Telecom Behnke

BEHNKE-STATION

AS INDOOR STATION

Technical Manual

Version 6.33

03/05/2026

! Important notes

Please note that Telecom Behnke products and accessories may only be installed and serviced by qualified electricians in compliance with all relevant safety provisions.
Before carrying out service and maintenance work, please ensure that the devices are safely disconnected from the power grid (unplug power supply unit) and are disconnected from any other network.

Prolonged direct exposure to sunlight may cause the device to heat up considerably, especially on devices with a dark front panel or when the device is installed in an insulated wall. n such a case, the device must be allowed to cool down sufficiently long before dismounting. Above all, be careful when touching the electronics housing!

To avoid security risks and unauthorised access, it is strongly recommended to change the passwords and codes provided at delivery and to deactivate functions that are not required.

For further legal information, please see the annexe.

Telecom Behnke GmbH
Robert-Jungk-Straße 3
66459 Kirkel
Deutschland / Germany

Info-Hotline: +49 6841 / 8177-700
Service-Hotline: +49 6841 / 8177-777

info@behnke-online.de
www.behnke-online.de

Télécom Behnke sàrl
15, rue du Parc
57600 FORBACH
France

Infoligne : +33 3 87 84 99 50
Hotline SAV : +33 3 87 84 99 55

info@behnke.fr
www.behnke.fr

Contents

Commissioning

Welcome.

The Behnke station is a high-quality hands-free station for professional use. It is available as indoor and outdoor station. This manual handles the indoor station.

The indoor station can be operated in different ways, namely as:

- SIP telephone on a SIP server (IP telephone system) or
  without SIP server together with other SIP telephones (direct SIP calls)
- IP intercom together with other devices

Typical areas of application of the indoor station are:

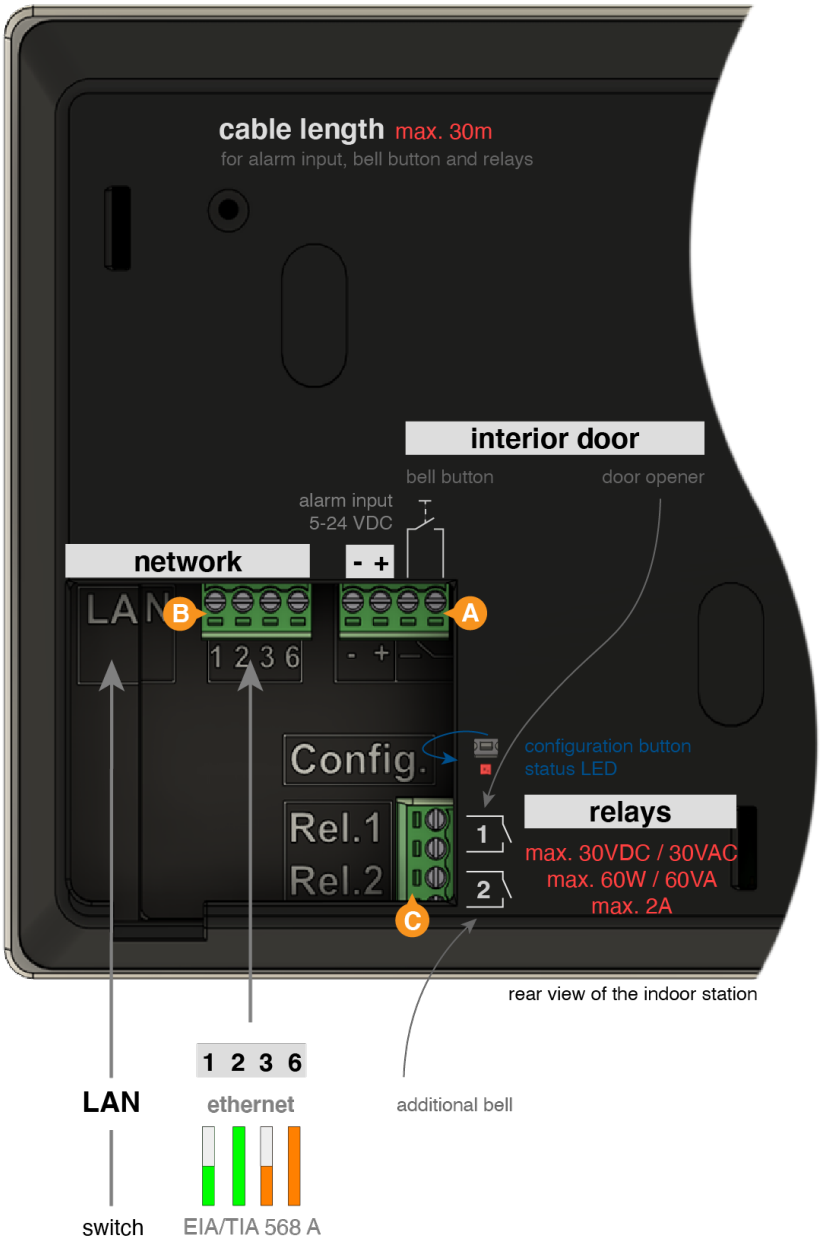
- indoor communication station to receive calls from the outdoor stations

This manual explains the Behnke station in general. This means that functions are also explained that may either not be available in your model or variant of the Behnke station or only if appropriate additional modules are connected.

