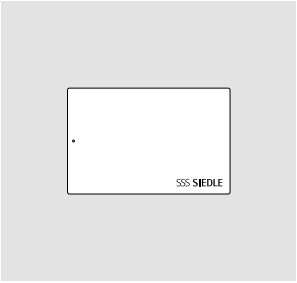
SSS SIEDLE

Commissioning instruction
Secure Controller



SC 600-0 (V. 2.12.7)

Contents

We accept no liability for modifications / additions, mistakes or printing errors.

General information

These commissioning instructions describe how to commission the SC 600-0 Siedle Secure Controller with the operation of Siedle read/input units in the Vario bus protocol.

This document is supplemented by:
• the Product Information Secure Controller SC 600-…
• the Planning and system manual for access control
The relevant current edition is located in the download area on www.siedle.com
• The FAQ help section which contains product-specific questions and answers on the Siedle website at www.siedle.com/faq_secure

Servicing
Statutory warranty conditions apply. If the device requires servicing, contact your specialist dealer or electrical installer.

Contact partners
Qualified contacts are on hand to offer a fast, professional service. By telephone, or if required we will be pleased to visit you on site.

• After-sales service
Customer service at the Furtwangen plant
+49 7723 63-434

• Siedle Engineering
In the case of customer-specific requirements or non-standard solutions, please contact Siedle Engineering at the Furtwangen plant
Tel. +49 7723 63-378
engineering@siedle.de

Safety remarks

Network security
Only use up-to-date components and terminals in the network in line with the latest state of the art. Regularly update the operating systems of all components and terminals. Exchange obsolete components and terminals for up-to-date models. Use professional protective software (antivirus, firewall, …) in all terminals. Issue secure passwords. Secure your network with the highest security standards available in the network. Protect your network against unauthorized attack from inside and outside.

Sabotage monitoring
The Secure Controller is supplied ex factory with active sabotage monitoring. This is immediately active when the device is ready for operation and monitors the housing.
If the housing is opened, alarm messages are output at the administration interface at regular intervals.
You can find information about the sabotage monitoring on page 87.

Secure Controller in the network
An Internet connection is not required for regular operation of the Secure Controller. Siedle recommends only operating the Secure Controller on the local network and not allowing access via the Internet.
Furthermore, access to the Secure Controller should only be granted to persons who need to access the access control system as part of their activities (e.g. user maintenance).

User accounts/passwords
Once the system has been handed over, all user accounts and their passwords are the responsibility of the customer/operator. Once the final handover has taken place, the customer/operator should change all the passwords.

Automatic logout
For security reasons, the Secure Controller logs each session out for a logged-in user if they have not entered anything in the administration interface for 5 minutes. In order to prevent the session time from being extended artificially due to the changes to the time settings, after every change of time setting, an automatic system logout takes place.

System update
During the update process, the power supply to the Siedle devices must not be interrupted, as this can result in damage. In this case, a repeat update is no longer possible, and the devices will have to be sent in for repair. You can find information about the system update on page 97.

Overview

Application
Secure Controller as the central controller for managing access rights in private buildings and commercial properties.

Performance features:
- 2 RS485 interfaces
- 4 doors per controller
- Protocol OSDP / Vario Bus
- Max. 500,000 users
- Max. 16 modules per controller
- Max. 64 controllers can be networked
- Log for 1,000,000 events
- Programming via web interface
- Wizard for easy commissioning

Controller extension
Each Siedle Secure Controller can be extended with up to 4 Siedle Secure Extensions (SE 600-…). The connection is established via the RS485 interface (operating mode: OSDP protocol) and requires firmware Version 2.12.7 or above for the Siedle Secure Controller.

Performance features:
- RS485 interfaces
- 4 relays per Extension
- 2 inputs per door (status/button)
- OSDP protocol
- max. 4 Extensions per Controller (2 pro RS485 interface)
- LED status display

System limits
- With 1 controller and 4 extensions, 20 outputs (relays) and 40 inputs (2 per output) and 3 control outputs can be used.
- A maximum of 12 access points (doors) can be configured on 1 controller and 2 extensions for the access control.
- All outputs/inputs can be used for other functions (e.g. lift controller).

Intended application
- This device is intended for operation with Siedle components (read and input units) for access control.
- The components connected to the Secure Controller (modules, wired outputs, etc.) must not exceed the controller's supply power in total during use (max. 20 Watt – depending on the controller's supply).
- Regular operation is only permitted in local networks (LAN). Ensure that the Secure Controller is adequately protected against attacks from the Internet (e.g. direct access to the administration interface from the Internet).
- All permitted operating modes and Siedle components permitted for operation are described in this document.
- Only the "Service" user account is to be used for commissioning the device.
- The "root" user account is only intended for the Siedle in-house service team for service purposes.
- Any use beyond this is regarded as non-intended use and Siedle does not provide any support for this.
- Siedle accepts no liability for damage that results from non-intended use.

As-delivered status
In the as-delivered status, the following accounts (user accounts for the controller's user interface) are available with pre-configured access data:
- **root**: Account with all rights. This account is only intended for service purposes.
- **Service**: Account with extensive authorisation for commissioning the access control system and managing the access control system users.
- **Facility**: Account with limited authorisation for managing the access control system users.

Access data (upon delivery)

Account/ username	**Password**
root	78120Furtwangen!
Service	Siedle1234
Facility	Facility1234

The "root", "Service" and "Facility" accounts cannot be deleted. Further accounts are only to be created via the "Service" account.

Commissioning
Commissioning is carried out via a web browser on a laptop. The laptop and controller must be connected to one another on the same network.

Controller characteristics
- The controller is ready for operation approximately 1 minute after the power is switched on.
- If no entry is made in the open menu interface for over 5 minutes, then the user is automatically logged out and the screen returns to the login. Any entries that were not saved will be lost.

Read/input units (Siedle)
When operated with the Siedle Vario bus protocol, up to 8 read/input units of the same type can be operated per RS485 interface (max. 16 read/input units: 8 x ELM… + 8 x COM… per RS485 interface = 32 read/input units per controller). The following read/input units are permitted for operation of the access control system with read/input units from Siedle:

Read/ input units	Max. number per interface
Electronic key reader (non-contact card reader) ELM 600-…	max. 8
Code lock COM 611-…	max. 8

An individual bus address (1-8) must be set for each read/input unit of the same type. Different types of read/input units (e.g. ELM… and COM…) can be operated with the same bus address. This enables the controller to also operate both read/input units as a combi module.
This setting is always made directly on the read/input unit using a rotary switch which is located under the rear cover next to the ribbon cable connection.

- The Vario bus address settings "0" and "9" are not permitted.
- The same types of read/input units (e.g. COM…) must be operated on the same RS485 interface with different bus addresses.

Combined operation (read/input unit)
In combined operation, a read unit and an input unit are configured with the same Vario bus address on a RS485 interface.
Combined operation is only possible in the Siedle Vario bus. For this operating mode, the "With keypad" option must be configured on both the read unit and the input unit. Depending on the configuration, either single (card or code) or double (card with PIN) identification is then possible.

Access points (doors)
The following connection options can be configured on the Secure Controller at four possible access points:

Connection	Quantity
Output for actuating a door release contact (potential-free change-over contact or voltage output) per access point. Details see page 10.	4
Input for state monitoring of an access point per potential-free feedback contact (input contact 2-pole).	4
Input for the operation of a (customer-provided) potential-free door release button (input contact 2-pole)	4
Control output	3

ID
The following Siedle IDs can be configured for operation of the access control system with read/input units from Siedle:

Read/ input units	ID
Read unit ELM 600-…	Electronic key (EK 600-…)
	Electronic key card (EKC 600-…)
Input unit COM 611-…	Numerical access code
Combi operation with read unit + input unit (ELM 600-… + COM 611-…)	Electronic key/ electronic key card + numerical PIN

The following operating types are possible in the network with the Secure Controller:

Individual operation
Operation of a single controller.

The following applies to individual operation of a controller in the network: The controller is already in individual operation upon delivery and can be commissioned right away.

Autonomous individual operation (several controllers in the same network)
Operation of several controllers independently from one another, including in the same network segment.

The following applies to autonomous individual operation of several controllers in the same network segment:
- If one controller fails it has no effect on whether the other controllers are ready for operation or the scope of function of the other controllers.
- Each controller is already in individual operation upon delivery and can be commissioned right away, independently of the other controllers.
- Each controller must be configured on its own and independently from the other controllers.

Operation with controller extension
Controller with up to 4 controller extensions per controller (all operating types).

For operation with controller extension, the following applies:
- Max. 4 extensions per controller.
- Max. 2 extensions per RS485 interface (OSDP) of a controller.
- Max. 12 doors can be configured (per controller with 4 extensions).
- In the case of several controllers in the device group, the extensions are integrated and configured centrally via the primary controller.
- If a controller with extensions fails, then none of the access control system components operated on it can be used.

Operation in a device group
Operating several controllers in a device group.

The following applies to the operation of several controllers in a group within a network (LAN):
- Max. 64 controllers can be networked together (1 primary device, 63 secondary devices)
- Max. 1 primary controller per group.
- Configuration is carried out centrally in the group via the primary controller.
- Data is exchanged (synchronisation) in the group securely and fully automatically during operation. However it must be carried out manually once in order to synchronise the commissioning configuration.
- Each controller in the group can be selected as the primary device. This can also be changed during operation. The controller selected as the primary device performs a restart and can be accessed again after approx. 1 minute via the logon screen.
- All controllers in the group must be in the same network segment. During operation across several network segments, the routing in the network for the controllers must be configured accordingly.
- If a controller fails in the group (including the primary device), the access control system continues to be fully accessible (except for the inputs and outputs of the failed controller).
- When replacing a controller within the group, the controller configuration is restored via data replication from the controller group.

Commissioning wizard or manual configuration
Once the user interface language, date/time and the network settings have been configured, the actual access control system is configured. The controller offers two commissioning options:
• Commissioning wizard: The commissioning wizard enables the device to be configured (access points and read/input units including all necessary pre-settings) in just a few steps. The optional detailed settings allow other specific settings to be made selectively and manually, if required.
• Fully manual commissioning: This type of commissioning is unguided and all the necessary configuration steps must be performed manually.

In either case, the user configuration for the access control system is carried out manually. Data can be imported by file (in the formats: *.Json, *.csv).

Week programmes
Three types of week programme can be configured in the controller:
• Door week programme: Time-controlled access control for an access point independent of users.
• User week programme: Time-controlled access control for a user at one or more access points (doors).
• General week programme: Time control of outputs (switching contacts) and configured logic operations from outputs/inputs and outputs.

Depending on the type of week programme, up to 1,000 week programmes can be configured for each controller or system with several controllers (device group).

Door week programme
For a newly created week programme, the week plan is always completely in "Normal" mode (an access point must be opened with ID). Other modes must also be configured (e.g. locked).

User week programme
For a newly created week programme, the week plan is always completely in "No access" mode (opening an access point is not permitted). Other modes must also be configured (e.g. access with card or code).
Three user week programmes are pre-configured upon delivery:
• "No access"
• "Access with card or code and PIN"
• "Access with card or code"

General week programme
For a newly created general week programme, the week plan is always completely in "Off" mode. The "On" mode must also be configured.

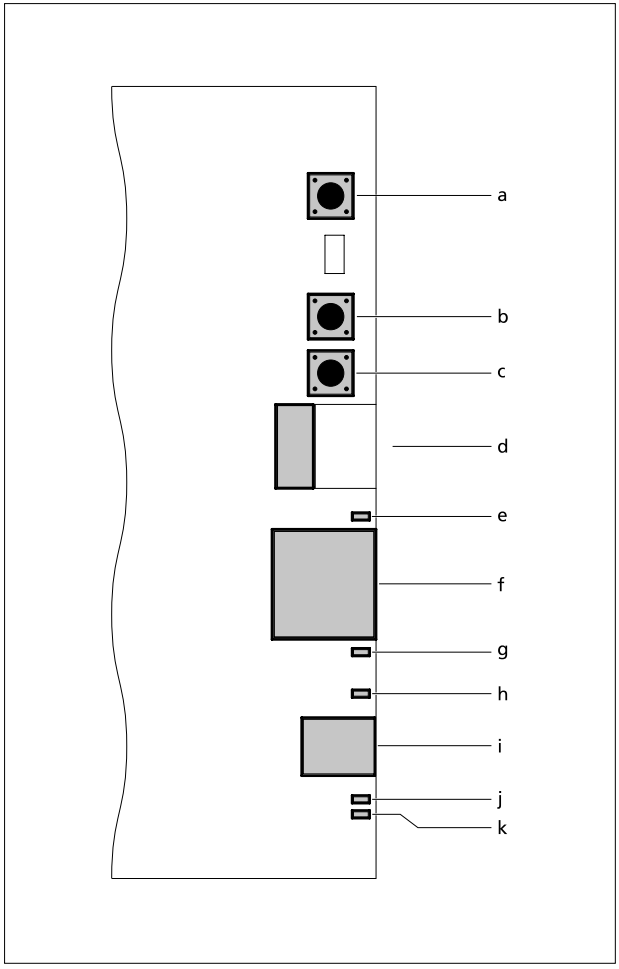
Priority rule
The following priority regulations (order according to priority) apply in the access control system:
1 Global door control
2 Door week programme
3 User week programme
4 General week programme
5 No week programme

User
Users that use the access control system all have equal rights upon creation. The following options are available for persons who require extended access rights:
• Individually configured week programme
• Additional user options for extended rights

Device overview

Display, operating and connection elements

The Secure Controller features several indicators, operating and connection elements for commissioning and/or operation. To view/access the majority of elements, the Secure Controller housing must be open. All the elements are located on the same side of the controller as the RJ45 connection.



Overview

a SD boot function button: Triggers a system start via SD card

b Function key RESET: Restart of the controller

c User button:
- Configurable function for protected access to the administration interface (web control) only by pressing a button.
- Hardware-side restoration of the default settings.
- Hardware-side reset of the network settings/activation of a pre-configured network setting.

d Slot for micro SD card

e LED (green): Status LED for indicating data transfer. If the LED flashes/flickers, data is being transferred.

f RJ45 connection: Network connection (LAN)

g LED (yellow): LED is active when there is a functional hardware-side connection to the network.

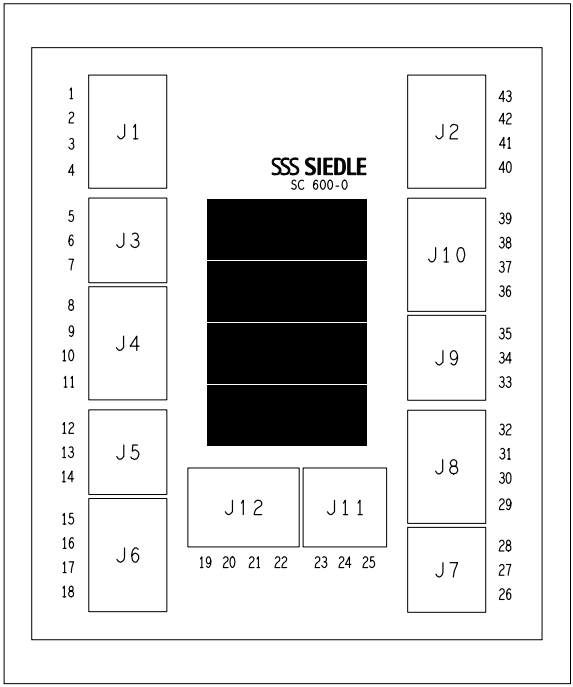
h LED (green): Indicates the controller's operating status:
- Normal operation: flashes (1 s)
- Firmware update: flashes (0.1 s)
- DHCP request: off
- Error (system): flashes (1 s)
- Error (controller): off

i Mini USB port (USB 2.0): Connection for service purposes

j LED (red): Indicates the controller's system status:
- Normal operation: off
- Firmware update: flashes (0.5 s)
- DHCP request: on (0.1 s flashing); off (2 s)
- Error (system): flashes (1 s)
- Error (controller): flashes (0.5 s) / pause (2 s)

k LED (green): Indicates the operating voltage 12 V DC

There are several terminals on the Secure Controller. To view/access them, the Secure Controller housing must be open.



Terminal overview	
J1	Read/input units (RS485-A interface)
J2	Read/input units (RS485-B interface)
J3	Input door 1 (feedback contact and door release button)
J4	Output door 1 (door relay 1: potential-free relay contact)
J5	Input door 2 (feedback contact and door release button)
J6	Output door 2 (door relay 2: potential-free relay contact)
J7	Input door 3 (feedback contact and door release button)
J8	Output door 3 (door relay 3: potential-free relay contact)
J9	Input door 4 (feedback contact and door release button)
J10	Output door 4 (door relay 4: potential-free relay contact)
J11	Output 1–3 (control outputs for small consumers)
J12	Power supply (external supply of the controller) and voltage output (supply of additional devices)

Terminal assignment

Strip	Connection	Lettering	Explanation
J1	1	D–	RS485-A data line
	2	D+	
	3	GND	Supply of OSDP
	4	OUT+12…	modules
J2	40	D–	RS485-B data line
	41	D+	
	42	GND	Supply for OSDP
	43	OUT+12…	modules
J3	5	EXIT	Button (DR)
	6	GND	Common connection
	7	CONTACT	Signalling contact
J4	8	NO	Door relay 1 with
	9	COM	changeover contact
	10	NC	(NO/COM/NC)
	11	GND	–
J5	12	EXIT	Button (DR)
	13	GND	Common connection
	14	CONTACT	Signalling contact
J6	15	NO	Door relay 2 with
	16	COM	changeover contact
	17	NC	(NO/COM/NC)
	18	GND	–
J7	26	EXIT	Button (DR)
	27	GND	Common connection
	28	CONTACT	Signalling contact
J8	29	NO	Door relay 3 with
	30	COM	changeover contact
	31	NC	(NO/COM/NC)
	32	GND	–
J9	33	EXIT	Button (DR)
	34	GND	Common connection
	35	CONTACT	Signalling contact
J10	36	NO	Door relay 4 with
	37	COM	changeover contact
	38	NC	(NO/COM/NC)
	39	GND	–
J11	23	OUT-3	Output 3
	24	OUT-2	Output 2
	25	OUT-1	Output 1
J12	19	Vin+24V	Supply
	20	GND	14– 30 V DC
	21	Vout+12V	Output 12 V DC
	22	GND	

The Secure Controller's two circuit boards feature several pin headers with jumpers for enabling/disabling various functions.
In the as-delivered status, the relay contacts of the door relay 1–4 are potential-free and the voltage outputs of the RS485-A/B interfaces are disabled.

