Manual
TCIP 603-03
TCIP SRV 603-0

Remarks

All the information contained in this Manual has been collated to the best of our knowledge and carefully tested. However, the possibility of errors cannot be completely excluded. For this reason, the information contained in this Manual does not constitute an obligation or a guarantee of any description. The authors, companies and publisher consequently accept no legal responsibility and are unable to assume any liability based on this document or any other liability arising from the use of this information or parts of it. This applies also to the infringement of patent rights and other third party rights which could result.

Table of contents

About this Manual
This Manual offers information required for commissioning the TCIP 603-…
During compilation of the Manual, attention was paid to ensuring that it may be understood even by beginners. Despite this, in certain chapters, specialist IT expertise is helpful as an aid to understanding. Those using the Manual should be familiar with the operation of a web browser.

Who this Manual is aimed at
This Manual is aimed at
- Planning engineers
- Installers
- Service technicians
- Administrators
- Users

Requirements
Programming the TCIP 603-… with a PC and installed Internet Explorer latest version.

1. Description

1.1. Access control

An access control system ensures that only authorized persons may enter certain areas. Time models are also available as an additional restriction, which determine when a certain user may gain access to the relevant area.
The central control system comprises a controller which is able to manage up to 8 doors. Each door may be fitted with a code lock, Easikey and fingerprint module. If the presented ID is valid, the controller switches a relay which controls, for instance, a door release, a rotating door or a turnstile.

1.2. Functions

The TCIP 603-… has the capability to control all generally used methods offered by a modern access system:
- Management of users, access groups and time profiles
- Attendance and absentee list
- Anti-passback function
- Log entries

1.3. Networking several TCIP 603-…

The additionally available server solution TCIP SRV 603-… offers scope for the central management of any optional number of TCIP 603-… units within a network from a PC. The server solution manages all TCIP 603-… units via the IP network on the basis of the IP address, permitting extremely convenient user management. For more information, refer to Chapter 4 of this Manual.

2. User interface
2.1. Login at the user interface

1 Enter the IP address in the Internet Explorer.
Login to the system takes place using a web user interface. This requires you to know the IP address of the TCIP 603-… As standard, 192.168.0.1 is used.

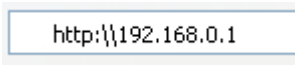


Fig. 1: Entry of the IP address in the Internet Explorer

2 Enter your access data.
The main user has the login name "**Service**" and the password "**Siedle**".
It is advisable to change the password when first commissioning the system. However, if the new password is forgotten, the TCIP 603-… can only be reset by the company Siedle.

Fig. 2: Login dialogue box

Within the login dialogue box, it is also possible to select the language.

3 Login at the TCIP 603-…
Start the login process using the "login" arrow.

Note

In the dialogue boxes, a number of fields appear with an asterisk. This indicates that these are mandatory fields.

2.2. General operation

The operating window is divided into three areas:

- The menu area (highlighted in yellow).
- The action area (highlighted in green).
- The door release area (highlighted in blue).

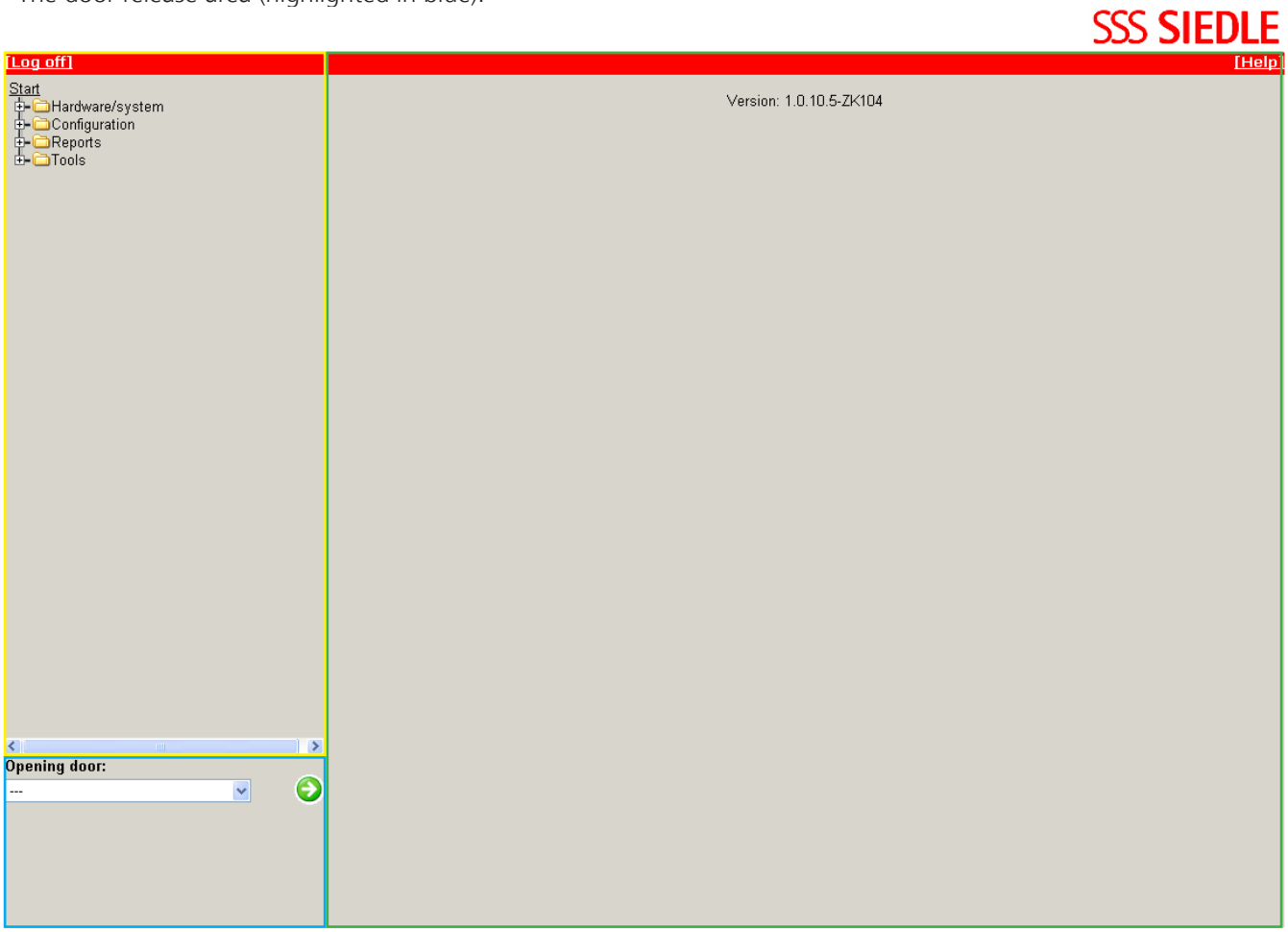


Fig. 3: User interface

All the possible configuration points are listed grouped in the **menu area** (yellow). Depending on the user authorization, these are either shown or blanked out.

In the **action area** (green) all dialogue boxes are shown which are selected using the menu.

The **door release area** (highlighted in blue) is used for quick opening of a door.

2.3. Menu tree and functionality

In the following, all the menu points and their functions are described.

2.3.1. Hardware/system

This point encompasses all the functions which affect the hardware or software.
The inputs, outputs and reader are dynamically managed. In total, 24 input modules such as Code lock modules, Electronic-key reading modules or Fingerprint modules are supported. In addition to this are also the "local" inputs and outputs on the TCIP 603-… and the extensions FSM 740-… and SCE 640-…

2.3.1.1. Inputs

The "Hardware/System -> Inputs" menu point provides a list of all configured inputs. A difference is drawn between "local" and "external" inputs.
The "local" inputs (inputs E1–E5) are located at the TCIP 603-01. "External" inputs are addressed via the FSM 740-… and SCE 640-…
If no FSM 740-… is found on startup (Power ON) of the TCIP 603-…, this function is disabled.

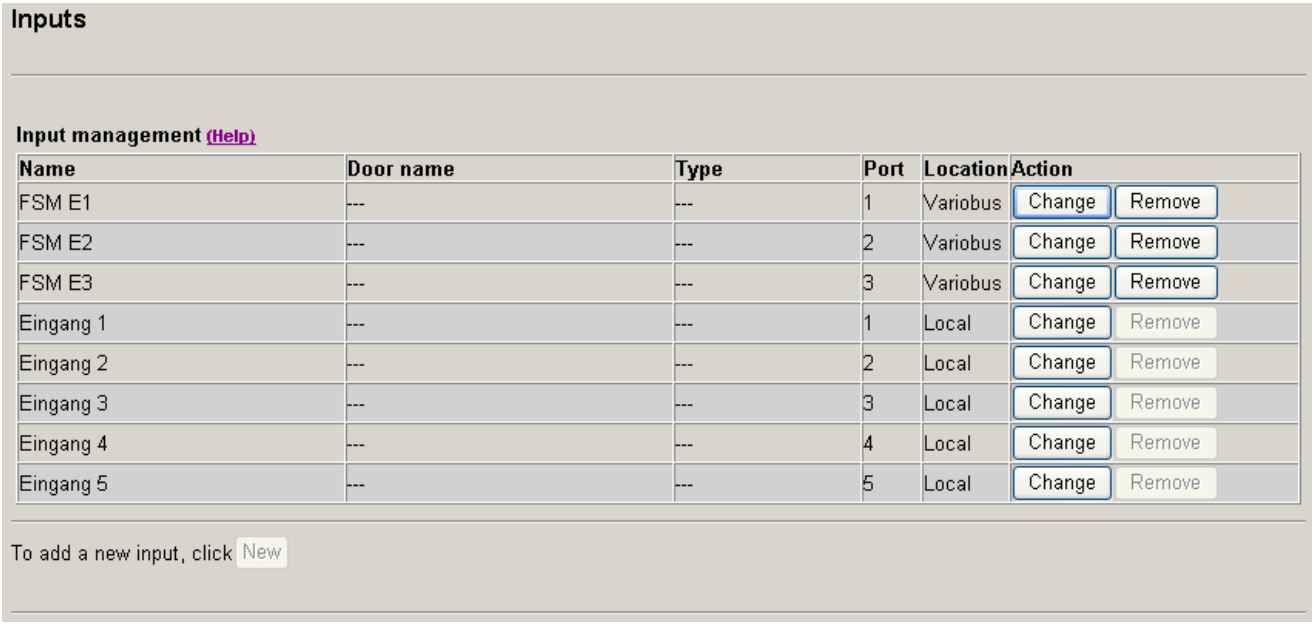


Fig. 4: List of inputs

Column name	Description
Name	This column describes the name of the input.
Door name	If the input is assigned to a door, the door name appears here.
Type	There are two different input types (door sensor and door button). One of these two is displayed here when the input is in use.
Port	Here, the port number of an input is displayed.
Location	A distinction is made between two different locations. The location "local" stands for local inputs E1–E4. "Vario bus" stands for external inputs via the FSM 740-…

Table 1: List of inputs: Column description

The two actions "Change" and "Remove" are assigned to each configured input. Using "Change", the name of the input and the device number can be changed. The action "Remove" removes the input.
However, these actions are subject to a number of restrictions:
- If an input is assigned to a door, this can no longer be changed or removed.
- Local inputs cannot be removed.

A new external input can be created using the action "New".

2.3.1.2. Creating inputs

Creating new inputs is only possible in conjunction with the FSM 740-…
If no FSM 740-… is found on the Vario bus when initializing the TCIP 603-…, this functionality is disabled.
A name and an input of the FSM 740-… is assigned to each input.

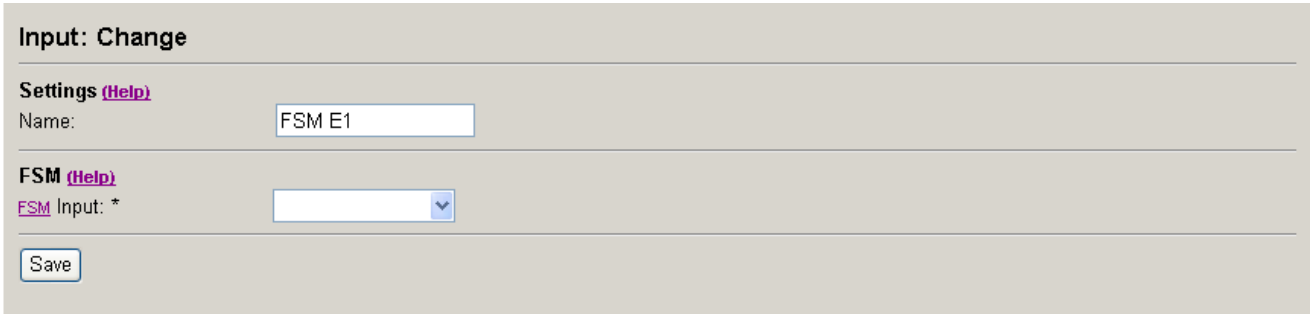


Fig. 5: Creating an input

Field name	Description
Name	Describes the name of the input.
FSM Input	Indicates the input at the FSM 740-… A maximum of 3 additional inputs can be created.

Table 2: Creating an input: Description of the fields in the dialogue box

This dialogue box contains the following action:

Action	Description
Save	This action creates the input.

Table 3: Creating an input: Action in the dialogue box

2.3.1.3. Changing/removing an input

If local inputs are changed, the section “Change” input does not appear.

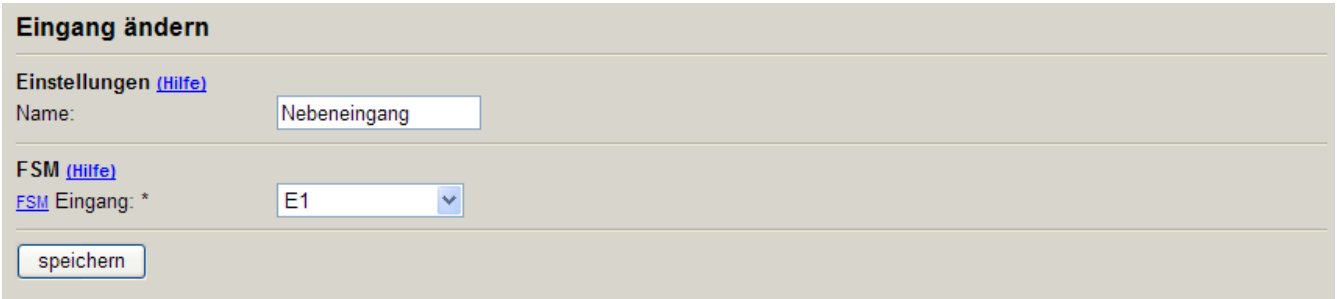


Fig. 6: Changing/removing an input

Field name	Description
Name	Describes the name of the input.
FSM Input	Indicates the input at the FSM 740-…

Table 4: Changing/removing an input: Description of the fields in the dialogue box

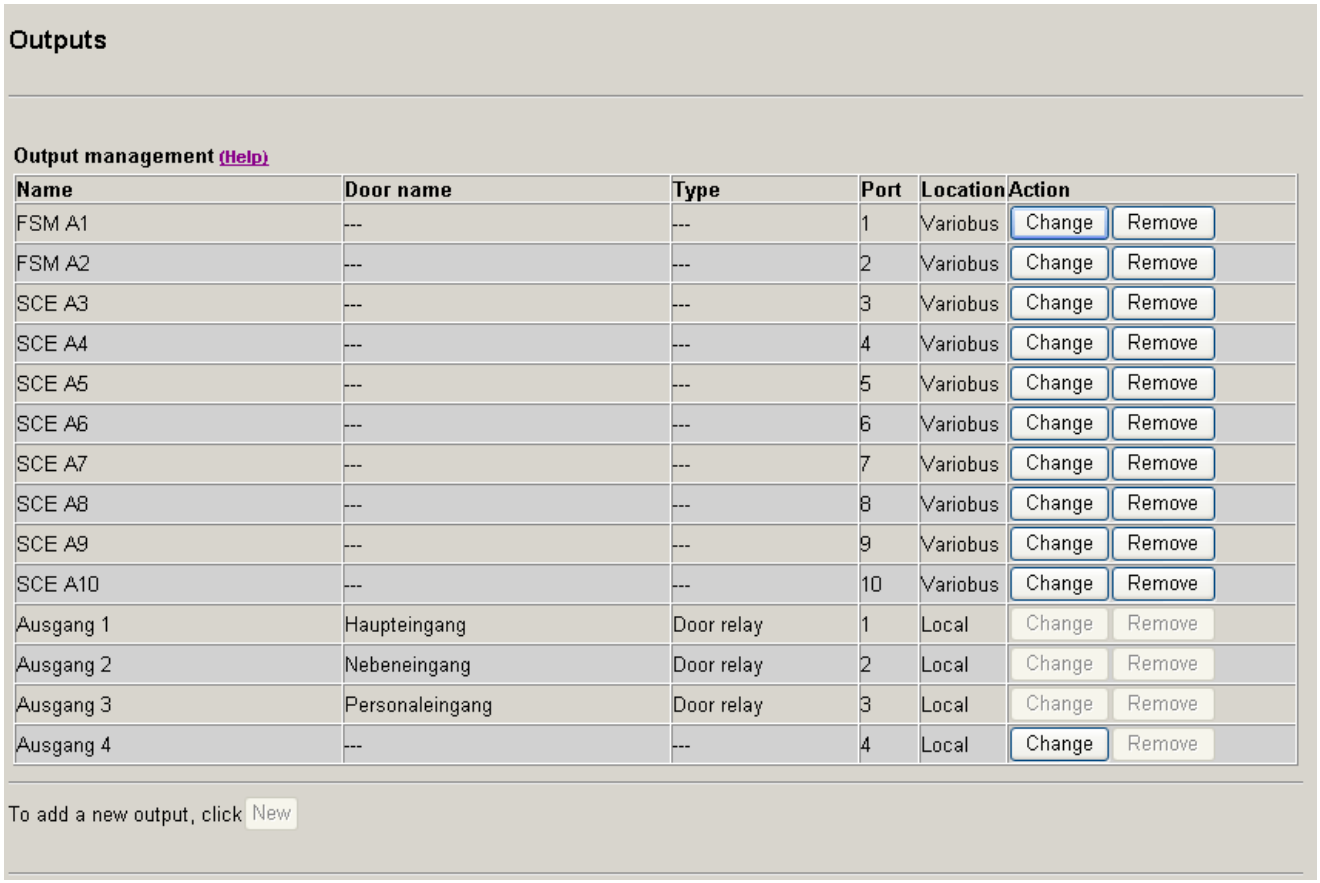
The page contains two actions:

Action	Description
Change/Remove	Depending on the selection in the previous menu, “Change” or “Remove” is indicated.

Table 5: Changing/removing an input: Actions in the dialogue box

2.3.1.4. Outputs

Via the menu point “Hardware/System -> Outputs” a list showing all configured outputs is displayed. A difference is drawn between “local” and “external” outputs. Local outputs (outputs A1–A4) are addressed physically directly at the TCIP 603-…, external outputs via the FSM 740-…
If no FSM 740-… is found on startup of the TCIP 603-…, no outputs can be created.



Name	Door name	Type	Port	Location	Action
FSM A1	---	---	1	Variobus	Change Remove
FSM A2	---	---	2	Variobus	Change Remove
SCE A3	---	---	3	Variobus	Change Remove
SCE A4	---	---	4	Variobus	Change Remove
SCE A5	---	---	5	Variobus	Change Remove
SCE A6	---	---	6	Variobus	Change Remove
SCE A7	---	---	7	Variobus	Change Remove
SCE A8	---	---	8	Variobus	Change Remove
SCE A9	---	---	9	Variobus	Change Remove
SCE A10	---	---	10	Variobus	Change Remove
Ausgang 1	Haupteingang	Door relay	1	Local	Change Remove
Ausgang 2	Nebeneingang	Door relay	2	Local	Change Remove
Ausgang 3	Personaleingang	Door relay	3	Local	Change Remove
Ausgang 4	---	---	4	Local	Change Remove

Fig. 7: List of outputs

Column name	Description
Name	This column describes the name of the output.
Door name	If the output is assigned to a door, the door name appears here.
Port	Describes the port number of the output.
Location	A distinction is made between two different locations. The location “local” stands for the local outputs. “Vario bus” stands for external outputs.

Table 6: List of outputs: Column description

The two actions “Change” and “Remove” are assigned to each configured output. Using “Change”, the name of the output and the port number can be changed. The action “Remove” removes the output.
However, these actions are subject to a number of restrictions:
- If an output is assigned to a door, this can no longer be changed or removed.
- Local outputs cannot be removed.

A new external output can be created using the action “New”. If no FSM 740-… is found, this option is disabled.

2.3.1.5. Creating an output

Creating new outputs is only possible in conjunction with the FSM 740-…
If no FSM 740-… is found when initializing the TCIP 603-…, this functionality is disabled. By linking an SCE 640-…, a further 8 outputs are provided.
When using the SCE 640-… at the FSM 740-…, the function in the FSM 740-… must be activated.

