Product information

IP video front door station ARGOS

CAE3x02-IP-015x

2nd generation

Table of contents

Scope of delivery

1 x IP video front door station ARGOS
1 x flush-mount box
1 x installation kit with screws, dowels and sealing
1 x allen key with SW 2.0
3 x RFID cards: 1 x green, 1 x red and 1 x grey
1 x assembly instruction
1 x product information

Article overview IP video front door station ARGOS 2nd generation

CAE3002-IP-0150	345x192x8 (HxWxD mm), colour: silver (anodised)
CAE3002-IP-0151	345x192x8 (HxWxD mm), colour: bronze (anodised)
CAE3002-IP-0156	345x192x8 (HxWxD mm), colour: black (anodised)
CAE3102-IP-0150	365x192x8 (HxWxD mm), colour: silver (anodised)
CAE3102-IP-0151	365x192x8 (HxWxD mm), colour: bronze (anodised)
CAE3102-IP-0156	365x192x8 (HxWxD mm), colour: black (anodised)
CAE3202-IP-0151	345x150x8 (HxWxD mm), colour: bronze (anodised)

Introduction

Notes on this product information

This product information refers exclusively to qualified electricians.

The product information contains important notes on intended use, installation and initial operation.
Please keep the product information at a suitable place, where it is easily accessible for maintenance and repair.
All product information are available in the download area under www.carus-concepts.com.

Used symbols and warning notices

Symbol	signal word	Explanation
	**DANGER!**	The signal word describes an endangering with a high level of risk. Failure to observe this warning will result in death or very serious injury.
	**WARNING!**	The signal word describes an endangering with a medium level of risk. Failure to observe this warning could result in death or very serious injury.
	**CAUTION!**	The signal word describes an endangering with a low level of risk. Failure to observe this warning could result in a minor or moderate injury.
	**CAUTION!**	The signal word indicates, that damages on equipment, environment and property can occur.

Further used symbols

	important note or important information
►	Step
☞	cross reference: For further information on this topic, see source
•	list, list entry 1 level
-	list, list entry 2 level
a)	Explanation

Safety instructions

General safety regulations

Assembly, installation, commissioning and repair of electronic devices must be carried out by qualified electricians.
Observe the latest regulations and standards for system installations.

WARNING! Danger to life due to electric shock
When working on main power connections of 230 V,
the safety regulations according to DIN VDE 0100 must be observed.

When installing TCS:BUS systems the general safety regulations for telecommunication systems according to VDE 0800 must be observed. Inter alia:

- separated cable routing of high and low voltage lines
- minimum distance of 10 cm in case of a common cable routing
- use of separators between high and low voltage lines within shared cable ducts
- use of standard telecommunication lines, e.g. J-Y (St) Y with 0.8 mm diameter,
- already existing lines (modernisation) with deviating cross-sections can be used in compliance with the loop resistance

Observe the general requirements for network installations according to DIN EN 50173.

Requirements to protect against lightning

CAUTION! Device damage due to over-voltage
By suitable lightning protection measures it has to be ensured that the electric voltage of 32 V DC at each connection is not to be exceeded.

Note for video surveillance according to DIN 33450

Creating and saving video recordings can infringe personal rights.
Always observe the current legislation and labelling requirements
during assembly and operation of video components.

Product description

Intended use

The IP video front door station ARGOS is a terminal for access control that combines access control and video door communication. Video door communication can be implemented in a network directly via SIP phones.
The IP video front door station ARGOS is suitable for flush-mount in the outdoor area.

	For applications, which differ from the intended use or go beyond, the manufacturer accepts no liability.

Short description

RFID
- integrated RFID reader
- MIFARE®
- optionally adaptable for LEGIC® and iCLASS®
- identification storage for up to 1000 persons
- integrated code lock
- identification via RFID and code can be queried combined

VIDEO
- integrated camera with 1.3 mega pixel CMOS colour sensor
- wide angle objective with 130 degree opening angle
- electronic PTZ control
- video compression H.264, MJPEG, JPEG
- video resolution VGA and CIF
- frame rate with up to 25 images per second
- 6 infrared LED for night lighting

AUDIO
- integrated microphone and loudspeaker
- full duplex high power echo suppression
- frequency range 200 - 16,000 Hz
- audio coding G.711 (A/µ-Law), G.711, G.729

Operation / configuration
- capacitive colour touch screen with 5.7'' LCD (640 x 480 pixel)
- brightness controlled by ambient light
- configuration via LCD menu and web interface
- customisable start screen
- integrated data base, up to 1000 call destinations can be stored

Access control
- via RFID and/or PIN
- optional time recording of employees (administration via software FaceAdmin, not included)

Event dealer
- assigning events to actions
- maximum 50 links can be configured

- Events:
  - access control (RFID and/or PIN)
  - tamper contact (contact, acceleration)
  - SIP (INFO/DTMF, INVITE, BYE)
  - trigger inputs
  - RFID
  - PIN
  - TIMER
- Actions:
  - video (PTZ, snapshot)
  - relay
  - SIP (INVITE, BYE, TALK)
  - IP (HTTP GET, UDP Broadcast)
  - LCD (Switch screen, Display ON/OFF)

Example 1:
An access event switches a relay. A video snapshot is taken and the screen displays *Access granted*.

Example 2:
A relay is switched on in case of a SIP-DTMF signal and switched off after the timer period has elapsed.

The configuration of the event dealer is only approved for trained system integrators.

Interfaces
- Ethernet, 10/100BaseT at RJ45 socket
- 2 x trigger input (door release button, feedback contact)
- 1 x relay changer (door release, light)
- Wiegand or RS485 or UART Rx/Tx
- 2-wire interface on spring-loaded terminal (with optional 2-wire kit)
- integrated register server for peer-to-peer operation

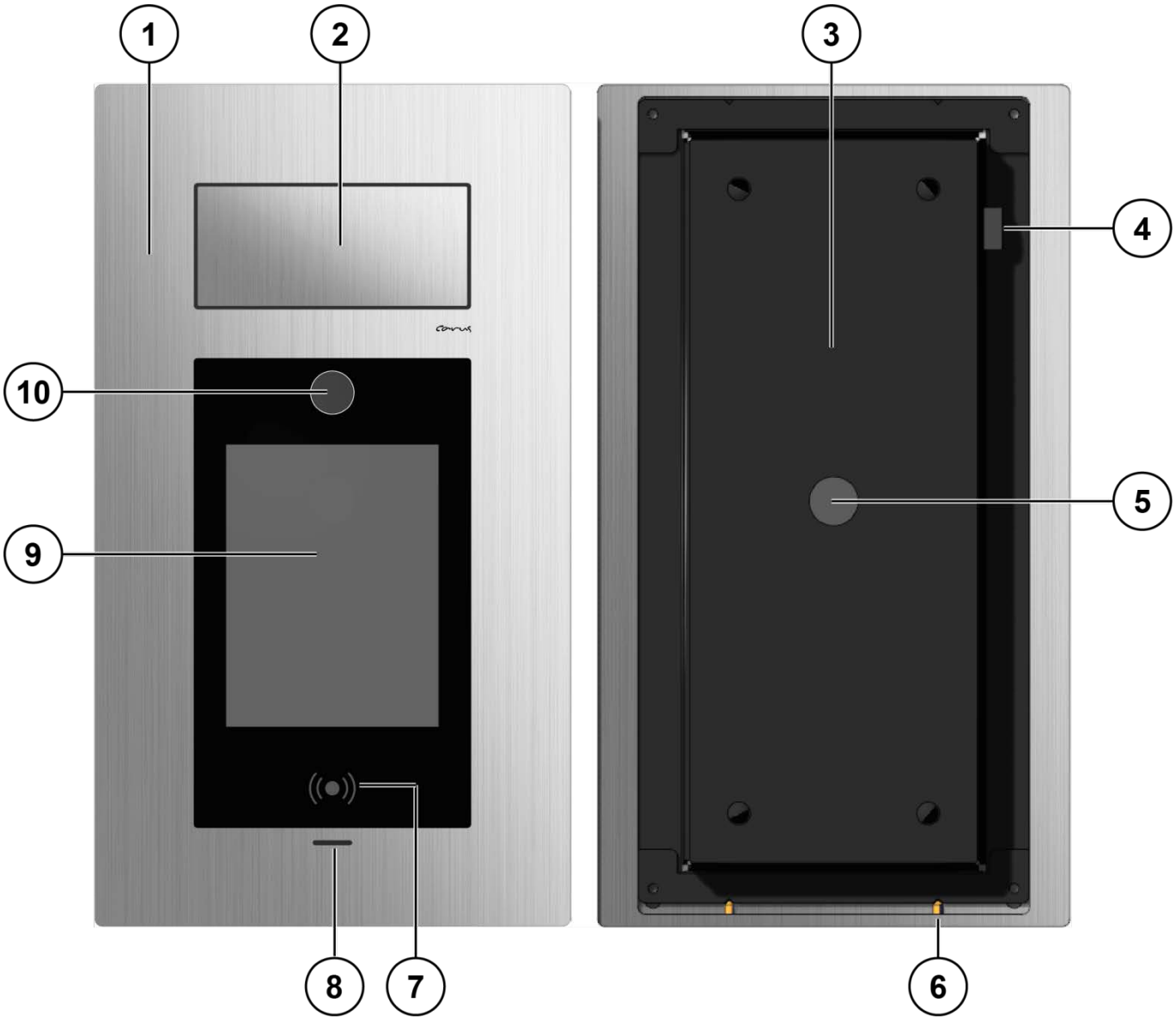
Protocols
- SIP RFC 3261, compatible to SIP (video) phones, softphones and Apps
- TCP/UDP/IP, RTP, http, DNS, NTP, DHCP (Client)

Ambient conditions
- temperature range: -20 °C to +60 °C
- humidity up to 95%, non-condensing
- ambient brightness up to 50,000 lx

Power supply
- Power over Ethernet (PoE) 802.3af and 802.3at
- alternative power supply 6-48 V DC 10 W (via 2-wire interface)