If you have any questions about installation, if anything is unclear or if you have problems, please contact our

Service hotline: +49 6841 / 8177-777

Connection board



vue de face de la station intérieure

Connections

network

Usually the device is connected to a 100 Mbit/s Ethernet network.
To do this, the network cable arriving from the switch is connected to the RJ45 socket 'LAN'.
Alternatively, if the incoming network cable does not have a connector, the two wire pairs 1/2 and 3/6 can also be connected via the plug B.

energy supply

If the device is connected to a network port with PoE , the power is supplied via the network cable.
If the network is not to be connected via the RJ45 socket but via the green plug, this is only possible with a PoE variant in which the energy is transmitted via the same wire pairs as the data (1/2 3/6). With a PoE variant that uses the free wire pairs, the connection must be made via the RJ45 socket.
If PoE is not available or the device is to be connected to the network via a wireless network or not at all, then the device can be supplied via a Behnke PoE injector.

relays

The device has 2 relays which are connected via the plug C. Relay 1 uses the two left terminals and relay 2 the two right terminals of the plug.
These are voltage-free switching contacts. The maximum values for switching voltage, switching current and switching capacity indicated in red must all be respected(cable length max. 30m).
For relay 1, the function as a door opener relay with normally open contact is preset and for relay 2 that the contact is closed while the ringing of an incoming call.
If other functions are required, for example a door opener relay with a NC contact or 2 door opener relays, this can be configured accordingly.

alarm input

An information can be transmitted to the device by a suitable DC voltage via the alarm input in order to trigger an action, for example a call or opening the door.
The voltage is connected to the two left terminals of the plug A (cable length max. 30m) , observing the polarity.

interior door

An interior door is the access to the area in which the indoor station is installed and where no Behnke-Station is installed.
If the interior door has a bell button and/or a door opener, it is possible to connecte these to the indoor station. If the bell button is pressed, a signal is sent to the indoor station and it is possible to activate the door opener of the interior door to open it.
The bell button (normally open contact, cable length max. 30m) is connected to the two right terminals of the plug A and the door opener to relay 1.

Startup

In most cases, the device is supplied with power via PoE, i.e. by connecting the network cable. If a PoE supply is not possible, the power supply can alternatively be implemented by connecting a Behnke PoE injector.

The start-up process begins as soon as the device is supplied with power.

Shortly thereafter, the status LED is switched on and lights up red continuously.

After about 20 seconds the software starts and a high-pitched beep is emitted and the Behnke logo is shown on the display.

Then the network is activated.

As soon as the device has an IP address, this is either announced if the device is in the delivery state, or a dark tone is emitted. The display briefly shows the IP address.

When the startup process is complete, the status LED changes. More information on this in the section status LED.

With a device in the delivery state, the configuration button can then be used to set the language and the operation mode.

If the device does not start as described here, read the section System startup problems in the annexe.

Configuration button

The configuration button is located on the connection board in the centre right-hand area under the rear panel cover.

configuration button for an unconfigured device in the delivery state

Important note

Although it is possible to perform a minimal initial configuration of the indoor station using the configuration button, it is strongly recommended that you perform the initial configuration using the touchscreen, as this is more detailed, easier to understand and simpler.

When you press the configuration button, you will first be asked to select the language.

So press the configuration button 4 times for English.

Then select the desired operation mode. So press the button
3 times for SIP phone or
4 times for intercom mode.

When used as an intercom, the intercom group must still be defined. All devices in the same group form together a sub-intercom. In simple cases, all devices belong to intercom group 1. In more complex cases, the devices can be distributed into different groups.

So, to set the desired intercom group, press the button

1 time for intercom group 1
2 times for intercom group 2
:
9 times for intercom group 9

When used as an intercom system, the intercom ID of the indoor station must also be specified. This is used within the intercom group to assign the buttons on the outdoor stations to the indoor stations.

In 'intercom mode', buttons for which no call number is configured call their button number: button 1 calls ID 1, button 2 calls ID 2, and so on.

To set the desired intercom ID, press the button

1 time for intercom ID 1
2 times for intercom ID 2
:

9 times for intercom ID 9

After selecting the operation mode respectively the intercom group and intercom ID , the settings made are saved. After this, these settings can no longer be changed using the configuration button, unless the device is reset to the factory settings.

It is always possible to change the selected settings via the web interface or the configuration mode.

configuration button for a device that has already been configured

Press the configuration button
1 time to announce the options,
2 times to announce the IP address,
3 times to start/terminate the network configuration mode,
4 times for explanations on how to access the device via WLAN or
for at least 5 seconds to reset the device to factory settings.

If you want to reset the device to factory settings, press the configuration button for at least 5 seconds. The device then emits a beep and asks for confirmation by pressing the configuration button twice. After confirmation, the factory settings are reset and the device restarts. If there is no confirmation, the process is cancelled.