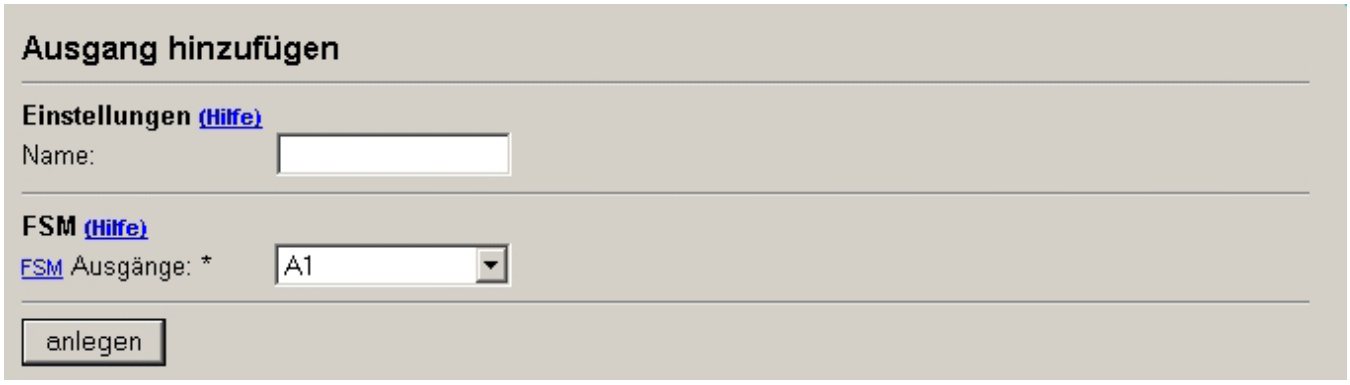


Fig. 8: Creating an output

Field name	Description
Name	Describes the name of the output.
FSM outputs	Defines one of the outputs of the FSM 740-… / SCE 640-…

Table 7: Adding an output: Description of the fields in the dialogue box

This page contains the following action:

Action	Description
Create	This action creates the output.

Table 8: Adding an output: Actions in the dialogue box

2.3.1.6. Changing/removing an output

If local outputs are changed, the section FSM does not appear.

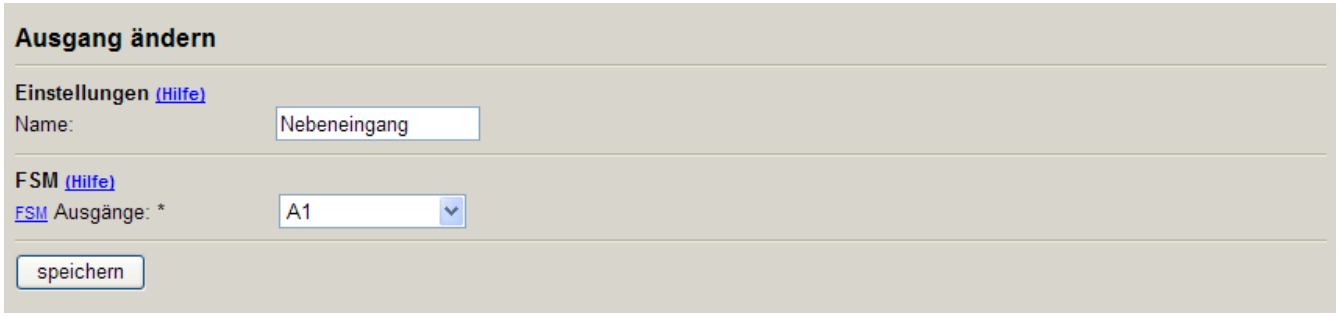


Fig. 9: Changing/removing an output

Field name	Description
Name	Describes the name of the output.
FSM outputs	Defines one of the outputs of the FSM 740-… / SCE 640-…

Table 9: Changing/removing an output: Description of the fields in the dialogue box

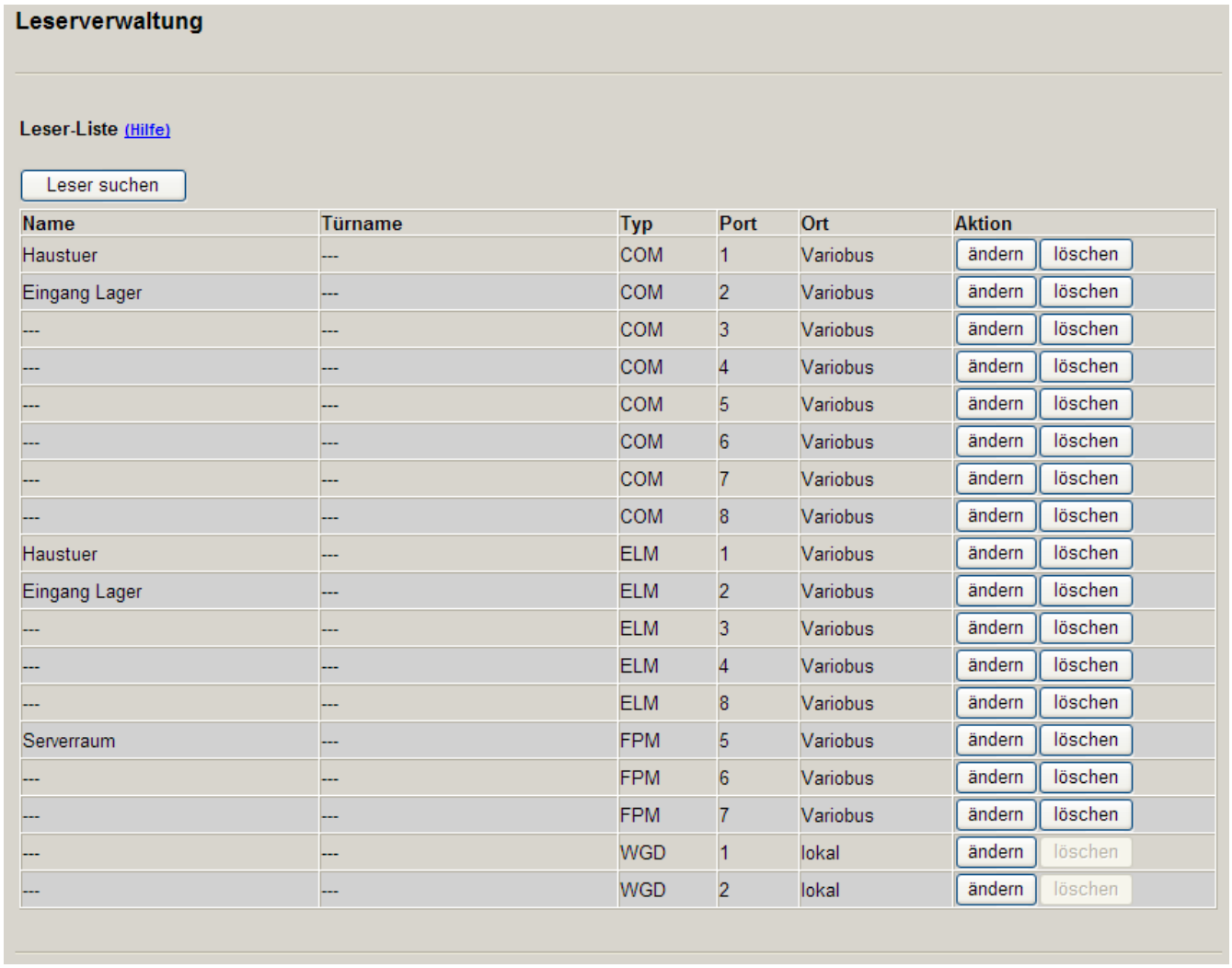
The page contains two actions:

Action	Description
Save/Remove	This action saves or removes the output.

Table 10: Changing/removing an output: Actions in the dialogue box

2.3.1.7. Readers

Selecting the menu point “Hardware/System -> Readers” takes you to the list containing the reading/input modules connected to the Vario bus.



Name	Türname	Typ	Port	Ort	Aktion
Haustuer	---	COM	1	Variobus	ändern löschen
Eingang Lager	---	COM	2	Variobus	ändern löschen
---	---	COM	3	Variobus	ändern löschen
---	---	COM	4	Variobus	ändern löschen
---	---	COM	5	Variobus	ändern löschen
---	---	COM	6	Variobus	ändern löschen
---	---	COM	7	Variobus	ändern löschen
---	---	COM	8	Variobus	ändern löschen
Haustuer	---	ELM	1	Variobus	ändern löschen
Eingang Lager	---	ELM	2	Variobus	ändern löschen
---	---	ELM	3	Variobus	ändern löschen
---	---	ELM	4	Variobus	ändern löschen
---	---	ELM	8	Variobus	ändern löschen
Serverraum	---	FPM	5	Variobus	ändern löschen
---	---	FPM	6	Variobus	ändern löschen
---	---	FPM	7	Variobus	ändern löschen
---	---	WGD	1	lokal	ändern löschen
---	---	WGD	2	lokal	ändern löschen

Fig. 10: List of readers

Find reader function

In the list, all the readers found using the “Find reader” function are displayed.

Column name	Description
Name	This column describes the name of the reader.
Door name	If the reader is assigned to a door, the door name appears here.
Type	Indicates the type of reader. • Code lock module (COM 611-…) • Electronic key reading module (ELM 611-…) • Fingerprint module (FPM 611-…) • Wiegand reader (WGD, when using a reader at this interface)
Port	Here, the device number / address of the read module is displayed. This address is set on the back of each module using a BCD switch.
Location	A distinction is made between two different locations. The location “local” stands for the local readers. “Vario bus” stands for external readers on the Vario bus.

Table 11: Reader management: Column description

Each reader is assigned two actions, “Change” and “Remove”.
However, the action “Remove” is subject to several restrictions:
• If a reader is assigned to a door, this can not be removed.
• Local Wiegand readers WGD cannot be removed.

If a new reader is connected to the bus, this can be found using the “Find reader” command. This is then automatically added to the reader list.

2.3.1.8. Changing/removing readers

Depending on the reader type, the functional scope of this dialogue box differs.

For readers type COM 611-… it is possible to adjust the name to the bleeping and flashing action.

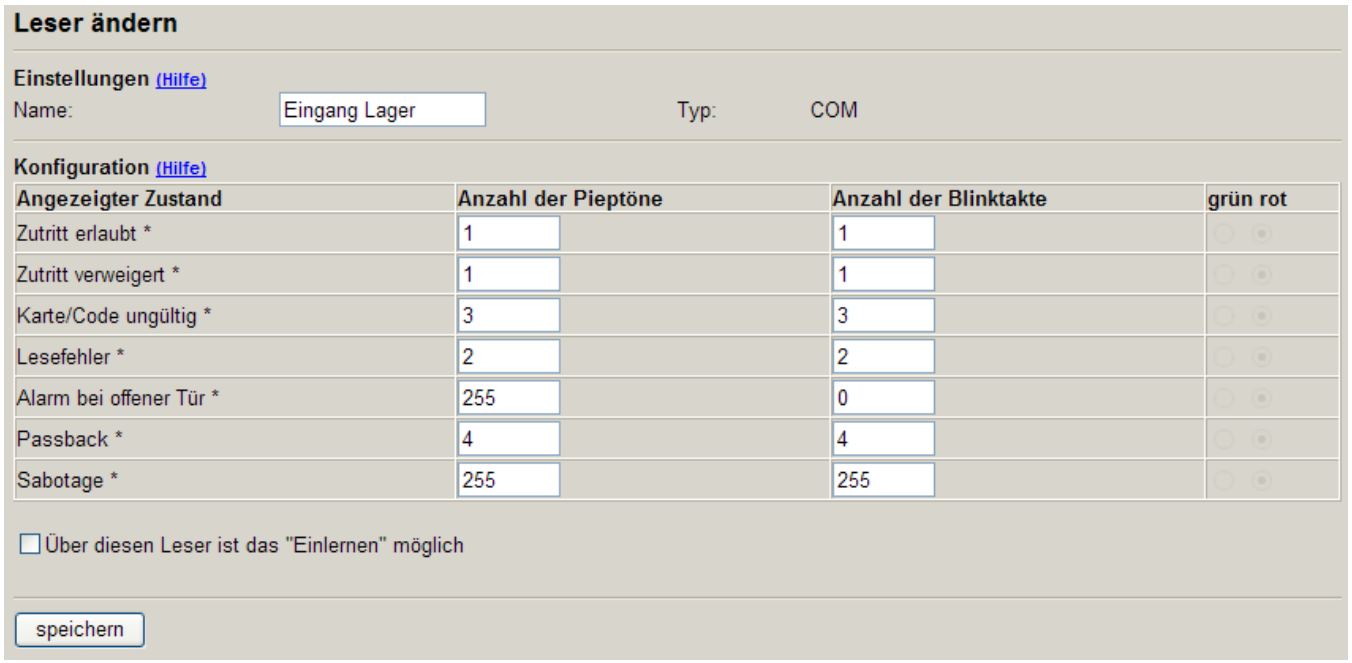


Fig. 11: Changing/removing readers

Readers type ELM 611-… can flash green and red.

The FPM 611-… units do not offer any adjustment facility.
NOTE By performing the additional action “Clear FPM” the fingerprints stored in the FPM 611-… are removed.

Fig. 12: Changing/removing readers (FPM)

Field name	Description
Name	Describes the name of the reader.
Displayed status	A reader can signal different statuses. Using this table, it is possible to configure how the reader should behave in which status. All fields can assume numbers from 0 to 255. The value "0" deactivates the signal, the value "255" sets the signal to continuous status until a different status occurs.
Teach-in is possible using this reader	If this option is enabled, it is possible to carry out a read-in process using this reader.

Table 12: Changing/removing readers: Description of the fields in the dialogue box

The page contains four actions:

Action	Description
Clear FPM	This action is only available in the fingerprint modules (FPM). If this action is activated, all saved fingerprints from this module are deleted.
Change/remove	This action changes or removes the reader.
Synchronize	Where several fingerprint modules are connected, the newly read-in fingerprint can be transferred from one module to all the others.
Reset	This function resets the fingerprint module, at the same time writing the TCIP code into the FPM. However, the fingerprint data is retained.

Table 13: Changing/removing readers: Actions in the dialogue box

2.3.1.9. Doors

Accessing the "Configurations -> Doors" menu brings up a list of all created doors.
A maximum of 8 doors are supported.

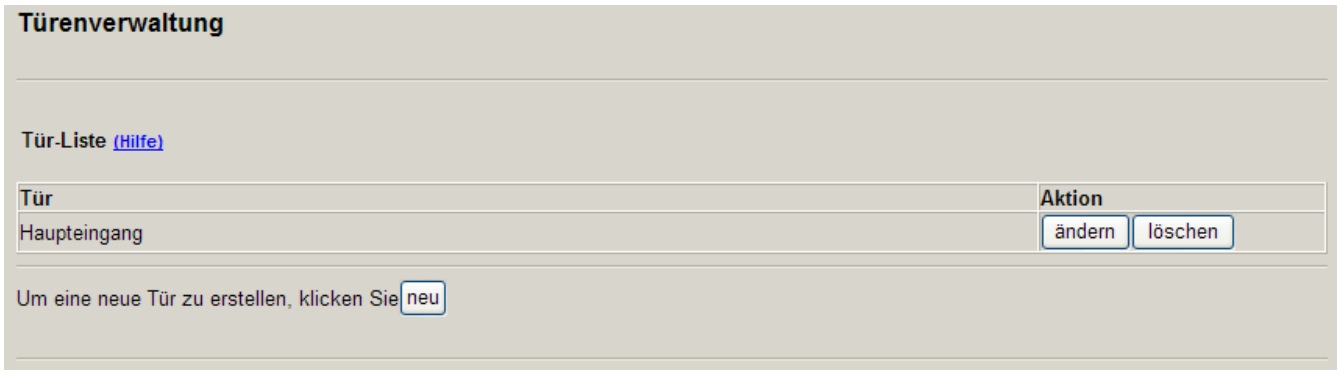


Fig. 13: List of all doors

Column name	Description
Door	This column describes the name of the door.

Table 14: Door management: Column description

Each door is assigned two actions, "Change" and "Remove". If you wish to create a new door, use the "New" function.

2.3.1.10. Creating a door

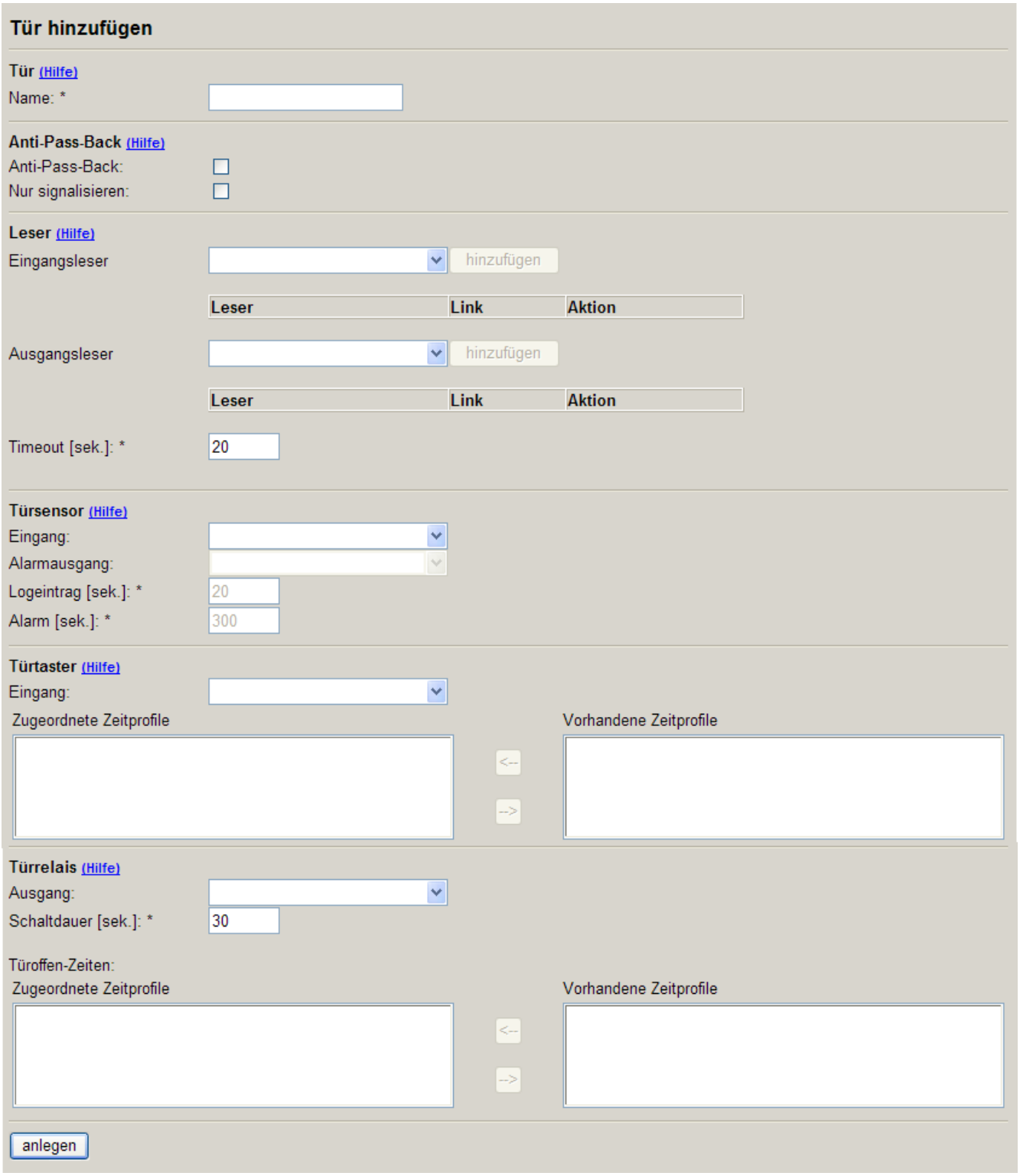


Fig. 14: Creating a door

Each created door depicts a real door. This groups together all the configured devices (inputs, outputs and reader) to a cohesive unit.

Using the anti-passback setting, it is possible to define whether a person may log in several times at a door before having first logged out at an output reader.
If the anti-passback function is enabled, a user can only log in to the input reader of a door if this user does not appear in the attendance list. Consequently it is essential to log out correctly.
If the option "Signal anti-passback" is enabled, the person in an anti-passback situation is admitted through the door, although this generates a signal to the effect that the user in question is already logged in.

Each door can be assigned to a maximum of two input readers and two output readers. These readers are linked by either a logical "AND" or "OR".
If readers are linked by a logical "AND", the period during which a login must be performed at both readers in order to validate the login is specified in the "Timeout time" field. If this time expires before both readers have signalled a valid login, the process must be started again from the beginning.

It is possible to assign a door to a door sensor. This is used to signal the "Door open" and "Door shut" status. If no door sensor has been assigned, every login/logout is evaluated as an entry/exit.

Via the door button, which can be assigned to one door, users have the possibility to actuate the door relay. A time profile must be assigned to the door button which regulates the times at which this button is active. In addition, the door relay can also be actuated via the web user interface.
The door relay is the output which is actuated when the door needs to be unlocked. By means of a switching time, it is possible to determine the period for which the relay should be actuated.
The time profile determines at which times the door relay needs to be permanently actuated.

Field name	**Description**
Name	Indicates the name of the door.
Anti-passback	Determines whether a person may log in to a secured area more than once.
Only signal	If an anti-passback situation arises, if this option is enabled the user is admitted but this status is signalled via the reader.
Input reader	Links a maximum of two readers with the door. These readers are counted as input readers and can be linked by a logical "AND"/"OR".
Output reader	Links a maximum of two readers with the door. These readers are counted as output readers and can be linked by a logical "AND"/"OR". **Note:** For exit readers, no time profiles or access groups apply, as the doors always have to be opened for leaving the building for safety reasons. Specific system configurations have to be reviewed on a case-by-case basis.
Timeout	Determines the time period in which a login process must be completed.
Door sensor input	Determines the input of the door sensor at the TCIP 603-…/FSM 740-…
Door sensor alarm output	The assigned output switches at sabotage or when the time "open door" is exceeded.
Door sensor – log entry	Configures the "Door open" time from which the log entry should be performed.
Door sensor alarm	Configures the "Door open" time from which an alarm should be signalled via the reader.
Door button – input	Determines the input of the door sensor at the TCIP 603-…/FSM 740-…
Door button – time profile	Determines the period in which the door button at the TCIP 603-…/FSM 740-… is enabled.
Door relay – output	Determines the output of the door relay.
Switching duration	Time for which the relay should be switched.
Door release – times	Determines the period during which the door release may be actuated.