Housing
- housing made of solid aluminium
- structured surface refined by hand
- for installation in a flush-mount box
- colour: silver, bronze or black anodised
- tamper contact and acceleration sensor against vandalism

Device overview



1 housing made of aluminium
2 loudspeaker
3 wall-mount case for surface- and flush-mount
4 pressure compensation element
5 cable gland
6 locking screw
7 RFID reader
8 microphone
9 display with touch screen
10 camera

Technical data

supply voltage	• PoE IEEE 802.3af and 802.3at • alternative power supply: 12-55 V DC 10 W (via 2-wire interface)
power consumption, in standby position	P = 6.6 W
maximum power consumption	P_{max} = 9,6 W
housing	aluminium
degree of protection	IP65
dimensions (H x W x D in mm)	**CAE3002-IP-015x:** housing dimensions: 345x192x8 (52 mm incl. flush-mount box) mounting dimensions: 350x192x8 (52 mm incl. flush-mount box) **CAE3102-IP-015x:** housing dimensions: 365x192x8 (52 mm incl. flush-mount box) mounting dimensions: 370x192x8 (52 mm incl. flush-mount box) **CAE3202-IP-0151:** housing dimensions: 345x150x8 (52 mm incl. flush-mount box) mounting dimensions: 350x150x8 (52 mm incl. flush-mount box)
weight	CAE3002-IP-015x: 3 kg (incl. installation box) CAE3102-IP-015x: 3 kg CAE3202-IP-0151: 2.9 kg
acceptable ambient temperature	-20 °C ... +60 °C
degree of protection	IP65

Mounting and installation

Installation

Use the enclosed installation kit for installing the flush-mount box.

Installation site

For an optimal operation we recommend a mounting height of 1.57 m (centre of the device above ground, Fig. 1).

To achieve an optimal video image quality do not point the camera to:
• solar radiation
• strong sources of light
• bright or strongly reflecting walls

Ensure that the ARGOS CAE3x02-IP-0156 (black anodised) is not exposed to direct solar radiation. The housing can heat up too much.

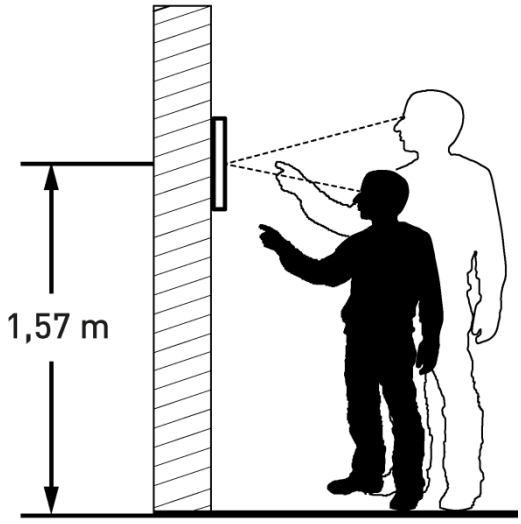


Fig. 1: Mounting height

Flush-mount

► Make a wall cut out for the flush-mount box.

	Use the flush-mount box as template for the wall cut out.

	• Do not wall in or foam in the pressure compensation element. • Observe that there is a gap between the masonry and the pressure compensation element.

► Mark the drilling holes with the help of the flush-mount box (Fig. 2). For fixing the flush-mount box you can use the outer holes **(1)** or the inner holes, depending on the type of installation **(2)**.

	• Ensure a vertical installation and the installation position **(3)**. • For the alignment use the integrated level. • The alignment of the device cannot be corrected later.

► Put the enclosed dowels into the holes.

	Use the enclosed sealing plugs (Fig. 3). There are no warranty claims due to improper installation.

► Insert the sealing plug **(4)** into the flush-mount box.
► Close the cable gland that is not used with the enclosed sealing plugs **(5)**.
► Guide the connection cable through the cable gland and the sealing plug.
► Fix the flush-mount box with 4 screws **(6)** to the wall (Fig. 4).

	• For marking the inner holes you can puncture the sealing plugs with a small screwdriver. • The screws need to be screwed through the sealing plugs. Thus, the device is sealed.

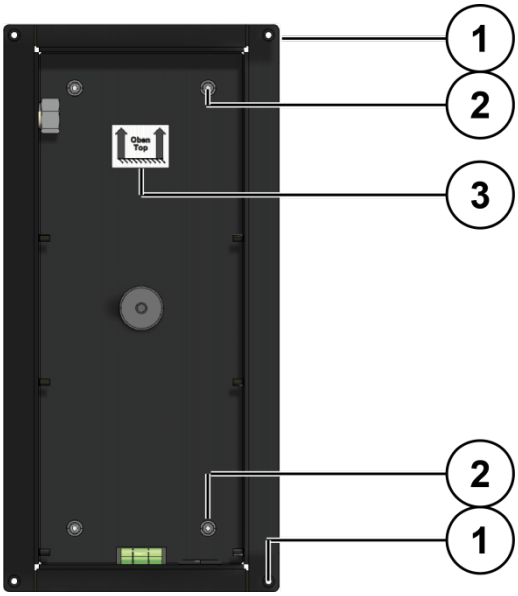


Fig. 2: attachment holes

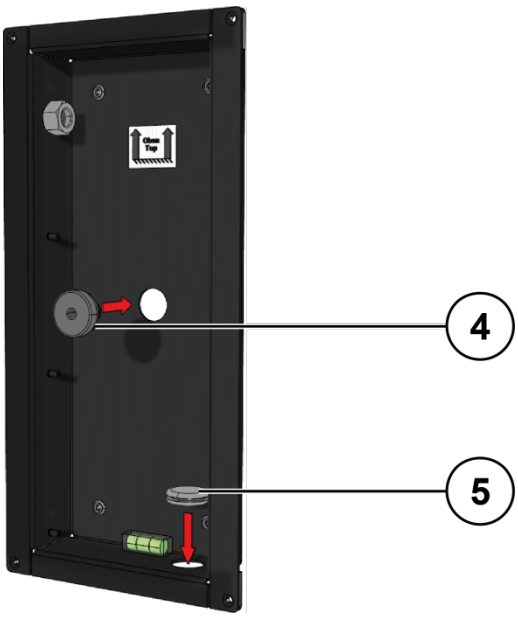


Fig. 3: sealing plug

Fig. 4: Fixing the flush-mount box

Connecting the lines

For connecting external devices the ARGOS front door station offers different interfaces. (Fig. 5).

Pos.	**designation**
1	ethernet connection (PoE power supply)
Wiegand:	
2	GND
3	Dat1
4	Dat0
relays:	
5	o.F.
6	COM
7	NO
2 WIRE:	
8	+
9	-
10	2x trigger input

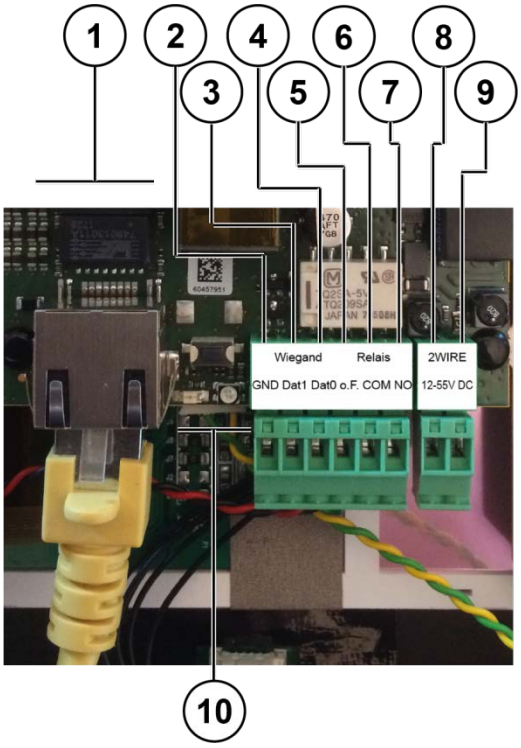


Fig. 5: Ports

For the installation you can remove the screw terminals from the circuit board and pin them back on later.

► Connect the lines according to the labelling.

The inputs have to be connected to ground for trigger function.

with tamper switch (for outdoor use):	IN1	Sabotage	o.F.	GND	
without tamper switch (for indoor use:	IN1	IN2	o.F.	GND	

Fig. 6: overview connection terminals

Put on the front plate

► Hang the clips **(1)** of the front plate **(2)** onto the guidance points **(3)** of the flush-mount box **(4)**.
► Push the front plate downwards.
► Secure the front plate with the locking screws **(5)**.

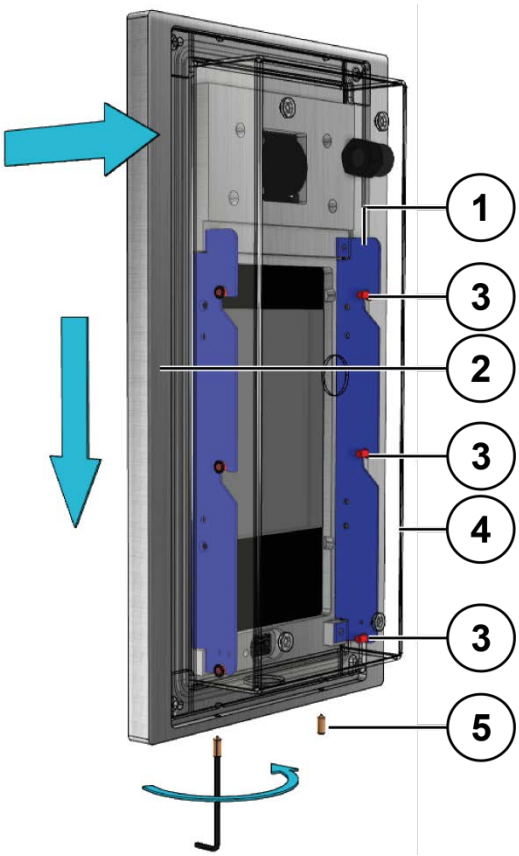


Fig. 7: Put on the front plate

Remove the front plate

► Screw out the locking screws **(5)**.
► Push the front plate upwards.
► Remove the front plate.
► Remove the lines.