Each jumper is already at the relevant pin header of the circuit board with open or closed connection:

- Open (jumper not plugged in): The jumper is only connected with one pole/not connected to two contacts of a pin header (function disabled/option specified).
- Closed (jumper plugged in): The jumper is connected with two poles/connected to two contacts of the pin header (function enabled/option specified).

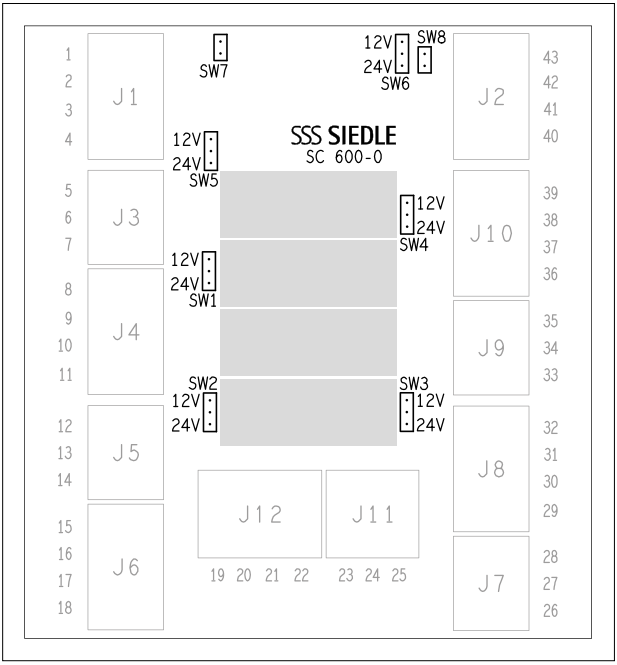
Overview – Upper circuit board: I/O connection unit

Pin header	Description	Connection (as-delivered status)
SW1 (Pin header: 3-pole)	Door relay 1: Operation as voltage output – optionally with 12 or 24 V DC at connection 9 (COM/+) and 11 (GND/–)	open (deactivated: relay contacts potential-free)
SW2 (Pin header: 3-pole)	Door relay 2: Operation as voltage output – optionally with 12 or 24 V DC at connection 16 (COM/+) and 18 (GND/–)	open (deactivated: relay contacts potential-free)
SW3 (Pin header: 3-pole)	Door relay 3: Operation as voltage output – optionally with 12 or 24 V DC at connection 16 (COM/+) and 18 (GND/–)	open (deactivated: relay contacts potential-free)
SW4 (Pin header: 3-pole)	Door relay 4: Operation as voltage output – optionally with 12 or 24 V DC at connection 37 (COM/+) and 39 (GND/–)	open (deactivated: relay contacts potential-free)
SW5 (Pin header: 3-pole)	RS485-A interface: Operation with power supply optionally with 12 or 24 V DC at connection 4 (OUT/+) and 3 (GND/–)	open (deactivated)
SW6 (Pin header: 3-pole)	RS485-B interface: Operation with power supply optionally with 12 or 24 V DC at connection 43 (OUT/+) and 42 (GND/–)	open (deactivated)
SW7 (Pin header: 2-pole)	RS485-A interface: Operation of the data cable with terminating resistor (240 Ohm)	open (deactivated)
SW8 (Pin header: 2-pole)	RS485-B interface: Operation of the data cable with terminating resistor (240 Ohm)	open (deactivated)

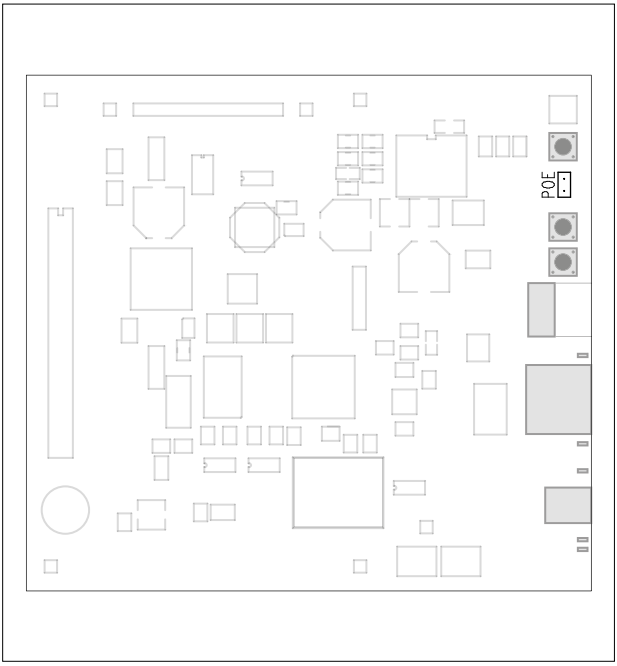
Overview – Lower circuit board: Processor unit

Pin header	Description	Connection (as-delivered status)
POE (Pin header: 2-pole)	Selectable PoE supply standard: • Open: Supply with "PoE" (max. 12.95 W) • Closed: Supply with "PoE+" (max. 25.5 W)	open (PoE supply)

**Jumper view –
upper circuit board:
I/O connection unit**



**Jumper view –
lower circuit board:
Processor unit**



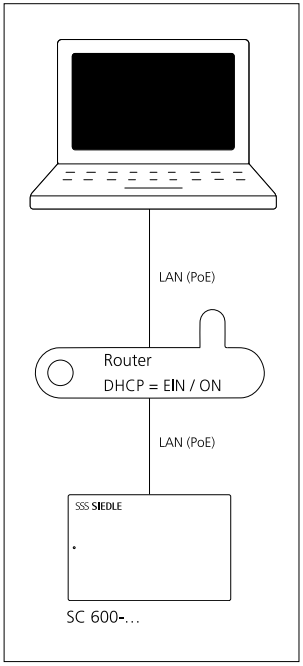
Power supply	**Explanation**
Power supply	• External power supply (14–28 V DC – via terminals (Vin / GND)) • PoE (IEEE 802.3af – type 1, class 3 , max. 12.95 W) **Important!** • The Secure Controller must not be simultaneously supplied with PoE/PoE+ when the supply is already provided via an external power supply (no redundancy/dual supply). • If (several) Secure Controllers and controller extension(s)(Secure Extension) are supplied by different power supply units (e.g. several PSM… or PSM… and PoE), the reference potentials (ground) of all controllers and extensions operated in the group must be connected together (common ground potential of all components).
Supply limits	The supply power available on the Secure Controller for connected components depends on the power supply used:

Power supply	**Max. supply power**
PoE (12.5 W)	10 W
External power supply with PSM 1 12 24 (24 V DC, 0.5 A)	10 W
PoE+ (25.5 W)	20 W

During planning and execution, ensure that the Secure Controller's available supply power is not exceeded at any point in time.

Inputs	
Current limiter (digital input)	• Digital input (is used within the system within the controller)
Door contact 1–4 (symmetrical input) Door release button 1–2 (symmetrical input)	• Inputs with optionally configurable line monitoring and configurable resistor network according to value selection • Configuration is carried out via the administration interface (see "Configuration of the inputs/outputs" > "Line monitoring") • No status change of the inputs due to an applied external voltage (max. permissible applied external voltage from connected input circuit: 30 V DC)
Door release button 3–4 (digital input)	• Inputs without line monitoring • No status change of the inputs due to an applied external voltage (max. permissible applied external voltage from connected input circuit: 30 V DC) • Individual features cannot be configured.
Outputs	
Voltage output	Depending on the controller supply, the following supply is possible via the controller for connection and operation of additional devices (max. 10 Watt): • Controller with external power supply: 12 V DC, max. 800 mA • Controller with PoE supply: 24 V DC, max. 400 mA)
Door relay 1– 4	Potential-free switching contact (changeover contact: 30 V DC, 10 A) or voltage output (details see page 10)
Output 1–3	Control output (open-drain output, max. 750 mA per output) for controlling small consumers with external power supply with max. 30 V DC

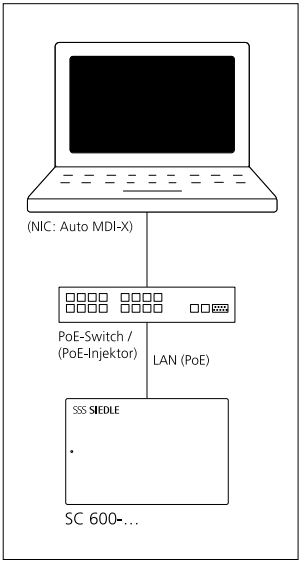
Connection via network (LAN)
LAN connection by an existing network (router/managed switch/server) with active DHCP server.



Conditions
• The controller and laptop are ready for operation.
• The network is ready for operation.
• The controller and laptop are connected to one another with a network cable each via a wired local network (LAN – router/switch/server). If the controller's power supply is provided via Power over Ethernet (PoE), then an PoE injector is also required.
• The controller's network settings are in the as-delivered status.
• The network connection (RJ45/LAN) is configured with "Obtain IP address automatically" on your laptop.

Procedure
1 Determine the IP address, as described in the following section "Determining the controller's IP address".

Direct connection
Direct connection between controller and laptop via network cable or via PoE switch/injector.



Conditions
• Controller and laptop are ready for operation and connected to one other via network cable directly (with external power supply), or via PoE switch/injector.
• The controller's network settings are in the as-delivered status.
• On your laptop, the network connection (RJ45/LAN) is configured with the fixed IP address: IP address: 192.168.1.200, subnet mask: 255.255.255.0.
• If the network connection of your laptop has the function "Auto-MDI-X", a direct connection with the Secure Controller via network cable or PoE injector is possible.

Procedure
1 Determine the IP address, as described in the following section "Determining the controller's IP address".

The Secure Controller is configured via its administration interface.
To access the administration interface and configuration, you need a laptop with a current web browser which is connected to the controller via the local network (LAN).
The controller can be accessed either via the network using the "Tech Tool" program or, if there is a direct connection between the controller and laptop, by manually calling up the IP address.

Calling up the controller's IP address
The controller can be reached with its IP address (https://<IP address>) via an encrypted connection.
We recommend always calling up the controller using "https" via an encrypted connection.

Connection via network – determining the IP address with the "Tech Tool"
You can download the Tech Tool from the download area on the Siedle website at www.siedle.com > Search: "Tech Tool". Once you have the tool on your laptop, you can determine the controller's IP address in the network and amend it if required.

Important!
• The tool can only find the controller in the network if the laptop and controller are in the same network segment (subnet) of the network (i.e. the first three blocks of the local IP address must be the same for the controller and laptop – e.g. 192.168.178.xxx).
• If access to the controller is not possible under these preconditions, then the alternative process "Direct connection – determining the controller's IP address manually" is recommended.

Procedure
1 Install the Tech Tool on your laptop.
2 Choose "Run as administrator" to run the Tech Tool on your laptop (by right-clicking on the program icon).
3 Confirm the Windows operating system message by clicking "Yes". This message may appear depending on the settings in the user account control.
4 Open "Manage" on the Tech Tool program interface.
5 Select "Configuration" in the open context menu.
6 Open "Search".
7 Select "All" in the open context menu to start the controller search.
8 The controllers found are listed in a table.
9 Select the controller from the list.
10 Run "WebConfig" to open the controller's administration interface.

Direct connection – configuring a static IP address
The network settings can be changed from DHCP mode to operation with the pre-configured IP address 192.168.1.100 by pressing the "User button" on the Secure Controller. The "user button" can only be pressed if the Secure Controller housing is open. For details on the "user button" and LED signalling, see page 8.

Procedure
1 Open the Secure Controller housing
2 Press the "user button" five times within five seconds.
3 The two LEDs for indicating the operating status (green) and the system status (red) flash.
4 An acoustic signal sounds and is repeated up to three times (interval: 3s acoustic signal followed by 3s pause).

If the button is not pressed by the last acoustic signal, the process is terminated automatically without a system change.

5 On the third acoustic signal, press and hold the user button until the acoustic signal ends.
6 The network settings are switched to operation with static IP address. The controller is automatically restarted and can be reached again after approximately one minute via the logon screen under https://192.168.1.100.

Assigning a new password

When each user account is first used to log onto the Secure Controller, the password change dialogue always appears first. Please enter a new password for the "root" account first.

Access data (upon delivery)

Account/ username	Password
root	78120Furtwangen!

Procedure
1 Log on on the controller's logon screen using the access data for the "root" account.
2 Under "Password", enter the previous password (as-delivered status: "78120Furtwangen!").
3 Enter a "new password".
4 "Repeat the new password".
5 Select "Save and close".
6 Select "Logout".
7 Note the password for handover to the operator.

New password (root)

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

Please enter a new password for the "service" account.

Access data (upon delivery)

Account/ username	Password
Service	Siedle1234

Procedure
8 Log on on the controller's logon screen using the access data for the "Service" account.
9 Under "Password", enter the previous password (as-delivered status: "Siedle1234").
10 Enter a "new password".
11 "Repeat the new password".
12 Select "Save and close".
13 Note the password for handover to the operator.

New password (Service)

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

To commission the controller, you need to log on with the "Service" account.

Language

The controller's administration interface can be used in different languages. You can change the language at any time. When the language is changed, the controller restarts. In its as-delivered status, "German" is pre-set as the language.

Procedure
1 Open "System" on the start screen.
2 Open "Administration".
3 Open "Language".
4 Select the desired language.
5 Select "Activate selected language".
6 The controller performs a restart and can be accessed again after approx. 1 minute via the logon screen.
7 Log on with the new access data with the "Service" account.

Precise time data (date/time) is required for correct operation of the controller.
Depending on the configuration, the controller can obtain its time data from a time server (NTP server) from the local network or from the Internet. Alternatively, the time data can be entered manually (not recommended).

Procedure
1 Open "System" on the start screen.
2 Open "Administration".
3 Open "Date/Time".
4 Check the content and amend if required (see "Configuration help: Date/Time").

Note

The following properties must be configured for operation with one or more time servers.:
- Time zone
- Time server 1, 2, …

Configuration help: Date/Time		
Date/Time	**Explanation**	**As-delivered status**
Date format	Drop-down box for how the date should be displayed in the controller's administration interface. Example: "dd/mm/yyyy" => day/month/year (e.g. 26/02/2021)	"dd/mm/yyyy"
Time format	Drop-down box for how the time should be displayed in the controller's administration interface. Example: "hh:mm:ss" => hour/minute/second (e.g. 16:29:59)	"hh:mm:ss"
Date	Field that is automatically filled with the data from the time server. Alternatively, the date can be set manually.	–
Time	Field that is automatically filled with the data from the time server. Alternatively, the time can be set manually.	–
Time zone	Drop-down box for selecting the regionally applicable time zone (e.g. Germany => regionally applicable time zone: "Europe/Berlin")	"Europe/Paris"
Time server status	Non-modifiable information field for the time server status: • "Connected": The controller automatically obtains its time data via the configured time server(s). All time servers can be reached. • "Connected (not all)": The controller automatically obtains its time data via the configured time server(s). At least one time server from the entered pool cannot be reached. • "Cannot be reached": The time server address cannot be reached via the network. The address is either incorrect or the NTP server is offline. • "Not connected": The configured time servers cannot be reached via the network or are offline. • "Not configured": No time server is configured.	–

Configuration help: Date/Time

Date/Time	Explanation	As-delivered status
Time server 1	IP address or URL of a time server from the local network or from the Internet (e.g. IP address of a time server on the local network). We recommend configuring different internal/external time servers/time server pools.	"uk.pool.ntp.org"
Time server 2	Alternative IP addresses or URL of other time servers from the local network or from the Internet.	–
Time server 3		–
Time server 4		–

The controller is pre-configured in the as-delivered status for automatically obtaining the network configuration via DHCP (DHCP client is active).