Table 15: Creating a door: Description of the fields in the dialogue box

Several actions are assigned to this form, which are described in more detail in the following:

Action	Description
Input reader – add	This action assigns a reader with the selected logic link to the door. A maximum of two readers can be assigned.
Input reader – remove	This action removes the reader from the door again.
Output reader – add	This action assigns a reader with the selected logic link to the door. A maximum of two readers can be assigned.
Output reader – remove	This action removes the reader from the door again.
Door button – "<-"	An "existing time profile" is assigned. Only one time profile can be assigned.
Door button – "->"	An already "assigned time profile" can be removed using this action.
Door relay – "<-"	An "existing time profile" is assigned. Only one time profile can be assigned.
Door relay – "->"	An already "assigned time profile" can be removed using this action.
Create	The door is created and initialized.

Table 16: Creating a door: Actions in the dialogue box

2.3.1.11. Changing/removing a door

Created doors can be changed or removed.

2.3.1.12. Network

Selecting the menu point “Hardware/System -> Network” takes you to a dialogue box in which the network configurations can be carried out. The TCIP 603-… is delivered as standard with the IP address “192.168.0.1” and network dialogue box “255.255.255.0”. In operation, the TCIP 603-… requires a valid IP address within a subnetwork.

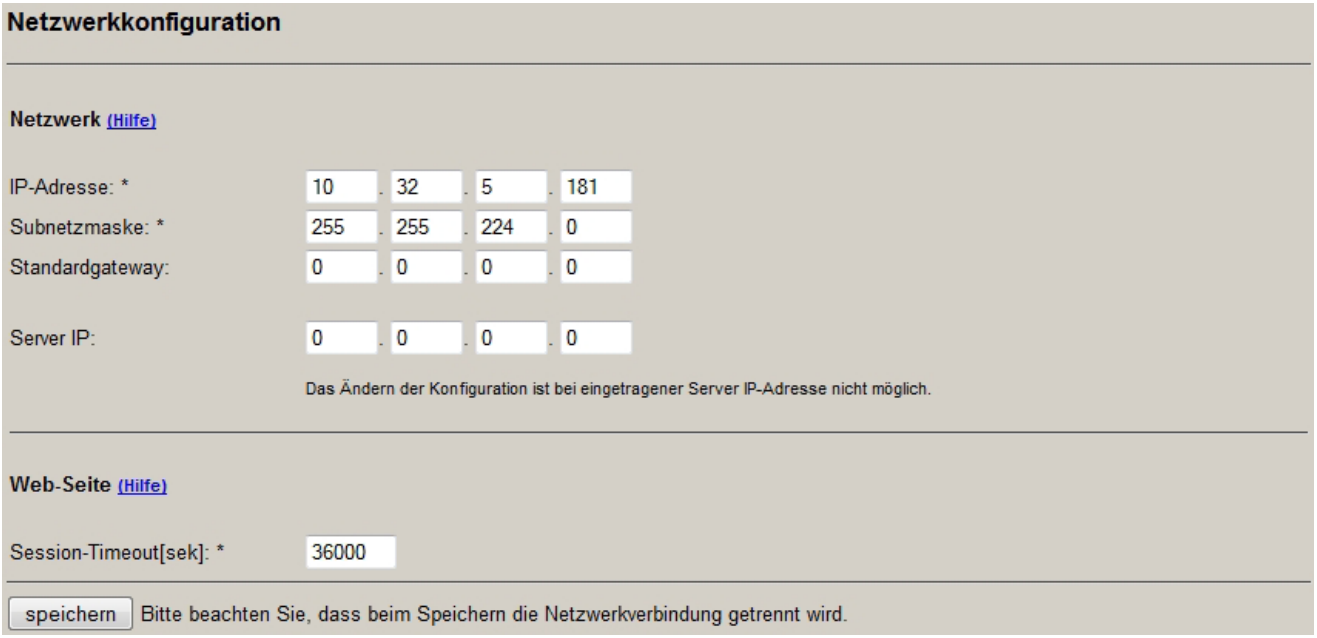


Fig. 15: Network configuration

Field name	Description
IP address	Indicates the IP address of the TCIP 603-…
Subnetwork dialogue box	Indicates the subnetwork dialogue box of the TCIP 603-…
Standard gateway	Indicates the standard gateway of the TCIP 603-…
Server IP	Indicates the IP address of the TCIP SRV 603-… Note: the Configuration menu point is hidden with an entered server IP address.
Session timeout	Using this field it is possible to specify in seconds the period for which a user login remains valid after the last user action. If this time has expired, the user will have to log in again. Note data can be lost after a timeout if it was not previously saved.

Table 17: Network configuration: Description of the fields in the dialogue box

Using the action “Save” the settings are saved and the parameters set. Please note that a change of the IP address or network dialogue box causes initialization of the network interface and the TCIP 603-… Web user interface is briefly not available.

2.3.1.13. System time/clock change

2.3.1.13.1. System time

The dialogue box “System time” is reached using the menu point “Hardware/System -> System time/clock” change.

Using this dialogue box, the time zone UTC and date/time are set or alternatively it is possible to synchronize the time automatically using an NTP server. For this purpose the TCIP 603-… has an SNTP client.

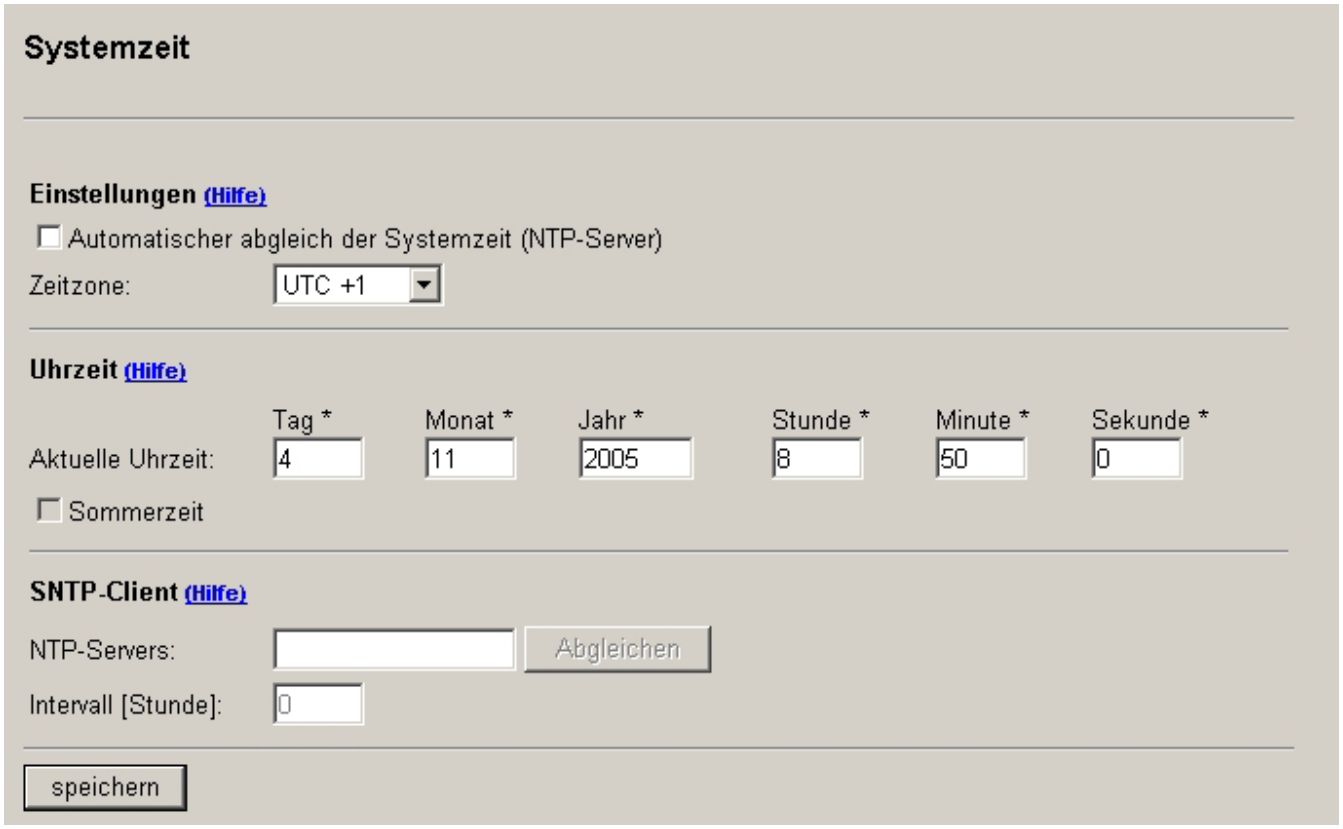


Fig. 16: System time

Field name	Description
Automatic adjustment	If you wish the time of the TCIP 603-… to be synchronized with a system time from an NTP server.
Time zone	Here, the time zone for “Normal time” must be entered (in Germany “UTC +1”). During summertime, UTC +2 must be entered.
Time	The settings for the time comprise both the date and the time.
Summer time	This field is always deactivated. If the field is set, then the TCIP 603-… is operating in summer time, otherwise it is operating in winter time.
NTP server	This field is used to specify the IP address of the NTP server.
Interval	This field describes at which intervals synchronization of the system time should take place with the NTP server. Synchronization is started with saving of the settings.

Table 18: System time: Description of the fields in the dialogue box

This dialogue box contains two actions, “Adjust” and “Save”. Using the “Adjust” action triggers immediate synchronization with the NTP server. Using the action “Save” the settings are adopted.

2.3.1.13.2. Clock change

The menu point "Hardware/System -> System time/Clock change -> Clock change" takes you to a dialogue box in which you can perform the clock changing settings.

If the option "Automatic clock change" is active, the clock change is automatically performed in accordance with the European directive.
If this directive is not applicable, the clock change date and time are entered manually. However, the actual clock change is also carried out automatically in this case.

Note
When entering the time manually, the configuration must be carried out again every year.

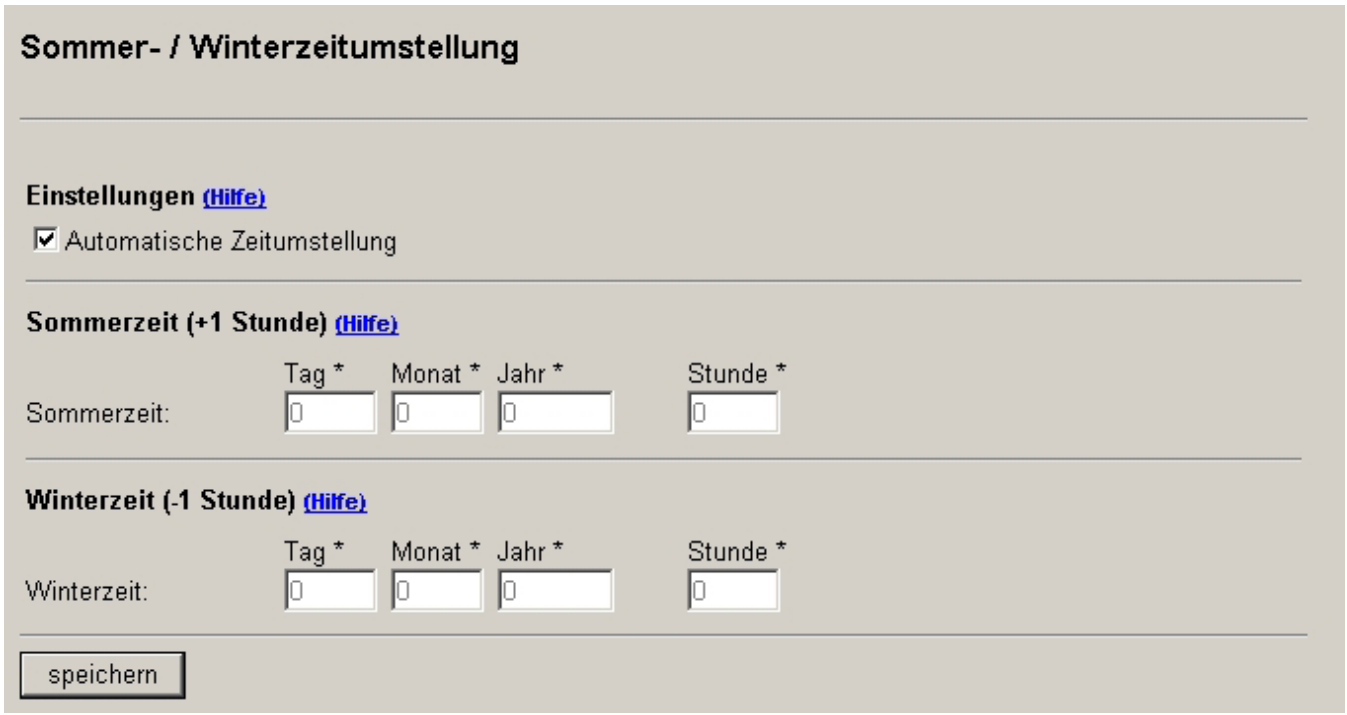


Fig. 17: Summer/winter clock change

Field name	Description
Automatic clock change	If this option is enabled, the clock is changed in accordance with the European directive.
Summer time	Indication of the date and hour at which the clock changes to summer time.
Winter time	Indication of the date and hour at which the clock changes to winter time.

Table 19: Summer/winter clock change: Description of the fields in the dialogue box

Using the action "Save" the settings are adopted.

2.3.2. Configuration

2.3.2.1. Time profiles

Accessing the menu point “Configuration -> Time profiles” takes you to the list of all created time profiles. It is possible to assign a maximum of 20 time profiles.

Fig. 18: List of all time profiles

Column name	Description
Time profile	This column describes the name of the time profile.

Table 20: Time profile management: Column description

Each time profile is assigned two actions, “Change” and “Remove”. If you wish to create a new time profile, use the “New” function. Time profiles which have been assigned to a function cannot be removed.

2.3.2.2. Creating a time profile

For each time profile, the start and end time can be specified per weekday/public holiday. 3 start-end times can be assigned to each day.

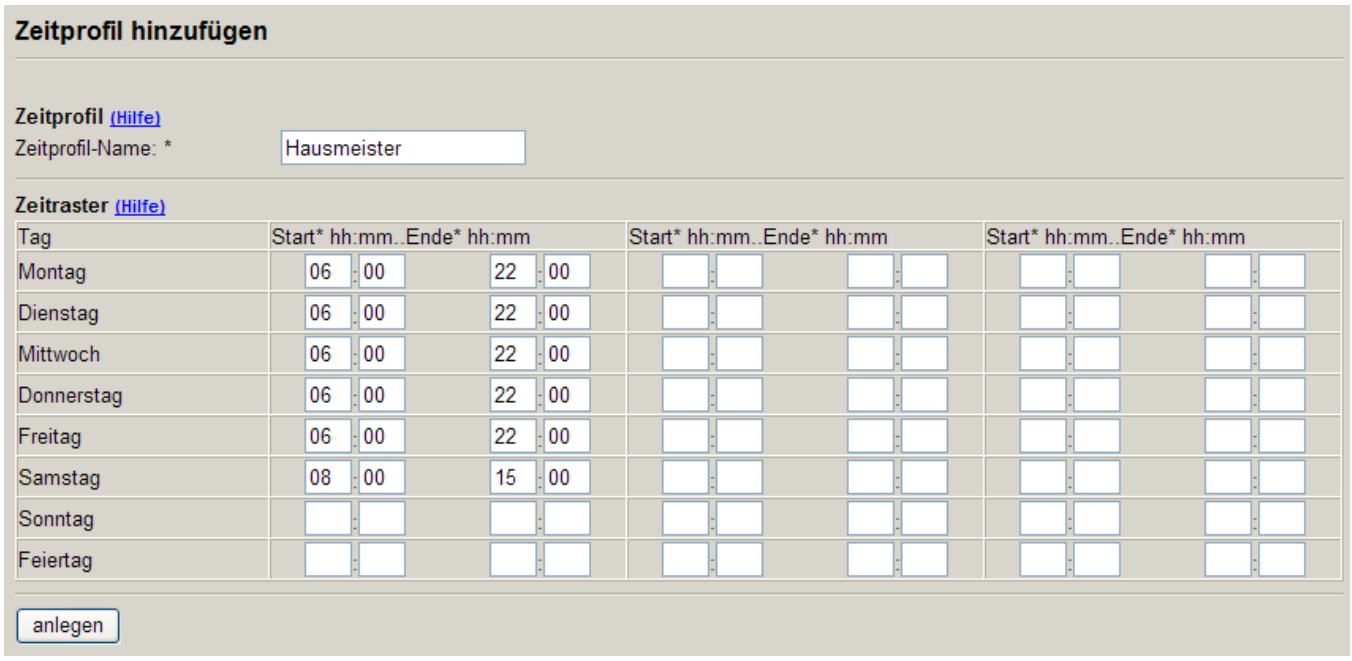


Fig. 19: Creating a time profile

When assigning times, ensure that the start time is before the end time. All fields are mandatory and must be filled in.

Field name	Description
Name	Specifies the name of the time profile.
Time grid	In this table, it is possible to specify a start-end time for Monday – Sunday and the public holidays using the "hour : minute" format (hh:mm). Three different start-end times can be managed per day.

Table 21: Adding a time profile: Description of the fields in the dialogue box

Using the action "Create", the time zone can be saved.

2.3.2.3. Changing/removing the time profile

Created time profiles can be changed or removed.

2.3.2.4. Public holidays/vacation

Accessing the menu point "Configuration -> Public holidays/profiles" takes you to the list of all created public holidays. Up to a maximum of 20 "fixed public holidays" and a maximum of 20 "variable public holidays" can be assigned.

Fig. 20: Defining public holidays

As described under the section Time profiles, it is also possible to set a time profile for public holidays. Using this configuration dialogue box, it is now possible to define days as public holidays.

A distinction is made between “fixed public holidays” and “variable public holidays”. “Fixed public holidays” are public holidays which occur every year on the same date. “Variable public holidays”, in contrast, fall on a different date each year and consequently have to be newly configured every year.

Field name	Description
Date	Indicates the date of the public holiday.
Name	Indicates the name of the public holiday.

Table 22: Public holidays/vacation: Description of the fields in the dialogue box

Several actions are assigned to this form, which are described in more detail in the following:

Action	Description
Save	Saves a “recurring” or “variable” public holiday.
Remove	Removes the public holiday from the list.

Table 23: Public holidays/vacation: Actions in the dialogue box

2.3.2.5. Access groups

Accessing the menu point “Configuration -> Access groups” takes you to a list of all created access groups. A maximum of 40 access groups can be created.

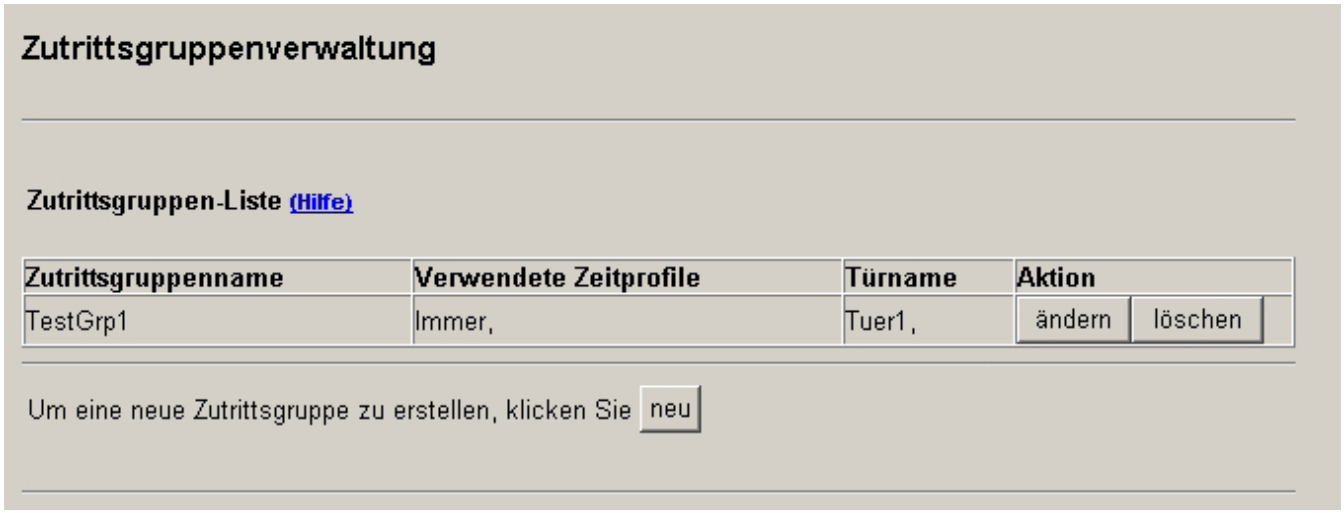


Fig. 21: List of all access groups

Column name	Description
Access group name	This column describes the name of the access group.
Used time profiles	Lists all time profiles assigned to this access group.
Door name	Lists all doors assigned to this access group.

Table 24: Access group management: Column description

Each access group is assigned two actions, “Change” and “Remove”. If you wish to create a new access group, use the “New” function.
Access groups which have been assigned to a function cannot be removed.