CAUTION! Damage of the front plate

- Due to improper handling the front plate can get damaged.
- Place the front plate on a clean and dry surface.

WARNING! Danger to life due to electric shock

Observe the safety regulations according to DIN VDE 0100, when working on main power connections of 230 V.

► Install the devices of the system voltage-free and completely.
► Switch on the mains voltage.

- The device is not equipped with a separate ON/OFF switch.
- After the mains power is connected, the device starts and displays the start screen.

Start screen

Fig. 8: variant 1: groups

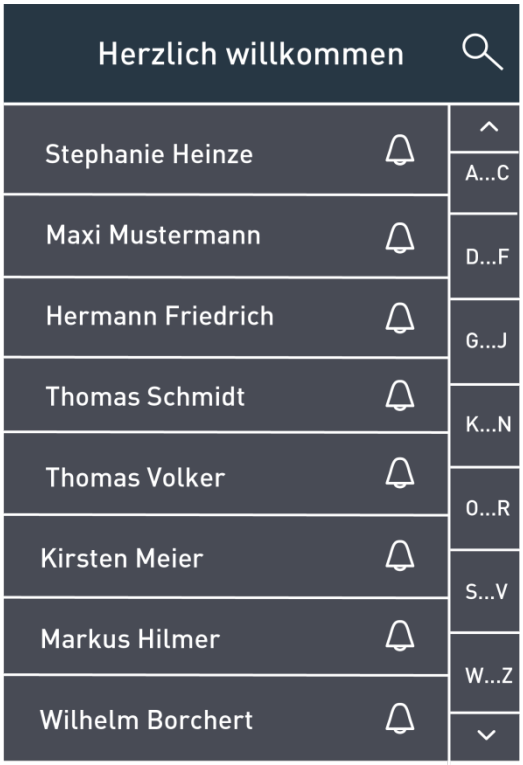


Fig. 9: variant 2: phone list

► Swipe with your finger upwards to display further groups/persons.
Alternatively you can skip to the contact with the selected initial letter by tapping the initial letter.
► Tap with your finger on a group to display the members of the group.
► Tap the required person. The person is called.

Menu access with PIN code:
► Swipe with your finger to the right to call up menu access via PIN.

Configuration via OSD menu

You need the red RFID card for the configuration via OSD menu (Fig. 10).

► Hold the red RFID card in front of the RFID reader. The configuration menu is displayed (Fig. 11).

- If there is no input within 30 sec, the configuration mode is left automatically.

Fig. 10: Red RFID card

Overview configuration menu

In the configuration menu you can select the following menus:

- camera
- audio
- display
- Network
- tamper protection (no settings possible).

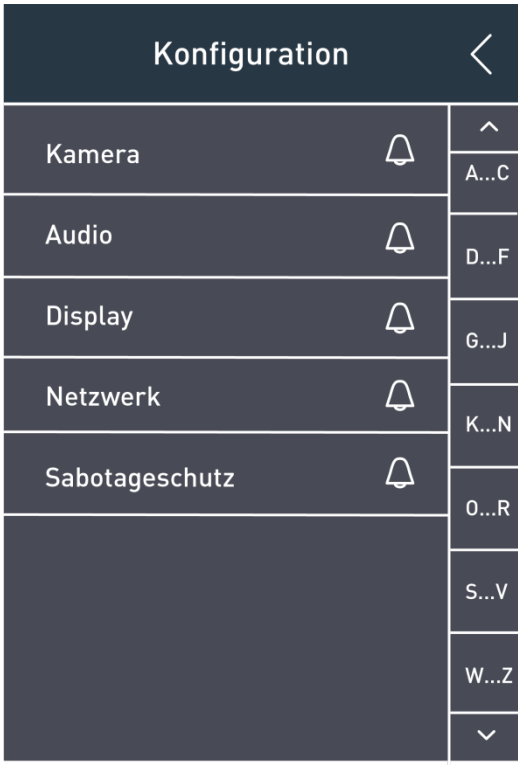


Fig. 11: Configuration menu

Camera

- In the menu *Camera* the *Live image* **(1)** of the camera is displayed (Fig. 12).
- In the menu *Camera* you can adjust and store 3 different detecting areas (wide angle) of the camera.

► Select the menu Camera from the *configuration menu*.
► Tap on a camera button **(3)**.
► Slide the zoom controller **(2)** to the right to zoom into the video image resp. to the left to zoom out of the video image.
► Tap on the camera button **(3)** until an acknowledgement tone sounds. The coverage is stored.
► Tap on the *Back button* to get to the configuration menu.

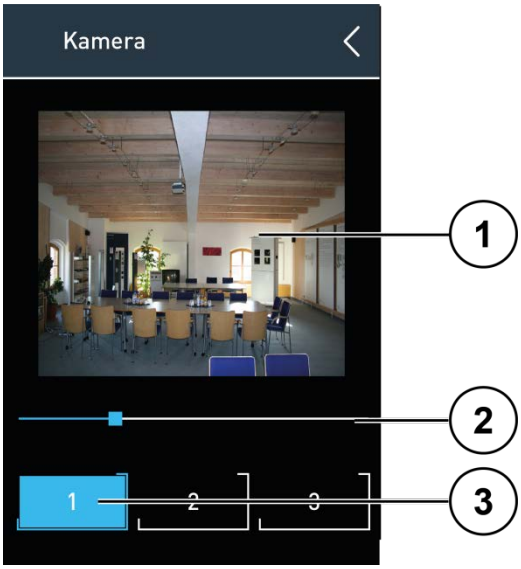


Fig. 12: camera

- In factory setting, the device is set at maximum wide angle.
- Select the image section in a way, that you have a clear view on the person in front of the door.

Audio

Volume

The volume of the voice and tone output can be adapted to the local conditions (Fig. 13).

► Select the menu *Audio* from the configuration menu.
► Slide the volume control of the *Voice* **(1)** resp. of the *Tones* **(2)** to the right to increase the volume resp. to the left to reduce the volume.

To check the volume, a voice record is played.

► Tap on the *Back button* to get to the configuration menu.

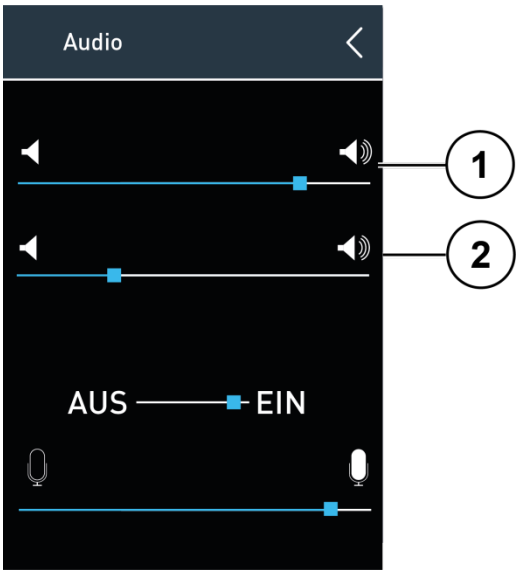


Fig. 13: Audio settings

Microphone

The microphone sensitivity offers 2 adjustment options:

- digital control (automatic control)
- analogue pre-amplification (Fig. 14).

	We recommend to switch on the automatic adaptation, if the local acoustic conditions vary greatly.

► Select the menu *Audio* from the configuration menu.
► Slide the slide switch automatic control to *ON* **(3)**.

	The sensitivity of the microphone can be adjusted independently from the fact, if an automatic control was selected or not.

► Slide the microphone control to the right to increase the microphone sensitivity resp. to the left to reduce it **(4)**.

	In factory setting an average value is set.

► Tap on the *Back button* to get to the configuration menu.

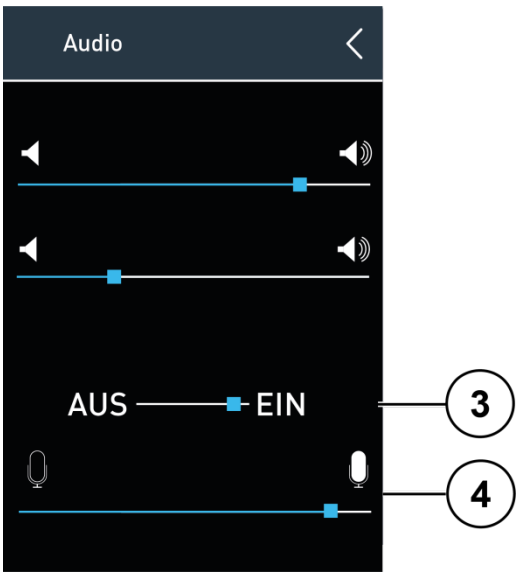


Fig. 14: Microphone settings

Display

Automatic control

- The bright of the display adapts automatically to the ambient bright.
- The measured bright is displayed under the slide **(1)** switch (Fig. 15).

► Select the menu *Display* from the configuration menu.
► Slide the slide switch to the position *Automatic* **(1)**. The bright of the display is adapted automatically to the ambient bright.

- In factory setting the slide switch is in position *Automatic*.
- The display is dimmed over night to minimise the power consumption.

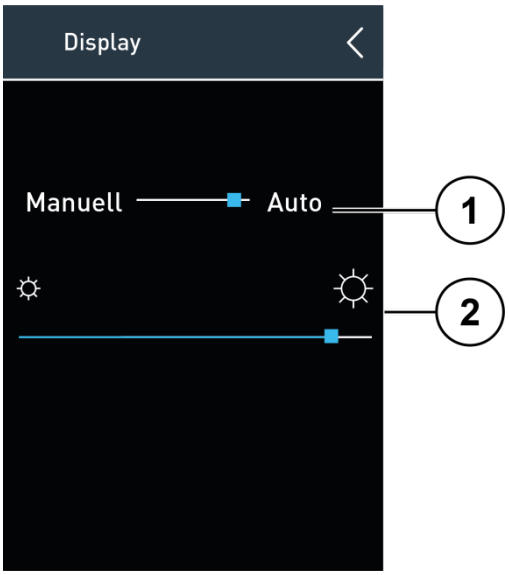


Fig. 15: Display settings

Manual control

► Slide the slide switch to the position *Manually* **(1)**.
► Slide the bright control **(2)** to the right to increase the bright resp.to the left to reduce it.
► Tap on the *Back button* to get to the configuration menu.