Status LED

The status LED is located on the bottom left of the connection board, directly below the configuration button. Depending on the operation mode and the status of the device, it lights up or flashes in certain colors.


start phase


reboot


SIP phone: all configured SIP accounts registered


SIP phone: configured SIP accounts only partially registered


SIP phone: no SIP account registered


SIP telephone for direct SIP calls


SIP telephone for direcct SIP calls without network


intercom mode


intercom mode without network

hybrid mode


hybrid mode: not all configured SIP accounts are registered


sabotage detected / safety shutdown activated

temporary shut down due to high temperature

firmware update

hardware error, see section System startup problems in the annexe

Implementation of an IP intercom system

Use of Behnke stations as an IP intercom system

Behnke stations can be used as IP intercoms if at least one outdoor station and one indoor station are connected to a common IP network.

In addition to this simple minimal system, more complex installations with up to 9 groups and up to 100 devices, which can be distributed across multiple networks, are also possible.

A very interesting variant is the hybrid mode. This allows an outdoor station to be operated simultaneously as a SIP phone and as an IP intercom. Buttons can then trigger calls via the SIP telephone system as well as establish connections to indoor stations in intercom mode, even in parallel.

The IP intercom system does not require a server, as Behnke stations can communicate directly with each other within their network. If the devices are distributed across different networks, cross-network communication can be enabled by setting up network bridges. However, it is essential that all devices in the intercom system are able to communicate with each other via the IP network.

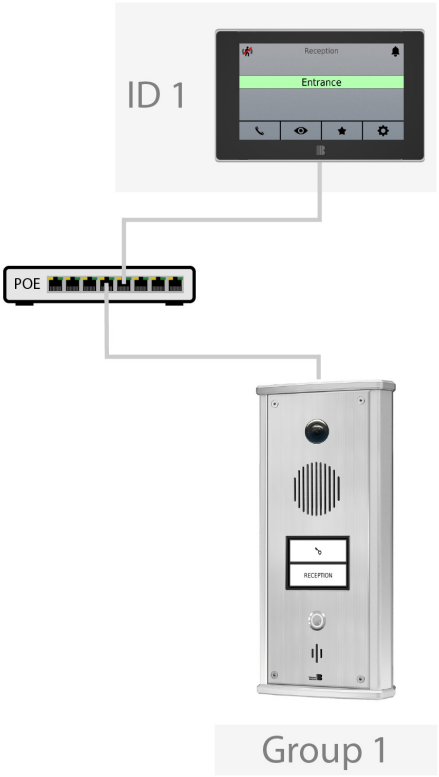
To use Behnke stations as an IP intercom system, observe the following points:

- The administrator password is a global setting and must be the same for all intercom devices.
- Each device belongs to a group. An intercom system can be divided into up to 9 groups.
- Outdoor stations have no ID. Indoor stations have an ID between 1 and 99.
- All outdoor stations of the same group are displayed in the phone book of an indoor station.
- An outdoor station can call indoor stations in the same group by dialling the ID as the call number.
- In the 'IP intercom' operation mode, buttons for which no call number is configured dial their button number: button 1 calls ID 1, button 2 calls ID 2 and so on. As a result, the buttons of an outdoor station are already assigned to the indoor stations of the same group in delivery state.
- A door opener code can be configured for each indoor station. This code can then be used at all outdoor stations in the same group that have a code lock function.
- All intercom devices require firmware version 5.85 or newer. Ideally, the firmware is synchronised, i.e. all devices use the same version.

Important note

Various application scenarios are explained below by way of example.
The examples focus exclusively on the commissioning and software configuration of the intercom devices. Proper mechanical assembly and electrical installation are assumed and are not covered.
For outdoor stations, this applies in particular to the connection for opening the access point, for example a door opener or a barrier. We assume that this is available and functional.

Minimal system



A minimal system requires the following components:

- 1 PoE/PoE+ switch
- 1 Behnke outdoor station
- 1 Behnke indoor station
- 2 network cables

In our example, we are using a Behnke All-in-one outdoor station. However, any other Behnke outdoor station, typically with a camera, can be used. However, a PoE+ switch is required for an outdoor station with a hearing loop.

We assume that the Behnke stations are in their delivery state.

For the minimal system, we only need a single intercom group, intercom group 1, in which we classify both Behnke stations.

Step 1: PoE switch

- Connect the switch to the power supply to put it into operation.
- In general, no special configuration of the switch is required.

Step 2: Behnke outdoor station

COMMISSIONING THE DEVICE

- Connect the outdoor station to the switch.
- The status LED on the rear lights up red and the device starts up.
- The device first attempts to obtain an IP address from the DHCP server. If there is no DHCP server, it performs a fallback to link-local and assigns itself an IP address in the 169.254 network.
- After about one minute, the self-assigned IP address is announced.

INITIAL CONFIGURATION

The initial configuration can be carried out using the configuration button on the rear or, for devices with a display, via the display. The initial configuration using the configuration button is described below.