2.3.2.6. Creating an access group

By means of the access group it is first of all possible to define the rights of users assigned to this access group. It is also possible to link access groups to a time profile and a door.
The individual options define which menu points a user is able to access. If a certain user should not be entitled to log in at the web user interface, the "Log in via browser" option should not be enabled.

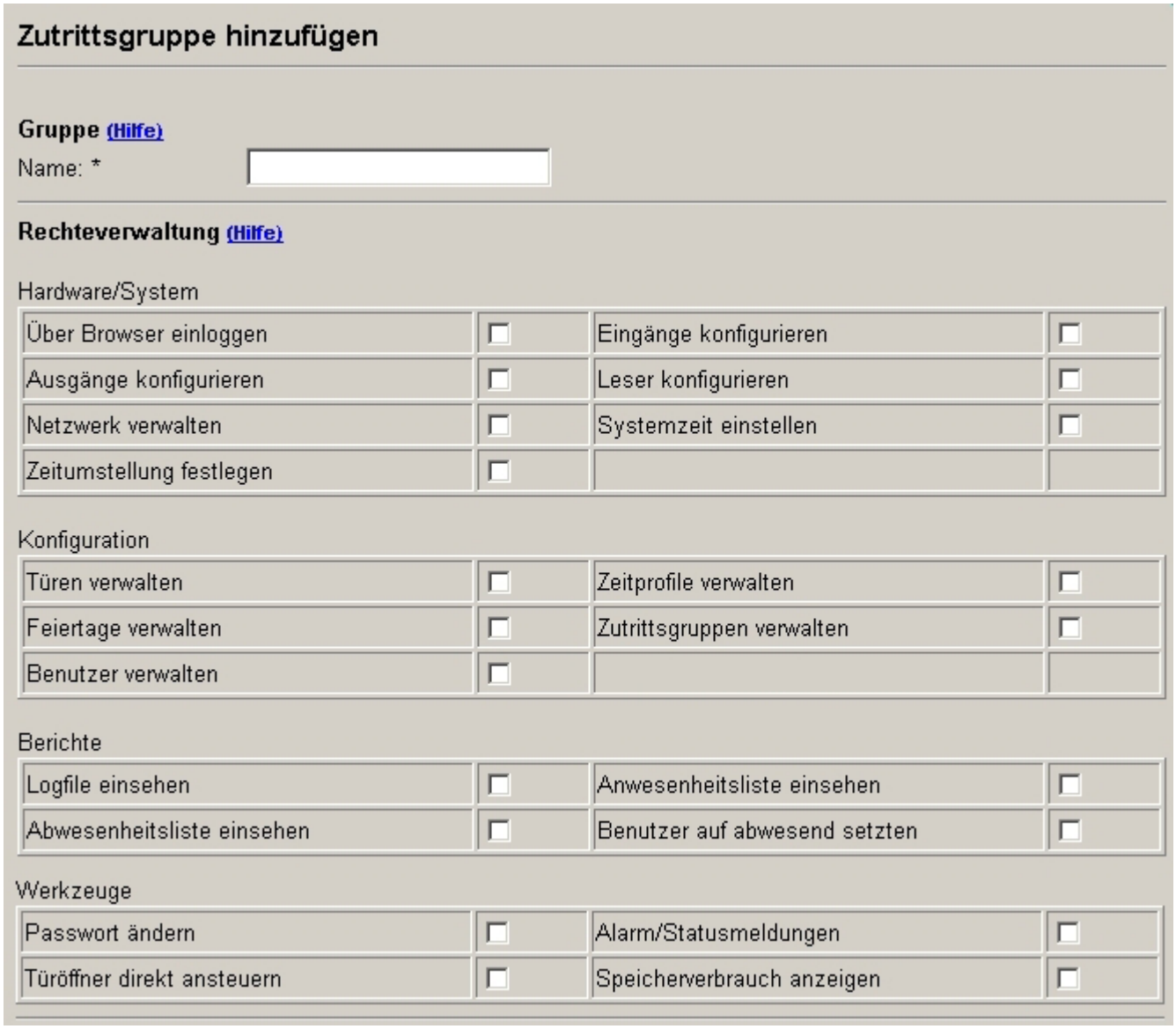


Fig. 22: Add access group (part 1)

In the second part of the access group configuration, time profiles and doors are assigned. A maximum of 3 time profiles and a maximum of 8 doors may be assigned to a user.

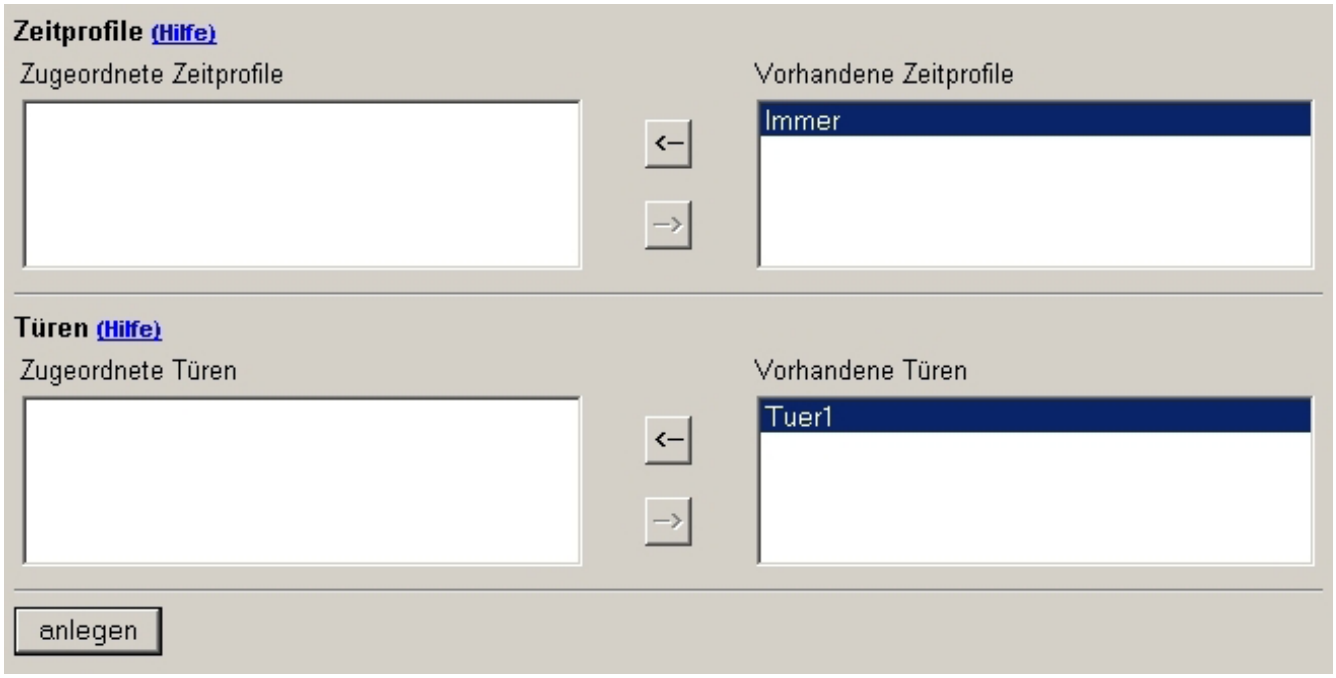


Fig. 23: Add access group (part 2)

Field name	Description
Name	Indicates the name of the access group.
Access rights management – options	Using these options, it is possible to define the various rights at the web user interface. It is not possible to differentiate between “Read only” or “Read-write”.
Assigned time profiles	Lists all time profiles belonging to the access group. It is possible to assign a maximum of 3 time profiles.
Existing time profiles	Lists all configured time profiles.
Assigned doors	Lists all doors assigned to the access group. A maximum of 8 doors can be assigned.
Existing doors	Lists all configured doors.

Table 25: Add access group: Description of the fields in the dialogue box

This dialogue box contains more action fields which are described in the following.

Action	Description
Time profile – “<-”	An “existing time profile” is assigned.
Time profile – “->”	An already “assigned time profile” can be removed using this action.
Doors – “<-”	An “Existing door” is assigned.
Doors – “->”	An already “assigned door” can be removed using this action.
Create	The access group is created.

Table 26: Add access group: Actions in the dialogue box

2.3.2.7. Changing/removing an access group

Created access groups can be changed or removed.

2.3.2.8. Users

Accessing the menu point “Configuration -> Users” takes you to a list of all created users. A maximum of 500 users can be created.

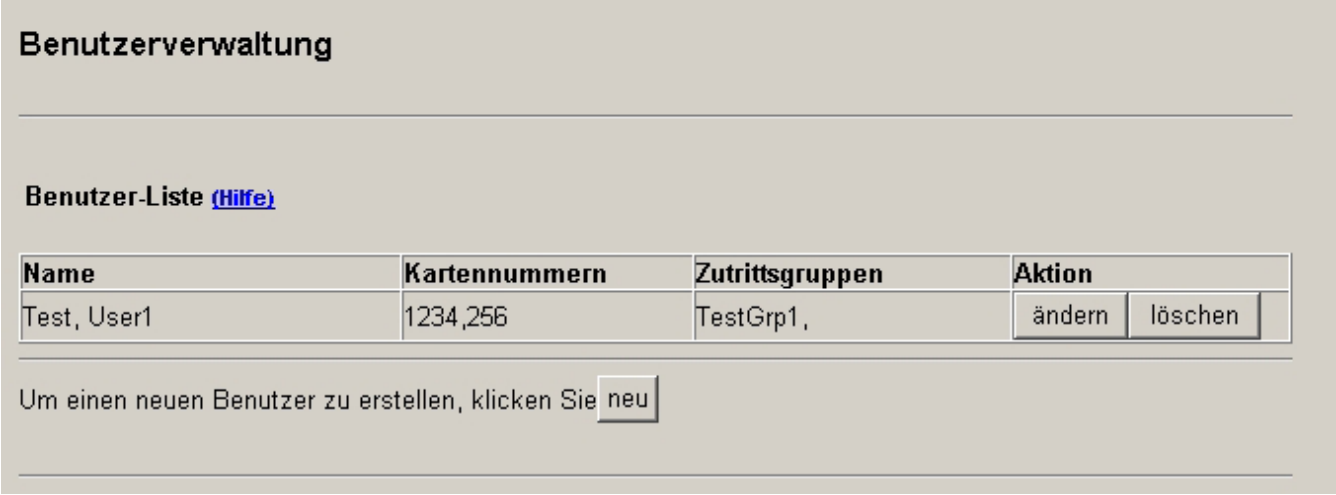


Fig. 24: List of all users

Column name	Description
Name	The user name (surname, first name).
Card number	List of all user identification characteristics.
Access groups	List of all assigned access groups

Table 27: User management: Column description

Each user is assigned two actions, “Change” and “Remove”. If you wish to create a new user, use the “New” function.

2.3.2.9. Creating a user

The “User” dialogue box is used for entering users by name. The surname and first name may not contain any special symbols except “space” and “hyphen”.
Here, all the characteristics and rights are entered which you wish to be assigned to this user from the viewpoint of access control.
The surname, first name and personnel number are requested for the user in question. In addition, the person can be assigned a total of 4 characteristics. Characteristics are card, code, fingerprint and Wiegand reader. These characteristics have a validity period.
If the respective user has to log in at the web user interface in order to make evaluations or changes, a profile name (login name) and a password must be issued.

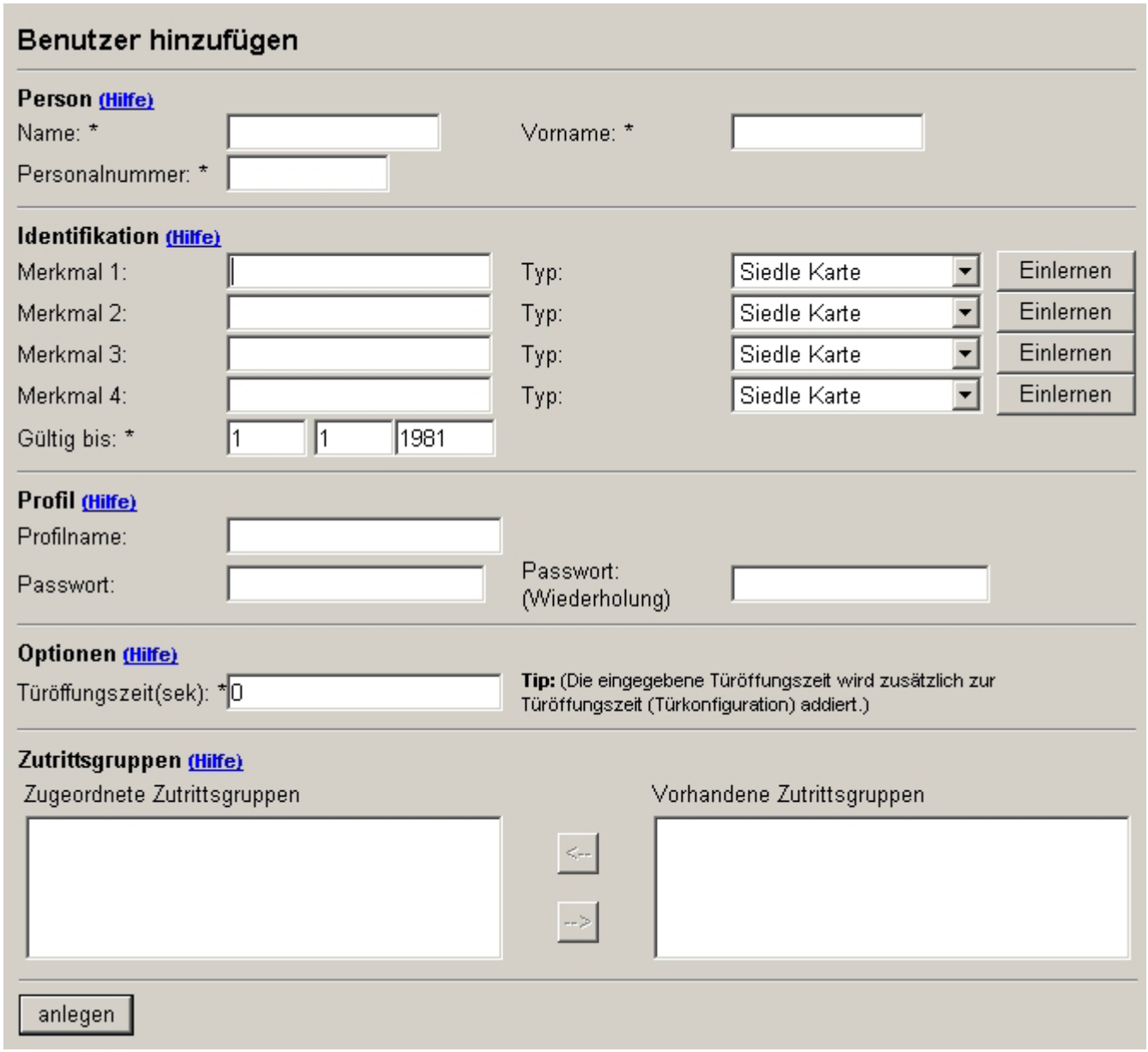


Fig. 25: Adding a user

Using the door release time, an additional relay switching period in seconds is stored for this user. If this user logs in, the door relay switches for the period set for this door (door relay – switching time) plus the door release time for the user. In order to assign the user rights to the web user interface and the door, the user is also assigned to an access group. Up to 3 access groups can be assigned.

Field name	Description
Name	Specifies the name of the user.
First name	Specifies the first name of the user.
Personnel number	Entry of the user's personnel number
Characteristics 1-4	Describes the identification characteristics 1-4
Type	Describes the type of characteristic 1-4
Valid until	Using this date, it is possible to define the validity of the characteristic.
Profile name	The profile name describes the login name on the web user interface.
Password	The password for logging into the web user interface
Door release time	Using this time, an additional door relay actuation time can be specified.
Access groups	By means of the assigned access groups, the rights of the user are defined.

Table 28: Adding a user: Description of the fields in the dialogue box

This dialogue box contains more action fields which are described in the following.

Action	Description
Teach-in	This action is used to start a teach-in process for the characteristic via one of the readers (for more details, see also the next point).
Access group – "<-"	An "Existing access group" is assigned to the user.
Access group – "->"	An already "assigned access group" can be removed using this action.
Create	The user is created.

Table 29: Adding a user: Actions in the dialogue box

2.3.2.10. Identification teach-in

The teach-in process is started, when the action "Teach-in" is executed for one of the characteristics.

1 Click on "Teach-In" for one og the characteristics.
A new window is opened in which a list is displayed showing all readers which are enabled for teach-in (Hardware/system – Readers). A reader may be selected from this list. The teach-in process is started with "Select".

2 Select reader and click on "Select".

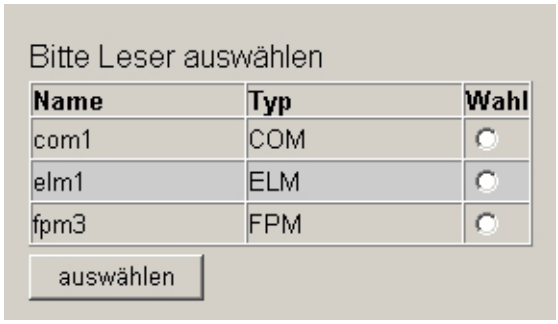


Fig. 26: Selecting reader for the teach-in process

Once the teach-in process is started, a window appears with the following content:

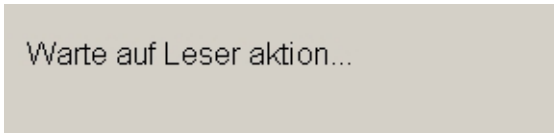


Fig. 27: Teach-in process

A card, code or fingerprint now has to be programmed.

3 Program card, code or fingerprint.
This window closes immediately when a characteristic has been received from the selected reader. If no characteristic is received from the reader, the window closes after around 1 minute (with the FPM after 15 seconds).

If a FPM is used, the operator must start the synchronization routine in the Menue "Readers Hardware / System" after the teach-in process of all FPMs. The FPM which has just been programmed serves as a basis for this (master). Synchronization is identified by this message:

Fig. 28: Synchronization of FPMs

If the teach-in process has been started with characteristic 1 and a fingerprint has been entered in this way, this part of the user configuration looks like this:

Fig. 29: Fingerprint teach-in performed via an FPM

Using the "Characteristic" option, it is now possible to determine which finger has been entered by teach-in.

2.3.2.11. Changing/removing a user

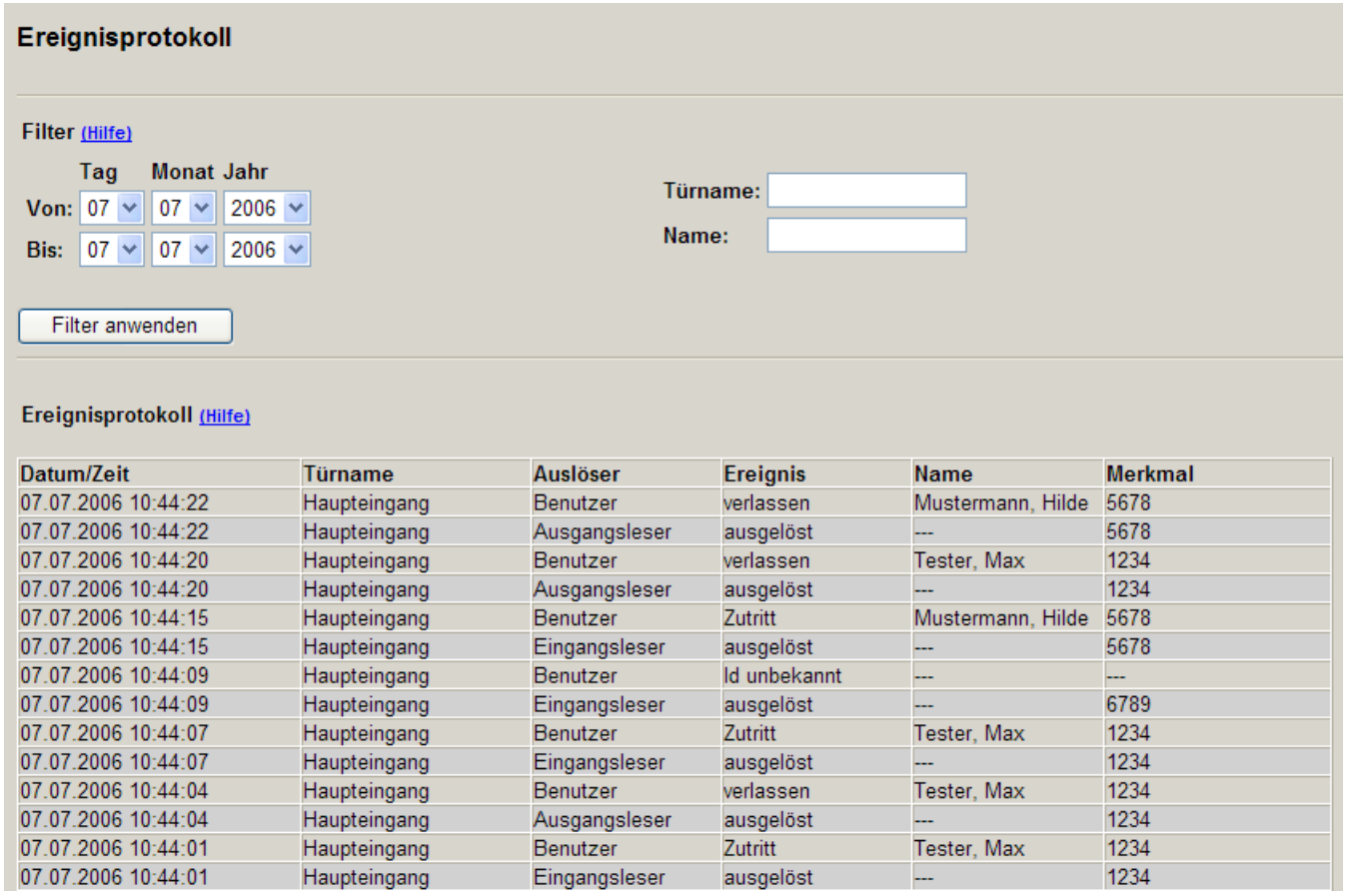
A description of the individual functions is provided under "Create access group" .

