt.
5 „Neu anlegen“ ausführen, um einen neuen Bericht zu konfigurieren
6 Im Bereich „Allgemein“ fehlende Angaben vervollständigen (siehe Konfigurationshilfe: Neuen Bericht konfigurieren).

Hinweis
Im Bereich „Parameter“ kann die gewünschten Datenabfrage bei Bedarf detailliert konfiguriert werden (z. B. ausgesuchter Zeitraum oder ausgesuchte Zutrittspunkte). Der Bereich „Parameter“ kann erst konfiguriert werden, wenn im Bereich „Allgemein“ eine Vorlage ausgewählt ist. Der Konfigurationsumfang ist abhängig von der ausgewählten Vorlage. Die Detailkonfiguration im Bereich „Parameter“ erfolgt per logische Operation verschiedener Variablen.
Erweiterte Kenntnisse über die Konfiguration von logische Operationen (Datenbankabfragen) sind bei der Konfiguration von Bedeutung.

7 Im Bereich „Parameter“ fehlende Angaben vervollständigen (siehe Konfigurationshilfe: Neuen Bericht konfigurieren).
8 „Speichern und Schließen“ ausführen.

Bericht ausführen
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Protokoll/Report“ öffnen.
3 „Berichte“ öffnen.
4 „Berichte“ wird angezeigt.
5 Konfigurierte Berichte werden nach Reihenfolge der Erstellung tabellarisch angezeigt.
6 „Ausführen“ eines Berichts ausführen, um einen Bericht angezeigt zu bekommen. Jeder Bericht kann im Dateiformat PDF (*.pdf) oder CSV (*.csv) exportiert und gespeichert werden.

Bedienung (Parameter)
- „Hinzufügen“: Erstellen einer neuen Bedingung.
- „Einfügen“ (bei ausgewählter Bedingung): Ergänzung weiterer Bedingungen an die ausgewählte Position.
- „Entfernen“: Entfernen einer ausgewählten Bedingung.

Konfigurationshilfe: Neuen Bericht konfigurieren

Allgemein	Erläuterung
Vorlage	Auswahlmenü mit verschiedenen Varianten der Erfassung von Ereignissen aus dem Zutrittskontrollsystem für die Protokollierung/ Dokumentation in einem Bericht (z. B. Bericht über die „Anzahl gewährter Zutritte je Tag"): • „Ereignisprotokoll": Erfassung aller Systemereignisse. • „Zutrittsprotokoll": Erfassung aller Zutrittsereignisse. • „Anzahl gewährter Zutritte je Tag": Erfassung aller Zutritte ohne Schließfächer. • „Anzahl gewährter Zutritte einzelner Benutzer je Tag": Erfassung einzelner Benutzer. • „Zutrittsprotokoll einschließlich Schließfach": Erfassung aller Zutrittsereignisse inkl. Schließfächer. • „Ereignisse zu geöffneten Schließfächern": Erfassung aller Schließfachereignisse. • „Kontonutzer in Zutrittsgruppe": Erfassung ausgewählter Benutzergruppen mit Zugang zum Controller. • „Benutzer in Zutrittsgruppe": Erfassung ausgewählter Benutzergruppen. • „Präsenz der Benutzer, Heute (erfordert erweiterte Parameter)": Erfassung ausgewählter Benutzer.
Titel	Zu vergebenden eindeutigen / aussagekräftigen Titel (Bezeichnung) für diesen Bericht. Bei Auswahl einer Vorlage wird die Bezeichnung der Vorlage automatisch eingefügt und kann manuell geändert werden.
Hinweis	Informationsfeld zum hinterlegen von zusätzlichen Informationen zu diesem Bericht.
Maximale Anzahl an Ereignissen	Anzahl an Ereignissen die im Bericht erfasst werden sollen (z. B. „1000": Es werden die ersten 1000 Ereignisse im Bericht dokumentiert).
Ereignisse für Bericht überspringen	Anzahl der Ereignisse die übersprungen werden sollen, um im Bericht die danach folgenden Ereignisse zu erfassen (z. B. „500": die ersten 500 Ereignisse werden im Bericht nicht berücksichtigt. Das erste Ereignis im Bericht ist das 501. Ereignis).

Konfigurationshilfe: Neuen Bericht konfigurieren

Parameter	Erläuterung
Operator	Auswählbares Bindeglied zwischen Variablen (z. B. Zeitpunkte) einer logischen Operation (Datenbankabfrage): • „(„: geöffnete Klammer • „)“: geschlossene Klammer • „NICHT“: für negierende Operationen (gegenteilig: z. B. nicht Zustand A) • „UND“: für zusammenfassende Operationen (z. B. Zustand A und Zustand B) • „UND NICHT“: für zusammenfassende Operationen mit Negation (z. B. Zustand A und nicht Zustand B) • „ODER“: für unterscheidende Operationen (Zustand A oder Zustand B) • „ODER NICHT“: für unterscheidende Operationen mit Negation (z. B. Zustand A oder nicht Zustand B) **Hinweis** Operatoren können beliebig kombiniert werden. Die Kombination muss aber sinnvoll sein, da sonst die Datenbankabfrage kein Ergebnis erzeugt. Die Anzahl der ausgegebenen Ereignisse ist abhängig von den tatsächlich vorhandenen Ereignissen und der im Bereich „Allgemein“ konfigurierten maximalen Anzahl an Ereignissen, die im Bericht ausgegeben werden sollen. **Beispiel** Für einen Bericht mit der Vorlage „Ereignisprotokoll“ sollen Ereignisse ausgegeben werden, mit dem Ereignisdatum 01.03.2021 oder 08.03.2021. Operation im Anzeigefeld: Ereigniszeit = '01/03/2021' ODER Ereigniszeit = '08/03/2021'