Procedure
1 Open "System" on the start screen.
2 Open "Network".
3 Check the content and amend if required (see "Configuration help network"):
- "IPv4 connection"
- "Web"
- "System access"

4 Select "Save".

Configuration help: Network		
IPv4 connection	**Explanation**	**As-delivered status**
Host name	The controller's designation in the network. The name entered here also serves to identify different controllers in the primary controller in the case of operation as a device group.	SC 600_…
DHCP	Option for whether the controller is assigned its network configuration from the network (insofar as the network is set up for this). If this option is disabled, the network configuration must be carried out manually.	activated
IP address	Ipv4 address of the controller's network interface.	–
Subnet mask	Specified network segment to which this network interface is connected.	–
Standard gateway	IP address of the network's router/interface (to other networks or the Internet) to which this network interface is connected.	–
Preferred DNS server	Preferred IP address for the network DNS server to which this network interface is connected.	–
Alternative DNS server	Alternative IP address for the network DNS server to which this network interface is connected.	–
MAC address	Unique hardware address for the controller.	–
Manual configuration	Option for manually changing the "Link speed" and "Duplex" settings.	deactivated
Link speed	The data transfer rate between the controller and network automatically negotiated via the network. The best possible value in the network is always selected.	–

Configuration help: Network

IPv4 connection	Explanation	As-delivered status
Duplex	Automatically negotiated operating mode via the network for data transfer between the controller and network: • "Full duplex": Simultaneous data transfer (sending and receiving) • "Half duplex": Two-way data transfer in one direction at a time (sending or receiving).	–
Web		
HTTP port (80)	Network port for unencrypted callup of the controller (http://[controller's IP address])	–
HTTPS port (443)	Network port for encrypted call up of the controller (https://[controller's IP address])	"443"
Access to system management	Operating mode governing the accessibility of the controller's system administration in the network: • "Always": The controller's system administration can be called up at any time. • "Only when the housing is open": Access to the controller's system administration is only possible when the housing is open. Otherwise, the controller is not accessible via browser call. The controller must be located in an adequately lit room for this function. • "Only with user button pressed": Access to the controller's system administration is only possible when the user button is pressed. Otherwise, the controller is not accessible via browser call. You can find an overview of the controller's operating elements in the "Display and operating elements" section on page 8.	"Always"
SSL certificate	The controller has a self-signed certificate to enable encrypted access via a browser. Current browsers do not recognise (accept) a self-signed certificate (security certificate that is not signed by a certificate authority). This means that an error message about browser security will appear once or always. Customers/operators of the controller can import their own certificate for secure operation.	–

Configuration help: Network

System access	Explanation	As-delivered status
SSH access	Operating mode for calling up the controller via SSH client. If this option is enabled, the controller can be reached via a secure connection with an SSH client. We recommend disabling this option after commissioning has been successfully completed.	activated
Ping response	Option for determining whether the controller should respond to requests (pings) via the network or not. If this option is enabled, the controller responds to every request from the network. We recommend disabling this option after commissioning has been successfully completed so that the controller no longer responds to any more search requests from the network.	activated

General information

- Each Siedle Secure Controller can be extended with up to 4 Siedle Secure Extensions (SE 600-…).
- The connection is established via the RS485 interface and requires firmware Version 2.12.7 or above for the Siedle Secure Controller.
- Each RS485 interface on the Secure Controller, on which a Secure Extension is to be operated (e.g. RS485 line A), must be in "OSDP" operating mode.
- Each address setting may be used once per RS485 interface.

Conditions

- The Secure Extension can only be supplied via the Secure Controller if the external power supply is active with 24 V DC (see jumper SW5 or SW6) on the Secure Controller's RS485 interface that is in use (RS485-A or B).
- The correct address has been set on each Secure Extension.
- The Secure Extension is connected to the Secure Controller via the RS485 interface and is ready for operation.

Configuration

- A maximum of 2 extensions can be configured on the Secure Controller for the full range of functions and a maximum of 2 extensions for the limited range of functions:

Range of functions	Functional scope
full	All available access control functions for up to 4 access points (doors) (e.g. regular access control) as well as all available switching and control functions (e.g. lift controller)
limited	Switching and control functions without access points (doors)

- To configure up to 12 access points (doors) on 1 Secure Controller, at least 2 extensions must be configured for the full range of functions.

Procedure

1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Configuration".
4 Open "Inputs/outputs".
5 Open "External I/O module".
6 With "Create new", select the corresponding option in the list according to the "Configuration table: range of functions":

Configuration table: Range of functions

RS485 line	Jumper position SE 600-…	OSDP bus address	Max. quantity	Range of functions	Option
A (or B)	J1	30	1	full	„Door I/O 5-8 – Secure Extension (OSDP)"
A (or B)	J2	31	1	full	„Door I/O 9-12 – Secure Extension (OSDP)"
B (or A)	J1	30	1	limited	„Switch I/O Secure Extension (OSDP)"
B (or A)	J2	31	1	limited	„Switch I/O Secure Extension (OSDP)"

7 For each extension, check the content and amend if required (see "Configuration help: extension").

Note
• Extensions for the full range of functions are automatically detected and just a name for the extension needs to be assigned for the configuration.
• In the case of extensions with limited range of functions, in addition to a name for the extension, the bus line used for the bus configuration (e.g. "RS485 line B") and the bus address (e.g. "30") must be configured in the "OSDP settings" menu.

8 Select "Save and close".
9 Configure further extensions in the same way.

Configuration help: Extension

General	**Explanation**
Name	Unique/meaningful designation for this extension. Assign the designation such that there is a clear distinction even among several extensions.
OSDP settings	
Bus communication	Assignment of a connection for this extension: • "Not used": This extension is not yet connected or not in operation. • "RS485 line A": This extension is connected to RS485 bus line A. • "RS485 line B": This extension is connected to RS485 bus line B.
Manufacturer	Non-modifiable information field with the product designation for this extension.
Secure channel	Non-modifiable information field with information about this extension's device connection.
Bus address	Reserved OSDP bus address for this extension, which must be configured according to the jumper position: "30" or "31".
Change settings	Option for changing already configured settings. If, for example, the bus address is to be changed, the new bus address must be entered and this option checked so that changes are applied by pressing "Save".
Model	Non-modifiable information field with the model number for this extension.
Version	Non-modifiable information field with the version number for this extension.
Serial number	Non-modifiable information field with the serial number for this extension.
Firmware version	Non-modifiable information field with the firmware version for this extension.
Input mode	Non-modifiable information field with the operating mode for this extension.

Simplified controller commissioning

Recommended process

The Secure Controller offers a wide range of functions. In just a few steps, the simplified commissioning results in an access control system that is ready for operation with a controller and a range of functions focussed on the essentials: Access is possible at any time with successful identification.

Getting started
- Assigning a new password
- Language
- Date/Time
- Network

Page 13

↓

Configuring controller extension(s) Page 21

↓

Commissioning wizard: Device configuration (guided commissioning)
- Doors (door relay for access points)
- Read/input units
- Optional: Doors week programme

Page 24

↓

Configuring a user with different IDs (card and code)
- User
- ID (card and code)

Page 41

↓

Function test Page 58

↓

Backup data/configuration Page 58

↓

Instruction/handover Page 58

↓

Password change Page 58

↓

User administration by the customer/operator
- Planning the user administration
- Optional: Configuring public holidays
- Optional: User week programme
- Optional: Access groups
- Users and ID (cards and codes)

Page 59

Simplified controller commissioning
Commissioning wizard

The Secure Controller's commissioning wizard offers guided commissioning for configuring the access points and read/input units attached to the access control system.

Operating elements (wizard)
- "Discard": Terminates the process and ends the wizard.
- "Restart the wizard": Terminates the process and restarts the wizard.
- "< Back": Switches back to the previous tab (commissioning step).
- "> Next": Switches to the next tab (commissioning step).
- "Refresh": Repeats the data request in the system and refreshes the information displayed.
- "Delete configuration": Deletes the existing configuration (only enabled if a configuration is available).
- "Save": Saves and stores the selection/input(s) in the system.
- "Defaults": Resets the changes.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Run the "Commissioning wizard" step by step:

1. Select Secure Controller
No selection possible if only a single controller is being configured.
a Select "Next".

2. Prepare
Only for information:
- "Secure Controller": Shows the name of the controller that is being configured with IP address.
- "Existing configuration": Shows all already configured access points and read/input units. There is no content here during the initial configuration.

a Select "Next".

3. RS485 communication
Assignment of the protocol for the read/input units per RS485 bus line ("Siedle Vario bus or OSDP").
a Select "Siedle Vario bus" for one or both RS485 bus lines.
b Select "Save".
c Select "Next".

4. Doors
Configuration of the access points (doors) which are connected to the controller's switching contacts (e.g. door release function).
a Select the access point to be configured which is connected to the controller (e.g. "Door 1").
b Enter a unique/useful designation in the input field next to it (e.g. Door 1 main entrance south).
c Disable the "Feedback contact" option of the door if state monitoring is not being used.
d Select "Save".
e Configure further access points (doors) in the same way.
f Select "Next".

5. Readers
Configuration of the read/input units connected to the controller (Reader).
a Select "Create new".
b Select the "Bus line/protocol" to which the read/input unit is connected (e.g. RS485 line A / Siedle Vario bus).
c Select "Access point" to assign the associated access point (e.g. read unit for "Door 1") to this read/input unit.
d Enter a unique/useful designation for the "Name" for the read/input unit (e.g. reader door 1 main entrance south ELM address2 line A).
e Enter the "Bus address" that was set on the read/input unit.
f Select the "Type" (device type) of read/input unit.
g Select "Save".
h Configure further read/input units in the same way.
i Select "Next".

6. Finish
This step completes the configuration of the devices (access points and read/input units). The report contains a concise overview of the configuration.
a Select "Finish".

Advanced commissioning of one or several controllers

Recommended process

The Secure Controller offers a wide range of functions. The extended commissioning enables complete configuration of a ready-for-operation access control system with several controllers.

Getting started
- Assigning a new password
- Language
- Date/Time
- Network

Page 13

↓

Networking several controllers (device group) Page 26

↓

Configuring controller extension(s) Page 21

↓

Commissioning wizard: Device configuration (guided commissioning)
- Doors (door relay for access points)
- Read/input units
- Optional: Doors week programme

Page 27

↓

Configuring a user with different IDs (card and code)
- User
- ID (card and code)

Page 41

↓

Optional: General week programme Page 44

↓

Optional: Configuration of the inputs/outputs
- Inputs
- Outputs
- Logic

Page 45

↓

Function test Page 58

↓

Backup data/configuration Page 58

↓

Instruction/handover Page 58

↓

Password change Page 58

↓

User administration by the customer/operator
- Planning the user administration
- Optional: Configuring public holidays
- Optional: User week programme
- Optional: Access groups
- Users and ID (cards and codes)

Page 59

The following applies to the operation of several controllers in a group within a network (LAN):
• Max. 64 controllers can be networked together (1 primary device, 63 secondary devices)
• Max. 1 primary controller per group.
• Configuration is carried out centrally in the group via the primary controller.
• Data is exchanged (synchronisation) in the group securely and fully automatically during operation. However it must be carried out manually once in order to synchronise the commissioning configuration.
• Each controller in the group can be selected as the primary device. This can also be changed during operation. The controller selected as the primary device performs a restart and can be accessed again after approx. 1 minute via the logon screen.
• All controllers in the group must be in the same network segment. During operation across several network segments, the routing in the network for the controllers must be configured accordingly.
• If a controller fails in the group (including the primary device), the access control system continues to be fully accessible (except for the inputs and outputs of the failed controller).
• When replacing a controller within the group, the controller configuration is restored via data replication from the controller group.

Procedure
1 Determine the IP address of the controller that is intended as primary device.
2 Call up the administration interface via web browser.
3 Login with the "Service" account.
4 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).
5 Select "Create new".
6 The controller to which you have logged on is shown.
7 Check the content shown (name, info) and amend or add if required.
8 Select "Save".
9 Select "Set as primary device".
10 Confirm the query with "Yes".
11 The controller selected as the primary device performs a restart and can be accessed again after approx. 1 minute via the logon screen.
12 Login with the "Service" account.
13 The start screen title is now "Secure Controller (Primary device)".
14 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).
15 The primary controller is shown in the list.
16 Select "Search for Siedle Secure Controller…".
17 The controllers found are displayed in a table.
18 Select the controllers which are to be operated in a group with the primary controller.
19 Accept the selected controllers by selecting "Import selection".
20 Confirm the query with "Yes".
21 Confirm the confirmation prompt with "OK".
22 The imported controllers are shown in the "Secure Controllers" list below the primary controller.
23 Select the imported controller (future secondary device).
24 "Editing Secure Controller…" is displayed.
25 Check the content shown (name, info) and amend or add if required.
26 Run the "Set as secondary device" or "Import as secondary device" option in the "Actions" drop-down menu:
• "Set as secondary device": The controller is accepted without existing/prepared configuration.
• "Import as secondary device": The controller is accepted with existing/prepared configuration.
27 Confirm the query with "Yes".
28 The secondary controller performs a restart and can be configured after approximately one minute.
29 Select "Save and close".
30 Carry out the process with all future secondary controllers.

31 Select "Refresh".
32 In the "Secure Controller" list under "Synchronisation", the primary controller is shown with "N/A" and all secondary controllers are shown with the status "Synchronised".

Note
The controllers are now working in operation as a device group and are prepared for the subsequent commissioning steps. From this point onwards, complete commissioning of all controllers in the device group is only possible via the primary controller.

The Secure Controller's commissioning wizard offers guided commissioning for configuring the access points and read/input units attached to the access control system.
In operation as a device group, all controllers are configured solely via the primary controller.

Operating elements (wizard)
- "Discard": Terminates the process and ends the wizard.
- "Restart the wizard": Terminates the process and restarts the wizard.
- "< Back": Switches back to the previous tab (commissioning step).
- "> Next": Switches to the next tab (commissioning step).
- "Refresh": Repeats the data request in the system and refreshes the information displayed.
- "Delete configuration": Deletes the existing configuration (only enabled if a configuration is available).
- "Save": Saves and stores the selection/input(s) in the system.
- "Defaults": Resets the changes.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Run the "Commissioning wizard" step by step:

1. Select Secure Controller
a Select the controller (e.g. primary controller) that you want to configure.
b Select "Next".

2. Prepare
Only for information:
- "Secure Controller": Shows the name of the controller that is being configured with IP address.
- "Existing configuration": Shows all already configured access points and read/input units. There is no content here during the initial configuration.

a Select "Next".

3. RS485 communication
Assignment of the protocol for the read/input units per RS485 bus line ("Siedle Vario bus or OSDP").
a Select "Siedle Vario bus" for one or both RS485 bus lines.
b Select "Save".
c Select "Next".

4. Doors
Configuration of the access points (doors) which are connected to the controller's switching contacts (e.g. door release function).
a Select the access point to be configured which is connected to the controller (e.g. "Door 1").
b Enter a unique/useful designation in the input field next to it (e.g. Door 1 main entrance south).
c Disable the "Feedback contact" option of the door if state monitoring is not being used.
d Select "Save".
e Select "Detailed settings".
f Check the content and amend if required (see configuration help on the following pages 28–31):
- "General"
- "Properties"
- "Times"
- "Security"
- "Logic"
- "Door week programme"
- "Lift"

g Select "Save and close".
h Configure further access points in the same way.
i Select "Save".
j Select "Next".