2.3.3. Reports

All logs are displayed in the section “Reports”.

2.3.3.1. Event log

The event log is found under the Reports menu point.
In the event log, all actions/reactions or statuses are saved. These can be displayed using this dialogue box. The event log is able to hold a maximum of 1000 entries. Once the 1000th entry is reached, the 1st entry is overwritten.



Datum/Zeit	Türname	Auslöser	Ereignis	Name	Merkmal
07.07.2006 10:44:22	Haupteingang	Benutzer	verlassen	Mustermann, Hilde	5678
07.07.2006 10:44:22	Haupteingang	Ausgangsleser	ausgelöst	---	5678
07.07.2006 10:44:20	Haupteingang	Benutzer	verlassen	Tester, Max	1234
07.07.2006 10:44:20	Haupteingang	Ausgangsleser	ausgelöst	---	1234
07.07.2006 10:44:15	Haupteingang	Benutzer	Zutritt	Mustermann, Hilde	5678
07.07.2006 10:44:15	Haupteingang	Eingangsleser	ausgelöst	---	5678
07.07.2006 10:44:09	Haupteingang	Benutzer	Id unbekannt	---	---
07.07.2006 10:44:09	Haupteingang	Eingangsleser	ausgelöst	---	6789
07.07.2006 10:44:07	Haupteingang	Benutzer	Zutritt	Tester, Max	1234
07.07.2006 10:44:07	Haupteingang	Eingangsleser	ausgelöst	---	1234
07.07.2006 10:44:04	Haupteingang	Benutzer	verlassen	Tester, Max	1234
07.07.2006 10:44:04	Haupteingang	Ausgangsleser	ausgelöst	---	1234
07.07.2006 10:44:01	Haupteingang	Benutzer	Zutritt	Tester, Max	1234
07.07.2006 10:44:01	Haupteingang	Eingangsleser	ausgelöst	---	1234

Fig. 30: Event log

In order to simplify the search in the event log it can be filtered according to the date, door name and user name.
When searching according to first name and surname, the following notation must be used -> Surname_First name

Column name	Description
Date/Time	The time at which the event took place.
Door name	The name of the door to which this event belongs or “---” if the event is not assigned to any door.
Trigger	Name of the trigger.
Event	Indicates the event which has been triggered.
Name/characteristic	Display of the name and the assigned characteristic

Table 30: Event log: Column description

2.3.3.2. Attendance list

The attendance list is located under “Reports -> Attendance list”. In the attendance list, all persons present are listed.

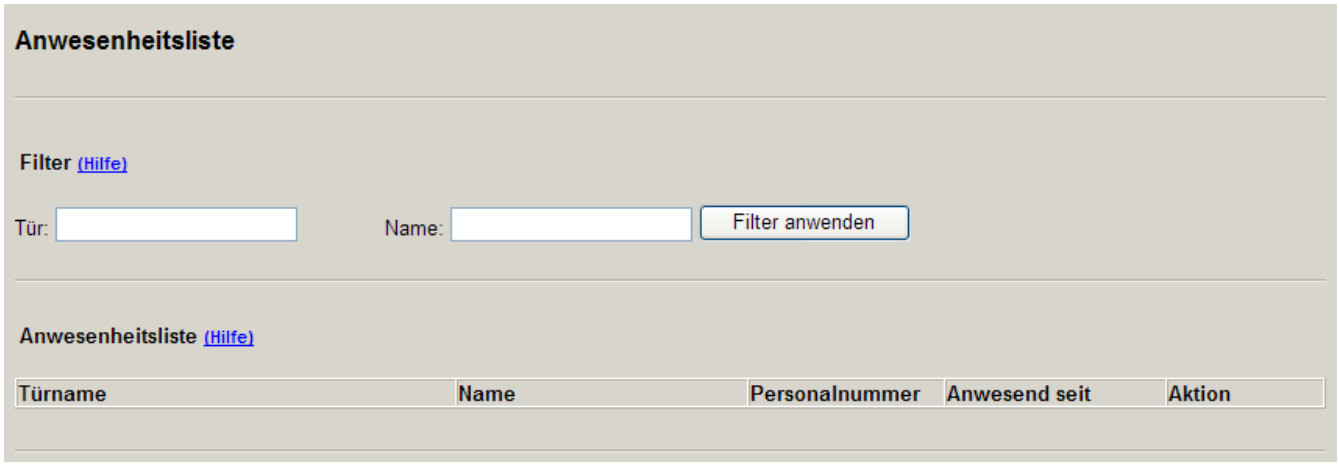


Fig. 31: Attendance list

The attendance list is filtered according to door and user name.

Column name	Description
Door name	Name of the door at which the user has logged in.
Name	Name of the user (Surname, first name)
Personnel number	The personnel number of the user
Present since	Indicates the date and time at which the user logged in.

Table 31: Attendance list: Column description

Using the action “Remove”, a user is set to absent.

2.3.3.3. Absentee list

The absentee list is located under “Reports -> Absentee list”. The absentee list is the reverse of the attendance list.

Fig. 32: Absentee list

Entries in the absentee list are filtered by name.

Column name	Description
Name	Name of the user (Surname, first name)
Personnel number	The personnel number of the user

Table 32: Absentee list: Column description

2.3.4. Tools

2.3.4.1. Changing the password

This dialogue box is reached via "Tools -> Change password". This dialogue box permits the currently logged-in user to change their password.

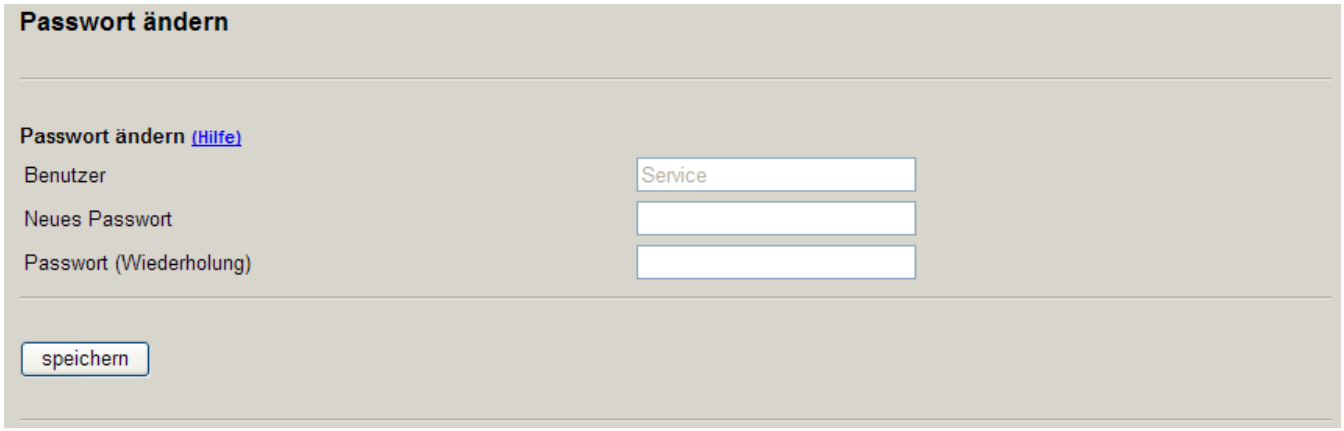


Fig. 33: Change password

Field name	Description
User	Name of the user (Surname, first name)
New password	Input of the new password

Table 33: Changing the password of the fields in the dialogue box

2.3.4.2. Alarms/status messages

This dialogue box is located under "Tools -> Alarms/status messages". It indicates the "live" status of the doors.

Fig. 34: Alarms/status messages

Column name	Description
Door	Name of the door.
Door status	Indicates the status (open/closed)
Sabotage reader	(currently not in use) Green LED means: No sabotage at the reader Read LED means: Sabotage at the reader
Sabotage door	Green LED means: No sabotage at the door Read LED means: Sabotage at the reader (the door has been opened without a previous login/logout)
Alarm	Green LED means: No alarm has occurred Read LED means: Alarm at this door (the door is open too long)

Table 34: Alarms/status messages: Column description

If for instance sabotage takes place at "Door1", the entry is as follows:

Fig. 35: Alarms/status messages: Sabotage at the door

2.3.4.3. Trigger door release directly

In order to trigger a door release directly, change to the menu "Tools -> Trigger door release directly".

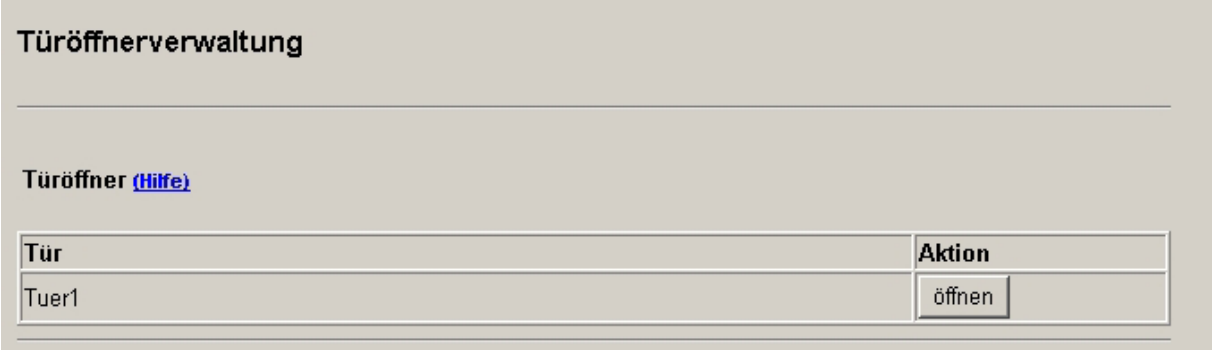


Fig. 36: Trigger door release directly

This page offers a list of all configured doors. Using the action "Open" the door release is directly triggered.

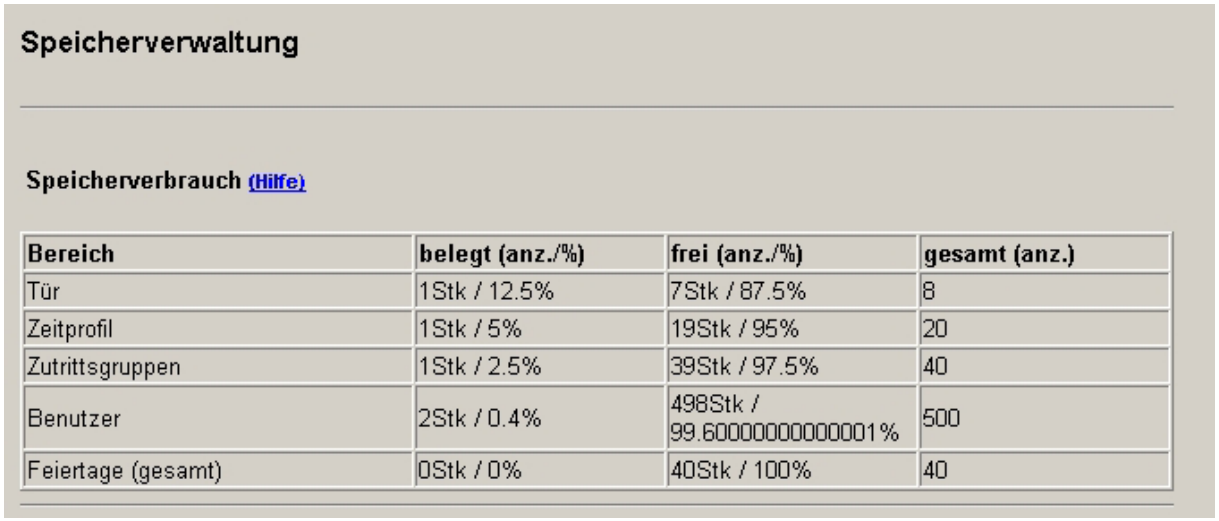
The "door button" frame under the menu provides a shortcut.

Fig. 37: Open door

Here, a door must e selected. This is then opened via the arrow.

2.3.4.4. Memory used

Information on the used memory capacity on the TCIP 603-… is provided by the dialogue box “Tools -> Memory used”.



Speicherverwaltung

Speicherverbrauch (Hilfe)

Bereich	belegt (anz./%)	frei (anz./%)	gesamt (anz.)
Tür	1Stk / 12.5%	7Stk / 87.5%	8
Zeitprofil	1Stk / 5%	19Stk / 95%	20
Zutrittsgruppen	1Stk / 2.5%	39Stk / 97.5%	40
Benutzer	2Stk / 0.4%	498Stk / 99.60000000000001%	500
Feiertage (gesamt)	0Stk / 0%	40Stk / 100%	40

Fig. 38: Memory used

The table describes the amount of memory capacity used on the TCIP 603-… for the individual areas both in piece number terms and as a percentage.

3. Instructions

3.1. Doors

These instructions describe the process used for "Creating a door". Starting with the inputs through to final set-up of the door.

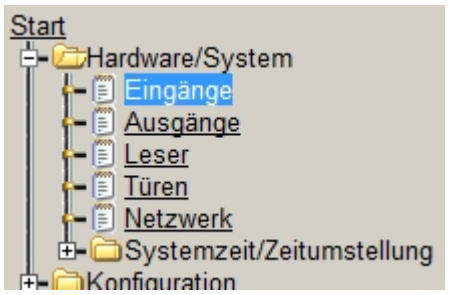
3.1.1. Complete set-up of a door

3.1.1.1. Inputs

The following inputs should exist:

Input	Name	Port	Description
Door sensor, side entrance	Secondary input TS	1/local	Door sensor of the side entrance
Door button side entrance	Secondary input TT	2/local	Door button to open the side entrance.

Table 35: Door set-up – Inputs



In order to manage the inputs of the TCIP 603-…/FSM 740-… the point "Inputs" must be selected using the menu.
There are 5 local inputs listed in the "Inputs" dialogue. Using the "Change" action, the change dialogue box for the relevant input is accessed.

Using this change dialogue, the name of the input can be changed.

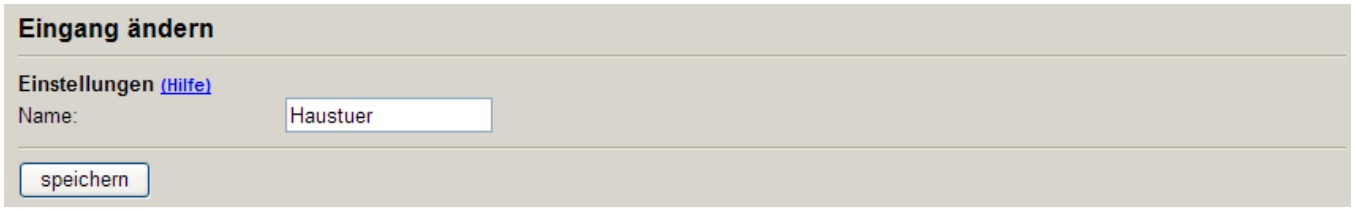


Fig. 39: Door set-up – Changing an input

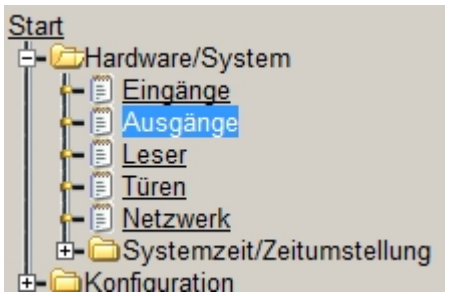
The change is saved by pressing "Save".

3.1.1.2. Outputs at the TCIP 603-…, FSM 740-…, SCE 640-…

In order to open the door, an output is required.

Output	Name	Port	Description
Secondary input	Secondary input	1/local	Door release actuation for the side entrance

Table 36: Door set-up – outputs



In order to manage the outputs, select the "Outputs" menu point.
In the "Outputs" dialogue box, 4 local outputs are listed. If you wish to change one of these outputs, the action "Change" must be executed for the relevant output.

The change dialogue offers the facility to change the name of the output.

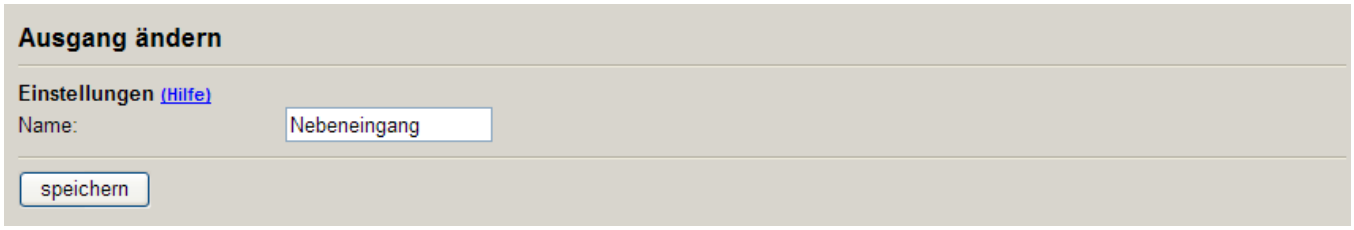


Fig. 40: Door set-up – Changing an output

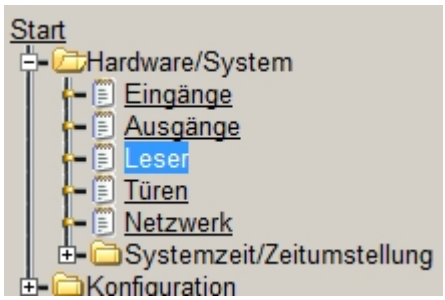
Pressing "Save" saves the change at the output.

3.1.1.3. Readers

For the side entrance, a COM 611-… and an ELM 611-… are used as input readers. These must be actuated one after the other to open the door. An additional ELM 611-… is used as an output reader.

Readers	Name	Port/Type	Description
Input reader 1	Secondary input E1	1/COM	Input reader for the side entrance
Input reader 2	Secondary input E2	1/ELM	Input reader for the side entrance
Output reader 3	Secondary input A1	2/ELM	Output reader for the side entrance
Teach-in reader	Teach-in reader	3/ELM	Teach-in reader (activate teach-in)

Table 37: Door set-up – readers



In order to manage the readers, select the "Readers" menu point.
In the "Readers" dialogue, all readers found on the bus are listed. If no readers are yet listed or if new readers are connected to the bus, these can be found using the "Find readers" action.

If you wish to change one of these readers, the action "Change" must be executed for the relevant reader.

Using the change dialogue box, it is possible to carry out various settings depending on the reader type.

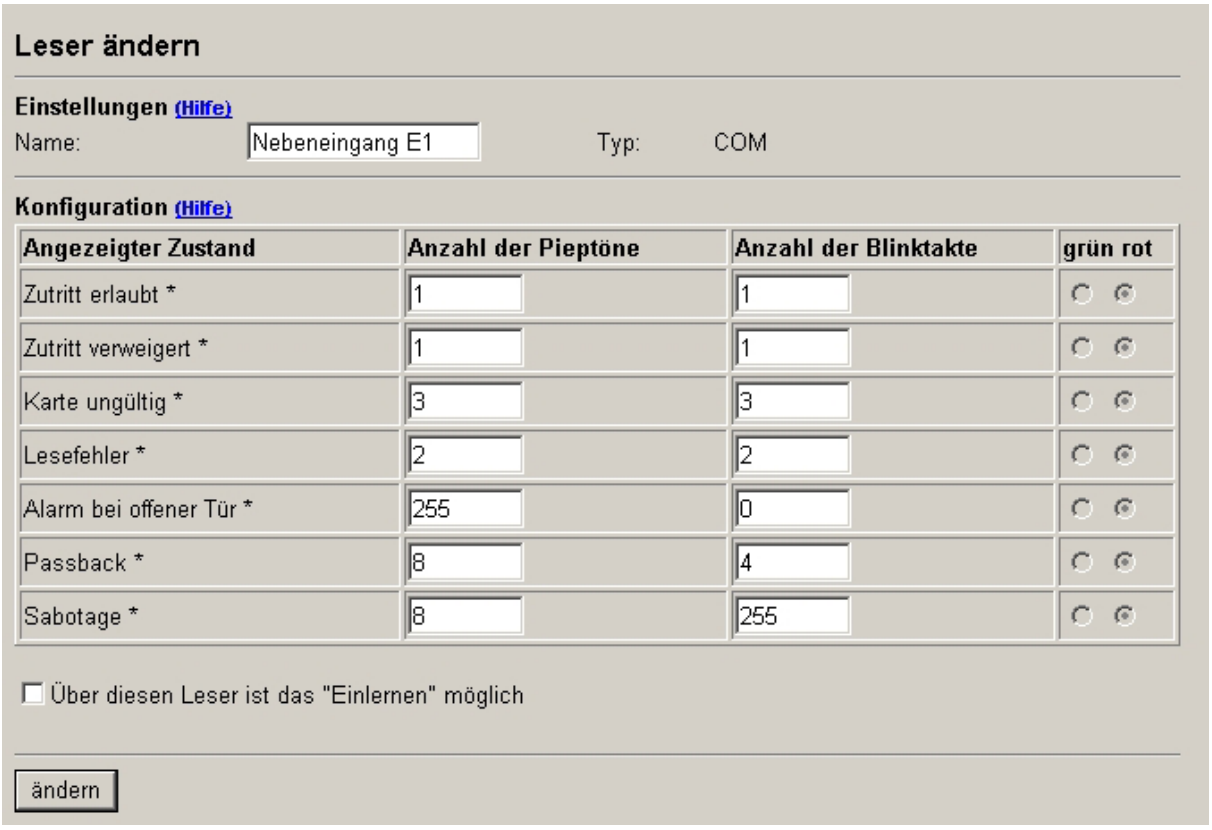


Fig. 41: Door set-up – Changing an reader

3.1.1.4. Time profile

The side entrance should be capable of being opened via a door button. A time profile must be assigned to the door button. Within the specified times, the door can be opened using the door button.