Konfigurationshilfe: Neuen Bericht konfigurieren

Parameter	Erläuterung
Variable	Platzhalter für eine belegbare veränderliche Größe (z. B. ausgewählter Zeitpunkt oder Zutrittspunkt) einer logischen Operation (Datenabfrage). Die auswählbaren Variablen sind abhängig von der unter „Allgemein“ gewählten „Vorlage“: • „Ereigniszeit“: Auswahl eines Zeitpunkts per Kalenderauswahl • „Benutzername“: Benutzer * • „Karten und Codes“: Identifikationsmittel * • „Türname“: Zutrittspunkte * • "Lesername“: Lese-/ Eingabeeinheiten * • „Ereignis“: Auswählbares Ereignis (z. B. „Zutritt verweigert“) • „Tür-ID“: Auswählbarer Zutrittspunkt (z. B. Tür 1 Haupteingang Süd) • „Leser-ID Auswählbare Lese-/ Eingabeeinheit (z. B. Leser Tür 1 Haupteingang Süd ELM Adresse2 Strang A) • „Schlüsselkasten“: Schlüsselkästen * • „Schlüsselkasten-ID“: Auswahl eines Schlüsselkastens (z. B. Schlüsselkasten 1) • „Zutrittsgruppen-ID“: Auswählbare Zutrittsgruppe (z. B. Mitarbeiter Produktion) *** Hinweis** Ist für eine ausgewählte Variable im Feld „Wert“ kein Auswahlmenü vorhanden, so kann im Feld „Wert“ eine Zeichenfolge eingegeben werden, nach der alle entsprechenden Ergebnisse für die logische Operation eingesetzt werden, deren Bezeichnung/Kennung mindestens die Eingabe in Feld „Wert“ enthält. Bleibt ein Auswahlmenü leer, ist keine Auswahl vorhanden.

Konfigurationshilfe: Neuen Bericht konfigurieren

Parameter	Erläuterung
Vergleich	Auswählbares Vergleichszeichen (z. B. „>“ oder „=“) für die Eingrenzung oder Ausgrenzung von Wertebereichen (z. B. Ereigniszeit > 01/03/2021) oder für die Zuweisung eines oder mehrerer Werte an eine Variable (z. B. Ereigniszeit = 01/03/2021) innerhalb einer logischen Operation (Datenbankabfrage). Die auswählbaren Vergleichszeichen sind abhängig von der gewählten „Variable“: • „=“: ist gleich • „<>“: ist ungleich • „>“: ist größer • „>=“: ist größer gleich • „<“: kleiner • „<=“: ist kleiner gleich • „innerhalb der letzten [x] Tage“: Alle der Ergebnisse der Variablen der angegebenen Anzahl an Tagen am dem Suchzeitpunkt. • „ist ungültig“: Alle Ergebnisse der Variablen die ungültig sind. • „enthält“: Alle Ergebnisse der Variablen, die die gesuchte Zeichenfolge im Namen oder Kennung enthält. Groß- und Kleinschreibung müssen beachtet werden.
Manuelle Eingabe	Ist diese Option aktiviert, wird ein manuell eingegebener oder per Auswahlmenü ausgewählten Wert im Feld „Wert“ („Standardwert“) durch einen manuell eingegebenen Wert im Feld „Manueller Eingabewert“ überschrieben. Hierfür öffnen sich die Eingabefelder „Manueller Eingabewert“ und das bisherige Feld „Wert“ wird zur klaren Unterscheidung mit „Standardwert“ bezeichnet.
Manueller Eingabewert	Eingabefeld für einen manuell eingegebenen Wert (Zeichenfolge, Namen, Ziffernfolge, …) der den Wert in Feld „Standardwert“ überschreibt. Der Wert wird für die logische Operation mit der Variablen verwendet.

Zutrittsprotokoll

Konfigurationshilfe: Neuen Bericht konfigurieren

Parameter	Erläuterung
Standardwert	Ursprüngliches Feld „Wert“, dass bei Aktivierung der Option „Manuelle Eingabe“ systemseitig in „Standardwert“ umbenannt wird. Eingabefeld für einen manuell eingegebenen oder per Auswahlmenü ausgewählten Wert (Zeichenfolge, Namen, Ziffernfolge, …). Der Wert wird für die logische Operation mit der Variablen verwendet.
Wert	Eingabefeld für einen manuell eingegebenen oder per Auswahlmenü ausgewählten Wert (Zeichenfolge, Namen, Ziffernfolge, …). Der Wert wird für die logische Operation mit der Variablen verwendet.

In diesem Bereich sind alle erfolgreichen Zutritte der letzten 12 Stunden protokolliert. Die Einträge werden nach Uhrzeit sortiert tabellarisch angezeigt. Das Zutrittsprotokoll ist über das Benutzerkonto „Service“ und „Facility“ aufrufbar.

Vorgehensweise

1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service“ oder „Facility“).
2 Menü „Protokoll/Report“ öffnen.
3 „Zutrittsprotokoll“ öffnen.
4 Erfolgreiche Zutritte der letzten 12 Stunden werden tabellarisch angezeigt.

Über die Administrationsoberfläche des Secure Controllers kann bei Bedarf ein Neustart ausgelöst werden. Diese Funktion ist an zwei Stellen im Controller, aber nur über ein Benutzerkonto mit zugeordneter Service-Rolle verfügbar.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Administration" öffnen.
4 „Firmware-Update" oder „Systeminformationen/Datenbank/Lizenz" öffnen.
5 Im Bereich nach unten scrollen.
6 „Gerät neu starten" ausführen.
7 Abfrage mit „Ja" bestätigen.
8 Eine Bestätigung wird angezeigt.
9 Der Controller führt einen Neustart durch und ist nach ca. einer Minute wieder mit der Anmeldeseite erreichbar.

Die Sabotageüberwachung des Secure Controllers überwacht mit optischer Sensorik das Öffnen des Controller-Gehäuses und ist ab der Betriebsbereitschaft des Geräts sofort aktiv.
Wird das Gehäuse geöffnet, werden in regelmäßigen Zeitabständen Alarmmeldungen auf der Administrationsoberfläche ausgegeben und diese protokolliert. Über die konfigurierbare Logik ist eine weitere Verarbeitung der Alarmmeldung möglich (z. B. Ausgang des Controllers schaltet eine Signalisierung).

Konfiguration
Im Benutzerkonto „root" ist die Sabotageüberwachung deaktivierbar und die Empfindlichkeit der optischen Sensorik veränderbar.

Vorgehensweise
1 Login mit Konto „root".
2 Menü „System" öffnen.
3 „Administration" öffnen.
4 „Systemeigenschaften" öffnen.
5 „Eigenschaften" öffnen.
6 Reiter „Sabotageüberwachung" auswählen.