Network

► Select the menu *IP address* from the configuration menu.

IP address

► Slide the slide switch **(1)** to position *DHCP ON*. The IP address is allocated to the device automatically.

- The IP address can change in the mode *DHCP ON* during operation.
- The address fields for the direct input of the IP address are deactivated.

Manual allocation of the IP address

► Slide the slide switch **(1)** to position *DHCP OFF*.
► Tap on a number group of the *IP address* **(2)**. A keyboard with 10 keys is displayed (Fig. 17).
► Put in the IP address.
► Press the C *button* to correct your input.
► Confirm your input with *OK.* The keyboard is faded out.
► Tap on the *Back button* to get to the configuration menu.

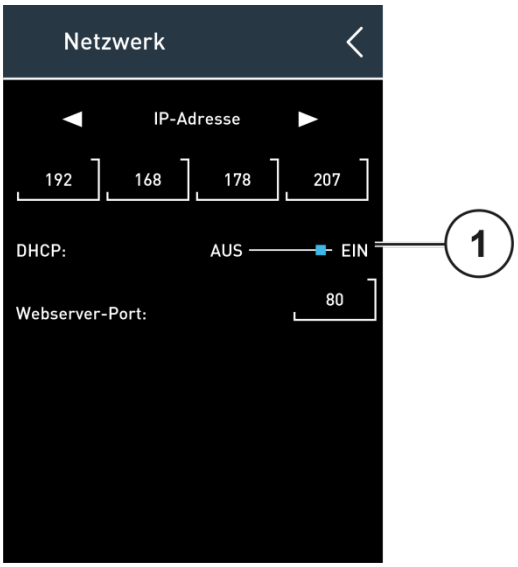


Fig. 16: IP address

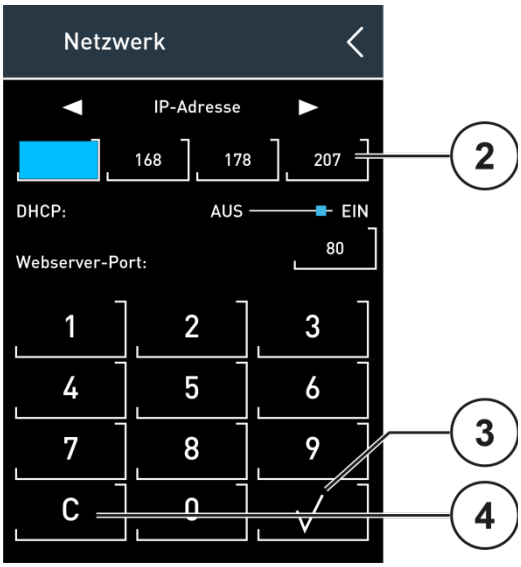


Fig. 17: 10-key keyboard

► Tap the *Scroll-Forward-Button* **(5)**, to change the address of the *Subnet*, the *Gateway*, the *DNS server 1* and *DNS server 2* (Fig. 18).

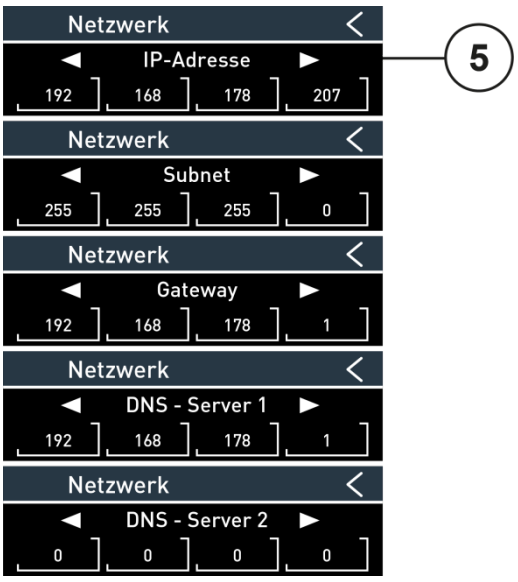


Fig. 18: Changing addresses

Intercom function for visitor communication

The Intercom function can be used to communicate with visitors, further for employees who, e.g. have forgotten their identification card. Due to the Voice over IP protocol SIP, the device is compatible to modern (video) telephony infrastructure. Thus, no additional end device is needed on the company side. The call can be forwarded to every Voice over IP end device that is accessible per network and SIP. The Intercom function is operated by selecting a contact person from the telephone list.

☞ *Further information on Setting up a phone book, you'll find in the chapter User (page 32).*

Trigger a call

If only one user is stored in the telephone book, the user can be called directly by tapping the phone book.

► Run your finger vertically over the telephone list and select your required contact.
- Alternatively you can skip to the contact with the selected initial letter by tapping the initial letter.

► Tap with the finger on the required initial letter.
► Tap the required entry. The required contact is called.

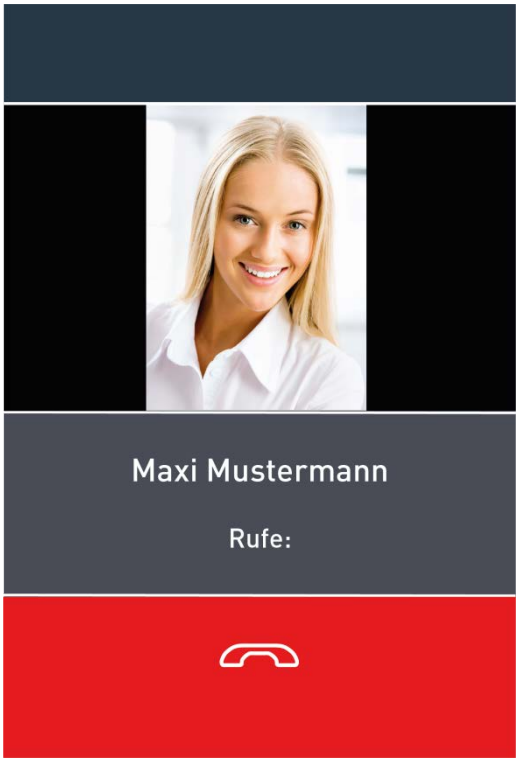


Fig. 19: Make a call

Cancel a call

► Tap the red handset. The call setup is cancelled resp. an established connection is terminated. The text *Call was cancelled* is displayed.

Accept a call

- If the call is accepted from the other part, the text *connected with: Maxi Mustermann.*

End a call

► Tap the red handset. The text *Connection interrupted* is displayed.

If an active call is not accepted within 10 sec from the call destination, no connection is established.

Control during a voice connection

- During an active voice connection to a telephone, image phone or Soft phone, orders can be entered via the telephone keyboard (Fig. 20).
- Depending on the end device, first the transmission of short cuts has to be permitted eventually.
- See the instruction manual of the end device under "SIP Info" resp. "DTMF signalling".

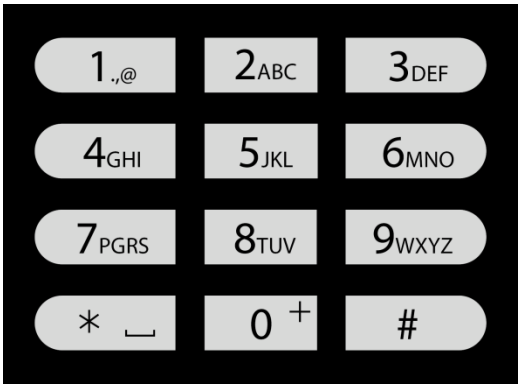


Fig. 20: Control buttons

7 PGRS **Door release relay 1**: By pressing the *key 7* the built-in relay 1 is triggered. Thus, the door release is controlled in standard. The message "Access granted" is displayed on the screen.

3 DEF **Accept a call**: By pressing the *key 3* a voice connection can be established.

9 WXYZ **End voice communication:** By pressing the *key 9* an established voice connection is terminated immediately.

2 ABC 4 GHI 5 JKL 6 MNO **Pan function**: The enlarged image section can be shifted upwards, downwards, to the left and to the right.

1 .,@ **Preset 1 function:** The modified image section is set back to its original position.

* ␣ **Zoom out:** The combination of a lower magnification with a larger image section provides an improved overview.

Zoom in: With a higher magnification and a smaller image section brings up details of the image.

0 + **Centre:** The image section is centred.

Set up the access control

The device offers 2 technologies for access control:
- RFID and/or
- access code

For assigning access rights to employees, their data needs to be added in the user list of the web interface and the accounts have to be released for access control.

In the web interface, there are comprehensive help texts to all fields.

Enrolment

Before using the access control, the RFID card of the user and/or a PIN must be linked to the system. This process is called Enrolment.

► Select the configuration menu *Enrolment* with the green RFID card.
► Select a contact from the phone list.
► Select one of the options PIN or RFID.

Fig. 21: Green RFID card

PIN:

► Tap PIN.
► Enter the required PIN via the numeric keyboard.
► Tap the check box to confirm. The information *New PIN stored!* is displayed.

PIN:
- minimum 3 numbers
- maximum 7 numbers
- PIN cannot start with a “0“
- PIN cannot be assigned twice
- PIN can be deleted only via web interface

RFID:

► Tap RFID. The notice *Please hold the new RFID card against the sensor!* is displayed.
► Hold the RFID card that is to be trained, against the RFID reader. The notice *Card added!* is displayed.