Time profile	Description
Secretarial department	Work hours in the secretarial department (is used for the door button and access groups)

Table 38: Door set-up – Time profile

In order to manage the time profiles, select the “Time profiles” menu point.
All the configured time profiles are listed in the “Time profiles” dialogue box. To generate a new time profile, the action “New” must be executed.

The dialogue box for generating a new time profile allows you to determine the name and time periods of the time profile.

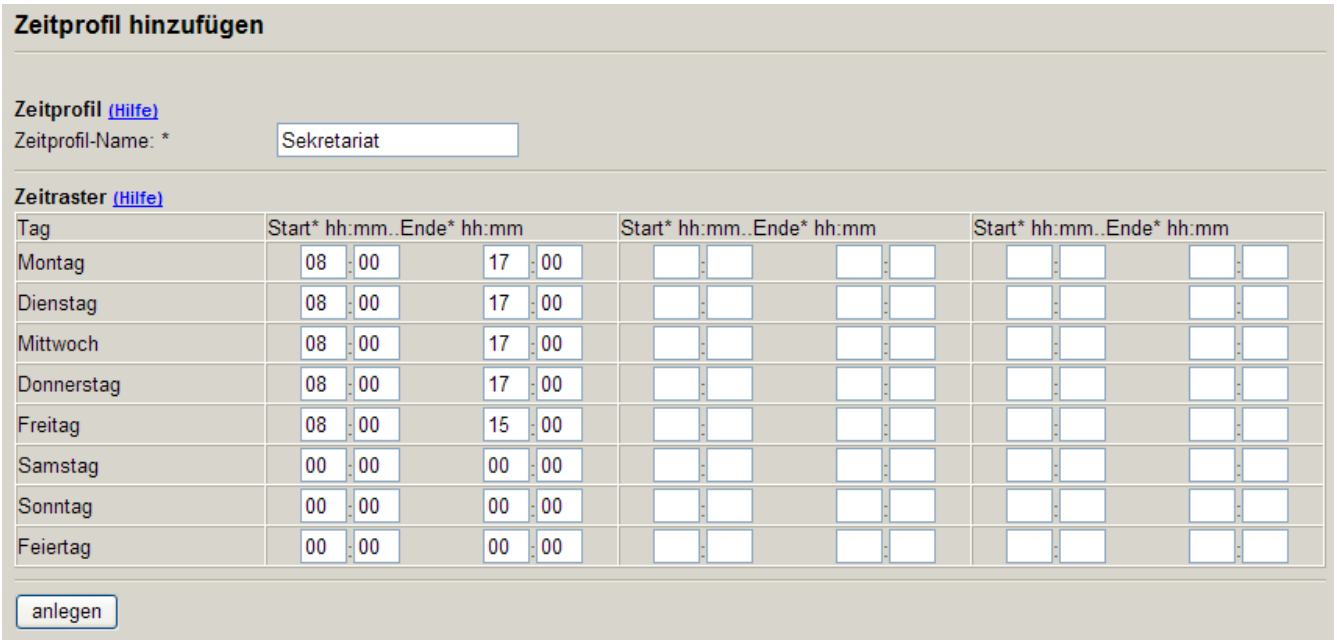


Fig. 42: Door set-up – Add time profile

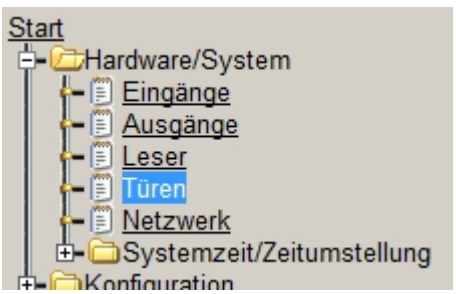
If this time profile is assigned to the door button, the door can only be opened using the door button from Monday to Thursday from 8 a.m. to 5 p.m. and from 8 a.m. to 3 p.m. on Friday.

3.1.1.5. Door

The door configuration groups together all components (inputs, outputs, readers). The "side entrance" is just such a door. The door should have this configuration.

Option	Description
Door name	Side entrance
Readers	**Input reader** • Side entrance I1 (AND) • Side entrance I2 (AND) **Output reader:** • Secondary input O1
Inputs	**Door sensor:** • Side entrance TS **Door button:** • Side entrance TT (with time profile: "Secretarial department)"
Outputs	**Relay:** Side entrance

Table 39: Door set-up – Door



In order to manage the doors, select "Doors" from the menu.
All the configured doors are listed in the "Doors" dialogue box. If you want to create a new door the action "New" must be performed.

The dialogue box links all the components with the door and assigns certain settings to the door.

Fig. 43: Door set-up – Add door 1

The anti-passback option is activated to ensure that no-one is able to log in twice. A user must always log in and out again before access will be afforded again. The anti-passback option only works with defined entrance and exit readers of a door. A stored output reader is not controlled by a time profile.

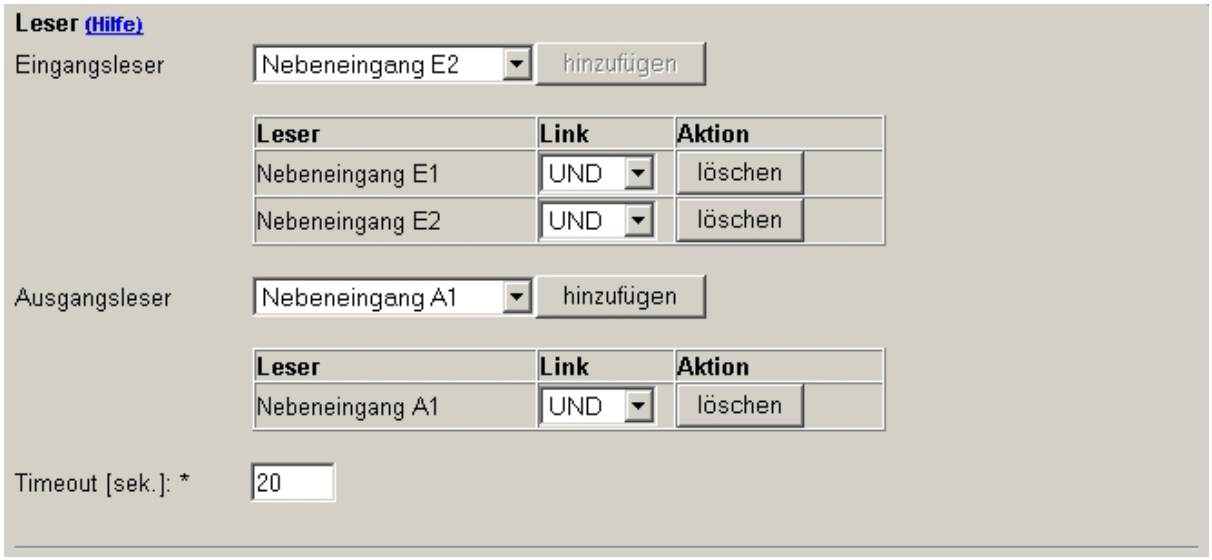


Fig. 44: Door set-up – Add door 2

Two input readers have been assigned. Both readers are linked by a logical AND. This means that a successful login process by the same user must be registered at both readers within the specified time period (timeout).

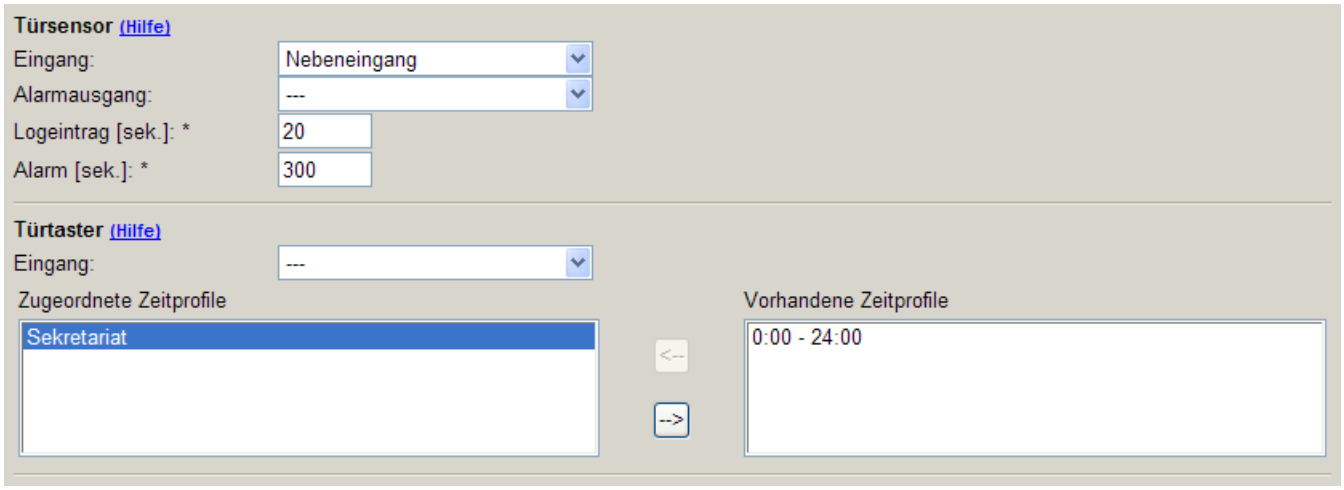


Fig. 45: Door set-up – Add door 3

Using the "Log entry" time level of the sensor, it is possible to define from which time during which the door remains open following a successful login an entry should appear in the event log. The second time "Alarm" initiates a signal at the reader (see reader configuration): "Alarm with door open").

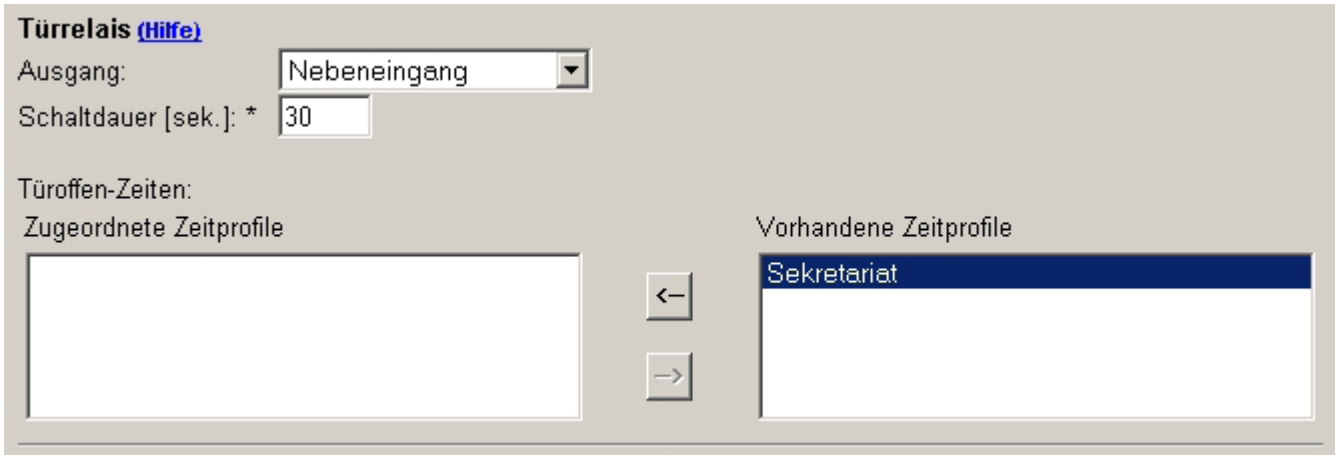


Fig. 46: Door set-up – Add door 4

The setting "Switching duration" indicates the period for which the output should be "Active". If a time profile is assigned to the door relay, this output is always active between the respective start and end times of the time profile. This function would make sense for a main entrance.

Using the action "Create", the door configuration can be saved.

3.1.2. End

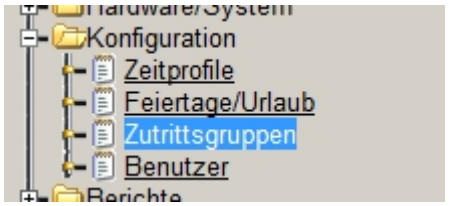
The door is now configured. The next section describes how to configure a user.
NOTE: For exit readers, no time profiles or access groups apply, as the doors always have to be opened for leaving the building for safety reasons. Specific system configurations have to be reviewed on a case-by-case basis.

3.2. Users
3.2.1. Complete create user process
3.2.1.1. Access groups

You require the employees of the secretarial department to be able to use the side entrance. However, they should not be permitted to log onto the web user interface.

Access group	Description
Secretarial department	This group is intended solely for the side entrance and the secretarial department. You wish to restrict access to working hours.

Table 40: User set-up – Access group



In order to manage the access groups, select “Access groups” from the menu. All the configured access groups are listed in the “Access groups” dialogue box. If you want to create an Access group, the action “New” must be performed.

The set-up dialogue box offers the possibility to enter the name, rights and assignment to up to 3 time profiles and up to 8 doors.

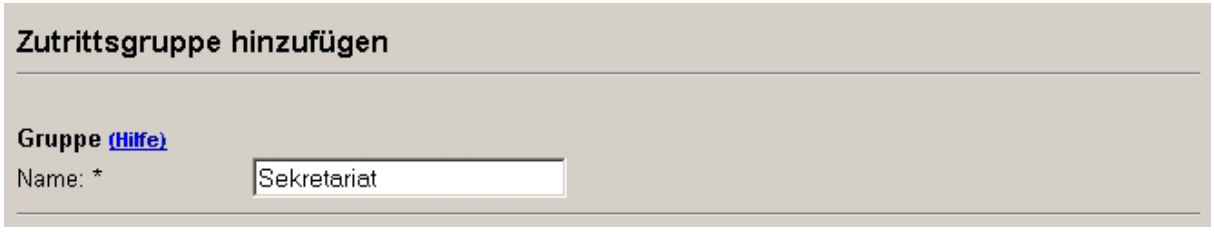


Fig. 47: User set-up – Create access group 1

The users who belong to this access group are not permitted to access the web user interface. For this reason, no rights are set.

Fig. 48: User set-up – Create access group 2

Using this time profile, you wish to be able to regulate that users assigned to the times specified in the "Secretarial department" time profile may enter through the side entrance.

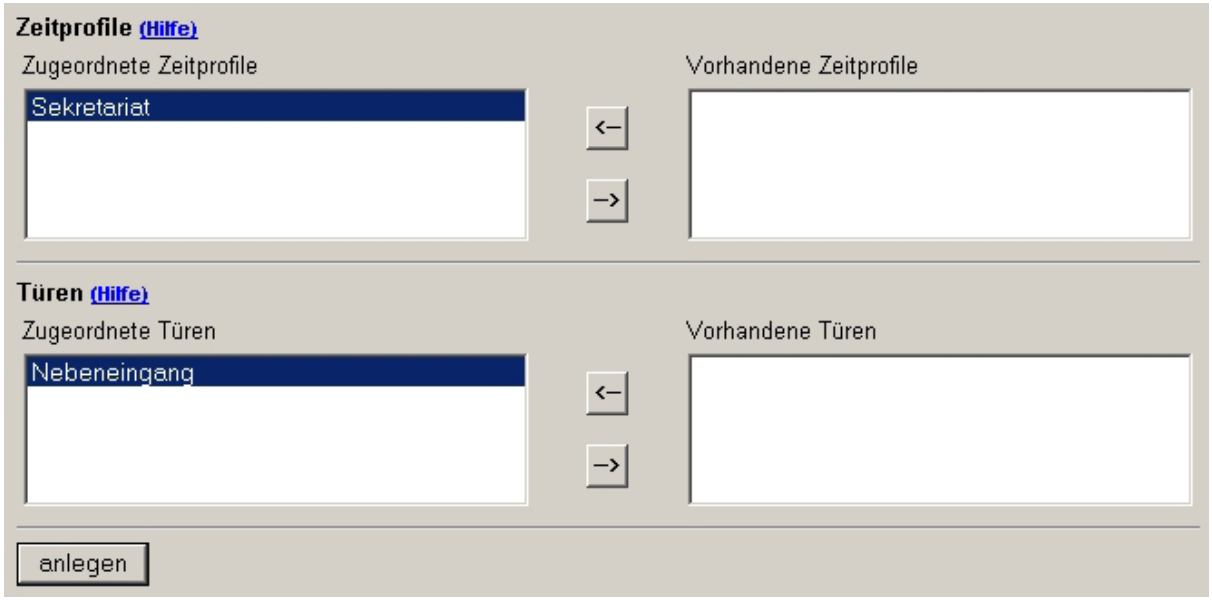


Fig. 49: User set-up – Create access group 3

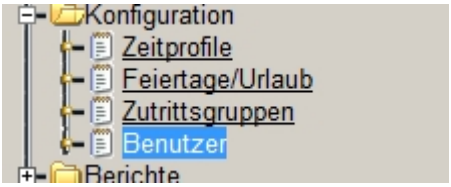
The access group is created using the "Create" action.

3.2.1.2. Users

Finally the employees from the secretarial department now have to be entered in the system.

User name	Characteristics	Description
Maria Elfenbrand (PN: 0003412)	COM: 34527 ELM: 08000000121405030108	In order to gain access through the side entrance, a key combination and a code card are required. The user is to remain valid until 01/01/2007.

Table 41: User set-up – Users



In order to manage the users, select the "Users" menu point.
All the configured users are listed in the "Users" dialogue box. If you want to create a new user, the action "New" must be performed.

Using the Create dialogue box for the user, the name, personnel number, up to 4 characteristics, the validity, login name, password, an additional door release time and up to 3 access groups are defined.

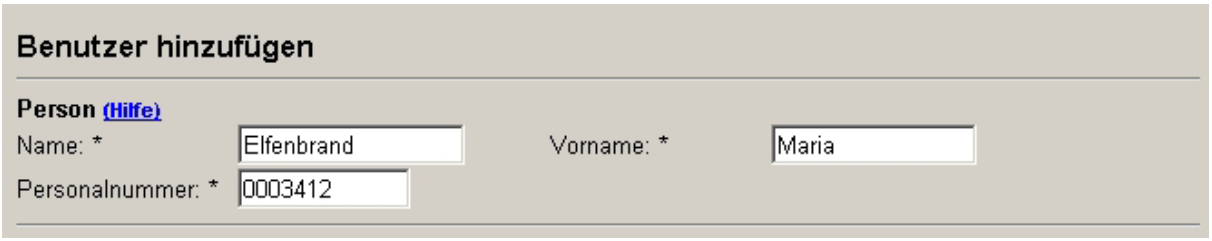


Fig. 50: User set-up – Create user 1

In the next area, the characteristics of the user are entered. Characteristic 1 is the key combination. This can be simply entered. The 2nd characteristic is not so easy to enter, as the number of the code card is generally not known. To enter this characteristic, the action "Teach-in" of characteristic 2 must be executed.

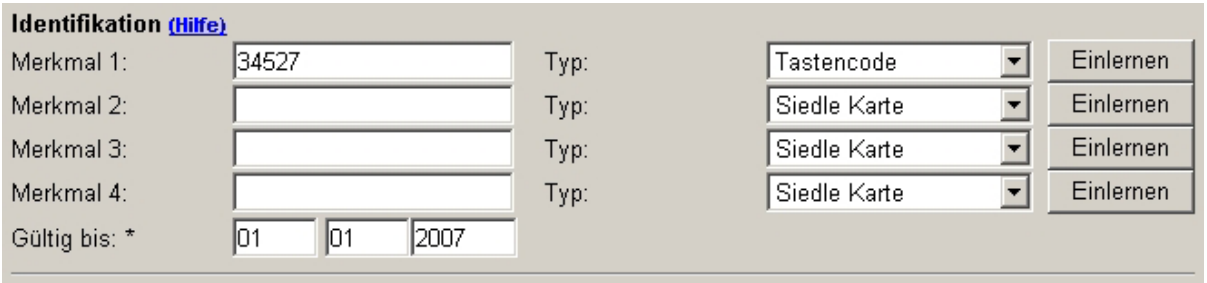


Fig. 51: User set-up – Create user 2

To start the teach-in process, initially a reader must be selected.

In the "Teach-in is possible with this reader" box, it is possible to determine the ELM at which cards EKC 601-… or keys EK 601-… are read in.