Konfigurationsmöglichkeiten:
• Option „Optischen Sensor deaktivieren" aktivieren, um die Sabotageüberwachung zu deaktivieren.
• Empfindlichkeit der optischen Sensorik im Feld „Schwellwert Umgebungslicht" verändern, um diese an die Umgebungsbedingungen des Controllers (z. B. Lichtverhältnisse im Technikraum) anzupassen. Je höher der Wert gewählt wird, umso mehr reagiert die optische Sensorik auf einfallendes Umgebungslicht, wenn das Gehäuse geöffnet ist.

7 „Speichern" ausführen.
8 Abmelden vom Konto „root".

Schwellwert für die optische Sensorik prüfen
Im Auslieferungszustand ist der Schwellwert für die Empfindlichkeit der optischen Sensorik auf „150"vorkonfiguriert.
Sollte aufgrund der Umgebungsbedingungen des Secure Controllers ein anderer Schwellwert erforderlich sein, können die Lichtverhältnisse mit geschlossenem und geöffnetem Gehäuse abgefragt werden.

Vorgehensweise
1 Das Gehäuse des Secure Controllers ist geschlossen.
2 Login mit Konto „root".
3 Menü „System" öffnen.
4 „Systemüberwachung" öffnen.
5 „Eingänge/Ausgänge" öffnen.
6 „Logische Eingänge" öffnen.
7 Bei „Sabotageüberwachung Helligkeit (Sensor)", die Aktion „Aktualisierung" ausführen.
8 Der Wert bei „Sabotageüberwachung Helligkeit (Sensor)" entspricht dem Helligkeitswert bei geschlossenem Gehäuse (z. B. 500).
9 Lichtverhältnisse ggf. so anpassen, wie sie bei einem unberechtigten Zugriff zu erwarten wären.
10 Gehäuse des Secure Controllers öffnen und ca. 10 Sekunden warten.
11 Bei „Sabotageüberwachung Helligkeit (Sensor)", die Aktion „Aktualisierung" ausführen.
12 Der Wert bei „Sabotageüberwachung Helligkeit (Sensor)" entspricht dem Helligkeitswert bei geöffnetem Gehäuse mit den Lichtverhältnissen (z. B. 150).
13 Gehäuse des Secure Controllers wieder schließen.
14 Empfindlichkeit der optischen Sensorik anpassen. Soll die Sabotageerkennung auf den ermittelten Helligkeitswert reagieren, so ist der Schwellwert ausreichend höher zu wählen (z. B. 200 oder höher).
15 Konfigurierten Wert durch Tests überprüfen.

Optional: Administration

Daten löschen

Über die Administrationsoberfläche des Secure Controllers können bei Bedarf alle Konfigurationsdaten von Geräten und Benutzern gelöscht werden. Diese Funktion ist nur über ein Benutzerkonto mit zugeordneter Service-Rolle verfügbar.

Hinweis
Es werden nur Konfigurationsdaten zu Zutrittspunkten, Lese- und Eingabeeinheiten, Benutzer und Wochenprogrammen sowie Kennwörter der Benutzerkonten gelöscht. Zusätzlich angelegte Benutzerkonten werden vollständig gelöscht. Die Netzwerkkonfiguration bleiben erhalten.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Administration" öffnen.
4 „Systeminformationen/Datenbank/Lizenz" öffnen.
5 „Datenbank" öffnen.
6 „Datenbank löschen" ausführen.
7 Abfrage mit „Ja" bestätigen.
8 Der Controller führt einen Neustart durch und ist nach ca. einer Minute wieder mit der Anmeldeseite erreichbar.

Werkseinstellungen wiederherstellen

Softwareseitige Ausführung
Über die Administrationsoberfläche des Secure Controllers können die Werkseinstellungen wiederhergestellt werden.
Alle gespeicherten Informationen und die gesamte Konfiguration des Controllers, der Geräte und der Benutzer werden dabei unwiederbringlich gelöscht.
Diese Funktion ist nur über ein Benutzerkonto mit zugeordneter Service-Rolle verfügbar.

Hinweis
Da auch die Netzwerkkonfiguration gelöscht wird, muss die IP-Adresse des Controllers ggf. neu ermittelt werden und die Anmeldung ist nur noch mit den vorkonfigurierten Anmeldedaten möglich – siehe Seite 4.

Vorgehensweise
1 Login mit Konto „Service".
2 Menü „System" öffnen.
3 „Administration" öffnen.
4 „Firmware-Update" öffnen.
5 „Werkseinstellungen" öffnen.
6 Funktion „Werkseinstellungen" ausführen.
7 Sicherheitsabfrage öffnet sich.
8 Angezeigten „Reset-Code" in das Eingabefeld eingeben. Der Button „Werkseinstellungen" ist erst aktiv und ausführbar, wenn der korrekte Reset-Code eingegeben wurde.
9 „Werkseinstellungen" ausführen, um das Rücksetzen auf die Werkseinstellungen zu starten.
10 Der Controller wird in die Werkseinstellungen zurückgesetzt und neu gestartet.

Hardwareseitige Ausführung
Durch Betätigung der „Benutzertaste" am Secure Controller können die Werkseinstellungen wiederhergestellt werden.
Alle gespeicherten Informationen und die gesamte Konfiguration des Controllers, der Geräte und der Benutzer werden dabei unwiederbringlich gelöscht.
Für die Betätigung der „Benutzertaste" muss das Gehäuse des Secure-Controllers geöffnet sein.
Details zur „Benutzertaste" und LED-Signalisierung siehe Seite 8.

Hinweis
Da auch die Netzwerkkonfiguration gelöscht wird, muss die IP-Adresse des Controllers ggf. neu ermittelt werden und die Anmeldung ist nur noch mit den vorkonfigurierten Anmeldedaten möglich – siehe Seite 4.

Vorgehensweise
1 Gehäuse des Secure Controllers öffnen
2 „Benutzertaste" innerhalb von fünf Sekunden fünf mal betätigen.
3 Die beiden LEDs für die Anzeige des Betriebszustands (grün) und des Systemstatus (rot) blinken.
4 Ein Signalton ertönt, der sich bis zu drei Mal wiederholen wird (Intervall: 3 s Signalton gefolgt von 3 s Pause).
5 Beim vierten Signalton die „Benutzertaste" betätigen und halten, bis der Signalton endet. Erfolgt bis zum letzten Signalton keine Tastenbetätigung, endet der Vorgang automatisch ohne eine Systemveränderung durchzuführen.
6 Der Controller wird in die Werkseinstellungen zurückgesetzt und automatisch neu gestartet und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.