RFID cards:
- RFID cards have to fit to the reader that is built-in (MIFARE®, LEGIC, HID)
- the card that is to be trained, must not be one of the system cards (red configuration and green enrolment card)
- RFID card cannot be assigned twice
- RFID card can be deleted only via web interface

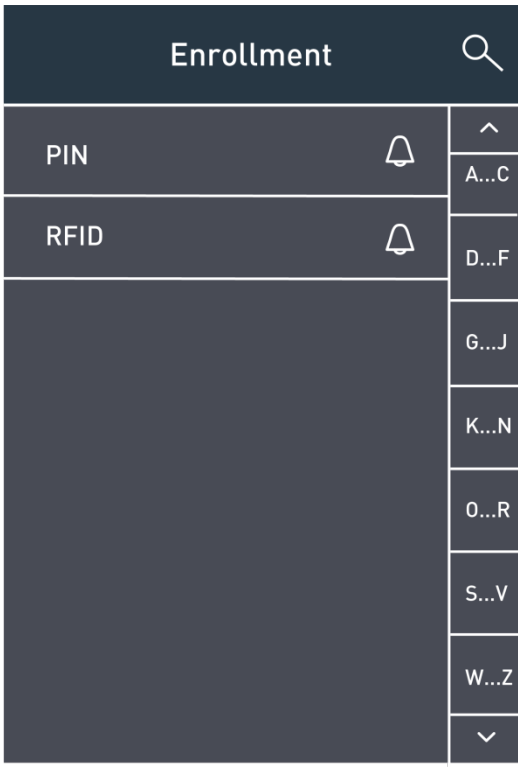


Fig. 22: Menu enrollment

Via the check box in the web interface menu Persons the access functions PIN and RFID can be selected and combined. The settings are stored in the personnel database.

Use the access control

Access via RFID card

► Hold the RFID card in front of the RFID reader. If an assigned card is recognised, access is granted.

	The card is recognised with a distance of 1 to 3 cm in front of the device.

	If the time registration is activated in the device, additionally the person is asked about whether he or she is coming or going.

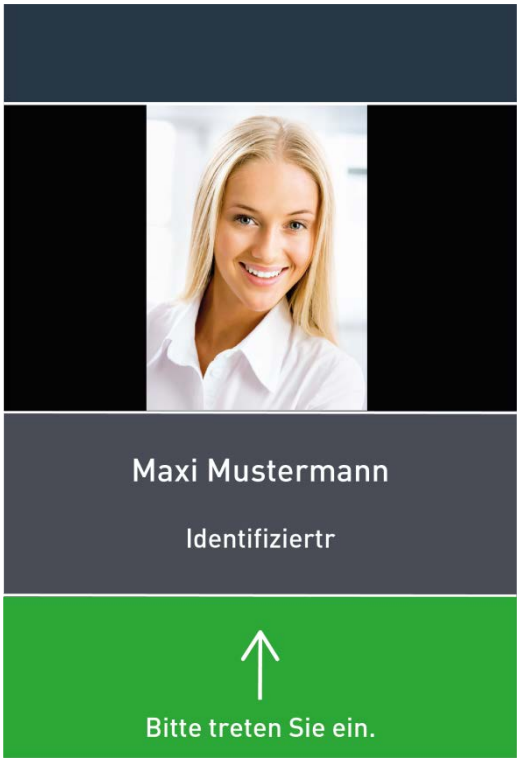


Fig. 23: access granted

Overview error messages RFID card

Error message	Cause	Solution
Card not accepted 	• The device does not know the RFID.	• Assign the RFID card to the device.
Access with card is not released 	• The device does know the RFID card, but no access rights are assigned.	• Put the missing check mark in the phone book entry.

Access with access code

► Swipe with your finger to the right to call up menu access via PIN.
► Enter your access code with the *10-key keyboard*.
► Correct your input with the C button.
► Confirm your input with the check mark. If the access code is correct, access is granted (Fig. 24).

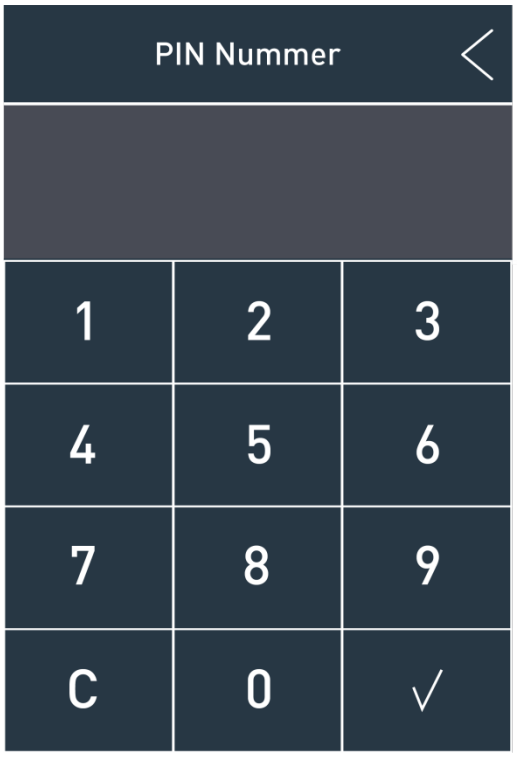
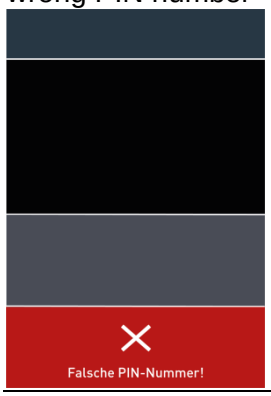
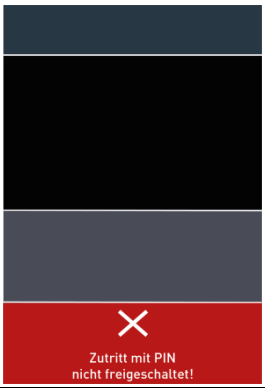


Fig. 24: Input of access codes

Overview error messages access code

Error message	Cause	Solution
wrong PIN number 	• A wrong PIN number was entered.	• Put in the correct PIN number.
Access with access code is not enabled for user. 	• The access code is blocked for access.	• Put the missing check mark in the phone book entry.

Set up video surveillance

- The function video surveillance provides an audio-visual control of the entrance area.
- The function is activated via a call from the outdoor device via the SIP or IP address.

- It is a hidden call. An active connection to the device is not visible.
- The video parameter can be adjusted during an active connection. The camera can be remotely controlled (swivel and tilt). You can zoom into and out of the image. (See *Control during the connection*, page 21).

- The bidirectional audio transmission provides an acoustic surveillance of the entrance area. The microphone of the telephone is deactivated, but it can be activated if necessary.

Loudspeaker on: The audio data from the indoor station are switched over to the loudspeaker of the ARGOS. The message *Connected* is displayed at the LCD screen.

Loudspeaker off: The audio output from the indoor station via the loudspeaker of the ARGOS is interrupted.

Extended configuration via web interface

The entire configuration of the device is implemented via the web interface. Thus, the device is equipped with an integrated HTTP server.
To use the comfortable configuration via web interface, the device needs to be connected to the Local Area Network (LAN).

- PC and ARGOS are connected to the same network.
- PA and ARGOS do use the same IP address range. Eventually, the IP address range needs to be adapted.

- Comprehensive help texts are available on the web interface.
- In principal, changes are only stored after confirming the assigned *SET button* .
- If pages are left without pressing the SET button, all changes get lost.

Home screen

The web interface consists of the following basic elements:

- Tree structure **(1)** on the left side with a hierarchical representation of all menus.
- Input window **(2)** with a complete overview of all menus.

The menus can be selected either via the icons **(3)** in the input window or via the tree structure **(1)**.

Persons

In the menu *User* you can set up the phone book.

► Select the menu *User* **(1)** from the tree structure.
► Click *New* **(2)**.
► Put in the user data into the text fields (Fig. 25).
► Click *SET* **(3)** to store the user.
► Repeat the steps for further entries.

Condition for the indication of a contact in the phone book is a *SIP URI* (network phone number) for each call destination.