Configuration help: Doors (Access points)

General	Explanation	As-delivered status
Name	Unique/useful designation for the switching contact being configured.	–
Type	The controller's switching contact. This field is already pre-configured in the wizard (e.g. "Door I/O 1" is assigned to "Door 1" in the wizard). In the manual configuration, this pre-selection (e.g. "Door 1") is not available and therefore a switching contact that has not yet been configured can be selected here and then configured.	–
Properties		
Respond to global door control	If this option is enabled, the controller allows higher-level (global) control of the relevant access point (e.g. via a control centre). Global control takes priority over the controller's control.	deactivated
Suppress feedback status	If this option is enabled, then no alarm messages from the door-feedback contact are output at the associated input/read unit for this door (access point) if the door is not opened with the provided methods and this should nonetheless not be alerted (e.g. door is only opened by employees from inside with the door handle to leave the building after work). This concerns the functions within the Secure Controller: "Manual door control" (status) and "Event log". Other monitoring functions are not affected by this function (e.g. exceeding the maximum door opening time, etc.).	deactivated
Suppress signalling	If this option is enabled, the acoustic signalling for the read/input unit belonging to this access point is fully disabled (e.g. if this is annoying). This option requires a read/input unit with acoustic signalling (such as a buzzer).	deactivated
Door-controlled switching contact	If this option is enabled, then the switching contact belonging to this access point remains in the operating position until the access point is closed again. This option requires a feedback contact and is only needed for access points that require a switching contact configured in this way for a complete opening and closing process.	deactivated

Configuration help: Doors (Access points)

Properties	Explanation	As-delivered status
Door relay does not respond to exit button	If this option is enabled, the switching contact belonging to this access point is not activated when the output button (door release button) integrated in the access point is pressed. This option requires an access point with integrated output button.	deactivated
Feedback contact	If this option is activated, the access point is operated with a feedback contact. A feedback contact is required for this option.	deactivated
SAI GUID	No function/cannot be used	deactivated
Re-trigger switching contact	If this option is enabled, then an access point can be re-opened following successful identification even though its closing process is not yet complete (e.g, closing barrier, lowering roller shutters). This option enables greater access throughput at suitable access points and requires a controller for the access point with this performance feature.	deactivated
Respond to threat situation	No function/cannot be used	deactivated
Log door status	If this option is enabled, the states of the feedback contact ("open" and "closed") for an access point are also logged. This is logged in the "Log/report" and "Events" and "Report" area. A feedback contact is required for this option.	deactivated
Operating mode	Operating mode that can be selected for this access point: • "Normal": The access point can be opened and closed with all authorised IDs (cards/codes). • "Key box": The access point can only be opened with the ID (card or code) that was used to close it.	"Normal"
Open in the event of incorrect intrusion signalling status	No function/cannot be used	deactivated

Configuration help: Doors (Access points)

Times	Explanation	As-delivered status
Door opening time (s)	The length of time in seconds that the switching contact (e.g. door release) is triggered. Either the "Door opening time (s)" or the "Longer door opening time (s)" can be assigned to each user.	"3"
Longer door opening time (s)	The length of time in seconds that the switching contact (e.g. door release) is triggered. This option is intended for users that need a longer door opening time (e.g. people who use wheelchairs). Either the "Door opening time (s)" or the "Longer door opening time (s)" can be assigned to each user.	"20"
Permitted opening time (s)	The length of time in seconds that the access point may be open in total before a warning signal is triggered. A feedback contact is required for this option.	"30"
Permitted longer opening time (s)	Extended time in seconds that the access point may be open in total before a warning signal is triggered. A feedback contact is required for this option.	"60"
Warning delay (s)	Time after which a warning message is output (delayed warning message) after the permitted (extended) opening time has been exceeded. A read/input unit with acoustic and/or optical signalling (such as a buzzer or flashing function LED) is required for this option.	"10"
Door closing delay (ms)	Time in milliseconds before closing of the access point is triggered. This function may be required to operate high-security doors with monitoring system.	"0"
Door opening delay (ms)	Time in milliseconds before opening of the access point is triggered. This function may be required to operate high-security doors with monitoring system.	"0"
Disable time when PIN mis-entered (s)	Time in seconds during which an access point is not opened by the system for a user with dual identification (card or code and PIN) after the PIN has been mis-entered the maximum number of times. The max. number of PIN mis-entries can be configured in the "Security" menu.	"60"
Re-trigger duration (ms)	Time in milliseconds after the last switching pulse until the switching contact once again triggers a switching pulse for renewed opening of an access point (contact in configured operating position). This field can only be configured if the "Re-trigger switching contact" function has been enabled.	"1000"

Configuration help: Doors (Access points)

Security	Explanation	As-delivered status
Log access only on open door	If this option is enabled, then the identification at the access point is only logged by the system when the feedback contact reports an open/ opened access point and therefore access into the building can be assumed. A feedback contact is required for this option.	deactivated
Only open switching contact securely	If this option is enabled, then the access point can only be re-opened following successful identification once the closing process is complete (e.g. turnstile etc.). This option enables secure access at suitable access points and requires a feedback contact.	deactivated
Max. number of PIN mis-entries	Number of permitted PIN mis-entries before the temporal block for the access point is activated. The disable time applies anew after each mis-entry to make further attempts more difficult due to the time lag. The disable time for PIN mis-entry can be configured in the "Times" menu.	"10"

Logic
In the logic area, several logic processes are pre-configured with regard to how the affected access point and system should respond to specific events/triggers. The links are pre-configured for the commonly used usage scenarios. Therefore, they do not normally need to be adjusted.

Door week programme
A week program for an access point is required if the use of the access control system is to differ depending on the time, regardless of the user (e.g. access to a property at this or all access points only Monday to Friday between 08:00 and 18:00).

Configuring a new week programme
In a newly created week program, the entire week is pre-assigned "Normal". In this operating mode, the access control system works at all times.

Procedure
1 Select "Create new".
2 Enter a unique/useful designation for the "Name" of the week programme.
3 Select "Week programme".
4 Open "Edit".
5 Select "Day" (e.g. "Monday")
6 Select function (e.g. "Locked"). For further information, see the "Configuration help, week programme" table.
7 Select a start time.
8 Select an end time.
9 Select "Accept".
10 Configure further functions in the same way.
11 The configured day is displayed.
12 To apply the same configuration to other weekdays, open "Copy to" and select a weekday or a special programme. Alternatively, configure other weekdays using the same process until the week programme is configured.
13 Select "Save".
14 Select "Assignment to doors".
15 Select the access points that are to be controlled using this week programme.
16 Select "Save and close" twice.

Configuration help: Week programme

Function	Explanation
Permanently open	The access point is permanently open and can be entered and exited without an ID.
Locked	The access point is closed and cannot be opened by regular users. Only users with enhanced authorisation or special authorisation can open this access point – provided it is configured (e.g. fire brigade, VIPs)
Normal	The access point can only be opened with an ID (card/code). Single identification is always used (either card or code).
Always with PIN	Dual identification (card or code + PIN) is required at the access point.
Permanently open after card or code	The access point is only permanently open once the first user has successfully identified using card or code.
Toggle	In the "Toggle" operating mode, users can change the access point's operating mode using their ID (card or code). They can switch between the "Permanently open" and "Normal" modes.

Lift (lift control in access control systems)

If access on specific floors of buildings is also to be ensured for lifts, this is possible with the Secure Controller and a corresponding extension.
For example, only authorised people may then access these floors with the lift.
For integration of lift control, please contact Siedle Engineering at the Furtwangen plant.
Tel. +49 7723 63-378
engineering@siedle.de

5. Readers
Configuration of the read/input units connected to the controller (Reader).
a Select "Create new".
b Select the "Bus line/protocol" to which the read/input unit is connected (e.g. RS485 line A / Siedle Vario bus).
c Select "Access point" to assign the associated access point (e.g. read unit for "Door 1") to this read/input unit.
d Enter a unique/useful designation for the "Name" for the read/input unit (e.g. reader door 1 main entrance south ELM address2 line A).
e Enter the "Bus address" that was set on the read/input unit.
f Select the "Type" (device type) of read/input unit.
g Select "Save".
h Select "Detailed settings".
i Check the content and amend if required (see configuration help on the following pages
- "General"
- "Protocol"
- "Access parameters"
- "Instant access"
- "Door commands"
- "Intrusion detection"
- "Data medium"
- "Siedle Vario bus"

j Select "Save and close".
k Configure further read/input units in the same way.
l Select "Save".
m Select "Next".

Configuration help: Read/input unit

General	Explanation	As-delivered status
Name	For assigning a unique/useful designation for the read/input unit	–
Type	The read/input unit's operating type: • "Standard": The read/input unit is in operation with one access point • "Reader for several doors": The read/input unit is in operation with several access points	"Standard"
Access point	Switching contact (door relay) that can be assigned to one or more read/input units. Under "Doors" you can see all the switching contacts (door relays) that have been created under "Doors".	–
Protocol		
Bus communication	Assignment of the link/connection for the read/input unit: • "Not used": The read/input unit is not yet connected or not in operation. • "RS485 line A": The read/input unit is connected to RS485 bus line A. • "RS485 line B": The read/input unit is connected to RS485 bus line B. • "TCP-IP": No function/cannot be used.	–
Protocol	Assignment of the operation protocol for the read/input unit's data transfer: • "Not used": The read/input unit is not yet connected or not in operation. • "OSDP": Protocol for communication between the controller and OSDP-compatible read/input units from Siedle or other manufacturers. • "Siedle Vario bus": Protocol for communication between the controller and Vario bus-compatible read/input units from Siedle. • The "Deister deBus", "Aperio", "Serial barcode reader", "Smart Intego IP" and "Wiegand" protocols are not provided on the Secure Controller for the configuration.	–

Configuration help: Read/input unit

Access parameters	Explanation	As-delivered status
Acknowledgement tone when ID is read	If this option is enabled, the read unit emits acoustic feedback when the ID (electronic key/ electronic key card) has been successfully read. This option requires a read unit with acoustic signalling (such as a buzzer).	deactivated
Acknowledgement tone when ID is accepted	If this option is enabled, the read unit emits acoustic feedback when the ID (electronic key/ electronic key card) has been accepted by the access control system. This option requires a read unit with acoustic signalling (such as a buzzer).	deactivated
Code/PIN time limit (s)	Time in seconds, within which the code/PIN code must be fully entered and confirmed before the system cancels the entry process. Once cancelled, the entry process must be restarted.	"10"
Digit entry time limit (ms)	Time in milliseconds which may elapse between the entry of the individual digits of a code/PIN as well as the confirmation of the input before the system cancels the entry process. Once cancelled, the entry process must be restarted.	"2000"
Signal timeout for digit entry	If this option is enabled, then the input unit emits acoustic feedback if the time for the "Digit entry time limit (ms)" setting is exceeded. This option requires an input unit with acoustic signalling (such as a buzzer).	deactivated
Office mode time limit (s)	No function/cannot be used	–
With keypad	This option is set automatically during configuration with the commissioning wizard if an input unit is selected (e.g. COM 611-…). A corresponding option must also be set on both the input unit and the controller. If one read and input unit each is to be used in combined operation (only Siedle Vario bus), then this option must also be set on the associated read unit (e.g. ELM 600-…) and the Vario bus address must be set the same on both devices. Depending on the configuration, either single (card or code) or double (card or code with PIN) identification is then possible. Further options must be set for operation with an input unit. For details, see page 39, 60	activated

Configuration help: Read/input unit

Access parameters	Explanation	As-delivered status
Ignore code input after card is read (ms)	Time following identification with electronic key/electronic key card during which all inputs on the input unit are ignored. Only after the configured time can an access code or PIN be entered. This function is intended for combi devices (read unit with integrated input unit), where accidentally touching the input unit's keyboard during identification with electronic key/electronic key card could lead to accidental input at the input unit (e.g. in the case of a capacitative input unit).	"0"
Teach-in read unit	If this option is enabled, then the read unit can be used to teach-in new electronic keys/electronic key cards.	deactivated
Allow PIN code	If this option is enabled, the read/input unit can be used to change a PIN (code for dual identification of a user after use of an electronic key/electronic key card).	activated
Read unit time limit (ms)	Length of time in milliseconds in which the controller only accepts one signal/message from a read unit if an ID (electronic key/electronic key card) is being read. This option serves to correct/prevent possible misinterpretations in the access control system if a read unit sends multiple signals/messages for each ID read.	"0"
Suppress exit push signalling	If this option is enabled, then there is no visual feedback from the read/input unit when an exit push button is pressed.	deactivated
Two person rule	If the "Two-person rule" is enabled, the controller requires identification from two persons (IDs that are assigned to two different users) before release: • "Control through week programme": The rule on this read/input unit is controlled via the configured week programme. • "Always two person rule": The rule on this read/input unit is always enabled. • "Suppress week programme": The rule on this read/input unit is disabled.	"Control through week programme"
Instant access	No function/cannot be used	–
Door commands	No function/cannot be used	–
Intrusion detection	No function/cannot be used	–

Configuration help: Read/input unit

Data medium	Explanation	As-delivered status
	The properties for the ID used (electronic key/ electronic key card) are configured in the "Data medium" section.	
Manufacturer	ID manufacturer: • General: Siedle ID No function/cannot be used: • "HISEC" • "TechSolutions"	"General"
Data format	Data format of the ID: • "Siedle Prox": Siedle ID • "UTF8 data": QR-code read unit (e.g. trade fair access areas with optical scanners/read units) No function/cannot be used: • "Chip ID" • "Hikvision LPR Wiegand (72bit)" • "Raw Data (Binary)" • "Nokas DESFire (NO)" • "HID SEOS" • "encrypted magnetic stripe format (1)" • "Cotag/Deister prox./Hands-Free Format (3)" • "HI SEC Hughes-Prox/Hands-Free Format (4)" • "Standard BCD Magstripe Format (13)" • "Free-Programmable-Bit-Format (Wiegand) (14)" • "MIFARE chip ID number decoded (30)" • "MIFARE format with 3-byte card number… (31)" • "MIFARE chip ID number not decrypted… (32)" • "Reichpass (NL)" • "MIFARE chip ID number not decrypted…(34)" • "KMD sector being read (35)" • "G4S sector read (36)"	"Siedle Prox"
Type of data medium	Type of data medium for the ID (only relevant for operation with offline read units): • "Native type" • "MIFARE classic 1K" • "MIFARE classic 4K" • "MIFARE desfire" • "Wiegandformat" • "HID UHF"	"MIFARE DESFire"

Configuration help: Read/input unit

Data medium	Explanation	As-delivered status
Enable cardless access for this device	This option is set automatically during configuration with the commissioning wizard if an input unit is selected (e.g. COM 611-…). A corresponding option must also be set on both the input unit and the controller. If one read and input unit each is to be used in combined operation (only Siedle Vario bus), then this option must also be set on the associated read unit (e.g. ELM 600-…) and the Vario bus address must be set the same on both devices. Depending on the configuration, either single (card or code) or double (card or code with PIN) identification is then possible. Further options must be set for operation with an input unit. For details, see page 37, 60	activated
Swap CSN	If this option is enabled, then the read direction is swapped and the card number (chip share number) is read in the other direction. This option is required when the ID is taught-in by the teach-in read unit in a different direction to that of the ID at the access point.	deactivated
Swap CSN (nibbles)	If this option is enabled, then the read direction is also swapped in pairs (nibbles) and the card number (chip share number) is read, swapped in pairs, in the other direction. This option is required when the ID is taught-in swapped in pairs by the teach-in read unit in a different direction to that of the ID at the access point.	deactivated
Siedle Vario bus	This area can always be configured in the wizard. In the case of manual configuration, the "Siedle Vario bus" option must first be selected for "Protocol".	
Type	For selecting the Siedle read/input unit: • COM 611-…: Input unit • ELM 600-…: Read unit	–
Bus address	Bus address (Vario bus) of the Siedle read/input unit. For more information, see page 5	–
Version	Non-modifiable information field with the firmware date for the read/input unit.	–

6. Finish
This step completes the configuration of the devices (access points and read/input units) as well as the system configuration (week programme). The report contains a concise overview of the configuration.
a Select "Finish".

Configuring a user with different IDs

In order to commission and carry out a function check of the access control system, at least one created user and, depending on the installed read/input units and the specified forms of ID (e.g. card or card and PIN), several IDs (e.g. card, code, PIN) may be required.

User administration
New and existing users (natural persons) of the access control system and their IDs are fully configured in the user administration. In addition, user groups and the week programme for users are configured here if required.

User
New and existing users and new and existing IDs are configured under "User".

Operating elements (user)
• "Refresh": Repeats the data request in the system and refreshes the information displayed.
• "Create new user": Function for creating a new user.
• "Search": Function for searching for users or narrowing down the user search.
• "Receive card number from teach-in read unit": Function for teaching-in a new, physical ID (electronic key/electronic key card)
• "New copy": For creating a new user with the same configuration of access groups, access rights and options. Suitable for creating several similar users.
• "Save": Saves and stores the selection/input(s) in the system.
• "Delete": For deleting selected users
• "Save and close": Saves and stores the selection/input(s) in the system and takes you back to the previous menu.
• "Close": Takes you back to the previous menu without automatically saving the data. A query always appears when there are unsaved changes.

Procedure
1 Login with the "Service" account.
2 Open the "User administration" menu.
3 Open the "User" menu.
4 Select "Create new user".
5 Enter the missing data in the "General" and "Cards/codes" area (see configuration help below).
To commission the read and input units, we recommend creating a user with several IDs (card and code as well as PIN) and access rights for all access points.
6 Select "Save and close".
7 Configure further users, either:
• using the same process (recommended if the user configuration is different in all areas)
• using the "New copy" function (recommended when the configuration of the access groups, access rights and options are the same)

Configuration help: Create new user

General	Explanation
Type	Non-modifiable information field showing "Standard".
First name	The user's first name
Middle name	The user's middle name
Surname	The user's surname
Company/department	The user's company affiliation
Note	Information field for adding additional information about this user.
Valid from	Time from which the user may use their ID in the access control system.
Valid indefinitely	If this option is enabled, the user can use their ID permanently in the access control system.
Valid to	Time up to which the user may use their ID in the access control system. This field is only enabled if the "Valid indefinitely" option is disabled.

Configuring a user with different IDs

Configuration help: Create new user

Cards/codes	Explanation	As-delivered status
Mode	This selection can be used to assign the number of available IDs that a user has: • "No ID": No IDs are assigned to the user. In this case, all the configuration options are greyed out in the administration interface. • "Single ID": One ID is assigned to the user. • "Several IDs": At least two IDs are assigned to the user.	"Single ID"
Card/code		
Card number/code	ID code: • for a manually entered series of digits (access code) or • a taught-in physical ID (electronic key/electronic key card). Each ID code may only be assigned once in the system.	–
Receive card number from teach-in read unit	Function button: Ready-to-use function for teaching-in physical IDs, provided a teach-in read unit has been configured in the system. The teach-in read unit can be any read unit installed in the property and connected to the access control system (e.g. ELM 600-…). Alternatively, a portable read unit can be used for direct connection to a laptop/PC (e.g. Siedle USB reader "readID One SE 1220 MNP").	–

Configuration help: Create new user

Card/code	Explanation	As-delivered status
PIN (digits)	Input field for assigning a PIN to a user. The PIN code is only required when dual identification is desired for greater security (e.g. identification with card or access code and additional PIN). Each user may be assigned any PIN (default: four-digit). **Important!** If users are to assign their PIN themselves in the case of a dual ID preconfigured by the system, then a value cannot be preconfigured. Users must then assign their PIN themselves by entering it and confirming it at the relevant input unit when first using their ID with this access control system.	–
Repeat PIN	Input field for confirming the PIN already entered in the "PIN (digits)" field.	–
Access rights		
Drop-down menu	Drop-down menu for filtering the displayed access rights: • "Show all doors": All already configured (available) access points are displayed. • "Show selected doors": The access points assigned to the user are shown. Access points from the access group are shown as already selected and non-modifiable, and cannot be selected and configured as individual access rights under "Access rights". **At least one access group or access right must be configured, for each user. Multiple selections are possible in both cases.**	–

Optional: General week programme

General week programme
A general week programme is required if outputs (switching contacts) and configured logic operations from outputs/inputs and outputs are available in the access control system and are also to be controlled depending on time.