Durch Betätigung der „Benutzertaste“ am Secure Controller können die Netzwerkeinstellungen auf zwei Varianten zurückgesetzt werden. Für die Betätigung der „Benutzertaste“ muss das Gehäuse des Secure-Controllers geöffnet sein. Details zur „Benutzertaste“ und LED-Signalisierung siehe Seite 8.

Hinweis
Da die Netzwerkkonfiguration gelöscht wird, muss die IP-Adresse des Controllers bei DHCP-Betrieb ggf. neu ermittelt werden.

Wichtig!
Das Zurücksetzen der Netzwerkeinstellungen ist in zwei Varianten möglich:
• DHCP-Betrieb: Die Netzwerkeinstellungen werden auf DHCP-Betrieb zurückgesetzt und der Controller neu gestartet.
• Statische IP-Adresse: Die Netzwerkeinstellungen werden gelöscht und die statische IP-Adresse: 192.168.1.100 konfiguriert.

Vorgehensweise
1 Gehäuse des Secure Controllers öffnen
2 „Benutzertaste“ innerhalb von fünf Sekunden fünf mal betätigen.
3 Die beiden LEDs für die Anzeige des Betriebszustands (grün) und des Systemstatus (rot) blinken.
4 Ein Signalton ertönt, der sich bis zu drei Mal wiederholen wird (Intervall: 3 s Signalton gefolgt von 3 s Pause).
5 Auswahl – zweiter/dritter Signalton
• Zweiter Signalton – DHCP-Betrieb: „Benutzertaste“ beim zweiten Signalton betätigen und halten, bis der Signalton endet.
• Dritter Signalton – Statische IP-Adresse: „Benutzertaste“ beim dritten Signalton betätigen und halten, bis der Signalton endet.
Erfolgt bis zum letzten Signalton keine Tastenbetätigung, endet der Vorgang automatisch ohne eine Systemveränderung durchzuführen.
6 Die Netzwerkeinstellungen werden wie ausgewählt zurückgesetzt/geändert. Der Controller wird automatisch neu gestartet und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.

Der Import/Export von Benutzerdaten und deren Zutrittsberechtigungen ist per Datei mit folgenden Dateiformaten möglich:

Dateiformat	Datentransfer
JSON (*.Json)	Import und Export möglich
CSV (*.csv)	Import möglich

Verwendungszweck
• JSON: Das JSON-Dateiformat ist vorgesehen, um die konfigurierten Benutzerdaten und deren Zutrittsberechtigungen aus dem Secure Controller für Sicherungszwecke (Archivierung) zu exportieren, um diese bei Bedarf wieder importieren zu können.
• CSV: Das CSV-Dateiformat ist vorgesehen für den Import neuer Benutzer und ggf. zugeordneter Kartennummern/Codes aus anderen Systemen oder Programmen. Daten aus anderen System oder Programmen müssen gemäß nachfolgender Anleitung vor dem Import aufbereitet werden. Details siehe „Aufbereitung von Datensätzen aus anderen Systemen".

Hinweis
Bei der Datenkonvertierung zwischen dem Dateiformat „CSV" (*.csv) und „MS Excel" (*.xslx) und zurück, ist bei der Verwendung von MS 365 oder MS Office 365 darauf zu achten, dass die erste Zeile der endgültigen CSV-Datei (für den Import in den Secure Controller) die Spaltenüberschriften aus der Musterdatei enthält.

Export einer Datendatei
Ein Export vorhandener Benutzerdaten und deren Zutrittsberechtigungen ist ausschließlich mit dem Json-Dateiformat (*Json) möglich (für die Datensicherung oder die manuelle Datenbearbeitung).

Vorgehensweise:
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service" oder „Facility").
2 Menü „Benutzerverwaltung" öffnen.
3 „Benutzer-Import/Export" öffnen.
4 „Exportiere…" ausführen.
5 Dateiformat je nach Verwendungszweck auswählen (z. B. „JSON export all").
6 Abfrage mit „Ja" bestätigen.
7 Im Dialog die Datendatei auf dem Laptop speichern.
8 Die Datendatei ist für den gewünschten Verwendungszweck verfügbar.

Aufbereitung von Datensätzen aus anderen Systemen
Eine Datenvorbereitung ist erforderlich, wenn Daten aus einem anderen System oder Verwaltungsprogramm exportiert wurden und für den Import in den Secure Controller verwendet werden sollen.

Erster Datenimport
Diese Anleitung beschreibt die Aufbereitung (und Übernahme) von Datensätzen im MS-Excel-Dateiformat (*.xlsx).

Vorlagendatei für den ersten Datenimport
Für den ersten Datenimport von Benutzerdaten in den Secure Controller nutzen Sie bitte die Vorlagendatei von Siedle.

Vorbereitung
Laden Sie sich die Siedle-Vorlagendatei „Musterdatei Benutzerverwaltung SC 600.xlsx" von der Siedle-Webseite herunter.

Wichtig!
• In der Vorlagedatei befinden sich beschriftete Spalten für die Befüllung mit den entsprechenden Daten der zukünftigen Benutzer des Zutrittskontrollsystems.
• Die Überschriften der Spalten dürfen nicht verändert werden.
• Alle Datenbereiche (Spalten) müssen mit dem Zellformat „Text" formatiert sein.
• Karten- oder Codenummern in der Spalte „CARDS_1" müssen einmalig sein.
• Gültigkeitsangaben mit Datum müssen mit der folgenden Schreibweise befüllt sein: [TT/MM/JJJJ] (z. B. „30/03/2024").
• Gültigkeitsangaben mit Datum und Uhrzeit müssen mit der folgenden Schreibweise befüllt sein: [TT/MM/JJJJ hh:mm:ss] (z. B. „30/03/2024 18:30:59").
• In der Spalte „DOORS" können ein oder mehrere Zutrittspunkte eingetragen werden. Bei mehreren Zutrittspunkten ist auf die Schreibweise mit Anführungszeichen (Hochkommata) und Strichpunkten (Semikolon) zu achten (z. B. „Eingang_ Nord;Lieferanteneingang").