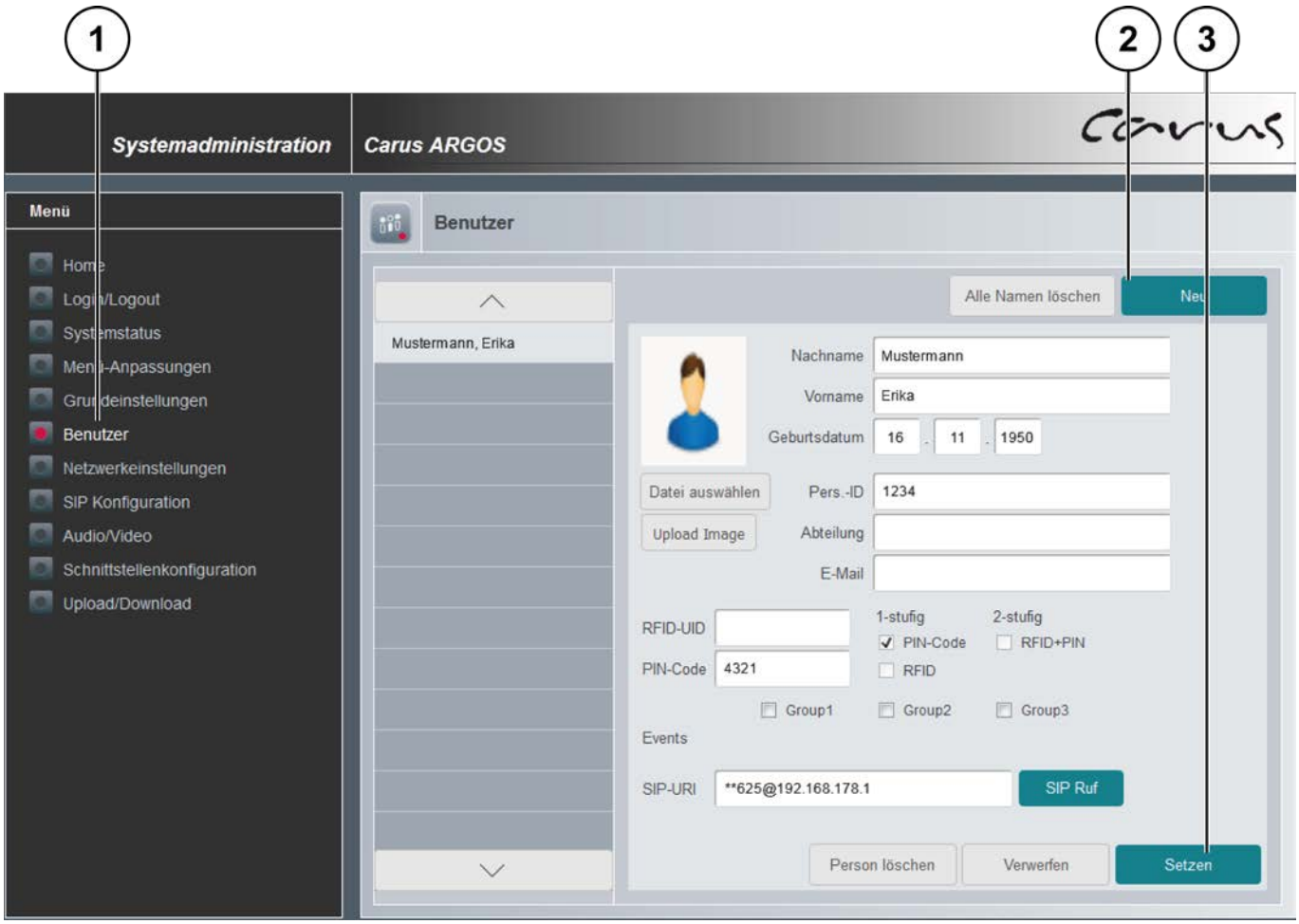


Fig. 25: Add user

The image for the *Upload Image* has to be a bitmap with 24 or 32 bit. The size of the image has to be 240 x 320 pixels.

If you have selected the telephone mode *Numeric* in the menu *Modifications*, put in the call number in the text field *Pers. ID* resp. the deposited number combination is used there.

Set up access control with RFID UID

► Select a user from the list.
► Put in the RFID card number in the text field *RFID UID*. The box *Access* with RFID is checked automatically.
► Click *SET*.

Set up access control with PIN code

► Select a user from the list.
► Put in a number with at least 3 digits into the text field *PIN code*. The box *PIN code* is checked automatically.
► Click *SET*.

PIN code:
- number with a minimum of 4 digits
- number with a maximum of 8 digits
- do put in a leading "0"

Access control with RFID UID and PIN code

- For security demands the two technologies for access control can be combined.

► Check the box **(1)** *2-stage*.
► Click *Save*.

- If user should no longer be able to have access via card, remove the check mark for *RFID*. Thus, the access with the assigned card is blocked. The card still is assigned to the user.
- If the card should be available again, delete the RFID UID number from the user account.

Fig. 26: combined access control

Groups

In the menu Groups you can assign several persons to a group.

One person cannot be assigned to several groups.

Fig. 27: Creating groups

1 persons from the phone book that are not assigned
2 persons that are assigned to a group
3 overview of the created groups
4 Settings

Login/Logout

Admin password

In delivery state the web interface is protected via default password. If you want to assign a new password, you can do this in this menu (Fig. 28).

	Keep the password carefully. If the password gets lost, you will not be able to access the web interface.

► Put in your password in the text field *Password* **(1)**.
► Put in your password again in the text field *Password confirmation* **(2)**.
► Tap the button *SET* **(3)**. Your new password is stored.

	default password user name: ***admin*** password: ***1234***

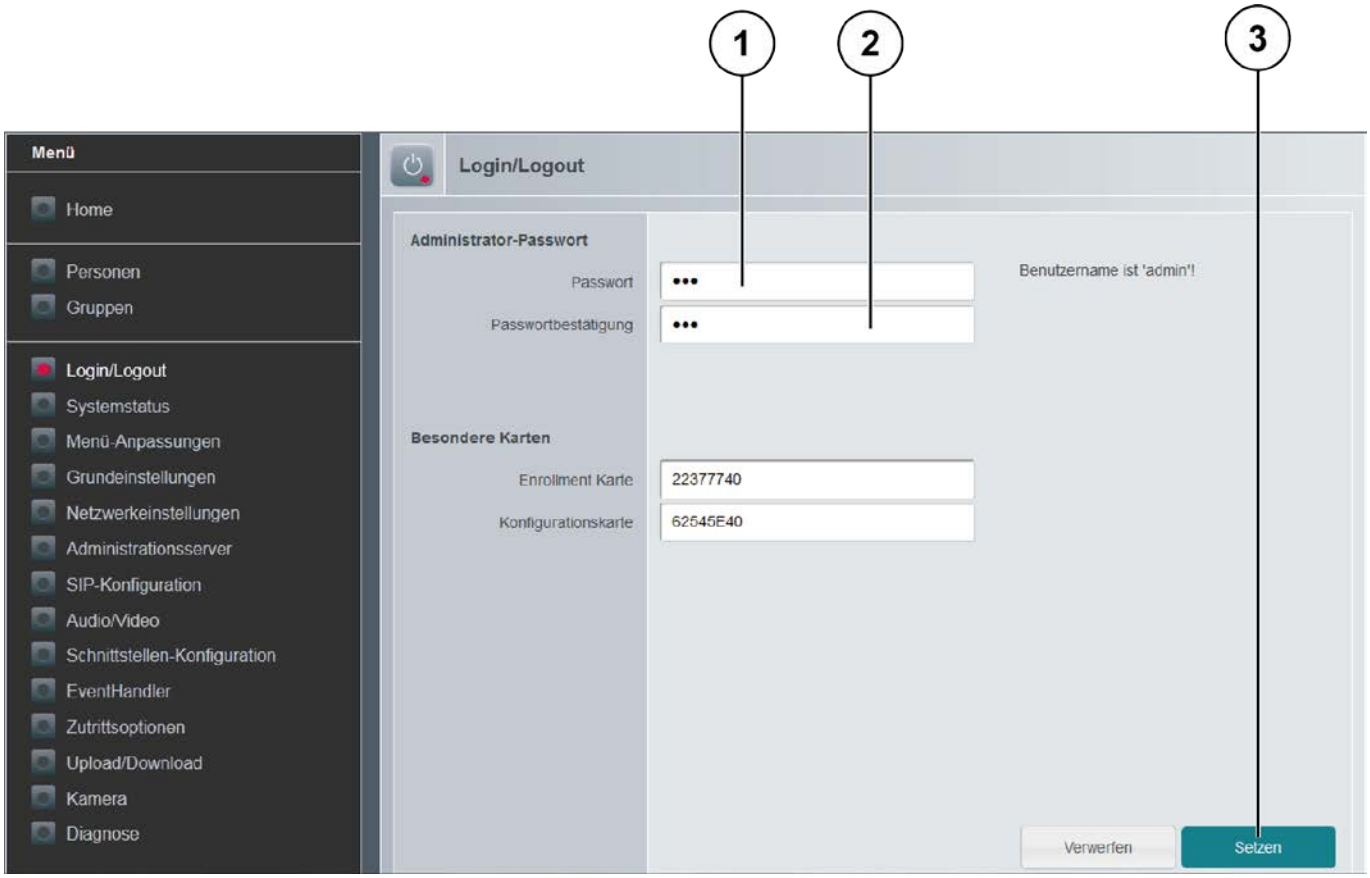


Fig. 28: Login/Logout

Special cards

With these cards you can open and close the LCD configuration. The assignment of the cards to the special functions is executed at the site of manufacture. If other cards should be used for these functions, the assignment can be changed in the following way:

***Option 1*:**

► Delete the two UID entries.
► Click *SET* to store.
► Hold the green card in front of the reader to open the LCD configuration. A message confirms the recognition of the card.
► Hold the red card in front of the reader to close the LCD configuration.
► Reload the web configuration. The new UIDs are displayed.

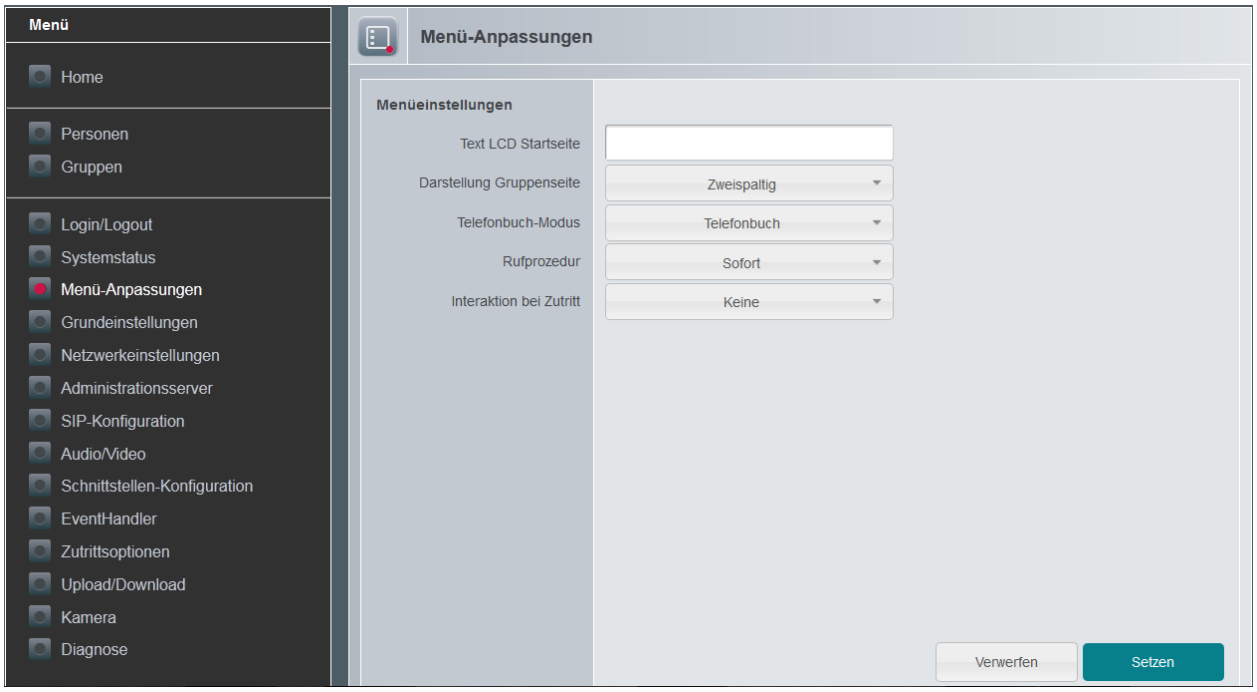
***Option 2*:**
► Put in the UIDs in the text fields *UID green card* and *UID red card*.
► Click *SET* to store.