Configuring a new week programme
For a newly created general week programme, the week plan is always completely in "Off" mode. The "On" mode must also be configured.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Configuration".
4 Open "Week programme".
5 Open "General week programme".
6 Select "Create new".
7 Under "General", enter a unique/useful designation for the "Name" of the week programme.
8 Select "Week programme".
9 Open "Edit".
10 Select "Day" (e.g. "Monday")
11 Select function (e.g. "On"). For further information, see the "Configuration help, week programme" table.
12 Select a start time.
13 Select an end time.
14 Select "Accept".
15 Configure further functions in the same way.
16 The day configuration is shown in a table.
17 To apply the same day configuration to other weekdays, open "Copy to" and select a weekday or a special programme. Alternatively, configure other weekdays using the same process until the week programme is configured.
18 Select "Save and close".

Configuration help: Week programme

Mode	Explanation
On	Outputs (switching contacts) and configured logic operations are switched on.
Off	Outputs (switching contacts) and configured logic operations are switched off.

Optional: Configuration of the inputs/outputs

Inputs/Outputs

When carrying out commissioning with the commissioning wizard, only selected inputs and outputs are provided for configuration. In this area, you can configure all the inputs and outputs on the Secure Controller. Under "I/O", inputs, outputs (switching contacts) and configured logic operations from outputs/inputs and outputs can be configured. Depending on the configuration, outputs and logic operations are controlled based on events (e.g. there is a signal at the input), via "General" week programme (time controlled) or a combination.

Inputs

In this area, you can configure all the inputs on the Secure Controller. One internal signal input (current limiter) and up to eight external inputs (six symmetrical, two digital) can be configured:

Procedure

1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Configuration".
4 Open "Inputs/Outputs".
5 Open "Inputs".
6 All the configurable inputs are listed in a table.
7 Select the desired input.
8 Editing input […] is displayed.
9 Complete the missing information under "Input settings" (see configuration help, inputs).
10 Select "Save and close".
11 Configure further outputs in the same way.

Type	Explanation
Current limiter (digital input)	• Digital input (is used within the system within the controller), cannot be connected externally, no line monitoring required. • Individual features cannot be configured.
Door contact 1–4 (symmetrical input) Door release button 1–2 (symmetrical input)	• Inputs with optionally configurable line monitoring and configurable resistor network according to value selection • Configuration is carried out via the administration interface (see "Configuration of the inputs/outputs" > "Line monitoring") • No status change of the inputs due to an applied external voltage (max. permissible applied external voltage from connected input circuit: 30 V DC)
Door release button 3–4 (digital input)	• Inputs without line monitoring • No status change of the inputs due to an applied external voltage (max. permissible applied external voltage from connected input circuit: 30 V DC) • Individual features cannot be configured.

Optional: Configuration of the inputs/outputs

Inputs

Configuration help: Inputs

General	Explanation	As-delivered status
Name	Non-modifiable information field with the input designation.	"[Input name]"
Properties		
Line monitoring	For selecting (only in the case of symmetrical inputs) whether a circuit with line monitoring (by resistor) for monitoring the line state is used at the input contact: • "2 states": No monitoring • "3 states": Simple monitoring • "4 states": Advanced monitoring You can find more details on the subject of line monitoring on page 48	"2 states"
Contact type	For selecting which type of contact is connected at the input: • NC contact: An NC contact is connected at the input (rest position: closed) • NO contact: An NO contact is connected at the input (rest position: open) The "current limiter" signal input is an input within the controller. By selecting the contact type, you can configure (invert) its response behaviour.	"NC contact"
End of line resistor	For selecting the resistor that was used for the line monitoring as "EOL resistor" (end of line). The following values can be selected (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) The end of line resistor and alarm resistor can be selected independently of one another.	"2k2"

Configuration help: Inputs

Properties	Explanation	As-delivered status
Alarm resistor	For selecting the resistor that was used for the line monitoring as "Alarm resistor" (AR). The following values can be selected (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) The alarm resistor and end of line resistor can be selected independently of one another.	"2k2"
Follow trigger	If this option is enabled, the input remains in the operating state until the triggering element (e.g. closed contact) switches back to the idle status. As soon as the triggering element is no longer active, the input switches back to its idle status. If this option is enabled, the "Duration (ms)" field cannot be configured.	
Delay (ms)	Length of time in milliseconds before the input switches to the operating state.	"10"
Duration (ms)	Length of time in milliseconds that the input remains in the operating state, regardless of the state of the triggering element at the input contact. This field can only be configured if the "Follow trigger" option has not been enabled.	"0"
Trigger delay again	If this option is enabled, then the switch to the next operating state is also delayed again if the trigger by the triggering element took place while the input was already in an operating state.	deactivated
Carry out when trigger back in idle status	If this option is enabled, then the input only switches to the operating state for the time specified under "Duration" once the triggering element is no longer active at the input contact (e.g. contact is no longer closed).	deactivated

Optional: Configuration of the inputs/outputs

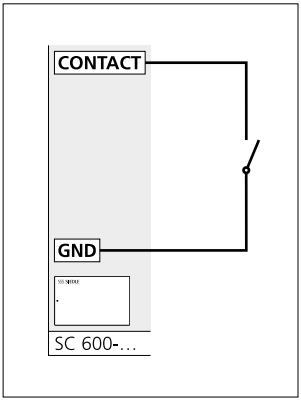
A note on: line monitoring

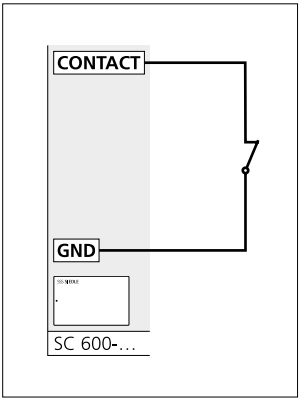
Line monitoring is used to monitor the state of a circuit connected to an input and its line. On the Secure Controller, there are six symmetrical inputs which can be operated with monitoring. The following wiring versions are possible:

Wiring for …	Circuit: NO contact (idle status: open)	Circuit: NC contact (idle status: closed)
2 states– (no monitoring) The line is not monitored with this version. The following statuses can be registered by the system at the input: • Open • Closed Therefore, the controller can recognise a "normal state" and an "alarm state". These depend on the circuit used and the configuration of the input.	**Properties** • Signalling according to the open-circuit principle. • Security: No monitoring, can be easily manipulated by "interrupting" the wire. • Manipulation detectable by the controller during operation: No	**Properties** • Signalling according to the closed-circuit principle. • Security: No monitoring, can be easily manipulated by "short circuiting" the wire. • Manipulation detectable by the controller during operation: No

State	Signal
Contact open	Normal
Contact closed	Alarm

State	Signal
Contact open	Alarm
Contact closed	Normal





Wiring for …

3 states –
(simple monitoring)
In the case of this version, each state is monitored, but cannot be clearly identified. Per circuit, there is the same signal for each two states, as they cannot be differentiated. The following states can be registered by the system at the input, but, depending on the circuit, cannot be uniquely signalled in every case:

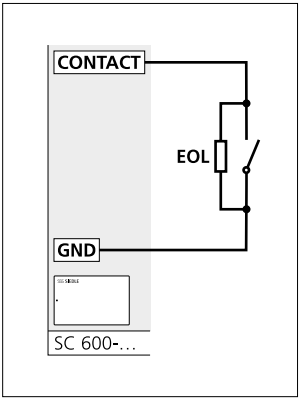
NO contact
- Open
- Closed/short-circuited
- Interrupted

NC contact
- Open/interrupted
- Closed
- Short-circuited

Circuit: NO contact
(idle status: open)

Properties
- Signalling according to the open-circuit principle with resistor.
- Security: Simple monitoring: against short-circuit and interruption of the line.
- Manipulation detectable by the controller during operation: Yes
- An end of line resistor must be configured.

State	Signal
Contact open	Normal
Contact closed	Alarm
Wire interrupted	Interruption
Wire short-circuited	Alarm

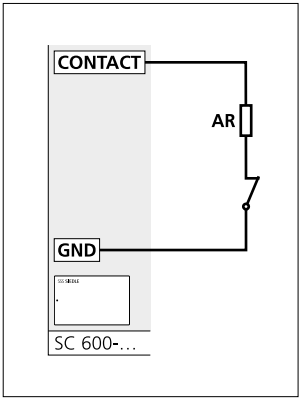


In this circuit, an end of line resistor is located in parallel to the trigger contact.

Circuit: NC contact
(idle status: closed)

Properties
- Signalling according to the closed-circuit principle with resistor.
- Security: Advanced monitoring: against short-circuit and interruption of the line.
- Manipulation detectable by the controller during operation: Yes
- An alarm resistor must be configured.

State	Signal
Contact open	Alarm
Contact closed	Normal
Wire interrupted	Alarm
Wire short-circuited	Short-circuit



In this circuit, an alarm resistor is located in series with the trigger contact.

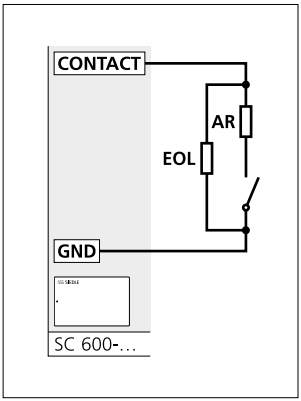
Optional: Configuration of the inputs/outputs

A note on: line monitoring

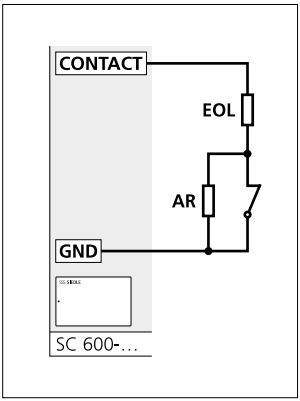
Wiring for …	Circuit: NO contact (idle status: open)	Circuit: NC contact (idle status: closed)
4 states – (advanced monitoring) In this version, each state is monitored and clearly identified – regardless of the type of circuit. The following states can be clearly registered by the system at the input and signalled via the controller: • Open • Closed • Interrupted • Short-circuited	**Properties** • Signalling according to the open-circuit principle with resistor network • Security: Advanced monitoring: against short-circuit and interruption of the line. • Highest manipulation protection as a different resistance value arises for each state. • Manipulation detectable by the controller during operation: Yes • An end of line resistor and an alarm resistor must be configured.	**Properties** • Signalling according to the closed-circuit principle with resistor network. • Security: Advanced monitoring: against interruption of the line. • Highest manipulation protection as a different resistance value arises for each state. • Manipulation detectable by the controller during operation: Yes • An end of line resistor and an alarm resistor must be configured.

State	Signal
Contact open	Normal
Contact closed	Alarm
Wire interrupted	Interruption
Wire short-circuited	Short-circuit

State	Signal
Contact open	Alarm
Contact closed	Normal
Wire interrupted	Interruption
Wire short-circuited	Short-circuit



This circuit requires an end of line resistor and an alarm resistor: The alarm resistor and contact are connected in series. The end of line resistor is connected in parallel to the series connection.



This circuit requires an end of line resistor and an alarm resistor: The alarm resistor and contact are connected in parallel. The end of line resistor is connected in series with the parallel connection.

In this area, you can configure all the outputs on the Secure Controller. A buzzer and up to seven outputs can be configured on the Secure Controller. The buzzer and outputs can each be triggered based on time, events or a combination (logic: time and event-controlled). The following outputs can be configured:

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Configuration".
4 Open "Inputs/Outputs".
5 Open "Outputs".
6 All the configurable outputs are listed in a table.
7 Select the desired output.
8 Editing output […] is displayed.
9 Complete the missing information under "Properties" and "Control" (see configuration help, outputs).
10 Select "Save and close".
11 Configure further outputs in the same way.

Type	Explanation
Buzzer	Configurable buzzer within the Secure Controller for acoustic feedback for configured events or for searching for/localising a controller using the "Tech Tool".
Door relay 1– 4	Potential-free switching contact (changeover contact: 30 V DC, 10 A) or voltage output (details see page 10)
Output 1–3	Control output (open-drain output, max. 750 mA per output) for controlling small consumers with external power supply with max. 30 V DC

Optional: Configuration of the inputs/outputs

Outputs

Configuration help: Outputs

General	Explanation	As-delivered status
Name	Non-modifiable information field with the output designation.	"[Output name]"
Properties		
Normally off	If this option is enabled, the output is in idle status when it is not triggered. If this option is disabled, the output switches to the operating state when it is not triggered (inverted).	activated
Follow trigger	If this option is enabled, the output remains in the operating state for as long as specified by the control via the triggering element (e.g. closed input contact). As soon as the triggering element is no longer active, the output switches back to its idle status. If this option is enabled, the "Duration (ms)" field cannot be configured.	activated
Mode	Configuration of the output behaviour in the operating state: • "On" (static): Output remains static in the triggered/active state • "Toggle 250 ms": Output switches its state every 250 milliseconds (toggle operation) for as long as the triggering control specifies an operating state. • "Toggle 500 ms": Output switches its state every 500 milliseconds (toggle operation) for as long as the triggering control specifies an operating state.	"Static"
Delay (ms)	Length of time in milliseconds before the output switches to the operating state.	"0"
Duration (ms)	Length of time in milliseconds that the output remains in the operating state, regardless of the state of the triggering control. This field can only be configured if the "Follow trigger" option has not been enabled.	"0"
Trigger delay again	If this option is enabled, the switch to the next operating state is then also delayed again, if the control trigger took place while the output was already in an operating state.	deactivated
Carry out when trigger back in idle status	If this option is enabled, the output only switches to the operating state for the time specified under "Duration", once the control has switched back to the idle status/the triggering element is no longer active (input contact is no longer closed).	deactivated

Configuration help: Outputs

Link to input	Explanation	As-delivered status
Secure Controller	Selection of controller via which the output control takes place. This selection is only shown if several controllers are configured for operation in the device group.	"[Name of the primary controller]"
Triggering element	For selecting how the output is controlled: • "None": There is no triggering element that triggers the output based on time or event. This selection disables the output and its control. • "Input": Physical input (such as a door contact) or internal system status point/configured logic (e.g. network error) within the controller with which the output can be triggered. • "Input of object": Event from a configured object (e.g. read/input unit or week calendar), within the controller/access control system (e.g. signalling of a read/input unit to the controller) with which the output can be triggered.	"None"
Object type	Selection filter for narrowing down the selectable "Objects". This selection is only enabled when "Object" is selected under "Trigger element".	–
Object	Selection filter for narrowing down selectable events in the "Input" selection for the output control. This selection is only enabled when "Object" is selected under "Trigger element". The selection shown depends on the selection under "Object type".	–
Input	Physical input, internal system status point/ configured logic, or an object's event for the output control. The selection depends on the selected trigger element.	–

Optional: Configuration of the inputs/outputs

Logic

In this area, several logic processes are pre-configured with regard to how the affected access point and system should respond to specific events/triggers. The logic is pre-configured for the commonly used usage scenarios. Therefore, they do not normally need to be adjusted. Advanced knowledge of the access control system's configuration is required for modifying the logic.

Operating elements

- "Add": Creates a new operator.
- "Remove": Removes a selected operator.
- "Defaults": Resets the changes.
- "Insert" (for selected operator): Adds another operator at the selected position.

Procedures

Check existing logic and adjust if applicable

1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Configuration".
4 Open "Inputs/Outputs".
5 Open "Logic".
6 Select logic (e.g. door alarm).
7 Change the "Name" in the "General" tab if required.
8 Select the "Operator" tab.
9 Check the configuration elements and adjust if applicable.
10 Select "Save".
11 Process further operators in the same way.

Adding new logic

1 Select "Create new".
2 Enter a unique/useful designation for the "Name" under the "General" tab.
3 Select the "Link" tab.
4 Select "Add".
5 Configure the link elements (operator, connection type, object type, item and input) by selecting the menus.
6 If required, repeat the process for further sub-links.
7 Select "Save".
8 Create further logic in the same way.

Remove existing logic

1 Select logic.
1 Select "Remove".
1 Select "Save" or "Save and close".

Configuration help: Logic

General	Explanation	As-delivered status
Name	For assigning a unique/useful designation for the logic.	–
Properties		
Follow trigger	If this option is enabled, the logic state remains in the operating state until the triggering element (e.g. closed contact) switches back to the idle status. As soon as the triggering element is no longer active, the logic state switches back to its idle status. If this option is enabled, the "Duration (ms)" field cannot be configured.	activated
Delay (ms)	Length of time in milliseconds before the logic state switches to the operating state.	"0"
Duration (ms)	Length of time in milliseconds that the logic state remains in the operating state, regardless of the state of the triggering element. This field can only be configured if the "Follow trigger" option has not been enabled.	"0"
Trigger delay again	If this option is enabled, then the switch to the next operating state is also delayed again if the trigger by the triggering element took place while the logic state was already in an operating state.	deactivated
Carry out when trigger back in idle status	If this option is enabled, then the logic state only switches to the operating state for the time specified under "Duration" once the triggering element is no longer active (e.g. contact is no longer closed).	deactivated
Idle status in event of sabotage	If this option is enabled, the logic state switches to the idle status for security reasons if there is a sabotage message.	deactivated

Configuration help: Logic

Logic	Explanation
Operator	Selectable connector between trigger elements (e.g. inputs or object inputs): • "(": Open bracket • ")": Closed bracket • "NOT": For negating operations (contrary: e.g. not state A) • "AND": For combining operations (e.g. state A and state B) • "AND NOT": For combining operations with negation (e.g. state A and not state B) • "OR": For differing operations (state A or state B) • "OR NOT": For differing operations with negation (e.g. state A or not state B) **Note** Operators can be combined as desired. But the combination must make sense as otherwise the operation cannot create any result or logic state change. **Example** To create a logic to monitor the status of the local network connection, possible error states must be linked together. Operation in display field: LAN address lost OR LAN address conflict OR LAN LINK lost For signalling, the logic can be configured as a trigger for an output, for example.