Vorgehensweise
1 Beide Dateien (Kunden-Datendatei und Siedle-Vorlagendatei) in MS Excel öffnen.
2 Alle Datenbereiche der kundenseitigen Datendatei müssen sich im Zellformat „Text" befinden, ansonsten betroffene Datenbereiche nachträglich formatieren und Inhalte kontrollieren.
3 Daten aus kundenseitiger Datendatei per Copy&Paste in die entsprechenden Bereiche der Siedle-Vorlagedatei kopieren (ggf. mit S-Verweis arbeiten).
4 Kundenseitigen Datendatei schließen.
5 Befüllte Siedle-Vorlagendatei mit einem neuen Namen speichern.

Hinweis
Die neue Datei muss jetzt als CSV-Datei mit der Unicode-Zeichenkodierung „UTF-8" gespeichert werden.

6 Funktion „Speichern unter" ausführen (Pfad im geöffneten MS Excel: Datei > Speichern unter).
7 Beliebigen Speicherort auswählen und Dateinamen vergeben.
8 In der Auswahl „CSV UTF-8 (durch Trennzeichen getrennt) (*.csv)" auswählen.
9 „Speichern" ausführen.

Wichtig!
Jegliche Datensätze in zu importierende Dateien müssen immer mit der Unicode-Zeichenkodierung „UTF-8" gespeichert worden sein! Andernfalls könnten Umlaute oder Sonderzeichen falsch interpretiert bzw. nicht erkannt werden.

Import einer Datendatei
Die CSV-Datendatei kann nun in den Secure Controller importiert werden. Der Import muss mit der Auswahl „CSV-Datei (Semikolon)" durchgeführt werden.

Vorgehensweise
1 Login mit dem jeweiligen Benutzerkonto (z. B. „Service" oder „Facility").
2 Menü „Benutzerverwaltung" öffnen.
3 „Benutzer-Import/Export" öffnen.
4 „Importiere …" ausführen.
5 Dateiformat auswählen (z. B. „CSV-Datei (Semikolon)").
6 Im Dialog die Datentatei auswählen und mit „Hochladen" importieren.
7 Bestätigungsmeldung mit „OK" bestätigen.
8 Importierte Benutzerdaten und deren Zutrittsberechtigungen werden tabellarisch angezeigt.
9 Importierte Daten auf Richtigkeit kontrollieren.
10 Im Falle eines Fehlers, importierte Datensätze löschen und Dateiimport mit korrigierter Datendatei wiederholen.

Einzelnen Controller ersetzen
Einen defekten Controller im (autonomen) Einzelbetrieb tauschen Sie nach folgender Vorgehensweise aus:

Voraussetzungen
• Für die Wiederherstellung des Zutrittskontrollsystems mit einem neuen Controller ist eine Datensicherung (Backup) erforderlich.
• Das Kennwort für das Benutzerkonto „Service", das zum Zeitpunkt der Datensicherung gültig war, muss bekannt sein.

Controller-Austausch vorbereiten
1 Alle am defekten Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) spannungsfrei schalten.
2 Externe Spannungsversorgung am defekten Controller ausschalten (falls extern versorgt).
3 Defekten Controller vom Netzwerk trennen.
4 Alle Anschlüsse/Drähte/Leitungen der am defekten Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) dokumentieren und deren Steckverbindung (Steckklemmen) abziehen.
5 Defekten Controller demontieren.
6 Neuen Controller montieren.
7 Alle Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) gemäß Dokumentation wieder korrekt mit dem neuen Controller verbinden.

Neuen Controller in Betrieb nehmen
8 Neuen Controller mit Netzwerk verbinden.
9 Externe Spannungsversorgung am neuen Controller einschalten (falls extern versorgt).

Hinweis
Die Netzwerkkonfiguration des neuen Controllers ist nicht Bestandteil der Wiederherstellung des Zutrittskontrollsystems.

10 IP-Adresse des neuen Controllers ermitteln. Weiterführende Informationen siehe Seite 13.
11 Auf der Anmeldeseite des Controllers mit den Zugangsdaten des Kontos „Service" anmelden.
12 Bei „Kennwort", das Kennwort „Siedle1234" (Auslieferungszustand) eingeben.

Hinweis
Mit der ersten Anmeldung am Secure Controller öffnet sich der Kennwort-Änderungsdialog.

13 Bitte vergeben Sie ein neues Kennwort für das Konto „Service".

Hinweis
Dieses Kennwort ist nur kurzzeitig gültig und wird mit der Systemwiederherstellung geändert.

Daten und Konfiguration wiederherstellen
14 Menü „System" öffnen.
15 „Administration" öffnen.
16 „Systeminformationen/ Datenbank/Lizenz" öffnen.
17 „Datenbank" öffnen.
18 „Datenbank wiederherstellen" ausführen.
19 Mit „Datei auswählen", die Datei für die Wiederherstellung der Datensicherung auswählen und mit „Hochladen" importieren.
20 Sicherheitsabfrage mit „Ja" bestätigen.
21 Die Wiederherstellung des Zutrittskontrollsystems auf dem neuen Controller wird durchgeführt.

Hinweis
Dieser Vorgang dauert in der Regel mehrere Minuten.

22 Zum Abschluss führt der neue Controller automatisch einen Neustart durch und ist danach wieder wie zum Stand der zuletzt durchgeführten Datensicherung nutzbar.

Sekundären Controller ersetzen
Einen Controller der im Geräteverbund als sekundäres Gerät konfiguriert ist, tauschen Sie nach folgender Vorgehensweise aus:

Systemaktualisierung prüfen!
• Alle Geräte im Bestandssystem und auch das Ersatzgerät müssen auf dem gleichen und aktuellen Softwarestand sein! Prüfen Sie im Vorfeld ob eine Systemaktualisierung verfügbar ist. Details siehe Seite 97.
• Falls das Ersatzgerät über eine neuere Systemversion als ihr Bestandssystem verfügt, ist vor dem Gerätetausch eine Systemaktualisierung aller im Geräteverbund betriebenen Controller erforderlich.