The risk of wrong inputs is higher in case of a manual input of the UIDs. For this reason, exclusively use option 1.

System status

The *System status menu* is divided into the areas system data and system protocol. Ask your system administrator or IT manager in case of any questions relating to the system protocol.

Menu modifications



Individual lettering

In the menu *Modifications* you can customise the start screen with an individual lettering **(1)** or logo (Fig. 29).

A maximum of 21 characters can be displayed.

► Click the menu *Menu Modifications*.
► Enter your individual lettering into the text field *Text LCD start screen*.
► Click *SET*. The text is displayed on the screen.

Fig. 29: start screen

Indication of the group page

Groups can be displayed in 1 column or 2 columns.

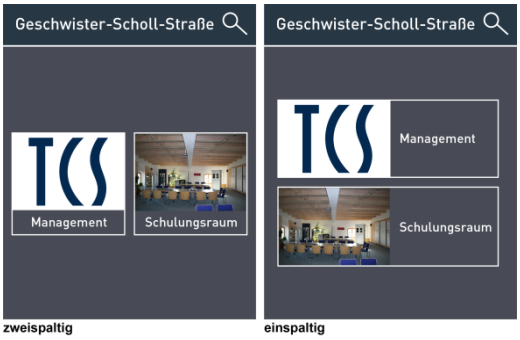


Fig. 30: group indication with 1 and 2 columns

Phone book mode

Here you can determine whether your required contact should be called via phone book or via numeric entry (call number).

► Click the button Phone book.
► Select the phone mode *Phone book* or *Numeric*.
► Click *SET*. Your changes are stored.

Make a call

With this setting you can select whether your required contact is called directly by pressing the phone book entry or the details of the contact are displayed first.

Basic settings

All general device settings are summarised in the menu *Basic settings* :

- *Language selection*
- *date/time*
- *LCD brightness*

Device date and device time: Internally the device is equipped with a real-time clock. In case of a voltage breakdown or when the device is transported, the clock continues its operation for more than a year. The chosen settings are preserved.

Network settings

In the menu *Network settings* you can make the following settings:

- *device name*
- *IP address*
- *subnet mask*
- *Gateway address*
- *DNS server 1*
- *DNS server 2*
- *Auto IP DHCP*
- *Server port*

- Changing the network settings should be handled with special care. If wrong values are put in, the device is no longer accessible by the web interface eventually.
- In this case the correct address has to be put it again via the LCD menu.

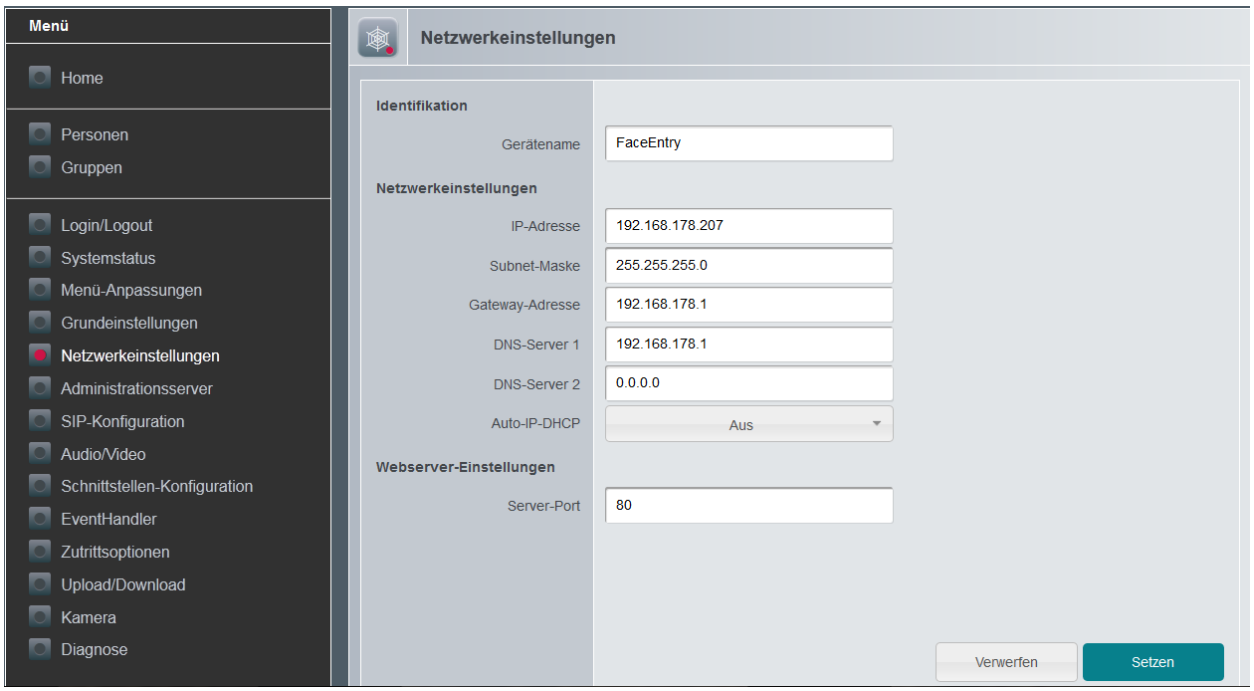


Fig. 31: Network settings

SIP configuration

The Intercom function is working according to the Voice-over-IP standard SIP. In combination with an external SIP server, further functions e.g. answering machine and call diversion can be used.

A full compatibility of functions from third-party providers cannot be guaranteed.

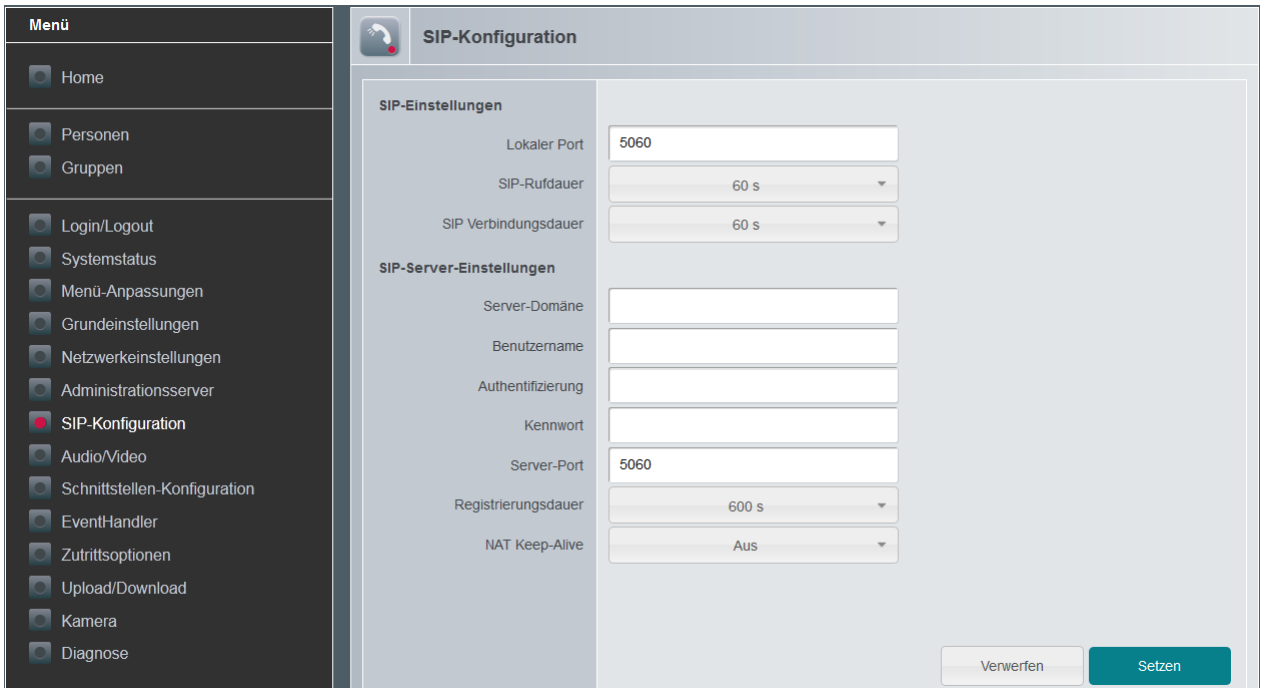


Fig. 32: SIP configuration

Audio/Video

The resolution for MJPG and H.264 can be changed only in the web interface.