- start initial configuration => press the configuration button once
- set language => press 4 times = English
- set operating mode => press 4 times = intercom mode
- set intercom group => press once = intercom group 1

This completes the initial configuration of the outdoor station.

Step 3: Behnke indoor station

START UP THE DEVICE

- Connect the indoor station to the switch.
- The device starts up, then also performs a fallback to link-local and assigns itself an IP address in the 169.254 network.
- After about one minute, the self-assigned IP address is announced.

INITIAL CONFIGURATION

It is strongly recommended that you perform the initial configuration of an indoor station via the display, as this is more detailed, easier to understand and simpler than using the configuration button on the rear. The configuration via the display is described below.

Selections and entries are confirmed by pressing the ✓ button. If an error occurs, you can return to the previous screen by pressing the ⮌ button.

- set language => press British flag
- select operation mode => select intercom mode
- select intercom group => select 1
- select intercom ID => select 1
- set name => enter Reception
- configure interior door => select no
- enter code for code lock => enter 1234
- automatic preview => select allow

This completes the initial configuration of the indoor station.

Step 4: Detailed configuration

The basic system is now ready for operation.

Further refinement of the configuration can now be carried out via the indoor station. To do this, use the indoor station's configuration mode, which can be started using the ⚙ button at the bottom right of the screen.

The indoor station's configuration mode can be used to change the configuration of the indoor station itself, as well as any other Behnke station that belongs to the IP intercom system.

As the name of the outdoor station has not yet been specified, it uses its host name. This is Behnke-station-1 followed by 5 further digits. The outdoor station is already displayed under this name on the main screen of the indoor station. The name of the outdoor station should now be changed to Entrance.

RENAME OUTDOOR STATION

- enter configuration mode by pressing the ⚙ button
- enter admin as administrator password
- select outdoor station Behnke-station-1.....
- configuration is loading
- select General
- select Name of the station

- enter Entrance
- press the SAVE button
- configuration is being saved
- press the ⮌ button and then exit configuration mode with YES

There are some settings, such as the administrator password, that must be configured uniformly on all devices in the IP intercom system. These are called global settings . Ensure that all devices are installed and operational before changing global settings.

We want to change the administrator password for all devices to admin2 as an example.

In addition, the IP address assignment of the devices should be changed to link-local. The devices will then immediately assign themselves an IP address in the 169.254 network and will not need to fall back to link-local.

CHANGE GLOBAL SETTINGS

- enter configuration mode by pressing the ⚙ button
- enter admin as administrator password
- select Global settings
- select Administrator password
- delete current password with ⌫ and enter admin2
- select IP address assignment
- select link-local
- press the SAVE button
- global settings are saved in all devices
- configuration mode is exited automatically
- devices restart and update their network configuration

Step 5: Usage

The minimal system is ready for operation.

In step 3, we gave the indoor station the name Reception and the intercom ID 1. This means that call button 1 on the outdoor station is automatically assigned to the indoor station. As our outdoor station has a display, call button 1 is shown and labelled with the name of the indoor station, i.e. Reception.

In the case of an outdoor station with a physical call button, the label on the button must of course be adjusted manually.

CALL FROM THE OUTDOOR STATION

- press call button Reception on the outdoor station

- press call button Reception on the outdoor station
- connection to the indoor station is established
- ringing tone on the indoor station and display of the video image from the outdoor station
- controls on the indoor station:
  accept call
  open door
  reject call / hang up
  adjust volume of indoor station

Important note

In intercom mode, the codes for the code lock function are set in the indoor station and not in the outdoor station. Each indoor station can set its own code, which can then be used for the code lock function at all outdoor stations in the same intercom group.

In step 3, we set the code 1234 for the code lock function during the initial configuration of the indoor station. Since our outdoor station has a display, the button can be displayed to use the code lock function.

For an outdoor station without a display, a physical keypad is of course required to use the code lock function.

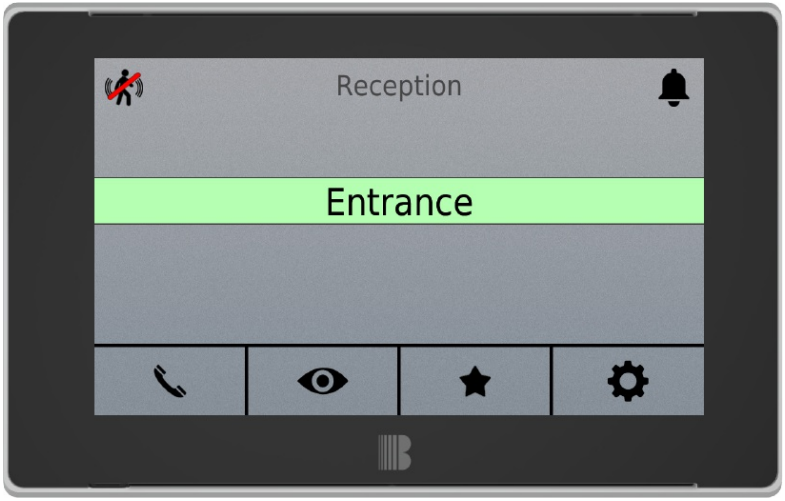
CODE LOCK FUNCTION OF THE OUTDOOR STATION

- press on the outdoor station
- enter 1234 as the code and confirm your entry with #
- door opens

All outdoor stations belonging to the same intercom group are displayed on the main screen of the indoor station Reception.