Controller-Austausch vorbereiten
1 Alle am sekundären Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) spannungsfrei schalten.
2 Externe Spannungsversorgung am sekundären Controller ausschalten (falls extern versorgt).
3 Sekundären Controller vom Netzwerk trennen.
4 Alle Anschlüsse/Drähte/Leitungen der am sekundären Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) dokumentieren und deren Steckverbindung (Steckklemmen) abziehen.
5 Sekundären Controller demontieren.
6 Neuen Controller montieren.
7 Alle Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) gemäß Dokumentation wieder korrekt mit dem neuen Controller verbinden.

Hinweis
Anbindung an die Spannungsversorgung und das Netzwerk erfolgen zu einem späteren Zeitpunkt!

8 Am dazugehörigen primären Controller mit Konto „Service“ anmelden.
9 Menü „Secure Controller“ öffnen (Pfad: System > Administration > Secure Controller).

Systemaktualisierung aller Bestands-Controller durchführen
Falls erforderlich, führen Sie eine Systemaktualisierung bei allen zum Geräteverbund gehörenden primären und sekundären Controllern durch. Details siehe Seite 97.

Neuen Controller in Betrieb nehmen
10 Neuen Controller mit Netzwerk verbinden.
11 Externe Spannungsversorgung am neuen Controller einschalten (falls extern versorgt).
12 „Suche Siedle Secure Controller …“ ausführen, um die IP-Adresse des neue Controllers ausfindig zu machen.
13 Es öffnet sich ein neues Fenster mit den Suchergebnissen.
14 Gefundene Controller werden tabellarisch aufgelistet.
15 IP-Adresse des neuen Controllers notieren.
16 Fenster mit den Suchergebnissen schließen.

Systemaktualisierung des neuen Controllers (Ersatzgerät) durchführen
Falls erforderlich, führen Sie eine Systemaktualisierung des neuen Controllers durch. Details siehe Seite 97.

Neuen Controller einbinden
17 Sekundären Controller, der ausgetauscht werden soll, in der Liste auswählen.
18 IP-Adresse des neuen Controllers eingeben.
19 Nach unten zum Feld „MAC-Adresse“ nach unten navigieren.
20 „Neue MAC-Adresse abrufen“ ausführen, um die MAC-Adresse des neuen Controllers zu übernehmen.
21 „Speichern und Schließen“ ausführen.
22 Im Menü „Aktionen“ die Funktion „Als sekundäres Gerät festlegen“ ausführen.
23 Sicherheitsabfrage mit „Ja“ bestätigen.
24 Der sekundäre Controller wird synchronisiert und in den Geräteverbund integriert.
Dieser Vorgang dauert in der Regel mehrere Minuten (mindestens ca. drei Minuten, abhängig von der Anlagengröße (Anzahl Controller und Benutzer)).
25 Der Vorgang ist vollständig abgeschlossen, wenn im Menü „Secure Controller“ der Status „synchronisiert“ angezeigt wird.
26 Funktionsprüfung mit allen am neuen sekundären Controller angeschlossenen Geräten durchführen.

Wichtig!
Bei Verwendung der Funktionen „Importiere als sekundäres Gerät“ und „Löschen“, wird die Konfiguration des zu ersetzenden Controllers immer gelöscht.

Primären Controller ersetzen
Einen Controller der im Geräteverbund als primäres Gerät konfiguriert ist, tauschen Sie nach folgender Vorgehensweise aus:

Systemaktualisierung prüfen!
• Alle Geräte im Bestandssystem und auch das Ersatzgerät müssen auf dem gleichen und aktuellen Softwarestand sein! Prüfen Sie im Vorfeld ob eine Systemaktualisierung verfügbar ist. Details siehe Seite 97.
• Falls das Ersatzgerät über eine neuere Systemversion als ihr Bestandssystem verfügt, ist vor dem Gerätetausch eine Systemaktualisierung aller im Geräteverbund betriebenen Controller erforderlich.

Controller-Austausch vorbereiten
1 Alle am primären Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) spannungsfrei schalten.
2 Externe Spannungsversorgung am primären Controller ausschalten (falls extern versorgt).
3 Primären Controller vom Netzwerk trennen.
4 Alle Anschlüsse/Drähte/Leitungen der am primären Controller betriebenen Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) dokumentieren und deren Steckverbindung (Steckklemmen) abziehen.
5 Primären Controller demontieren.
6 Neuen Controller montieren.
7 Alle Geräte (Lese- und Eingabeeinheiten, sonstige Komponenten) gemäß Dokumentation wieder korrekt mit dem neuen Controller verbinden.

Hinweis
Anbindung an die Spannungsversorgung und das Netzwerk erfolgen zu einem späteren Zeitpunkt!

Rolle des primären Geräts einem sekundären Controller zuweisen
8 An einem beliebigen sekundären Controller mit Konto „Service“ anmelden.
9 Menü „Secure Controller“ öffnen (Pfad: System > Administration > Secure Controller).
10 „Primäres Gerät ändern“ ausführen.
11 Der sekundäre Controller bestimmt einen neuen primären Controller aus allen bestehenden sekundären Controllern.
12 Der neue primäre Controller führt einen Neustart durch.
13 Am neuen primären Controller mit Konto „Service“ anmelden.
14 Menü „Secure Controller“ öffnen (Pfad: System > Administration > Secure Controller).

Systemaktualisierung aller Bestands-Controller durchführen
Falls erforderlich, führen Sie eine Systemaktualisierung bei allen zum Geräteverbund gehörenden primären und sekundären Controllern durch. Details siehe Seite 97.

Neuen Controller in Betrieb nehmen
15 Neuen Controller mit Netzwerk verbinden.
16 Externe Spannungsversorgung am neuen Controller einschalten (falls extern versorgt).
17 „Suche Siedle Secure Controller …“ ausführen, um die IP-Adresse des neue Controllers ausfindig zu machen.
18 Es öffnet sich ein neues Fenster mit den Suchergebnissen.
19 Gefundene Controller werden tabellarisch aufgelistet.
20 IP-Adresse des neuen Controllers notieren.
21 Fenster mit den Suchergebnissen schließen.

Systemaktualisierung des neuen Controllers (Ersatzgerät) durchführen
Falls erforderlich, führen Sie eine Systemaktualisierung des neuen Controllers durch. Details siehe Seite 97.