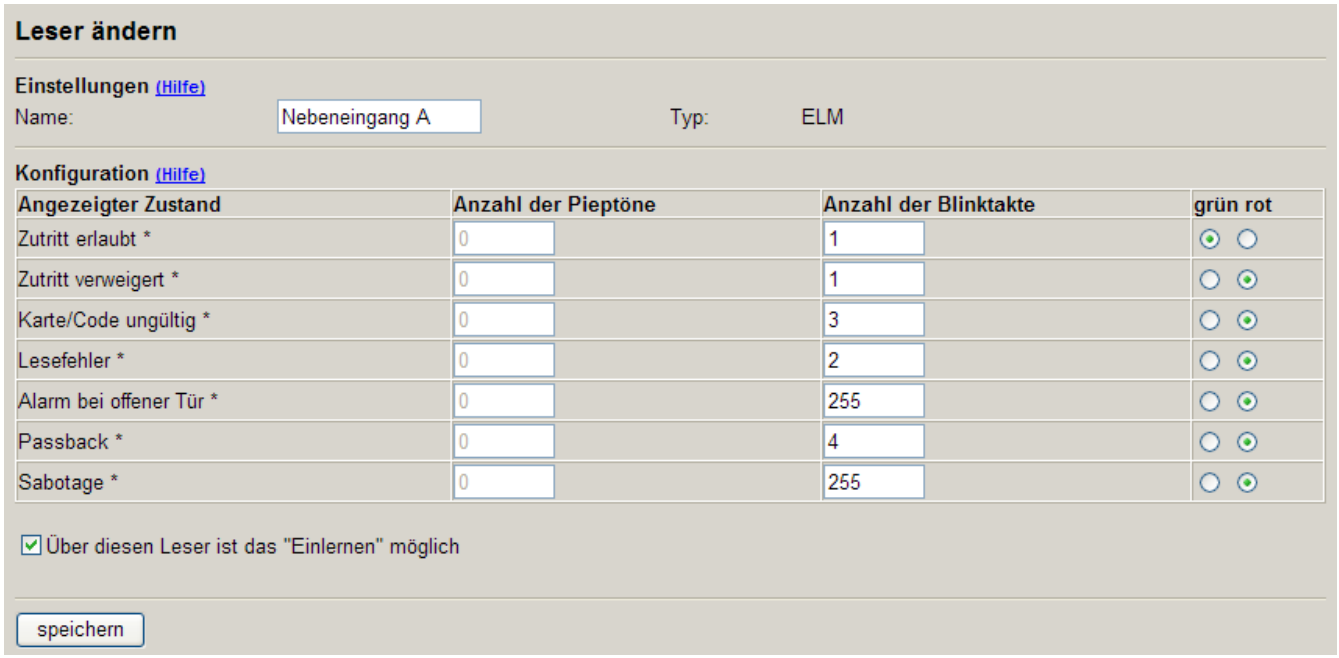


Fig. 52: User set-up – Create user 3

The teach-in process is selected using "Select".

Fig. 53: User set-up – Create user 4

The code card now has to be held up at the relevant reader. The number of the card now appears as a characteristic:

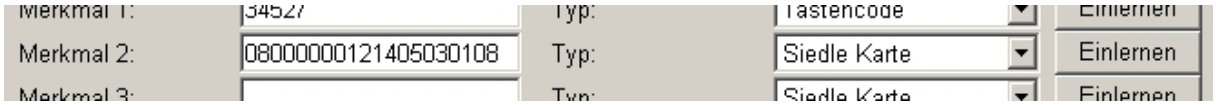


Fig. 54: User set-up – Create user 5

As this user is not permitted to access the web user interface, no login name and password are required. Only the access group still has to be assigned.

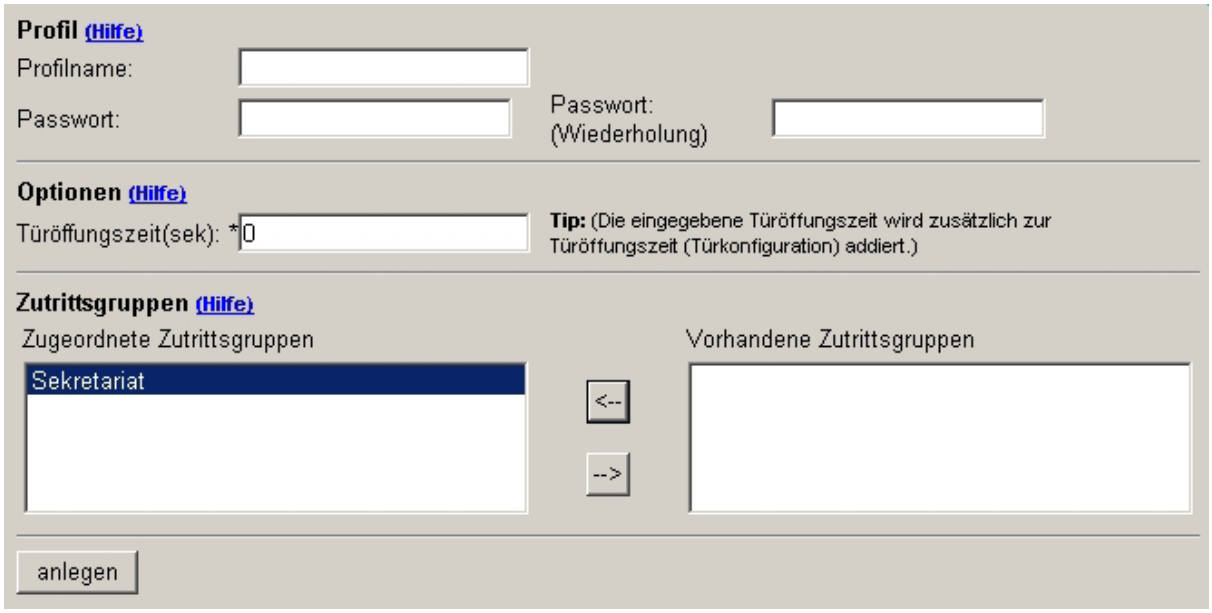


Fig. 55: User set-up – Create user 6

The user is saved using the “Create” action.

3.3. Reading reports

3.3.1. Absentee list

The absentee list shows all users who are not currently logged into the "secured" area.

Elfenbrand, Maria	0003412

Fig. 56: Reading reports – Absentee list

In the absentee list, the names and personnel number of the user is displayed.

3.3.2. Attendance list

The attendance list indicates all users who have logged into the "secured" area.

Nebeneingang	Elfenbrand, Maria	0003412	03.02.2006 11:06:26	löschen

Fig. 57: Reading reports – Attendance list

For each line, the doors, the users, the personnel numbers and the time of entry are described. In addition, a user can be set to absent using the action "Remove".

3.3.3. Event log

In this log, all system events, users and doors are entered. This example illustrates what a login and logout process looks like.
The login process:

03.02.2006 11:06:35	Nebeneingang	Türsensor	geschlossen	---	---
03.02.2006 11:06:34	Nebeneingang	Türsensor	geöffnet	---	---
03.02.2006 11:06:26	Nebeneingang	Benutzer	Zutritt	Elfenbrand_Maria	34527
03.02.2006 11:06:16	Nebeneingang	Eingangsleser	ausgelöst	Elfenbrand_Maria	08000000121405030108

Fig. 58: Reading reports – Event protocol (login process)

The door "side entrance" has two input readers with a logical "AND" link. The entry at 11:06:16 is the ELM (side entrance I2). In the line with the time stamp 11:06:26 the key combination was actuated (side entrance I1). In addition, this line also contains the information that this user has logged on. The lines with the time stamp 11:06:34 and 11:06:35 appear only when a door sensor is connected. The first shows that the door has been opened and the second that the door has been closed again.

The logout process:

03.02.2006 11:13:09	Nebeneingang	Türsensor	geschlossen	---	---
03.02.2006 11:13:08	Nebeneingang	Türsensor	geöffnet	---	---
03.02.2006 11:13:03	Nebeneingang	Benutzer	verlassen	Elfenbrand_Maria	08000000121405030108

Fig. 59: Reading reports – Event protocol (logout process)

The input at 11:13:03 indicates that a user has logged out. The other two signal – if a door sensor is present – that the door has opened and shut.

3.3.4. TCIP 603 table inputs – outputs

Outputs

The outputs can be used as door releases at a door, or in combination with different readers (or as a lock function).

Outputs (Contacts)	TCIP 603 Basic structure	FSM 740 Extension (I/O)	SCE 640 Extension (O)	Contact type (2 A)
Output 1	Relay O1 (local)	---	---	Changeover contact
Output 2	Relay O2 (local)	---	---	Changeover contact
Output 3	Relay O3 (local)	---	---	Changeover contact
Output 4	Relay O4 (local)	---	---	Changeover contact
Output 5	---	Relay 1 (Vario bus)	---	Changeover contact
Output 6	---	Relay 2 (Vario bus)	---	Changeover contact
Output 7	---	---	N.O. contact S1 (Vario bus)	N.O. contact
Output 8	---	---	N.O. contact S2 (Vario bus)	N.O. contact
Output 9	---	---	N.O. contact S3 (Vario bus)	N.O. contact
Output 10	---	---	N.O. contact S4 (Vario bus)	N.O. contact
Output 11	---	---	N.O. contact S5 (Vario bus)	N.O. contact
Output 12	---	---	N.O. contact S6 (Vario bus)	N.O. contact
Output 13	---	---	N.O. contact S7 (Vario bus)	N.O. contact
Output 14	---	---	N.O. contact S8 (Vario bus)	N.O. contact

Inputs

The inputs can be used as door buttons or door sensors.

Inputs (Contacts)	TCIP 603 Basic structure	FSM 740 Extension (I/O)
Input 1	Input I1 (local)	---
Input 2	Input I2 (local)	---
Input 3	Input I3 (local)	---
Input 4	Input I4 (local)	---
Input 5	Input I5 (local)	---
Input 6	---	Input I1 (Vario bus)
Input 7	---	Input I2 (Vario bus)
Input 8	---	Input I3 (Vario bus)

3.4. Backup-Tool

Using the back-up tool, the entire programming (with the exception of the network address) of a TCIP 603-… can be read out and stored as a file. This permits the same programming to be saved to several TCIP 603-… units. The backup files are saves as *.zkn

3.5. Time recording tool

With the Time recording tool, it is possible to read out input and output times of the TCIP 603-… The times are in the format *. xls or *. csv provided. In the download area "Software" on www.siedle.de is the latest version available for download.

4. Server Software

For setup and configuration of the server an experienced administrator is required. If necessary, an appropriate service is offered by the company Siedle.

This server was developed to extend the maximum number of manageable users within a TCIP 603-… to over 500, and to centrally manage and store frequent settings and changes under the chapters Time profiles, Public holidays/vacation, Access groups and Users for several TCIP 603-… units. Changes to the read modules, doors, inputs and outputs are still locally managed at each individual TCIP 603-… The limitations to other parameters continue to correspond to those of the TCIP 603-… with the exception of the number of access groups. This has been extended from V 2.0.0.0 to a maximum of 400 in the server. The extended number of users greater than 500 is available from the TCIP 603-… firmware V 1.2.1.4. The TCIP 603-01 with the old firmware can be updated by Siedle against a charge.

Depending on the capacity of the network, it is now possible to manage over 1000 users with one or more TCIP 603-… units. In this case, the first 500 entered users and all the time profiles, public holidays/vacations and access groups are stored locally in the TCIP 603-… All users with fingerprint data are stored locally. If the server should fail or not be available over the network, the TCIP 603-… remains fully functional using the locally stored data. Only those users who are stored only on the server will not be able to gain access. In the TCIP 603-…, as a rule only those users are locally stored who also have local access entitlement.

The menu points Inputs, Outputs, Readers, Network, System time/Clock change and Doors are configured at the individual TCIP 603-… units.
The TCIP server is pre-installed delivered and should generally run uninterrupted.

Backups of the server database and also of the individual TCIPs with fingerprints are possible manually or on a time-controlled basis using local storage capacity or also with transmission of the backup file by email to local mail servers which do not require authentication.

The previously used time recording tool can continue to be used for central storage of the event logs of different TCIP 603-… units in a joint database.

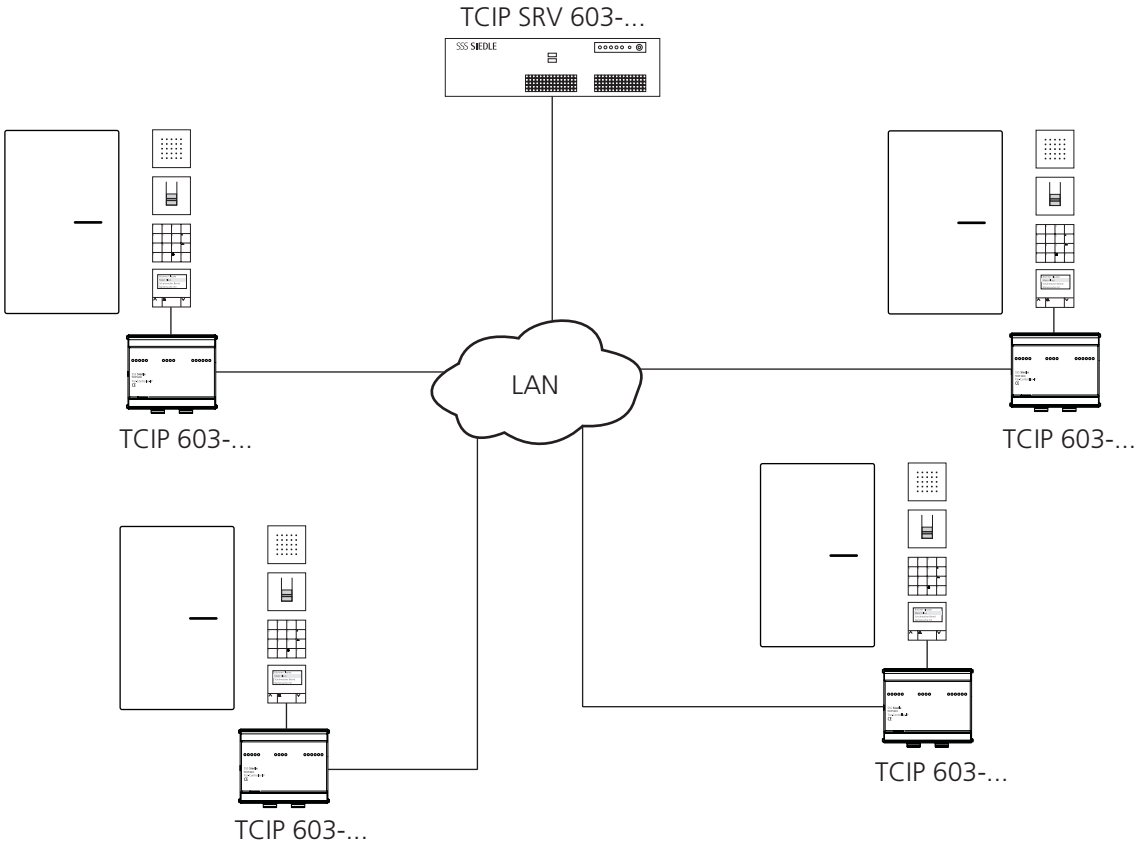


Fig. 60: Schematic server breakdown

4.1. Commissioning requirements

- Experienced system administrator versed in the use of Linux
- Connection to a local network
- Monitor and keyboard for commissioning
- Required in the as-delivered status:
  - Access to an NTP server in the Internet, alternatively the system time is made available by the TCIP SRV 603-…
  - A local mail server is required for sending mails

4.2. Operating mode with fingerprint module

A maximum of 100 fingerprints are managed in the overall system. These are copied from a (freely definable) server master FPM within the entire system to other master FPMs at a TCIP 603-… Finally all FPMs are synchronized at every TCIP 603-…
After 100 scanned fingerprints, it is not possible to scan in any further fingerprints. (The FPM no longer appears in the reader selection).
If users are deleted, a repeated synchronization must be carried out.

4.3. Safety instructions

All data connections to a TCIP 603-… or the server software TCIP SRV 603-… are not encrypted. In cases involving elevated security requirements, the connection must be made using a VPN tunnel. While generating/restoring backups, and also during synchronization, connected PFM units can temporarily not be used for access control, as they are in the configuration mode.

4.4. Login at the server software

Login to the system takes place using a web user interface. This requires you to know the IP address of the TCIP Server As standard, 192.168.0.100 is used.

Fig. 61: Login server

User: Service
Password: Siedle

4.5. Settings in the server software

Commissioning is described in detail in chapter 7.

4.5.1. Hardware/system

Doors

Display of the entered doors for all TCIP 603-… units. The IP address and the name of the TCIP 603-… are visible for identification purposes. The door configuration cannot be changed in the server.

Reader

Under this menu point, all readers of the TCIP 603-… units existing in the system can be viewed, provided they have also been read out under configuration -> TCIPs in the TCIP management. Readers can only be configured in the TCIP.
If fingerprints are used in the individual TCIPs, then for each TCIP a master FPM must be entered to allow the fingerprint data to be transferred during synchronization. After teach-in of all the fingerprints, the operator must launch the synchronization process in the menu "Hardware/System – Reader".

TCIPs

Here, the TCIP 603-… units located in the same network are assigned to the server software. Entry is carried out on the basis of the IP address of the individual TCIP 603-… units. All boxes must be completed in the input screen.

4.5.2. Configuration

Time profiles

Display and processing of created time profiles in all TCIP 603-… units. The entered time profiles can be subsequently assigned to different user groups in the Access groups menu.

Public holidays/vacation

Here, the public holidays/vacations of all TCIP 603-… units are created and processed.

User groups

Access groups can be created and processed here. Existing time profiles can be assigned to the access groups. From V2.0.0.0 onwards, up to 400 access groups can be created in the server. However, the device-specific limitations continue to apply for each TCIP.

User

The "User" dialogue box is used for entering users by name. Here, all the characteristics and rights are entered which you wish to be assigned to this user from the viewpoint of access control.
The surname, first name and personnel number are requested for the user in question. In addition, the person can be assigned a total of 4 characteristics. Characteristics are card, code, fingerprint and Wiegand reader. These characteristics have a validity period.
If the respective user has to log in at the web user interface in order to make evaluations or changes, a profile name (login name) and a password must be issued. In addition, the user must be given a user group which has the necessary entitlements.

4.5.3. Backup

Generating a backup

A backup can be generated using this screen. The backup is stored in the server directory in the following path:
/var/www/backup/export
Below are the times for creating backups:
- Without fingerprint module, appr. 5 mins for each TCIP.
- With fingerprint module, appr. 15 mins for each TCIP.

We recommend making backups after major changes and additionally saving these backups externally.

Restoring

Selection and restoration of a previously generated backup file in individual TCIP 603-… units or in several TCIP 603-… units. For this, a previously created backup must either be copied from the directory /var/www/backup/export on the server or from a connected mail server to the administration computer.

4.5.4. Reports

Event log

Logging the entire event history of all TCIP 603-… units. The log is a summary of the individual local TCIP 603-… event logs. It is updated every 24 hours. Manual updates are possible at any time. The 24 hours refers to automated import of the event protocols.

Task list

In the task list, all waiting processes are displayed such as creating new users, deleting users or processing users, generating backups. Suitable filters can be used for the search function. Entries marked red in the task list indicate an error. However, these are regularly restarted. Tasks marked yellow are currently being processed or have not yet been started if they are shown with a red cross. Tasks marked yellow with blue edge are selected for deletion. Tasks marked blue have been deleted. The current status of the task list is additionally displayed in colour in the browser status bar.
If tasks cannot be executed, this results in a situation where all the subsequent tasks are also not processed.

4.5.5. Tools

General settings

Input of how many days the created *.log files remain before being deleted. A default value of 100 is set.

Only required with fingerprint module FPM 611-…
Selection of the server master FPM for reading all fingerprints into the system for subsequent distribution to the local FPM. All master FPMs of the local TCIP are available for selection.

Backup

Indication of the time intervals at which backups are made and of whether these are transmitted by e-mail. The sending of e-mail is only possible if a local email server exists. Alternatively set-up must be performed by the customer's administrator or Siedle works service.

4.6. Server behaviour

Task

- All failed tasks are automatically restarted (e.g. if the TCIP 603-… cannot be reached when creating a user).
- If a task could not be correctly executed, the system attempts to execute the task again with every start of the scheduler until it has been either executed or deleted.
- The task list is configured in such a way that after an error executing a task, all subsequent tasks on the same TCIP are suspended to prevent confusing the sequence. For this reason, it is advisable to check the task list at regular intervals. The relevant status is shown in colour in the browser status bar.

4.7. Users in the TCIP

The first 500 stored users are saved in the local TCIP in the sequence in which they were stored. All users with fingerprint data are stored locally. Depending on the access group, however, deviations from this procedure can occur, i.e. the number of users which can be managed locally on the TCIP 603-… does not need to be identical, nor does it need to be equal to 500.

4.8. Resetting the TCIP server to the default settings

A complete copy of the Siedle server application is located on the server. This can replace the working version if required. This will completely wipe the user database. Linux-specific settings such as IP address or NTP server settings are not changed as a result.

The user's own inputs are shown in the following in bold type.

Log in directly at the server
TCIP-S login: **Service**
Password: **Siedle**

Change to the folder "home/Service/siedle/" with **cd siedle**
Access the script: **sudo bash i-script.sh**

The sequence of individual script commands is subsequently documented. After completion of the script, the system must be rebooted. This can be initiated with the following command:
Service@TCIP-S:~/siedle$ **sudo reboot**

[sudo] password for Service : **Siedle**

5. Access to the TCIP server

The access via Putty or WinSCP is only encrypted possible. For this connection method a key pair must be generated by the administrator and register on the server.

5.1. Backup

It is possible to program the system to carry out automatic backups. As a special case, facility also exists for these backups to be emailed. When using this functionality, note that these mails can be very large if there are a lot of TCIPs and possibly FPMs connected to the server. Automated backup only makes sense if the event lists need to be archived and there is no program which can be used for this such as the "TCIP time server" software.
There are many possible ways in which backups can be produced and saved, also on other computers as well as the server. A small overview of different possibilities is provided below.