Configuration help: Logic

Logic	Explanation	As-delivered status
Secure Controller	Selection of the controller via which the logic control takes place. This selection is only shown if several controllers are configured for operation as a device group.	
Triggering element	For selecting how the output is controlled: • "None": There is no triggering element that triggers the output based on time or event. This selection disables the output and its control. • "Input": Physical input (such as a door contact) or internal system status point/configured logic (e.g. network error) within the controller with which the output can be triggered. • "Input of object": Event from a configured object (e.g. read/input unit or week calendar), within the controller/access control system (e.g. signalling of a read/input unit to the controller) with which the output can be triggered.	"None"
Object type	Selection filter for narrowing down the selectable "Objects". This selection is only enabled when "Object" is selected under "Trigger element".	–
Object	Selection filter for narrowing down selectable events in the "Input" selection for the output control. This selection is only enabled when "Object" is selected under "Trigger element". The selection shown depends on the selection under "Object type".	–
Input	Physical input, internal system status point/ configured logic, or an object's event for the output control. The selection depends on the selected trigger element.	–

Final assignments

Function test

Perform a function check of the access control system.

Procedure

1 Perform a complete function check of the access control system.
2 Check the function of all access points, read and input units as well as configured functions.

Backup data/configuration

Create a complete data and configuration backup.

Procedure

1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "System information/ Database/Licence".
5 Open "Database".
6 Select "Backup database".
7 Confirm the query with "Yes".
8 Confirm the browser query with "OK" to save the backup file to your laptop.

Handover/passwords

Handover the access control system to the customer/operator.

Procedure

1 Handover all documents/files associated with commissioning to the customer/operator:
• These commissioning instructions with the entered newly assigned passwords.
• Configuration backup file.
• System documentation
2 After a successful handover, delete all the commissioning files from your laptop.
3 Note for your customer (owner/ operator of the access control system)
For data security and secure operation, Siedle recommends that the customer/operator assigns new, secure passwords themselves for all user accounts after handover. The newly assigned access data should no longer be known by third parties (such as electricians, commissioning technicians).
Please inform your customers of this.

The Secure Controller offers the option of configuring the user structures from different perspectives. Customers/operators of an access control system should therefore consider which is the best user structure for them in advance.

User administration	Explanation
Access parameters	Control the configuration options for the various means of identification (card, code, PIN) within the user administration and expand or reduce these according to the configuration of the access parameters.
User week programme	Control the time of access of users at one or more access points (doors). If week programmes are needed, these should be configured in advance by the customer/operator as these need to be stored when configuring the access groups and users. Changes affect the user for which the week program is directly (access rights) or indirectly (access groups) stored. Alternatively, week programmes can be created directly for the access point. In this case, the same access rules always apply for all users at this access point. You can find further information about the “week programmes“ and the existing “priority rule“ and “week programme“ in the Secure Controller on page 7
Access groups	Control the time and location-based access for one or more access points. Different users can easily be assigned the same access rules in access groups to make configuration easier. Several access groups can be assigned to a user. Changes affect all users which are assigned to this access group. In the case of large structures with lots of users and access rules, it makes sense to use access groups to make configuration simpler. If access groups are required, these should be created before the users themselves, as these must be saved during user configuration.
Users and ID	ID is always tied to a user. Several IDs can be configured for each user. Access rights for individual or several access points can be configured at user level (access rights), at the access group level or a combination. Access options can also be configured at user level. Changes only affect the individual user. It is only advisable to configure at user level without access groups for small access control systems with few users or access rules.

This is where different access parameters for the various IDs (card, code, PIN) can be configured.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "Card holder management".
5 Open "Access parameters".
6 Check the content and amend if required (see Configuration help: Access parameters).

Configuration help: Access parameters

Allgemein	Explanation	As-delivered status
Access configuration (card holders)	For selecting which rights for access configuration can be configured for individual users: • All doors + week programmes: Several access areas and different week programmes can be assigned to each user. Another week programme can be optionally selected for each access area. • All doors, one week programme: Several access areas can be assigned to each user, but only one week programme in total. This week programme applies to all assigned access areas. • All access groups: At least one or more access groups can be assigned to each user, in which one or more access areas and associated week programmes are pre-defined. • All access groups + doors + week programmes: Individual or several access groups (in which one or more access areas and associated week programmes are pre-defined), access areas and week programmes can be freely assigned to each user.	"All access groups + doors + week programmes"
Validity period with date/time	If this option is enabled then a date with time can be specified for the time from which an ID (card/code) may (can) be used in the access control system. If this option is disabled, only a date can be entered.	activated

Configuration help: Access parameters

General	Explanation	As-delivered status
Code length for cardless access	This selection enables the operation of input units at access points for access attempts/identification with code: • "– (not allowed)": The operation of input units for access attempts/identification with code is not possible in the system. • "4 digits": The operation of input units for access attempts/identification with code is possible in the system. Entry is limited to a maximum of 4 digits/only the first 4 digits entered are evaluated. • "5 digits": Same function as for "4 digits", but with 5 digits • "6 digits": Same function as for "4 digits", but with 6 digits • "Any length": Same function as for "4 digits", but with any number of digits. **Important!** The "Any length" setting is required in order to operate the Siedle COM 611-… input unit, as the code input must always be confirmed with the "F" function button to transmit it to the Secure Controller!	"Any length"
Code entry with leading zeroes	If this option is enabled, then leading zeroes are permitted in codes (e.g.code: "0015"). If this option is disabled, then codes with leading zeroes cannot be used.	activated
PIN		
Length of the PIN	For selecting the length of the PIN to be assigned to users: • "4": PIN must always be four digits long. • "5": PIN must always be five digits long. • "6": PIN must always be six digits long.	"4"
Log events only with card/code + PIN	If this option is enabled, only events from access attempts with dual identification (card + PIN or code + PIN) are recorded. If this option is disabled, the individual identification steps are also logged.	deactivated

Configuration help: Access parameters

PIN	Explanation	As-delivered status
PIN never expires	If this option is enabled, all assigned PINs remain valid indefinitely. If this option is disabled, all PINs expire according to the entry in the "PIN expires after [x] days" field, depending on the validity period of the user's ID.	activated
PIN expires after [x] days	Field for entering the number of days after which the PIN can no longer be used. The time period begins from the moment at which the PIN was assigned to a user and saved. Once the validity period expires, it can be extended/ renewed for the affected user in the user administration.	"90"
Block card/code in event of PIN misuse	If this option is enabled, then once the maximum number of PIN mis-entries is reached, the associated ID (card/code) is permanently blocked. For details on the maximum number of PIN mis-entries, see page 31.	deactivated
Attack PIN	PIN which gives the user the opportunity of opening the access area in a seemingly normal way and at the same time triggering a (silent) alarm in the event of an attack (being forced to open the access area by another person). After identifying themselves with their card or code, the user enters the attack PIN instead of their usual PIN. The PIN and attack PIN must be the same length. An output contact, which is connected to a danger warning system/alarm system, must be configured for this function.	"1234"
Attack code	Code add-on, added to the usual code, which gives the user the opportunity of opening the access area in a seemingly normal way and at the same time triggering a (silent) alarm in the event of an attack (being forced to open the access area by another person). The user enters the code and the attack code in succession and then confirms the input on their input unit. The code and attack code can vary in length. An output contact, which is connected to a danger warning system/alarm system, must be configured for this function.	–

Seven special programmes are available in the Secure Controller for configuring special dates or time periods (e.g. public holidays).
You can change the name of the special programmes in this area.

Examples

Name in as-delivered status	Customer name
Special programme I	Public holiday
Special programme II	Stocktaking
Special programme III	Christmas

Operating elements
"Refresh": Repeats the data request in the system and refreshes the information displayed.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "User administration".
5 Open "Special days (Week programme)".
6 Open the required special programme by clicking it.
7 Change the content (see configuration help: Special day (week programme)).

Configuration help: Special day (week programme)

General	Explanation	As-delivered status
Name	For assigning a unique/useful name for the special programme (e.g. public holiday). If the name in the as-delivered status (e.g. special programme I) is to be shown again instead, the entry in the name field must be deleted and the change saved.	–

User administration by the customer/operator

Login

The login using the "Facility" account is intended for user administration by the customer/operator. This account does not provide access to the actual system and device configuration.

Access data (upon delivery)

Account/ username	**Password**
Facility	Facility1234

Procedure

1 Log on on the controller's logon screen using the access data for the "Facility" account.

Assigning a new password

The password change dialogue will appear the first time you log on with this account.

Procedure

1 Under "Password", enter the previous password (as-delivered status: "Facility1234").
2 Enter a "new password".
3 "Repeat the new password".
4 Select "Save and close".
5 Note the password for handover to the operator.

New password (Facility)

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

User administration

This is where new and existing users (natural persons) of the access control system and their IDs are fully configured. In addition, user groups and the week programme for users are configured here if required. Users can also be imported/exported.

Procedure

1 Login with the "Facility" account.
2 Open the "User administration" menu.

Optional: Public holidays

Individual time points or periods which cannot be represented via a week programme are configured here. No "public holidays" are pre-configured in the as-delivered status. These must be configured by the customer/operator if required. Public holidays can be configured using the "Service" and "Facility" user accounts.
Public holidays (e.g. regional public holidays, company holidays and other closures) can be bundled and categorised in different special programmes and used for mapping irregular exceptions in week programmes. Up to seven special programmes can be used for this (e.g. special programme I = company holiday, special programme II = regional public holidays). Different week programmes (e.g. with and without public holidays) can be used to assign different access rights to users/user groups.

Procedure
1 Login with the "Facility" user account.
2 Open the "User administration" menu.
3 Open "Public holidays".
4 Public holidays that are already configured are shown in a table and can be changed by selecting them directly.
5 Select "Create new".
6 Under "General", enter a unique/useful designation for the "Name" of the public holiday.
7 Enable the "Repeat annually" option if applicable.
8 Open "Time period".
9 Select "Add".
10 Select a start point in the calendar for the "Start".
11 Select an end point in the calendar for the "End".
12 Select a special programme for "Assumed weekday". Siedle recommends having the time points/periods of all public holidays in special programmes so they can be easily used in week programmes.
13 Configure further time points/periods for this public holiday in the same way.
14 Select "Save and close".
15 Configure further public holidays in the same way.

A user week programme is required if the use of the access control system is to differ based on time for access groups and/or users (e.g. access to the property at this or all access points (doors) only from Monday - Friday and from 08:00 – 18:00 daily).

Configuring a new week programme
In a new user week programme, the entire week plan is preallocated the "Access with card or code" mode. In this mode, the access control system works at all times for access with card or code.

Procedure
1 Login with the "Facility" user account.
2 Open the "User administration" menu.
3 Open "User week programme".
4 Select "Create new".
5 Under "General", enter a unique/useful designation for the "Name" of the week programme.
6 Select "Week programme".
7 Open "Edit".
8 Select "Day" (e.g. "Monday")
9 Select function (e.g. "Access with card or code"). For further information, see the "Configuration help: User week programme" table.
10 Select a start time.
11 Select an end time.
12 Select "Accept".
13 Configure further functions in the same way.
14 The day configuration is shown in a table.
15 To apply the same day configuration to other weekdays, open "Copy to" and select a weekday or a special programme. Alternatively, configure other weekdays using the same process until the week programme is configured.
16 Select "Save and close".

Configuration help: User week programme

Mode	Explanation
No access	Access is not possible.
Access with card or code	Access is possible with either card or code.
Access with card or code and PIN	Access is only possible with card or code and the PIN.
Toggle with card or code	Users can always switch between the operating modes "Access with card or code" and "Permanently open" with card or code.
Toggle with card or code and the PIN	Users can always switch between the operating modes "Access with card or code" and "Permanently open" with card or code and the PIN.
Two-person rule with card or code	Access is only possible with the card or code of two users.
Two-person rule with card or code and the PIN	Access is only possible with card or code and the PIN of two users.
Permanently open until closed with card or code	Users can switch between the operating modes "Permanently open" and "Access with card or code" as a one-off with card or code.
Permanently open until closed with card or code and the PIN	Users can switch between the operating modes "Permanently open" and "Access with card or code" as a one-off with card or code and the PIN.
Office mode with card	No function/cannot be used
Office mode with card and PIN	No function/cannot be used

An access group contains time and location-based access rules for one or more access points which can be assigned to several users. This means there is no need to configure this for each individual user and reduces the amount of configuration work. This also applies to subsequent changes.

Configuring a new access group
Time and location-based access rules are combined in an access group. These are assigned to users in the user configuration.

Procedure
1 Login with the "Facility" user account.
2 Open the "User administration" menu.
3 Open "All access groups".
4 Select "Create new".
5 Complete the missing information under "General" (see "Configuration help: Access group").
6 Select the required access point in the "Access rights" area.
7 Select the required week programme for the selected access point under "Week programme".
8 Select and configure further access points for this access group in the same way.
9 Select "Save and close".
10 Configure further access groups in the same way.

Configuration help: Access group

General	Explanation	As-delivered status
Name	For assigning a unique/useful designation for the access group (e.g. production employee)	–
Priority (low value has higher priority)	The priority controls which access groups take precedence if these conflict (e.g. if several access groups are assigned to a user). The following priority rule is set by the system: • The access group with the lowest value has the highest priority (priority above all other access groups). • If access groups with the same priority conflict, the access group with the stricter access rules (e.g. access with card or code and PIN instead of access with card or code) is applied.	"50"
Note	Information field for adding additional information about this access group	–
Access rights		
Drop-down menu	Drop-down menu for filtering the displayed access points: • "Show all doors": All already configured (available) access points are displayed. • "Show selected doors": The access points assigned to the access group are shown.	
Week programme	Drop-down menu for assigning a week programme for the access point in this access group. The week programme must be individually selected for each access point. The selection only applies to this access group.	

User
This is where new and existing users and new and existing IDs are configured.

Operating elements (user)
• "Refresh": Repeats the data request in the system and refreshes the information displayed.
• "Create new user": Function for creating a new user.
• "Search": Function for searching for users or narrowing down the user search.
• "Receive card number from teach-in read unit": Function for teaching-in a new, physical ID (electronic key/electronic key card)

Procedure
1 Login with the "Facility" account.
2 Open the "User administration" menu.
3 Open the "User" menu.
4 Select "Create new user".
5 Enter the missing data in the "General" and "Cards/codes" area and assign access options (see configuration help below).
6 Select "Save and close".
7 Configure further users and IDs in the same way.

Configuration help: Create new user

General	Explanation
Type	Non-modifiable information field showing "Standard".
First name	The user's first name
Middle name	The user's middle name
Surname	The user's surname
Company/department	The user's company affiliation
Note	Information field for adding additional information about this user.
Valid from	Time from which the user may use their ID in the access control system.
Valid indefinitely	If this option is enabled, the user can use their ID permanently in the access control system.
Valid to	Time up to which the user may use their ID in the access control system. This field is only enabled if the "Valid indefinitely" option is disabled.