Neuen Controller einbinden
22 Sekundären Controller (ehemaliger primärer Controller) der ausgetauscht werden soll, in der Liste auswählen.
23 IP-Adresse des neuen Controllers eingeben.
24 Nach unten zum Feld „MAC-Adresse“ nach unten navigieren.
25 „Neue MAC-Adresse abrufen“ ausführen, um die MAC-Adresse des neuen Controllers zu übernehmen.
26 „Speichern und Schließen“ ausführen.
27 Im Menü „Aktionen“ die Funktion „Als sekundäres Gerät festlegen“ ausführen.
28 Sicherheitsabfrage mit „Ja“ bestätigen.
29 Der sekundäre Controller wird synchronisiert und in den Geräteverbund integriert.
Dieser Vorgang dauert in der Regel mehrere Minuten (mindestens ca. drei Minuten, abhängig von der Anlagengröße (Anzahl Controller und Benutzer)).
30 Der Vorgang ist vollständig abgeschlossen, wenn im Menü „Secure Controller“ der Status „synchronisiert“ angezeigt wird.
31 Funktionsprüfung mit allen am neuen sekundären Controller angeschlossenen Geräten durchführen.

Wichtig!
Bei Verwendung der Funktionen „Importiere als sekundäres Gerät“ und „Löschen“, wird die Konfiguration des zu ersetzenden Controllers immer gelöscht.

Sekundären Controller aus dem Geräteverbund löschen

Wichtig!
Soll ein sekundärer Controller aus einem Geräteverbund entfernt werden, so muss dieser gelöscht werden. Dabei gehen alle Berechtigungen und Konfigurationsdaten des zu löschenden sekundären Controllers verloren und angebundene Endgeräte des Zutrittskontrollsystems (z. B. Leser) werden nicht mehr nutzbar sein.

Vorgehensweise
1 Am dazugehörigen primären Controller mit Konto „Service“ anmelden.
2 Menü „Secure Controller“ öffnen (Pfad: System > Administration > Secure Controller).
3 Sekundären Controller, der entfernt werden soll, in der Liste auswählen.
4 Menü „Bearbeiten von Siedle Secure Controller [<Name des Controllers>]“ öffnet sich.
5 „Löschen“ ausführen.
6 In der Sicherheitsabfrage soll über die Option entschieden werden, ob der sekundäre Controller aus dem primären Controller entfernt werden soll oder nicht.
7 Sicherheitsabfrage mit „Ja“ bestätigen.
8 Menü „Bearbeiten von Siedle Secure Controller [<Name des Controllers>]“ schließt sich.
9 Alle Konfigurationsdaten des sekundären Controllers bis auf die IP-Adresse und den Hostnamen sind gelöscht. Benutzerkonten und Kennwörter befinden sich wieder im Auslieferungszustand.

Optional: Service
Servicemodus aktivieren

Durch Betätigung der „Benutzertaste“ am Secure Controller kann der Service-Modus des Secure Controllers aktiviert werden. In diesem Modus ist der Secure Controller nicht mehr über die Administrationsoberfläche erreichbar. Diese Funktion ist ausschließlich für den Einsatz für den Siedle-Service vorgesehen. Für die Betätigung der „Benutzertaste“ muss das Gehäuse des Secure-Controllers geöffnet sein. Details zur „Benutzertaste“ und LED-Signalisierung siehe Seite 8.

Wichtig!
Bei versehentlicher Aktivierung kann der Service-Modus nur durch eine Unterbrechung der Spannungsversorgung des Secure Controllers deaktiviert werden.

Vorgehensweise
1 Gehäuse des Secure Controllers öffnen
2 „Benutzertaste“ innerhalb von fünf Sekunden fünf mal betätigen.
3 Die beiden LEDs für die Anzeige des Betriebszustands (grün) und des Systemstatus (rot) blinken.
4 Ein Signalton ertönt, der sich bis zu drei Mal wiederholen wird (Intervall: 3 s Signalton gefolgt von 3 s Pause).
5 Bereits beim ersten Signalton die „Benutzertaste“ betätigen und halten, bis der Signalton endet.
6 Der Controller befindet sich nun im Service-Modus und ist über die Administrationsoberfläche nicht mehr erreichbar.
7 Um den Service-Modus zu deaktivieren, Spannungsversorgung des Secure Controllers für ca. 10 Sekunden unterbrechen. Ab dem Neustart ist der Secure Controller nach ca. einer Minute wieder über die Administrationsoberfläche erreichbar.

Erfolgt bis zum letzten Signalton keine Tastenbetätigung, endet der Vorgang automatisch ohne eine Systemveränderung durchzuführen.

Wichtig!

• Ist ein neues Update für den Secure Controller verfügbar, laden Sie die Firmware-Datei für die Systemaktualisierung herunter und speichern diese auf Ihrem Computer.

• Die Firmware-Datei für den Secure Controller stellen wir für Siedle-Partner und Fachpartner im Serviceportal „Mein Siedle“ unter www.siedle.de/meinsiedle zum Download bereit. Der Zugang erfordert eine Registrierung. Endverbraucher wenden sich bitte an einen Siedle-Partner in ihrer Nähe.

• Während einer Systemaktualisierung ist der Secure Controller und damit das gesamte Zutrittskontrollsystem kurzzeitig nicht betriebsbereit. Führen Sie die Systemaktualisierung zu einem passenden Zeitpunkt durch und kommunizieren Sie das Vorhaben rechtzeitig im Voraus.

• Führen Sie vor jeder Systemaktualisierung (Upgrade) eine vollständige Systemsicherung durch. Bewahren Sie alle Systemsicherungen dauerhaft auf.

Vorgehensweise

1 Auf der Anmeldeseite des Controllers mit den Zugangsdaten des Kontos „Service“ anmelden.
2 Auf der Startseite „System“ öffnen.
3 „Administration“ öffnen.
4 „Firmware-Update“ öffnen.
5 Im Bereich „Allgemein“, „Firmware-Datei hochladen“ ausführen.
6 Im Dialog „Durchsuchen …“ ausführen.
7 Im Dialog die Firmware-Datei auswählen und mit „Öffnen“ bestätigen.
8 „Hochladen“ ausführen.
9 Die Firmware-Datei wird in den Controller geladen und geprüft. Wenn die Firmware-Datei vom Controller für ein System-Update freigegeben ist, wird sie installiert. Andernfalls erscheint eine Fehlermeldung, die zum Abbruch des System-Updates führt.
10 Um die Systemaktualisierung abzuschließen, ist ein Neustart des Controllers erforderlich und es erscheint ein Dialog, dass ein automatischer Neustart des Controllers innerhalb von 15 Sekunden erfolgen wird. Es besteht die Möglichkeit, den Neustart mit "Neustart später" zu verschieben.
11 „Jetzt neu starten“ ausführen oder 15 Sekunden warten, bis der automatische Neustart erfolgt.
12 Der Controller führt einen Neustart durch und ist nach ca. einer Minute wieder über die Anmeldeseite erreichbar.
13 Den neuen Firmware-Stand überprüfen Sie nach erneuter Anmeldung am Controller im Menü „Firmware-Update“, Bereich „Allgemein“, Feld „Firmware-Version“.