In a minimal system, this is only the outdoor station Entrance. In a system with more outdoor stations, additional arrow keys are displayed, which can be used to select an outdoor station.

The currently selected station is marked by the coloured bar (green by default).



OPERATING THE INDOOR STATION

- call station
- open preview (video/call/door open)
- set/cancel preferred device (= ☆)
- search for station by initial letter
- call up configuration mode

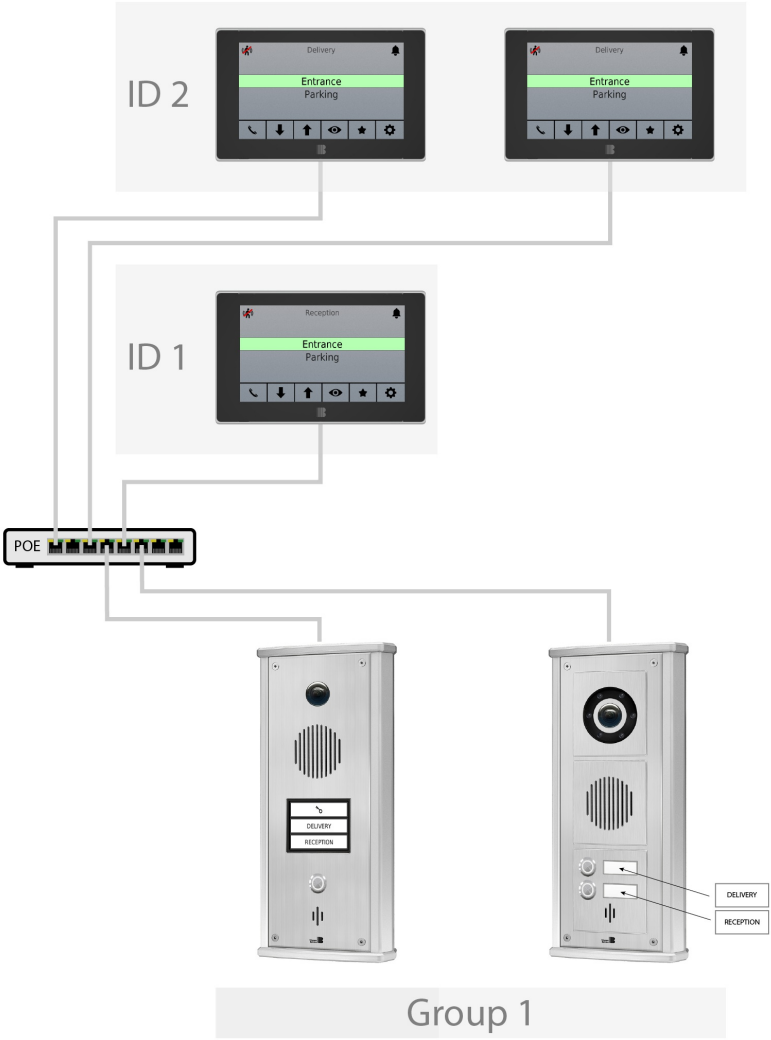
- automatic preview off
- automatic preview of preferred device
- automatic preview of preferred device not available
- automatic preview on

- play ringtone
- mute ringtone
- play low ringtone

- automatic preview history
- call history / last incoming call

- return
- answer call
- open door
- reject call / hang up
- adjust indoor station volume

System with multiple outdoor and indoor stations



Next, we want to expand the minimal system with an outdoor station with two call buttons and two additional indoor stations. The outdoor station is to be installed at the parking and the two indoor stations at different locations in the delivery area.

Both outdoor stations should call the indoor station at reception with the first button and the two outdoor stations in the delivery area with the second button.

Only one intercom group is required for this system, so we will assign all Behnke stations to intercom group 1.

OUTDOOR STATION

- carry out commissioning and initial setup as for the minimal system
- wait briefly after initial setup
- after about 1 to 2 minutes, the device will be automatically integrated into the existing intercom system

  The integration will apply the global settings:
  administrator password: admin2
  IP address assignment: link-local

- outdoor station restarts and updates its network configuration
- wait until the outdoor station is displayed on the indoor station
- rename the outdoor station as shown in the minimal system in Parking

- label the call buttons:
  call button 2: Delivery
  call button 1: Reception

This completes the setup of the outdoor station. Call button 1 can now be used to call the indoor station Reception.

INDOOR STATIONS

Since the two indoor stations of the Delivery are to be called using the second call button, they are both assigned the intercom ID 2. When call button 2 is pressed, both indoor stations are called simultaneously.

- perform commissioning and initial setup as for the minimal system
- select intercom ID => select 2
- set name => enter Delivery
- enter administrator password => enter admin2

This completes the setup of the indoor stations.