Configuration help: Create new user

Cards/codes	Explanation	As-delivered status
Mode	This selection can be used to assign the number of available IDs that a user has: • "No ID": No IDs are assigned to the user. In this case, all the configuration options are greyed out in the administration interface. • "Single ID": One ID is assigned to the user. • "Several IDs": At least two IDs are assigned to the user.	"Single ID"
Card/code		
Card number/code	ID code for a taught-in physical ID (electronic key/electronic key card) or a manually entered series of digits (code).	–
Receive card number from teach-in read unit	Function button: Ready-to-use function for teaching-in physical IDs, provided a teach-in read unit has been configured in the system. The teach-in read unit can be any read unit installed in the property and connected to the access control system (e.g. ELM 600-…). Alternatively, a portable read unit can be used for direct connection to a laptop/PC (e.g. Siedle USB reader "readID One SE 1220 MNP").	–
Note	Information field for adding additional information about this ID.	–
Locked	If this option is enabled, the ID cannot be used in the access control system.	deactivated

Configuration help: Create new user

Card/code	Explanation	As-delivered status
PIN (digits)	Input field for assigning a PIN to a user. The PIN code is only required when dual identification is desired for greater security (e.g. identification with card or access code and additional PIN). Each user may be assigned any PIN (default: four-digit).	–
Repeat PIN	Input field for confirming the PIN already entered in the "PIN (digits)" field.	–
Usage count	Number of times that this ID (card or code) may be used depending on the reloading time.	–
Reloading time (min)	Time in minutes, after which the remaining usage count is reset to the value of the usage count to enable regular repeated use: • "0": The ID can be used once for the relevant count according to the configured usage count. • "[Numerical value]" (e.g. "600"): The ID can be used multiple times for the relevant count. Example "600": Every 600 minutes, the configured usage count is reset to the relevant number of uses according to the configured usage count.	–
Residual usage count	Count indicating the number of times it is still possible to use this ID (card or code).	–

Configuration help: Create new user

All access groups	Explanation	As-delivered status
All access groups	Selectable access group(s) which are to apply to this user. At least one access group or access right must be configured, otherwise the user will have no access. Multiple selections are possible in both cases.	–
Valid from	If this option is enabled, then a time point can be configured for this user, from which the access rules of the selected access group apply.	–
Valid to	If this option is enabled, then a time point can be configured for this user, from which the access rules of the selected access group no longer apply.	
Access rights		
Drop-down menu	Drop-down menu for filtering the displayed access rights: • "Show all doors": All already configured (available) access points are displayed. • "Show selected doors": The access points assigned to the user are shown. Access points from the access group are shown as already selected and non-modifiable, and cannot be selected and configured as individual access rights under "Access rights". **At least one access group or access right must be configured, for each user. Multiple selections are possible in both cases.**	–

Configuration help: Create new user

Options	Explanation	As-delivered status
Whitelist card	No function/cannot be used	deactivated
Open locked doors	If this option is enabled, authorised users can open the access point with their ID even in "No access" mode.	deactivated
Track card	No function/cannot be used	deactivated
Authorisation for intrusion detection	No function/cannot be used	deactivated
Approver (two person rule)	If this option is enabled, a user authorised for this can approve access to an access point as the second person, where this is secured by a two-person rule.	deactivated
Fire brigade access card	If this option is enabled, an authorised user is given unrestricted access rights to all access points with this ID.	deactivated
Longer door opening time	If this option is enabled, an extended opening time applies to this user at all assigned access points (e.g. people who use wheelchairs).	deactivated
Override intrusion detection rules	No function/cannot be used	deactivated
Allow commands from input units	If this option is enabled, an authorised user can control the access point manually via the access point's input unit, if the door commands have been configured on the input unit (see reader configuration "Door commands" on page 37).	deactivated
Use secondary validity period	No function/cannot be used	deactivated
General offline card	No function/cannot be used	deactivated
Read offline alarms	No function/cannot be used	deactivated

User administration by the customer/operator

Backup data/configuration

Create a complete data and configuration backup.

Procedure

1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "System information/ Database/Licence".
5 Open "Database".
6 Select "Backup database".
7 Confirm the query with "Yes".
8 Confirm the browser query with "OK" to save the backup file to your laptop.

Backup (export) the user data and access rights.

Note

Available user data and their access rights can only be exported with the Json file format (*Json).

Procedure

1 Login with the "Service" account.
2 Open the "User administration" menu.
3 Open "User import/export".
4 Select "Export…".
5 Select the file format "JSON file export".
6 Confirm the query with "Yes".
7 Save the data file to the laptop in the dialogue box.

Optional: Accounts
Creating an account

In the as-delivered status, two accounts (user accounts for the controller's user interface) are available with pre-configured access data:
• Service: Account with extensive authorisation for commissioning and managing the access control system.
• Facility: Account with limited authorisation for managing the access control system users.

Further accounts can only be created via the "Service" account.

Procedure
1 Login with the "Service" account.
2 Open the "Accounts" menu.
3 Open "Accounts".
4 Existing accounts are listed in a table.
5 Select "Create new" if you want to create a new account or select an existing account for editing or creating a new copy.
6 Complete the missing information under "General" (see the configuration help below).
7 Select "Save and close".
8 Create further new accounts or edit accounts, either:
• in the same way (recommended if the roles and menu rights differ significantly in detail for the account)
• using the "New copy" function (recommended if the roles and menu rights are the same for the account)

Configuration help: Create/edit account

General	Explanation	As-delivered status
User name	For assigning a unique/useful designation for the user account. The username is part of the log on for the controller.	–
Info	Information field for adding additional information about this user account.	–
Password	Password to be assigned for logging onto the controller. The password must contain at least six digits (letters, numbers, special characters).	–
Repeat password	For confirming the entered "password".	–
Password must be changed	If this option is enabled, a new password must be set when the user logs on for the first time.	deactivated
User	Optional selection of a user (responsible natural person for the user account) of the access control system that can be assigned to a user account.	–
Role	Role with corresponding rights for assignment for the user account: • Regular user: Configurable role with extensive authorisation for commissioning, and managing the access control system. Further roles can be created via a user account with this role. • Maintain session: Option for the "Regular user:" role for creating a user account without automatic logoff from the administration interface if no entries are made for 10 minutes.	–
Menu rights	The "Menu rights" area is only shown and can be configured if "Regular user" is selected as the role. Permitted menu access can be configured in detail here for the user account.	

Changing the password

Only the password for the user account with which one is logged onto the controller can be changed in this area.
Passwords for other user accounts can only be changed via the "Service" user account in the "Accounts" area directly on the selected user account.

Procedure

1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "Accounts" menu.
3 Open "Password".
4 The username for the user account is shown in the "General" area.
5 Open "Change password".
6 Enter the previous password in the "Password" field.
7 Enter a new, secure password in the "New password" field.
8 Repeat the new password in the "Repeat new password" field.
9 Select "Save and close".

Optional: Door management

Manual door control (status)

In this area, all configured access points can be manually operated (remote controlled) via the Secure Controller's administration interface. Five functions can be selected for the access points. It can be accessed via the "Service" and "Facility" user account.

Procedure

1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "User administration" menu.
3 Open "Door management".
4 Open "Manual door control (status)".
5 All the configured access points are listed in a table with state and status information.
6 Select the desired access point.
7 Execute the selected function. The status changes at the relevant access point in line with the function executed (see "Manual door control" table).

Function overview – manual door control

Function	Explanation	Access point state display	Access point status display
"Open"	Opens the access point. The opening duration depends on the access point configuration.	"Open" (only indicated during the opening duration)	–
"Close"	Closes the access point again. This function is required for permanently open access points. The access point is then in the "Normal" state again.	"Secured"	–
"Open permanently"	Opens the access point permanently. This state persists until the access point is closed again (manually or via week programme).	"Open"	"Permanently open"
"Normal"	The access point can only be opened with an ID (card/code).	"Secured"	–
"Lock"	The access point is closed and cannot be opened by regular users. Only users with enhanced authorisation or special authorisation can open this access point – provided it is configured (e.g. fire brigade, VIPs)	"Secured"	"Locked"

Optional: System monitoring

In this area you can see the current status of the interfaces, inputs and outputs, connections to other controllers (device group) as well as their synchronisation status. The system cannot be configured in this area. System monitoring can only be viewed via a user account with the "Service" role assigned.

Procedure

1 Log in with the "Service" user account.
2 Open the "System" menu.
3 Open "System monitoring".
4 Select the required area (e.g. Inputs/Outputs).
5 If other sub-areas can be selected, then navigate through the required sub-areas until the required information is shown.

Optional: Log/report
Events

This is where all system events are logged. Entries are displayed in a table sorted by time. Each event is assigned a category (info, attention, alarm). The events shown can be filtered and sorted by time ("time period") or category ("tags/types"). The "Events" area can be called up via the "Service" and "Facility" user account.

Procedure

1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "Log/report" menu.
3 "Events" is shown.
4 Logged entries are displayed in a table sorted by time.
5 If required, select "Filter" and adjust the filter details for "Categories" so that only the desired events are shown.

Reports can be configured in this area. A report contains selected events that are logged by the system (e.g. "Number of times access granted per day") and can display these for a configured period. Each report must be individually configured. Each report can be re-configured at any time after it has been saved. Up to 1000 lines (events) can be displayed with each report. Larger reports (with "Unlimited" configured for the quantity) are only possible directly using the file export in CSV format (*.csv).
The database can save up to one million events. If further events occur, the oldest events are deleted.

Note
When several controllers are operated in a device group, the events and reports for all controllers and controller extensions can only be accessed centrally via the primary controller. The secondary controller can still access its own events and reports.

Configuring a new report
1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "Log/report" menu.
3 Open "Reports".
4 Configured reports are shown in a table in the "Reports" area according to the order in which they were created.
5 Select "Create new" to configure a new report
6 Complete the missing information under "General" (see the configuration help: Configure new report).

Note
In the "Parameter" area, the desired data request can be configured in detail if required (e.g. selected time period or access point). The "Parameter" area can only be configured once a template has been selected in the "General" area.
The scope of the configuration depends on the selected template.
The detailed configuration in the "Parameter" area is carried out using logical operations of various variables.
Advanced knowledge of how to configure logical operations (database queries) is important for the configuration.

7 Complete the missing information under "Parameter" (see the configuration help: Configure new report).
8 Select "Save and close".

Running a report
1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "Log/report" menu.
3 Open "Reports".
4 "Reports" is shown.
5 Configured reports are shown in a table according to the order in which they were created.
6 Select "Run" a report to display a report. Each report can be exported and saved as a PDF (*.pdf) or CSV (*.csv) file.

Operation (parameters)
- "Add": Creates a new condition.
- "Insert" (for selected condition): Adds another condition at the selected position.
- "Remove": Removes a selected condition.

Configuration help: Configure a new report

General	Explanation
Template	Drop-down menu with various ways to record events from the access control system for logging/documentation in a report (e.g. report on the "Number of times access granted per day"): • "Event log": Record of all system events. • "Access log": Record of all access events. • "Number of times access granted per day": Record of all access events without lockers. • "Number of times access granted for individual card holders per day": Record of individual users. • "Access log including lockers": Record of all access events incl. lockers. • "Events for open lockers": Record of all locker events. • "Account users in access group": Record of selected user groups with access to the controller. • "Users in access group": Record of selected user groups. • "Card holder presence today (requires adv. params)": Record of selected users.
Title	For assigning a unique/useful title (designation) for this report. When selecting a template, the template's designation is automatically added and can be manually changed.
Note	Information field for adding additional information about this report.
Maximum number of events	Number of events that are to be recorded in the report (e.g. "1000": The first 1000 events will be documented in the report).
Skip events for report	Number of events that are to be skipped so that the following events are recorded in the report (e.g. "500": The first 500 events are not included in the report. The first event in the report if the 501th event.)

Configuration help: Configure a new report

Parameters	Explanation
Operator	Selectable link between two variables (e.g. time period) of a logical operation (database query): • "(": Open bracket • ")": Closed bracket • "NOT": For negating operations (contrary: e.g. not state A) • "AND": For combining operations (e.g. state A and state B) • "AND NOT": For combining operations with negation (e.g. state A and not state B) • "OR": For differing operations (state A or state B) • "OR NOT": For differing operations with negation (e.g. state A or not state B) **Note** Operators can be combined as desired. However the combination must make sense, otherwise the database query will not produce any results. The number of events that are output depends on the actual events available and the maximum number of events to be output in the report as configured in the "General" area. **Example** For a report with the template "Event log", events with the event date 01.03.2021 or 08.03.2021 are to be output. Operation in display field: Event time = '01/03/2021' OR event time = '08/03/2021'

Configuration help: Configure a new report

Parameters	Explanation
Variable	Place holder for an allocatable, variable quantity (e.g. selected time point or access point) of a logical operation (data query). The selectable variables depend on the "template" selected under "General": • "Event time": For selecting a time point via the calendar • "User name": User * • "Cards and codes": ID * • "Door name": Access points * • "Reader name": Read/input units * • "Event": Selectable event (e.g. "Access denied") • "Door ID": Selectable access point (e.g. door 1 main entrance south) • "Reader ID": Selectable read/input unit (e.g. reader door 1 main entran ce south ELM adresse2 line A) • "Key box": Key box * • "Key box ID": Key box selection (e.g. Key box 1) • "Access group ID": Selectable access group (e.g. produc- tion employee) *** Note** If there is no drop-down menu for a selected variable in the "Value" field, then a character string can be entered in the "Value" field, according to which all corresponding results for the logical operation, whose designation/identifier contains at least the input in the "Value" field, are applied. If a drop-down menu is empty, there is no selection available.

Configuration help: Configure a new report

Parameters	Explanation
Comparison	Selectable relational operator (e.g. “>“ or “=“) for limiting or excluding value ranges (e.g. event time >01/03/2021) or for assigning one or more values to a variable (e.g. event time =01/03/2021) within a logical operation (database query). The selectable relational operators depend on the selected “variable“: • “=“: Equals • “<>“: Does not equal • “>“: Is greater than • “>=“: Is greater than or equal to • “<“: Is less than • “<=“: Is less than or equal to • “within the last [x] days“: All the results of the variables for the specified number of days at the time of the search. • “Is invalid“: All the results of the variables which are invalid. • “Contains“: All the results of the variables which contain the searched-for character string in the name or identifier. Upper/lower case must be taken into account.
Manual input	If this option is enabled, a value that has been manually entered or selected via drop-down menu in the “Value“ field (“standard value“) is overwritten by a manually entered value in the “Manual input value“ field. The “Manual input value“ input fields open for this and the previous “Value“ field is denoted the “Standard value“ so the distinction is clear.
Manual input value	Input field for a manually entered value (character string, name, series of digits, etc.) which overwrites the value in the “Standard value“ field. The value is used for the logical operation with the variables.

Configuration help: Configure a new report

Parameters	Explanation
Standard value	Original "Value" field, which is renamed to "Standard value" if the "Manual input" option is activated in the system. Input field for a value that has been manually entered or selected via drop-down menu (character string, name, series of digits, etc.) The value is used for the logical operation with the variables.
Value	Input field for a value that has been manually entered or selected via drop-down menu (character string, name, series of digits, etc.) The value is used for the logical operation with the variables.

Access log

All successful access events within the last 12 hours are logged in this area. Entries are displayed in a table sorted by time. The access log can be called up via the "Service" and "Facility" user account.

Procedure

1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "Log/report" menu.
3 Open "Access log".
4 Successful access events within the last 12 hours are shown in a table.

A restart can be initiated via the Secure Controller's interface if required. This function is available in two locations on the controller, but only by using a user account with assigned service role.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "Firmware update" or "System information/Database/ Licence".
5 Scroll down in the area.
6 Select "Restart the device".
7 Confirm the query with "Yes".
8 A confirmation is displayed.
9 The controller performs a restart and can be accessed again after approx. 1 minute via the logon screen.

The Secure Controller's sabotage monitoring monitors the opening of the controller housing with an optical sensor system and is immediately active once the device is ready for operation.
If the housing is opened, alarm messages are output and logged at the administration interface at regular intervals. The alarm message can be processed further via the configurable logic (e.g. controller output switches a signal).

Configuration
The sabotage monitoring can be deactivated and the sensitivity of the optical sensor system can be changed in the "root" user account.

Procedure
1 Login with the "root" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "System properties".
5 Open "Properties".
6 Select the "Sabotage monitoring" tab.

Configuration options:
• Activate the "Deactivate optical sensor system" option to deactivate the sabotage monitoring.
• Change the sensitivity of the optical sensor system in the "Ambient light threshold value" field to adjust this to the controller's environmental conditions (e.g. lighting conditions in the engineering room). The higher the value, the more the optical sensor system responds to incident ambient light when the housing is opened.

7 Select "Save".
8 Log off from the "root" account.

Check the threshold value for the optical sensor system
In the as-delivered status, the threshold value for the sensitivity of the optical sensor system is pre-configured to "150".
If a different value is required due to the Secure Controller's environmental conditions, the lighting conditions with closed and open housing can be queried.

Procedure
1 The Secure Controller housing is closed.
2 Login with the "root" account.
3 Open the "System" menu.
4 Open "System monitoring".
5 Open "Inputs/outputs".
6 Open "Logical inputs".
7 Select the "Update" action for "Sabotage monitoring brightness (sensor)".
8 The value for "Sabotage monitoring brightness (sensor)" corresponds to the brightness value when the housing is closed (e.g. 500).
9 Adjust the light conditions such that they are as would be expected in the event of unauthorised access.
10 Open the Secure Controller housing and wait approximately 10 seconds.
11 Select the "Update" action for "Sabotage monitoring brightness (sensor)".
12 The value for "Sabotage monitoring brightness (sensor)" corresponds to the brightness value when the housing is open with the lighting conditions (e.g. 150).
13 Close the Secure Controller housing again.
14 Adjust the sensitivity of the optical sensor system. If the sabotage monitoring responds to the determined brightness value, a sufficiently higher threshold value must be selected (e.g. 200 or higher).
15 Carry out tests to check the configured value.

Deleting data

All configuration data for devices and users can be deleted via the Secure Controller's administration interface, if required. This function is only available by using a user account with assigned service role.

Note
Only configuration data for access points, read and input units, users and week programmes as well as user account passwords are deleted. Additionally created user accounts are completely deleted. The network configuration is retained.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "System information/ Database/Licence".
5 Open "Database".
6 Select "Delete database".
7 Confirm the query with "Yes".
8 The controller performs a restart and can be accessed again after approx. 1 minute via the logon screen.

Restoring default settings

Software-based execution
The default settings can be restored via the Secure Controller's administration interface.
This permanently deletes all saved information and the entire configuration for the controller, the devices and the users.
This function is only available by using a user account with assigned service role.

Note
As the network configuration is also deleted, the controller's IP address may need to be re-determined and only the pre-configured logon data can be used for logon - see page 4.