Firmware-Stand prüfen (Geräteverbund)

Der Firmware-Stand einzelner Controller, die sich im Betrieb als Geräteverbund befinden, kann zentral über den primären Controller eingesehen werden.

Vorgehensweise

1 Am primären Controller mit Konto „Service“ anmelden.
2 Menü „Secure Controller“ öffnen (Pfad: System > Administration > Secure Controller).
3 In der Auflistung sind alle Secure Controller die mit dem primären Controller betrieben werden enthalten und die jeweilige Firmware-Version angegeben.

Index

Abschlussarbeiten 58
Administration 87, 89
Allgemeine Hinweise 3
Anschlussklemmen 3, 9
Anwendung 4
Anzeige-, Bedien- und Anschlusselemente 8
Aufbereitung von Datensätzen aus anderen Systemen 90
Aufruf der IP-Adresse des Controllers 14
Ausgänge 51
Auslieferungszustand 4
Automatische Abmeldung 3
Autonomer Einzelbetrieb 6
Benutzer 7, 41, 69
Benutzer und Identifikationsmittel anlegen 69
Benutzerkonten/ Kennwörter 3, 15, 64
Benutzerverwaltung 41, 59, 64
Berichte 81
Bestimmungsgemäße Verwendung 4
Betriebsdaten 12
Betriebsformen 6
Controller ersetzen 92–94
Controller neu starten 87
Controller und Laptop verbinden 13
Controller-Eigenschaften 4
Controller-Erweiterung 21
Daten löschen 88
Daten/Konfiguration sichern 58, 74
Datum/Uhrzeit 16
Direkte Verbindung 13, 14
Eingänge/Ausgänge 45
Einfache Überwachung (3 Zustände) 49
Eingänge 45
Einzelbetrieb 6
Empfohlener Ablauf 23, 25
Ereignisse 80
Erste Schritte 13
Erster Datenimport 91
Erweiterte Inbetriebnahme von einem oder mehreren Controllern 25
Erweiterte Überwachung (4 Zustände) 50
Exkurs: Leitungsüberwachung 48
Export einer Datendatei 90
FAQ (Fragen und Antworten) 3
Firmware-Update 3, 97
Feiertage 65
Funktionsprüfung 58
Geräteübersicht 8
Identifikationsmittel 5
Import einer Datendatei 91
Import/Export Benutzer 90
Inbetriebnahme 4
Inbetriebnahme-Wizard 24, 27
Inbetriebnahme-Wizard oder manuelle Konfiguration 7
Inhalt 2
IP-Adresse des Controllers ermitteln 14
Keine Überwachung (2 Zustände) 48
Kennwort ändern 15, 64, 77
Kombinationsbetrieb (Lese-/Eingabeeinheit) 5
Konfiguration der Geräte 28
Konfiguration E/A (Eingänge/Ausgänge) 45
Konfiguration eines Benutzers mit verschiedenen Identifikationsmitteln 41
Konfiguration sichern 58, 74
Konfigurationsmöglichkeiten 7
Konfiguration E/A (Eingänge/Ausgänge) 45
Konto anlegen 75
Kundenservice 3
Leitungsüberwachung 48
Lese-/Eingabeeinheiten 5
Protokoll/Report 80
Logik 32, 54
Login 64
Manuelle Türsteuerung (Status) 78
Primären Controller ersetzen 94
Betrieb im Geräteverbund 6, 26
Mehrere Controller vernetzen 6, 26
Netzwerk 18
Netzwerkeinstellungen zurücksetzen 89
Netzwerksicherheit 3, 4
Neue Logik hinzufügen 54
Neue Zutrittsgruppe konfigurieren 67
Neuen Bericht konfigurieren 81
Neuen Controller einbinden 93, 94
Neues Wochenprogramm konfigurieren 32, 44, 66
Obere Leiterplatte: E/A-Anschlusseinheit 10
Parameter 60
Planung der Benutzerverwaltung 59
Report 80
Sabotageüberwachung 3, 87
Secure Controller im Netzwerk 3
Secure Extension 21
Service 3
Servicemodus aktivieren 96
Sicherheitshinweise 3
Sekundären Controller ersetzen 93
Sekundären Controller aus dem Geräteverbund löschen 95
Sondertag (Wochenprogramm) 63

Sprache	15
Steckbrücken (Jumper)	10
Systemaktualisierung	3, 97
Systemübersicht	5
Systemüberwachung	79
System-Update	3, 97
Türverwaltung	78
Übergabe/Kennwörter	58
Übersicht	4
Untere Leiterplatte: Prozessoreinheit	10
Verbindung über Netzwerk (LAN)	13
Vereinfachte Inbetriebnahme eines Controllers	23
Versorgungsgrenzen	12
Vorlagendatei für den ersten Datenimport	91
Vorrangregelung	7
Werkseinstellungen wieder-herstellen	88
Wochenprogramm Allgemein	7, 44
Wochenprogramm Benutzer	7, 66
Wochenprogramm Tür	7, 32
Wochenprogramme	7
Zugangsdaten (bei Auslieferung)	4
Zutrittsberechtigungen	72
Zutrittsgruppen	67
Zutrittsparameter	60
Zutrittsprotokoll	86
Zutrittspunkte (Türen)	5

SSS SIEDLE

S. Siedle & Söhne
Telefon- und Telegrafenwerke OHG

Postfach 1155
78113 Furtwangen
Bregstraße 1
78120 Furtwangen

Telefon +49 7723 63-0
Telefax +49 7723 63-300
www.siedle.de
info@siedle.de

© 2022/05.24
Printed in Germany
Best. Nr. 210010870-01 DE