All settings to transmit audio and video data can be made here.
Video formats:

- H.264
  - is used in combination with SIP
- MJPEG, JPEG
  - is used in combination with HTTP/TCP
  - a single JPEG image or a MJPEG stream can be requested via HTTP-Get
  - up to 15 streams can be displayed simultaneously
  - single image: <ip-Adresse>:<videoport>/singleframe or <ip-Adresse>:<videoport>/video.jpg
  - video stream: <ip-Adresse>:<videoport>/stream or <ip-Adresse>:<videoport>/video.mjpg

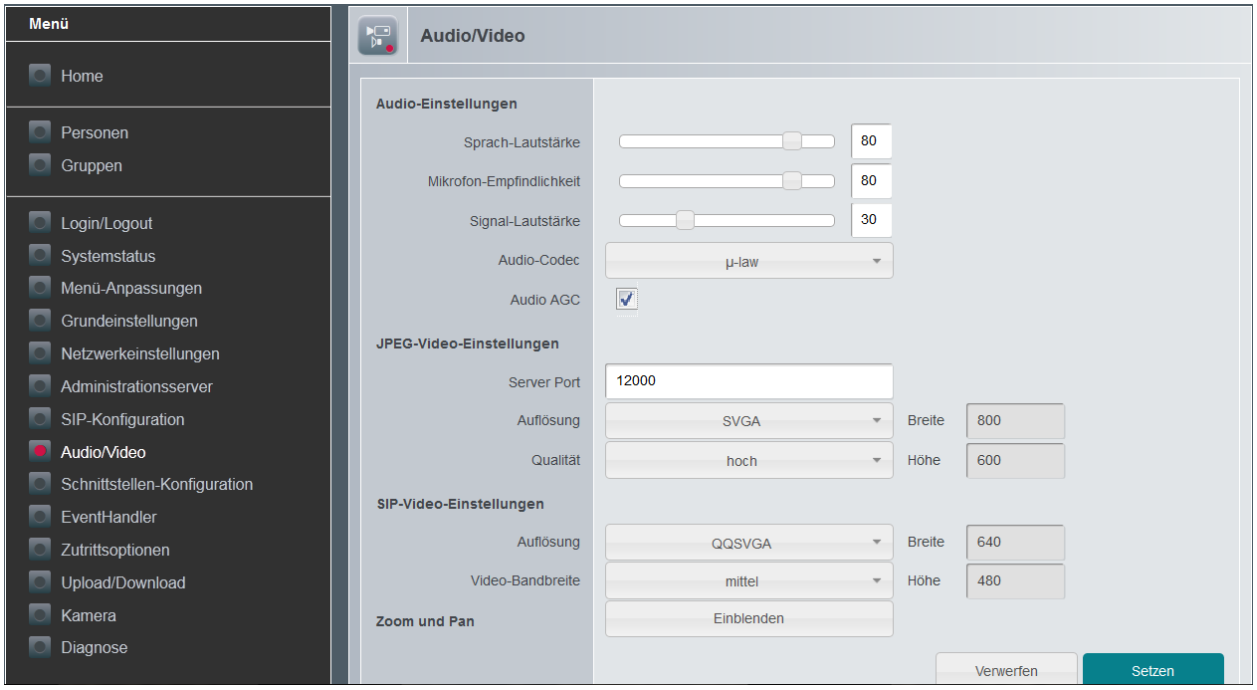


Fig. 33: Settings Audio/Video

Configuration of pan, tilt and zoom

- Settings can be made only in the web interface or directly at the device
- maximum 3 camera positions can be stored
- the zoom factor depends on the selected resolution (the larger the resolution, the lower the zoom)
- if the image resolution is identical to the camera resolution it is not possible to zoom or pan

► Click Display in in the menu Audio/Video the Live image as well as the menu Zoom/Pan is displayed.
► Click + or - to zoom in or out.
► Click the navigation buttons to scroll the image section.
► Click Save to store a selected camera position as fixed position.
► Click Set to store your settings.

Interface configuration

The device is equipped with 2 ports: a relay output and a serial interface. Both can be configured extensively.

> The available call destinations have to be configured previously in the menu *User* including the SIP URI.

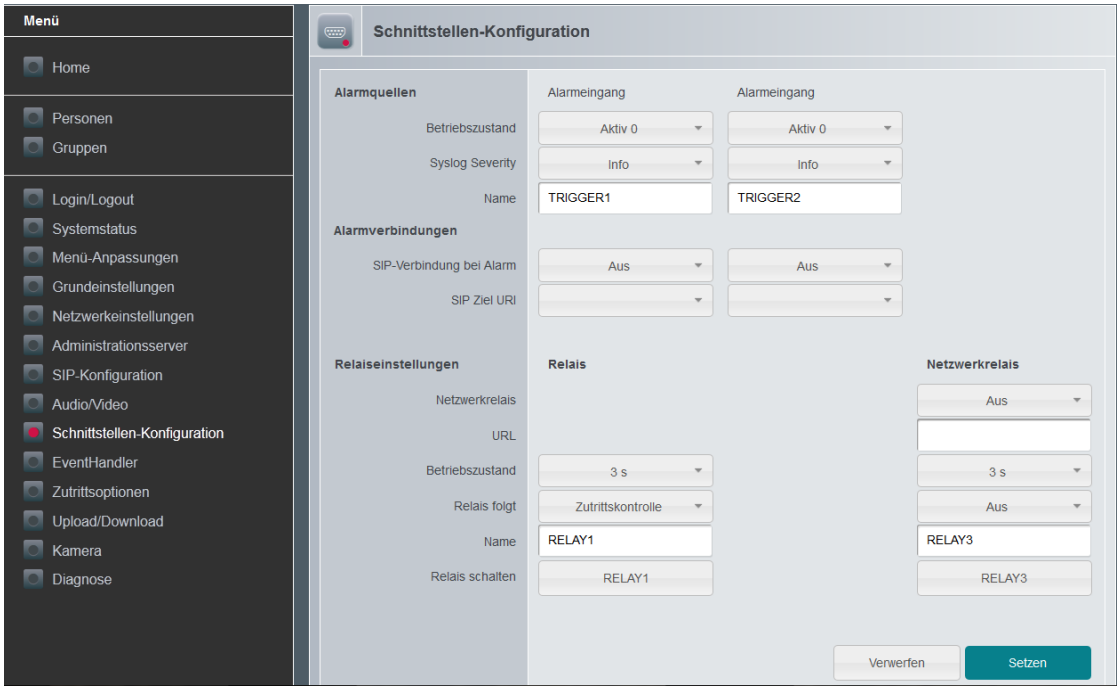


Fig. 34: interface configuration

Upload/Download

Via the menu item *Upload/Download* a new firmware can be installed on the device. The already installed firmware version can be read off in the menu *System status*.
Files for configuration and access can also be uploaded to or stored in the device. The download of configuration files is recommended for safety reasons (Backup) and for similar device configurations.

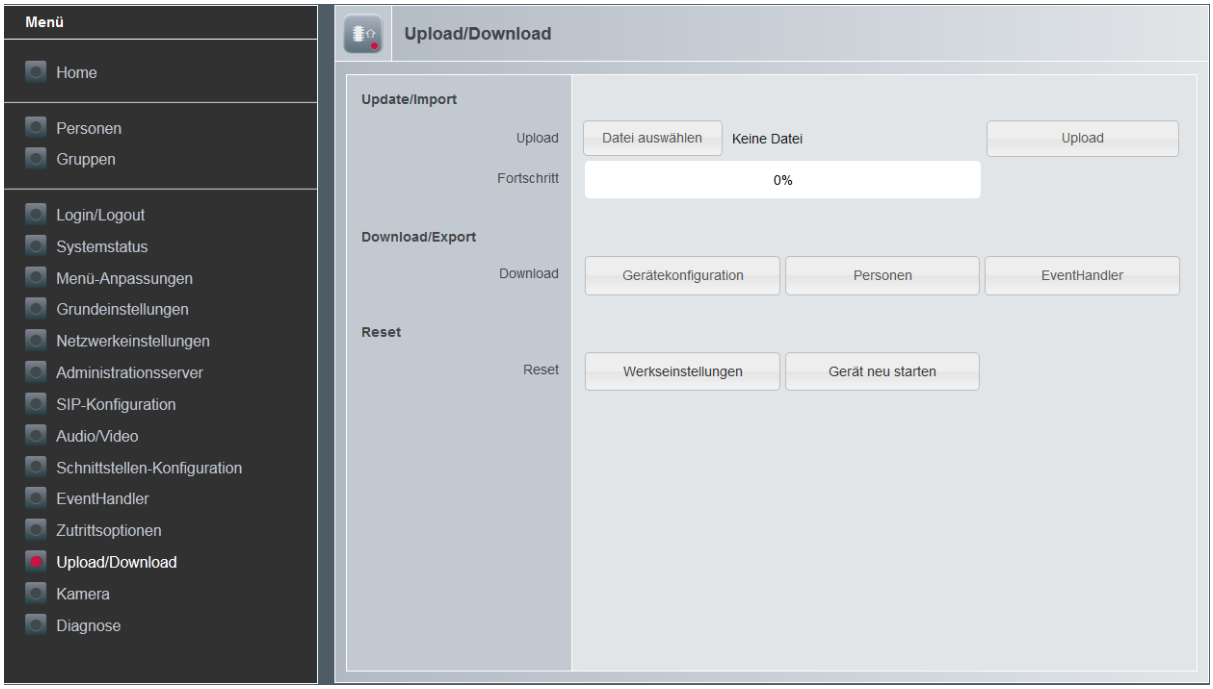


Fig. 35: Upload/Firmware

Cleaning

CAUTION! Device damage or malfunction caused by short-circuit and corrosion

Water and cleaning detergents that enter the device can cause short-circuits and corrosion of electronic components.
Avoid water and detergents from entering the device!

CAUTION! Damages on the surface of the device

Do not use any aggressive cleaning detergents for cleaning the surface of the device.

► Clean the front-door station with a dry or slightly wet cloth.
► Remove stronger stains with a pH neutral household cleaner.

Conformity

CE Declarations of conformity are available for download under *www.tcsag.de*, Downloads.

Information on disposal

Dispose the device separately from domestic waste via a collection point for electronic scrap. Ask your county administration for the responsible collection point.

Dispose the parts of the packaging in collecting tanks for cardboard and paper resp. plastics.

Warranty

We offer **a simplified processing** in case of warranty for qualified electricians.

- Please contact the **TCS HOTLINE** under **hotline@tcsag.de**.
- Our **standard terms and conditions of sale** fyou'll find under *www.tcsag.de*, Downloads as well as our current product catalogue.

Service

Please send your questions and inquiries to
hotline@tcsag.de

Headquarters
TCS TürControlSysteme AG, Geschwister-Scholl-Str. 7, 39307 Genthin | Germany
FON: Fax +49(0)3933 8799/-10 +49(0)3933 8799-11 www.tcsag.de

TCS Hotline Germany
FON: +49(0)4194 9881-188 FAX: +49 4194 988-129
Mail: hotline@tcsag.de

Subject to technical changes.

time of printing: 08/2018
PI_CAE3x02-IP-015x 1 A