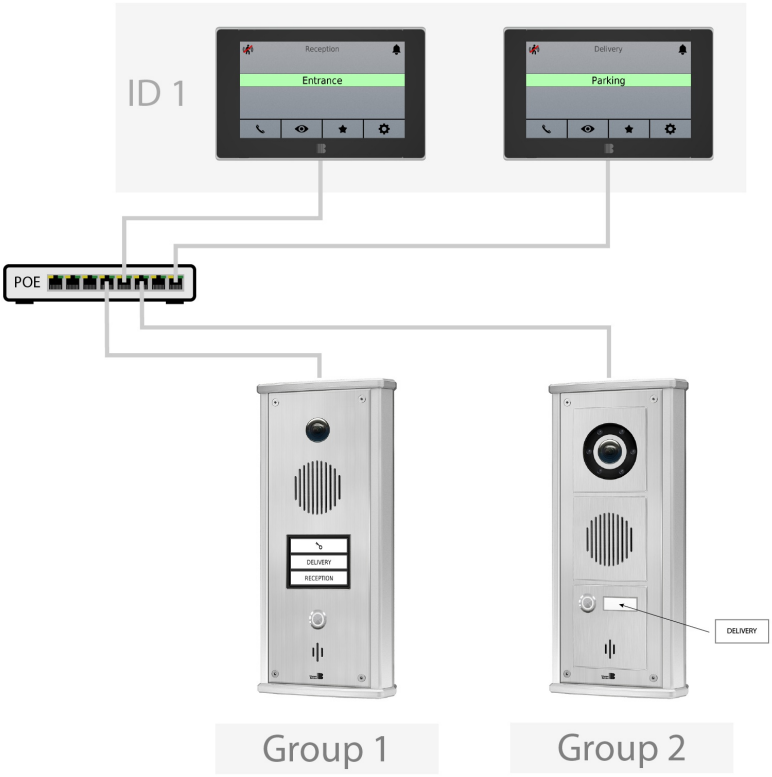
GLOBAL SETTINGS

To ensure that the global settings are the same in all devices after adding Behnke stations, use an indoor station that was already in the system and proceed as follows.

- enter configuration mode by pressing the ⚙ button
- enter admin2 as administrator password

- select Global settings
- press the SAVE button
- global settings are saved in all devices
- configuration mode is exited automatically

System with multiple intercom groups



In the following example, an outdoor station at the entrance is to call the indoor station at reception, and a second outdoor station at the parking is to call a second door station in the delivery area.

To implement this system, the intercom system is divided into two intercom groups, 1 and 2. The outdoor station at the entrance and the corresponding indoor station at reception are placed in intercom group 1, and the other two devices are placed in intercom group 2.

INTERCOM GROUP 1

- outdoor station at the entrance & indoor station at reception
- setup as for the minimal system (except for global settings)

INTERCOM GROUP 2

- outdoor station at the parking & indoor station at delivery area
- setup as for minimal system (except global settings), but:
  - intercom group: 2
  - name of indoor station: Delivery
  - name of outdoor station: Parking
- label outdoor station button with Parking

GLOBAL SETTINGS

- change after all devices are installed and ready for operation
- procedure as for the minimal system

This completes the setup and the system is ready for operation.

We now want to extend the example with the following functionality: If the outdoor station at the entrance calls the indoor station at reception, but reception does not answer the call, the indoor station in the delivery area should be called.

No telephone number has been configured for button 1 of the outdoor station Entrance. In intercom mode, an unconfigured button dials its button number (i.e. 1 for button 1) to call the indoor stations with intercom ID 1 in the same intercom group.

So if we configured the call number 1 for button 1, the behaviour would be identical.

Instead of just dialling the intercom ID, you can also specify the intercom group by dialling a 3-digit call number. The first digit is the intercom group (1-9), followed by the 2-digit intercom ID (01-99).

To call intercom ID 1 of intercom group 2, you would dial the number 201.

This enables cross-group calls and assignments. We need this to implement the required functionality.

To first call intercom ID 1 (1) of your own intercom group and then intercom ID 1 of intercom group 2 (201), we need a call chain (;). This means that we have to configure 1;201 as the call number.

The necessary configuration can be carried out via one of the two indoor stations.

INDIVIDUAL BUTTON CONFIGURATION

- call up configuration mode by pressing the ⚙ button
- enter administrator password
- select outdoor station Entrance
- configuration is loading
- select Button 1
- select Call number
- enter 1;201
- press the SAVE key
- configuration is being saved
- press the ⮌ button and then exit configuration mode with YES

This completes the individual configuration of the button.

Since the outdoor station Entrance is now also assigned to the indoor station Delivery via the individual button configuration, it is also displayed in the phone book of the indoor station Delivery to enable preview, call and door opening.

The assignment also means that the code for the code lock function of the Delivery indoor station can also be used for the code lock function of the entrance outdoor station.

More complex application scenarios

In many cases, an intercom system can be configured via an indoor station, as shown in the previous examples.