Procedure
1 Login with the "Service" account.
2 Open the "System" menu.
3 Open "Administration".
4 Open "Firmware update".
5 Open "Default settings".
6 Run the "Default settings" function.
7 A security prompt appears.
8 Enter the displayed "Reset code" into the input field. The "Default settings" button is only active and able to be actuated once the correct reset code has been entered.
9 Press "Default settings" to begin the reset to default settings.
10 The controller is reset to its default settings and restarted.

Hardware-based execution
The default settings can be restored by pressing the "User button" on the Secure Controller.
This permanently deletes all saved information and the entire configuration for the controller, the devices and the users.
The "user button" can only be pressed if the Secure Controller housing is open. For details on the "user button" and LED signalling, see page 8.

Note
As the network configuration is also deleted, the controller's IP address may need to be re-determined and only the pre-configured logon data can be used for logon - see page 4.

Procedure
1 Open the Secure Controller housing
2 Press the "user button" five times within five seconds.
3 The two LEDs for indicating the operating status (green) and the system status (red) flash.
4 An acoustic signal sounds and is repeated up to three times (interval: 3s acoustic signal followed by 3s pause).
5 On the fourth acoustic signal, press and hold the user button until the acoustic signal ends.
If the button is not pressed by the last acoustic signal, the process is terminated automatically without a system change.
6 The controller is reset to its default settings and automatically restarted and can be reached again after approximately one minute via the logon screen.

The network settings can be reset to two versions by pressing the "user button" on the Secure Controller. The "user button" can only be pressed if the Secure Controller housing is open. For details on the "user button" and LED signalling, see page 8.

Note
As the network configuration is deleted, the controller's IP address may need to be re-determined for DHCP mode.

Important!
The network settings can be reset to two versions:
• DHCP mode: The network settings are reset to DHCP mode and the controller is restarted.
• Static IP address: The network settings are deleted and the static IP address: 192.168.1.100 is configured.

Procedure
1 Open the Secure Controller housing
2 Press the "user button" five times within five seconds.
3 The two LEDs for indicating the operating status (green) and the system status (red) flash.
4 An acoustic signal sounds and is repeated up to three times (interval: 3s acoustic signal followed by 3s pause).
5 Selection – second/third acoustic signal
• Second acoustic signal - DHCP mode: On the second acoustic signal, press and hold the "user button" until the acoustic signal ends.
• Third acoustic signal - static IP address: On the third acoustic signal, press and hold the "user button" until the acoustic signal ends.
If the button is not pressed by the last acoustic signal, the process is terminated automatically without a system change.
6 The network settings are reset/ changed as selected. The controller is automatically restarted and can be reached again after approximately one minute via the logon screen.

User data and their access rights can be imported/exported via file with the following file formats:

File format	Data transfer
JSON (*.Json)	Import and export possible
CSV (*.csv)	Import possible

Application
• JSON: The JSON file format is intended for exporting the configured user data and their access rights from the Secure Controller for backup purposes (archiving) so that it can be re-imported if required.
• CSV: The CSV file format is intended for importing new users and if required assigned card numbers/codes from other systems or programs. Data from other systems or programs must be prepared before import according to the following instructions. For details, see "Preparing datasets from other systems" on page 92.

Template file for data import
The following options are available for a template file from Siedle for the first import of user data into the Secure Controller:
• Either download the Siedle template file "Sample_file_SC_600-0.xlsx" from the Siedle website,
• or carry out an export in the Secure Controller using the "CSV file (semicolon)" selection. For details, see "Exporting a data file".

Important!
The template file contains labelled columns for filling out with the relevant data for the future access control system users.

Exporting a data file
The following options are available for export:
• Available user data and their access rights can only be exported with the Json file format (*Json) (for data backup or manual data processing).
• An empty data file (container) for manual maintenance of user data can be created with the CSV file format (* .csv).

Procedure
1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "User administration" menu.
3 Open "User import/export".
4 Select "Export…".
5 Select file format according to the intended use (e.g. "CSV file (semicolon)").
6 Confirm the query with "Yes".
7 Save the data file to the laptop in the dialogue box.
8 The data file is available for the desired intended use.

Preparing datasets from other systems
This preparation is required when data has been exported from another system or administration program and is to be used for import into the Secure Controller.
These instructions describe how to prepare data records in MS Excel and from a file export in MS Excel file format (.xlsx).

Preparation
• Either download the Siedle template file "User administration template file SC 600" (File: "Sample_file_SC_600-0.csv") from the Siedle website or carry out a data export with "CSV file (semicolon)" in the Secure Controller.
• The template file contains labelled columns for filling out with the relevant data for the future access control system users.

Important!
• The column headings must not be changed.
• All data areas (columns) must be formatted with the "Standard" cell format apart from the validity information ("VALID_FROM" and "VALID_TO").
• Validity information with date and time (optional) must be filled out in the "Text" cell format and with the following notation: [DD/MM/YYYY hh:mm:ss] (e.g. 20/03/2021 18:30:59).

Procedure
1 Open both files (customer data file and Siedle template file) in MS Excel.
2 Data areas in the data file provided by the customer must be in the "Standard" or "Text" cell format as described above, otherwise format the affected data areas and check the content afterwards.
3 Use copy&paste to copy data from the file provided by the customer into the relevant areas of the Siedle template file (work with VLOOKUP if required).
4 Close the data file provided by the customer.

5 Save the completed Siedle template file with a new name.

Note
Steps 6-10 are only required if you have used the Siedle template file (*.xlsx) from the Siedle website.

6 Open the following path in MS Excel: File > Export >Change file type
7 Select "CSV (delimiter-separated) (*.csv)".
8 Select "Save as".
9 Save the Siedle template file with a new name as a CSV file.
10 Confirm the query in MS excel with "Yes".

Note
The CSV file must be edited with a text editor.

11 Select CSV file with the mouse.
12 Right-click.
13 Use the mouse pointer to select the "Editor" via "Open with" to open the CSV file.
14 The editor opens with the CSV file.

Note
The semicolons must be replaced with commas.

15 Open the "Replace…" function (path in open editor: Edit > Replace …).
16 Enter a semicolon in the "Find …" field.
17 Enter a comma in the "Replace with …" field.
18 Select "Replace all".

Note
The edited CSV file must now be saved with "UTF-8" Unicode character encoding.

19 Open "Save as …" function (path in open editor: File >Save as …).
20 Assign any file name.
21 Select "UTF-8" under the "Coding" selection.
22 Select "Save".

Important!
Any data records in files to be imported must always be saved with Unicode "UTF-8" character encodings. Otherwise umlauts or special characters could be misinterpreted or not recognised.

23 The CSV file can now be imported into the Secure Controller. The import must be performed with the "CSV file (comma)" selection.

Importing a data file
User data and their access rights can be imported via file with all the file formats that can be selected under "Import".

Procedure
1 Login with the relevant user account (e.g. "Service" or "Facility").
2 Open the "User administration" menu.
3 Open "User import/export".
4 Select "Import …".
5 Select file format (e.g. "CSV file (comma)").
6 Select the data file in the dialogue and select "Upload" to import it.
7 Confirm the confirmation prompt with "OK".
8 Imported user data and their access rights are displayed in a table.
9 Check the imported data is correct.
10 In the event of an error, delete the imported data records and repeat the data import with a corrected data file.

Replacing single controllers
Replace a faulty controller in (autonomous) individual operation as follows:

Conditions
• A data backup is required to restore the access control system with a new controller.
• The password for the "Service" user account, which was valid at the point of backup, must be known.

Preparing for the controller changeover
1 De-energise all devices operated on the faulty controller (read and input units, other components).
2 Switch off the external power supply on the faulty controller (if externally supplied).
3 Disconnect the faulty controller from the network.
4 Document all connections/wires/cables for the devices operated on the faulty controller (read/input units, other components) and disconnect their plug-in connections (plug-in terminals).
5 Remove the faulty controller.
6 Install the new controller.
7 Correctly re-connect all devices (read and input units, other components) to the new controller again according to the documentation.

Starting up the new controller
8 Connect the new controller to the network.
9 Switch on the external power supply on the new controller (if externally supplied).

Note
The network configuration of the new controller is not part of the access control system restoration process.

10 Determine the IP address of the new controller. For further information, see page 13.
11 Log on on the controller's logon screen using the access data for the "Service" account.
12 For "Password", enter the password "Siedle1234" (as-delivered status).

Note
The password change dialogue will appear the first time you log on to the Secure Controller.

13 Please enter a new password for the "service" account.

Note
This password is only temporary and is changed during the system restoration.

Restoring the data and configuration
14 Open the "System" menu.
15 Open "Administration".
16 Open "System information/Database/licence".
17 Open "Database".
18 Select "Restore database".
19 Use "Select file" to select the file for restoring the data backup and "Upload" to import it.
20 Confirm the confirmation prompt with "Yes".
21 The access control system will then be restored on the new controller.

Note
This generally takes several minutes.

22 Finally, the new controller automatically restarts and can then be used again in the same state as per the last backup.

Replacing the secondary controller
You can replace a controller which is configured as a secondary device in device group as follows:

Check system update!
• All devices in the existing system and also the replacement device must have the same and latest software version. Check beforehand whether a system update is available. For details, see page 97.
• If the replacement device has a newer system version than the existing system, then a system update must be carried out for all controllers in the device group before device replacement.

Preparing for the controller changeover
1 De-energise all devices operated on the secondary controller (read and input units, other components).
2 Switch off the external power supply on the secondary controller (if externally supplied).
3 Disconnect the secondary controller from the network.
4 Document all connections/wires/cables for the devices operated on the secondary controller (read/input units, other components) and disconnect their plug-in connections (plug-in terminals).
5 Remove the secondary controller.
6 Install the new controller.
7 Correctly re-connect all devices (read and input units, other components) to the new controller again according to the documentation.

Note
The connection to the power supply and network takes place at a later point in time.

8 Log on to the associated primary controller with the "Service" account.
9 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).

Carry out a system update for all existing controllers
If required, carry out a system update for all primary and secondary controllers belonging to the device group. For details, see page 97.

Starting up the new controller
10 Connect the new controller to the network.
11 Switch on the external power supply on the new controller (if externally supplied).
12 Select "Search for Siedle Secure Controller …" to find the IP address of the new controller.
13 A new window opens with the search results.
14 The controllers found are listed in a table.
15 Note down the IP address of the new controller.
16 Close the window with the search results.

Carry out a system update for the new controller (replacement device)
If required, carry out a system update for the new controller. For details, see page 97.

Integrating a new controller
17 Select the secondary controller that is to be replaced from the list.
18 Enter the IP address of the new controller.
19 Navigate down to the "MAC address" field.
20 Select "Call up new MAC address" to adopt the MAC address of the new controller.
21 Select "Save and close".
22 Select the "Set as secondary device" function in the "Actions" menu.
23 Confirm the confirmation prompt with "Yes".
24 The secondary controller is synchronised and integrated into the device group. This process generally takes several minutes (at least around three minutes, depending on the system size (number of controllers and users)).
25 The process is fully complete when the status "synchronised" is displayed in the "Secure Controller" menu.
26 Perform a function check with all devices connected to the new secondary controller.

Important!
When using the "Import as secondary device" and "Delete" functions, the configuration of the controller that is to be replaced is always deleted.

Replacing the primary controller
You can replace a controller which is configured as a primary device in device group as follows:

Check system update!
• All devices in the existing system and also the replacement device must have the same and latest software version. Check beforehand whether a system update is available. For details, see page 97.
• If the replacement device has a newer system version than the existing system, then a system update must be carried out for all controllers in the device group before device replacement.

Preparing for the controller changeover
1 De-energise all devices operated on the primary controller (read and input units, other components).
2 Switch off the external power supply on the primary controller (if externally supplied).
3 Disconnect the primary controller from the network.
4 Document all connections/wires/cables for the devices operated on the primary controller (read/input units, other components) and disconnect their plug-in connections (plug-in terminals).
5 Remove the primary controller.
6 Install the new controller.
7 Correctly re-connect all devices (read and input units, other components) to the new controller again according to the documentation.

Note
The connection to the power supply and network takes place at a later point in time.

Assigning the primary device role to a secondary controller
8 Log onto any secondary controller with the "Service" account.
9 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).
10 Select "Change primary device".
11 The secondary controller determines a new primary controller from all existing secondary controllers.
12 The new primary controller performs a restart.
13 Log on to the new primary controller with the "Service" account.
14 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).

Carry out a system update for all existing controllers
If required, carry out a system update for all primary and secondary controllers belonging to the device group. For details, see page 97.

Starting up the new controller
15 Connect the new controller to the network.
16 Switch on the external power supply on the new controller (if externally supplied).
17 Select "Search for Siedle Secure Controller …" to find the IP address of the new controller.
18 A new window opens with the search results.
19 The controllers found are listed in a table.
20 Note down the IP address of the new controller.
21 Close the window with the search results.

Carry out a system update for the new controller (replacement device)
If required, carry out a system update for the new controller. For details, see page 97.

Integrating a new controller
22 Select the secondary controller (former primary controller) that is to be replaced from the list.
23 Enter the IP address of the new controller.
24 Navigate down to the "MAC address" field.
25 Select "Call up new MAC address" to adopt the MAC address of the new controller.
26 Select "Save and close".
27 Select the "Set as secondary device" function in the "Actions" menu.
28 Confirm the confirmation prompt with "Yes".
29 The secondary controller is synchronised and integrated into the device group. This process generally takes several minutes (at least around three minutes, depending on the system size (number of controllers and users)).
30 The process is fully complete when the status "synchronised" is displayed in the "Secure Controller" menu.
31 Perform a function check with all devices connected to the new secondary controller.

Important!
When using the "Import as secondary device" and "Delete" functions, the configuration of the controller that is to be replaced is always deleted.

Deleting the secondary controller from the device group

Important!
If a secondary controller is to be removed from a device group, the secondary controller must be deleted. In doing so, all rights and configuration data for the secondary controller that is to be deleted are lost and connected end devices for the access control system (e.g. readers) are no longer useful.

Procedure
1 Log on to the associated primary controller with the "Service" account.
2 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).
3 Select the secondary controller that is to be removed in the list.
4 The "Editing Siedle Secure Controller [<name of the controller>]" menu opens.
5 Select "Delete".
6 The confirmation prompt allows you decide whether the secondary controller is to be removed from the primary controller or not.
7 Confirm the confirmation prompt with "Yes".
8 The "Editing Siedle Secure Controller [<name of the controller>]" menu closes.
9 All configuration data for the secondary controller except for the IP address and the host name is deleted. User accounts and passwords return to the as-delivered status.

Optional: Service
Activating service mode

The Secure Controller's service mode can be enabled by pressing the "user button" on the Secure Controller. In this mode, the Secure Controller is no longer accessible via the administration interface. This function is only intended for use by Siedle service. The "user button" can only be pressed if the Secure Controller housing is open. For details on the "user button" and LED signalling, see page 8.

Important!
If the Service mode is accidentally enabled, it can only be disabled by disconnecting the Secure Controller's power supply.

Procedure
1 Open the Secure Controller housing
2 Press the "user button" five times within five seconds.
3 The two LEDs for indicating the operating status (green) and the system status (red) flash.
4 An acoustic signal sounds and is repeated up to three times (interval: 3s acoustic signal followed by 3s pause).
5 On the first acoustic signal, press and hold the user button until the acoustic signal ends.
6 The controller is now in service mode and cannot be accessed via the administration interface.
7 To disable service mode, interrupt the Secure Controller's power supply for approx. 10 seconds. Following the restart, the Secure Controller can be accessed via the administration interface again after approximately one minute.

If the button is not pressed by the last acoustic signal, the process is terminated automatically without a system change.

Important!

• If a new update is available for the Secure Controller, download the firmware file for the system update and save it on your computer.

• The firmware file for the Secure Controller is available for Siedle partners and specialist partners to download in the "My Siedle" service portal at www.siedle.de/meinsiedle. Registration is required to gain access. End users should contact their nearest Siedle partner.

• During a system update the Secure Controller and thereby the entire access control system is temporarily not operational. Carry out the system update at a suitable time and communicate the plan well in advance.

• Every time before updating the system (upgrade), carry out a complete system backup. Ensure that all system backups are safely and permanently stored.

Procedure

1 Log on on the controller's logon screen using the access data for the "Service" account.
2 Open "System" on the start screen.
3 Open "Administration".
4 Open "Firmware update".
5 Select "Upload firmware file" in the "General" area.
6 Select "Search …" in the dialogue box.
7 Select the firmware file in the dialogue box and confirm with "Open".
8 Select "Upload".
9 The firmware file is loaded into the controller and checked. Once the firmware file has been approved by the controller for a system update it is installed. Otherwise an error message appears which leads to cancellation of the system update.
10 To complete the system update, the controller must be restarted. A dialogue box appears stating that the controller will automatically restart within 15 seconds. The restart can be postponed by selecting "Restart later".
11 Select "Restart now" or wait 15 seconds for the automatic restart to begin.
12 The controller performs a restart and can be accessed again after approx. 1 minute via the logon screen.
13 Check the new firmware status after logging back onto the controller in the "Firmware update" menu, "General" area, "Firmware version" field.

Check the firmware status (device group)

The firmware status of individual controllers which are in operation as a device group can be viewed centrally via the primary controller.

Procedure

1 Log on to the primary controller with the "Service" account.
2 Open the "Secure Controller" menu (path: System > Administration > Secure Controller).
3 The list contains all Secure Controllers that are operated with the primary controller and the relevant firmware version is indicated.

Index

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

Printed in Germany
Best. Nr. 210010871-01 EN