5.1.1. Creating a local one-off backup

Fig. 62: Generate backup

After pressing "Save" the backup is immediately listed as a task and launched after one minute at the latest. Depending on the system size, the backup can take up to 15 minutes per TCIP. During the creation process, the data is saved in the server folder /var/www/backup/tmp and after completion of the backup, in /var/www/backup/export. All file names are completed with a precise date and time stamp – provided the correct time is set in the server.
With WinSCP, for example, the created backup can be copied from the folder /var/www/backup/export to a different computer and deleted on the server. We recommend keeping a list with the time and date, and entering the saved TCIPs with any remarks. It is not possible to determine at a later date which TCIPs with which contents were saved at any given time.

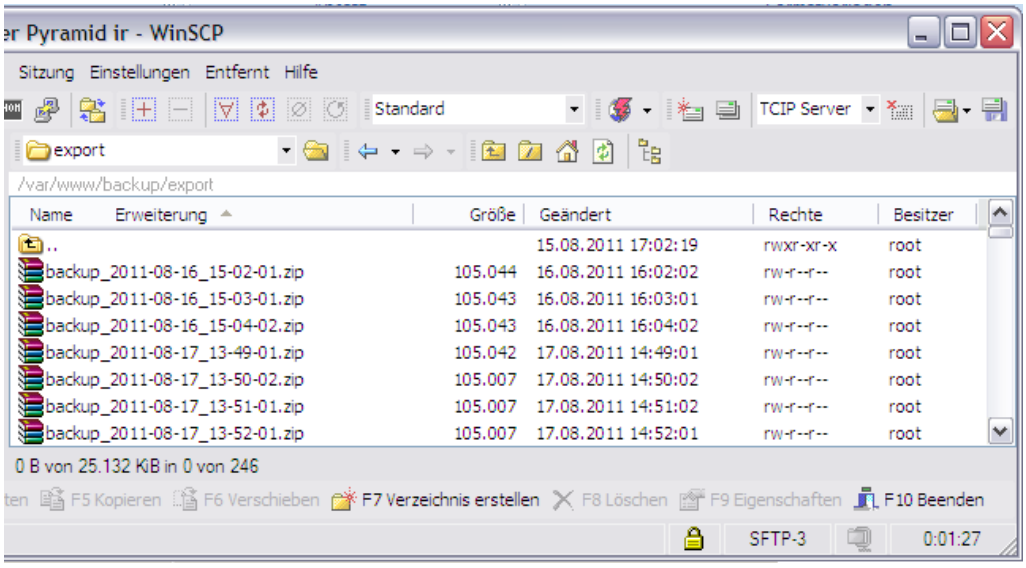


Fig. 63: Restore backup

In order to restore a backup, the backup file must be copied to the external computer from which the backup restoration process is started.

5.1.2. Generating regular backups and saving them outside the server

Fig. 64: Automatic backup

In deviation to the above description, it is also possible in this screen to enter a time, date, or day of the week on which you wish an automatic backup to be created. For this, the screen under 1. needs to be filled in accordingly. Example here: Every first of the month at 0:00 hrs.

5.1.3. Sending the backup by mail to an internal mail server, either once or on a regular basis

A backup can be generated by mail either once or on a regular basis. In addition, it is also necessary to specify a mail address here.

5.1.4. Sending a backup by mail to an external mail server

In order to send a mail to an external mail address, there are a number of different solutions possible.
One example: the internal mail server within the network can send the backup mail to an external mail server.
A central issue here is authentication without a password. This is frequently also possible if the used IP address of the target server is classified as trustworthy. This is generally possible when using a fixed IP address or if the IP address of the target server or target system is self-assigned (deutsche Telekom). In the case of dynamically assigned IP addresses, it is normally not possible to send a backup mail directly to an external mail server. This leaves only the possibility of setting up a mail server on a computer in the local network which then forwards the mail to the external server.

5.2. IP address settings

Selection of the file: /etc/network/interfaces
This file contains all configurations of the network cards.
(Lines preceded by # are only comments and are not taken into consideration.)

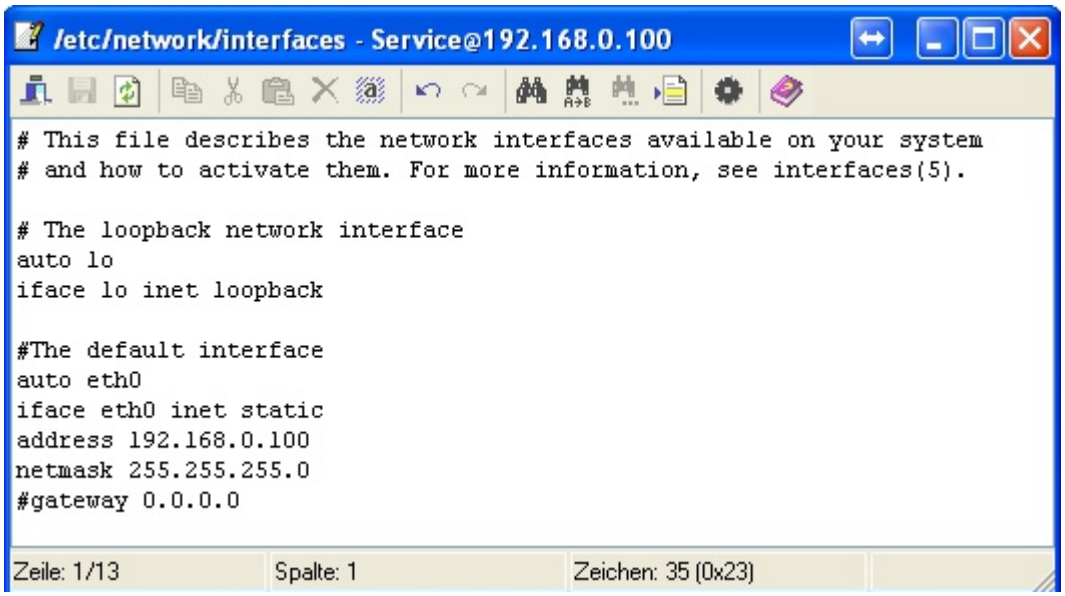


Fig. 65: IP address settings

Once the changes have been made, the server has to be rebooted for the network settings to take effect.

5.3. Static IP address

Remove all entries under “auto eth0”.
Now enter the following lines (these are sample addresses):

iface eth0 inet static
address 192.168.0.100
netmask 255.255.255.0
#gateway 0.0.0.0

If you require a gateway entry, remove the lozenge in front of “gateway” and instead of the “0.0.0.0” enter a correct IP address.
Now save and close the file, and reboot the server.

5.4. DNS server

When using a static IP address, to ensure correct matching of the NTP server, the DNS server address must be entered. This address is saved in the file /etc/resolv.conf.

```
1  # DNS Servereintraege, zum Bsp.:
2  nameserver 10.32.0.1
3
```

Fig. 66: DNS server

5.5. NTP server

Time matching of the TCIP SRV takes place using an integrated NTP service. In the as-delivered status, matching takes place automatically over the internet. If required, the enquiry can be adjusted in the file /etc/ntp.conf.

Selection of the file: **/etc/**ntp.conf

```
1  # /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
2
3  driftfile /var/lib/ntp/ntp.drift
4
5
6  # Enable this if you want statistics to be logged.
7  #statsdir /var/log/ntpstats/
8
9  statistics loopstats peerstats clockstats
10 filegen loopstats file loopstats type day enable
11 filegen peerstats file peerstats type day enable
12 filegen clockstats file clockstats type day enable
13
14
15 # You do need to talk to an NTP server or two (or three).
16 server pool.ntp.org
17
18
```

Fig. 67: Time server settings

5.6. Task list

• Tasks marked green have been successfully processed.
• Tasks marked yellow are currently being processed or have not yet been started if they are shown with a red cross. Tasks marked yellow with blue edge are selected for deletion.
• Tasks marked in red have been aborted due to a fault and are restarted at regular intervals.
The following tasks cannot be processed until all the previous tasks have been successfully completed or deleted by the operator.
• Tasks marked blue have been deleted.

Tasks marked yellow and red can be deleted by clicking on the red cross.

For all entries and changes, check the "Task list" under "Reports" in order to recognize error messages in good time.

Aufgaben (Hilfe)

Erstellt	Letzter Zugriff	TCIP	Vorgang	Benutzer	Fehlermeldung	Status
22.11.2011 09:00:41	22.11.2011 09:00:41	TCIP 2 (10.32.5.197)	Schreibe TCIP TCIP 2 (10.32.5.197)	Service	---	
22.11.2011 09:00:22	22.11.2011 09:01:05	TCIP 1 (10.32.5.196)	Schreibe Kalender und Zeitprofile auf TCIP TCIP 1 (10.32.5.196)	Service	Scheduler konnte nicht auf dem TCIP 10.32.5.196 einloggen. Sollte das Problem weiterhin bestehen, kontaktieren Sie einen Servicetechniker.	
22.11.2011 08:59:02	22.11.2011 08:59:22	TCIP 2 (10.32.5.197)	Lege Benutzer B4, b4 auf dem TCIP TCIP 2 (10.32.5.197) an	Service	---	
22.11.2011 08:58:08	22.11.2011 08:59:03	TCIP 2 (10.32.5.197)	Bearbeite Zutrittsgruppe z3 auf dem TCIP TCIP 2 (10.32.5.197)	Service	---	

Fig. 68: Task list

If tasks are deleted by the server's administrator, then the administrator must ensure that the resulting inconsistencies between the server data and the data of the TCIP terminals are manually corrected.
For this, the data in the server and also in the local TCIP must be compared.
In the case of differences which cannot be remedied, we recommend restoring a functioning backup. Any changes made in the interim must be repeated.

6. FAQ

How many browsers can access a server simultaneously?
"Access only with 1 browser at any one time"

The event log only shows events up to the previous day, although the correct date is set in the server and in the TCIP, and events occurred at the TCIP.
In the event log of the server, the events of the local TCIP are shown. These are automatically loaded once every 24 hours. This process can also be started manually using the function Event logs.

There is an entry marked in red in the task list with a note saying that a data record could not be created or changed at a TCIP.
If, for instance, the system was unable to create or change a particular user, then try removing the access group(s) for this user which give it the relevant rights at the TCIP in question and save the user. Then add the previously removed access group(s) again to this user. The user should then be created again on the local TCIP.

The entries from the local TICP do not agree with those on the server.
There are many different reasons for lack of synchronicity in the server and terminals:
• If the data transmission is interrupted
• If a change has been carried out directly at the TCIP
• If tasks have not been executed / downstream tasks are executed first.

Measures to increase defect tolerance:
• If a task has not been successfully completed (red status or if applicable yellow "interim status"), then the downstream tasks may also not be executed.
• If when attempting to make a change to a TCIP, for instance the user you wish to change is missing, a fault is indicated and no change is carried out. In this case, the user should be completely rewritten. This applies equally to all changes.
• When deleting, use a corresponding procedure.
• If when attempting to create a data record (user), it is discovered that the user already exists, a fault is indicated. In this case, the data record should simply be overwritten.
Check the access groups and users. Check whether a task is marked red in the task list, and delete it. If there is no corresponding task active for describing / changing the local TCIP, it is possible to activate the command "Write TCIP" behind the deviating TCIP under the menu point "Hardware/System – TCIPs". Only the information which is required at a particular TCIP is transferred to it. Example: If a user has more than one access group, only those are transferred which are required for this TCIP.

Access by the server to one or more TCIP units no longer appears to be working correctly.
Check the task list. Change the filter date in front of it and set the date under "from" to a date which is around 10 days in the past. Then activate the button "User filter" and check the task list for entries marked in red. These entries may under some circumstances block the following tasks. They need to be deleted. However, the cause of these error messages has to be remedied.

It is not possible to actuate the “select” button

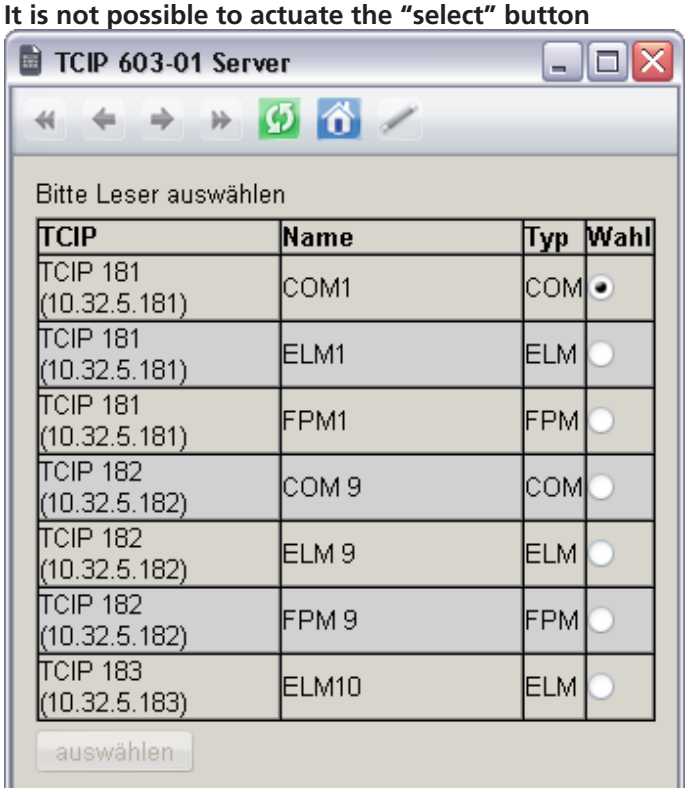


Fig. 69: Select reader

Here, all readers need to be read in again. If there is no problem at the reader itself or at the local TCIP, the button will subsequently be enabled again. This block always affects all the readers at the same TCIP.

When creating a user with fingerprint, the input is refused.

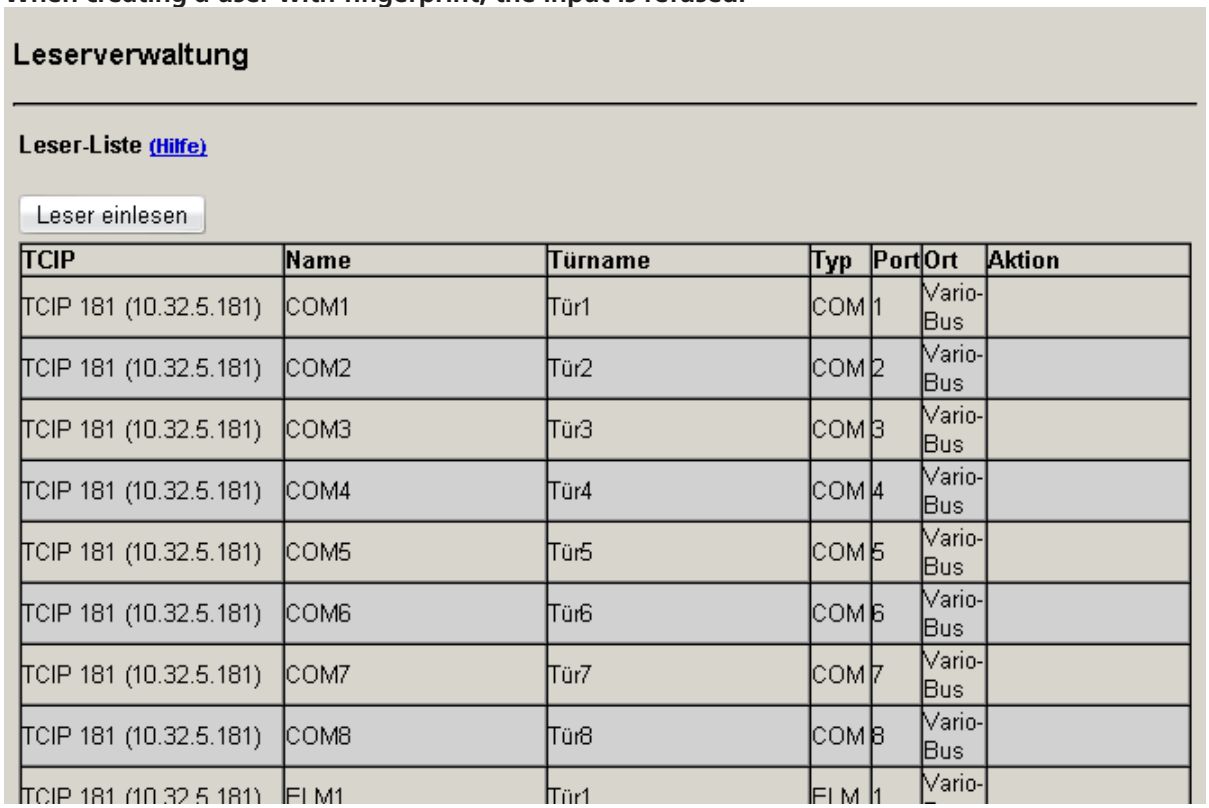


Fig. 70: Reader management

“User already exists / wrong input” means that a user (with fingerprint) has been created for which no fingerprint has yet been read in. Always ensure when creating a user with fingerprint that you complete the entry.

7. Commissioning

7.1. Recommended commissioning sequence

When commissioning the server solution, it is advisable to carry out the following points in sequence:

1. Carry out all backup settings and all settings in the operating system which deviate from the standard.
2. Server – Enter TCIP addresses
3. TCIP – Carry out network settings
4. Recommendation: 1. Generate a backup to allow you to restore the "as-delivered status" at a later date
5. TCIP – Define inputs
6. TCIP – Define outputs
7. TCIP – Read in readers, define the name, **define one master (teach-in) FPm per TCIP where this exists.**
8. TCIP – Set system time / clock change
9. TCIP – Create doors (leaving users, access groups, time profiles and public holidays free)
10. Entering the TCIP – IP address into the individual TCIPs
11. Server – Read readers
12. Server – Read doors
13. Server – Synchronize FPMs
    Wenn auf dem importierten TCIP-Datensatz FPM-Leser enthalten sind, muss eine FPM-Lesersynchronisation durchgeführt werden:
    - In der Leserverwaltung, auf dem Server, kann über den Button „synchronisieren" die FPM Synchronisierung gestartet werden
    - Abgleich der FPM auf dem Master-TCIP (Master-TCIP das TCIP auf welchem der Master-FPM definiert wurde)
    - Backuperstellung des Master-TCIP
    - Kopieren des backup auf alle weiteren TCIP
    - Abgleich der FPM auf den weiteren TCIP mittels des überspielten Backups
14. Recommendation: Generate backup
15. Server – Create time profiles
16. Server – Create public holidays/vacation
17. Server – Create access groups
18. TCIP – Doors: where applicable assign time profiles
19. Server – If doors are changed in TCIP 603-…, then read doors
20. Server – Tools/general settings: Set delete cycle for the log file
21. Server – Tools/general settings: If available, select server-master-FPM
22. Server – Tools/general settings: Carry out backup settings
23. Server – Create users
24. Recommendation: Generate backup
25. Move the previously set backup files from the server to a PC from which the settings are performed

7.2. Migration TCIP SRV 603-…

Transfer of data from an existing system

If several TCIP 603-… units are located in an existing system, it is possible to transfer the configuration of one of the TCIP 603-… units into the server database.
The adoption of data is possible from the TCIP 603-02 with firmware 1.2.1.4 or higher. Importing older TCIP 603-0/01 units must be clarified on a case-by-case basis. For details please contact the Siedle Aftersales Service.

1. Carry out all backup settings and all settings in the operating system which deviate from the standard.
2. Server – Enter the TCIP address and read in from this device.
3. Reset all other TCIP units to their as-delivered status
4. TCIP – Carry out network settings
5. Server – Enter all other TCIP addresses in the server.
6. TCIP – Define inputs
7. TCIP – Define outputs
8. TCIP – Enter the reader, define the name, **define one master (teach-in) FPm per TCIP where this exists.**
9. TCIP – Set system time / clock change
10. TCIP – Create doors, leaving users, access groups, time profiles and public holidays free
11 Entering the TCIP – IP address into the individual TCIPs
12. Server – Read the readers
13. Server – Read the doors
14. Server – FPM synchronization
    If the imported TCIP data record contains FPM readers, FPM reader synchronization must be carried out:
    - Enter the master FPM of the read-in TCIP under "Tools -> General settings"
    - Start FPM synchronization in the reader management using "Synchronize".
15. Recommendation: Generate backup
16. Server – Check time profiles
17. Server – Check public holidays/vacation
18. Server – Check access groups
19. TCIP – Doors: where applicable assign time profiles
20. Server – If doors are changed in TCIP 603-…, then read doors
21. Server – Tools/general settings: Set delete cycle for the log file
22. Server – Tools/general settings: If available, select server-master-FPM
23. Server – Tools/general settings: Carry out backup settings
24. Server – Create/change user (with all users read by the TCIP for which profile names and profiles are entered under "Profile", the passwords have to be entered again in the server user interface, as these cannot be read by the TCIP for security reasons.)
25. Recommendation: Generate backup
26. Move the previously set backup files from the server to a PC from which the settings are performed

Attention
The function Read TCIP deletes all the entries in the TCIP server and then reads in the data of the selected TCIP. In running operation, the function read TCIP should not be used.

7.3. Special cases

Exchange / deletion of an FPM

Synchronized system with functioning server-master-FPM
In this system, a defective FPM can be simply replaced by a new one. Subsequently, a synchronization process must be executed from the server.

Synchronized system with defective server-master-FPM
Here, a different master FPM must be defined temporarily as a server-master-FPM. Subsequently, the defective module must be exchanged as described above.

Unsynchronized system or system with only one FPM
If the only FPM has to be replaced and there is no backup available, all fingerprint characteristics of all users must be deleted in the project menu.
If an FPM is used which has previously been operated on a different system, then first the menu point “Reset identifier” must be accessed in the relevant FPM reader menu in the TCIP 603-…

List of figures

List of tables