The configuration mode of an indoor station can be used to configure the indoor station itself, but also any other Behnke station in the intercom system. The configuration mode allows you to change the most important settings, but not all of them.

More complex application scenarios, such as hybrid mode or the implementation of a multi-network intercom system, require settings that are not possible via the configuration mode. In such cases, the devices can be accessed via the web interface in order to access the full range of settings.

In addition, the web interface displays the topology of the intercom system in the 'IP intercom' section. The topology is a list of all Behnke intercom stations and shows how they are divided into intercom groups. The topology also allows you to easily switch to the web interface of the other devices.

The 'IP intercom' section also includes synchronisation, which allows you to easily install new firmware on all Behnke stations of the intercom system, and the option to set up a network bridge for implementing a multi-network intercom system.

Hybrid mode

Behnke outdoor stations are often connected to a SIP telephone system as a SIP phone. Any telephone can then be called via the telephone system.

If the outdoor station has a camera, the camera image can either be displayed on a PC in conjunction with the IP video software or via SIP video on a SIP video phone.

If the SIP telephone system does not support SIP video or if no SIP video telephone or PC is available, a Behnke indoor station can also be used.

We assume that a Behnke outdoor station has been successfully set up and is operating in 'SIP phone' mode. A Behnke indoor station is now to be installed in the same IP network, which is called in intercom mode using the button 2.

For implementation, we only need intercom group 1. The indoor station is assigned intercom ID 1.

Since the outdoor station is used in the main operation mode 'SIP phone', if we want to make a call to the indoor station using button 2, we must specify in the call number with the prefix com: that it is an intercom call. Since we want to call intercom ID 1, we configure the call number com:1.

INDOOR STATION

- perform commissioning and initial setup as for the minimal system, but:
  - use the administrator password of the outdoor station as the administrator password

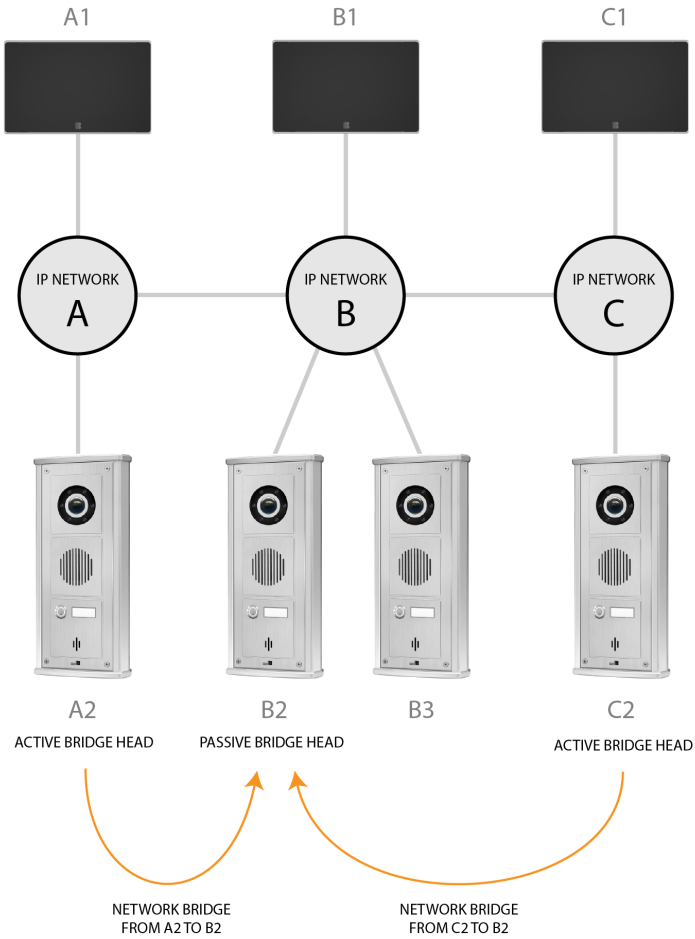
OUTDOOR STATION

Since the outdoor station is already set up as a SIP phone, further setup is carried out via the outdoor station's web interface. Proceed as follows.

- log in to the outdoor station's web interface
- activate hybrid mode in the 'General' section & SAVE
- the device can now also be used in intercom mode
- set the intercom group to 1 in the 'Intercom' section & SAVE
- in the 'Buttons' section, configure the name Reception and the call number com:1 for button 2 & SAVE

This completes the setup and the system is now ready for use.

Multi-network intercom



Intercom devices can automatically find each other within the same network and exchange information.

If the devices are distributed across several networks, it is necessary to connect the networks with each other by setting up network bridges.

To set up a network bridge, specify in the 'IP intercom' section via the 'Remote station'

setting the IP address or host name of a device in another network.

This makes this device the active bridgehead. It attempts to establish a connection to the remote station, the passive bridgehead. If this is successful, the bridge goes 'online' and information is regularly exchanged in both directions.

If the devices are distributed across more than two networks, additional network bridges can be set up.

Important notes

- For a multi-network intercom system to function reliably, every device in the intercom system must be able to reach every other device directly via the network - regardless of which network it is in.
- If the passive bridgehead is specified via an IP address that it has received via DHCP, it is essential to create a reservation for this address so that it does not change.
- The same device can take on the role of one active bridgehead and up to 3 passive bridgeheads.
- If a bridgehead fails, it can take up to 3 minutes before this is recognised and the devices previously transmitted via the bridge are removed.
- A network bridge always works in both directions. It is not necessary to set up a network bridge for the return path.
- If you set up a bridge between A and B and another one between B and C for networks A, B and C, then A is also connected to C. It is not necessary to set up a network bridge between A and C.
- To avoid unnecessary network traffic, you should refrain from setting up unnecessary network bridges.

Firmware synchronisation

Synchronisation allows new firmware to be easily installed on all devices in the IP intercom system.

SYNCHRONISATION

Synchronisation is carried out via the web interface of a Behnke station and takes place in two steps:
- step 1: install new firmware on one device
- step 2: distribute new firmware to all other devices

- log in to the web interface of a Behnke station
- select the 'IP intercom' section
- click on 'check for update' under 'synchronisation'
- download the latest firmware version
- click on 'update' and install the new firmware

- wait until the firmware update has been successfully completed

- log in again and select the 'IP intercom' section
- click on 'synchronise'
- the firmware is distributed to all devices that have a different version
- devices will install the new version and then restart

Once all devices have installed the new firmware, the firmware status will change to 'synchronised' and synchronisation will be complete.

Important notes:

- In the delivery state or after a hardware reset, synchronisation is not possible because no firmware file is available. In these cases, the firmware of the device must be updated first, even if it is the same version.
- If devices from different platforms (P1, P2 and so on) are part of the intercom system, at least one device for each platform must have the firmware version to be synchronized to.
- While synchronisation is in progress, no firmware updates or synchronisation on another device may be performed, otherwise the synchronisation will be aborted and fail.

Connecting an interior door

An interior door is the access to the area in which the indoor station is installed and where no

Behnke-Station is installed.

If the interior door has a bell button and/or a door opener, it is possible to connect these to the indoor station. If the bell button is pressed, a signal is sent to the indoor station and it is possible to activate the door opener of the interior door to open it.

You can specify whether and how an internal door is connected.

bell button
When the bell button is pressed, an acoustic and visual signal is emitted at the indoor station.
The ringtone used can be set in the 'acoustics' area.

door opener
When a door opener is connected, a door opener button for the interior door is displayed on the indoor station.
If this is pressed, relay 1 is activated if it has been configured as a door opener relay.

Automatic video preview

automatic preview off
automatic preview of preferred device
automatic preview of preferred device not available
automatic preview on

automatic preview history

An indoor station can request an automatic preview from a specific or all Behnke outdoor stations in its intercom group, provided that these have a camera and motion detection is enabled.

With automatic preview, the outdoor station informs the indoor station about any detected movement.

An acoustic signal is then emitted at the indoor station and the preview of the outdoor station is automatically displayed.

To request an automatic preview of a specific outdoor station, use the 'preferred device' setting and select the relevant outdoor station as the preferred device.

The automatic preview can also be switched via the main screen of the indoor station,

provided that this is permitted via the 'toggle automatic preview' setting.

Important note
Check whether the use of the automatic preview is possible and permissible under the legal regulations of your country or your company.

Integrating non-Behnke stations

Using Behnke stations (=BS, Generation 3) as intercom devices is very easy, as they can communicate directly with each other via the IP network.

In addition, a Behnke indoor station also allows the integration of IP stations. IP stations are other SIP telephones with IP cameras, such as Behnke SIP telephones (=BT-IP) of generations 1 and 2, or IP cameras.

Up to 9 IP stations can be integrated per indoor station. The information required for integration must be configured manually via the indoor station's web interface. If an IP station with multiple indoor stations is to be used, a suitable IP station must be configured in each indoor station.

Please note that functionality is not guaranteed when integrating SIP telephones from other manufacturers.

The functionality of the indoor station in conjunction with IP stations is limited to preview, connection and door opening or only to video preview when an IP camera is integrated. IP stations are not displayed in the topology, are not included in firmware synchronisation, and the codes set in the indoor station for the code lock function do not apply to IP stations.

CALLS / IP STATION CALL NUMBER

Calls to and from IP stations can be made either as direct SIP calls or via a SIP account.

direct SIP calls
Direct SIP calls can be made directly in 'IP intercom' mode. Hybrid mode is not required.

calls via a SIP account
The indoor station must be operated in hybrid mode so that intercom and SIP telephone functionality can be used, and the indoor station must be connected to a SIP telephone system via a SIP account.
The phone number of the IP station must always be specified with the prefix sip1: for the first SIP account or sip2: for the second SIP account.

DOOR OPENING VIA UDP CODE

IP stations of the 'BT-IP' type allow doors to be opened via the UDP remote control protocol, regardless of whether a connection exists or not.

A code can be set that must be sent to the IP station via the UDP remote control protocol in order to open access.

For a 'BT-IP generation 1' device, the UDP code is configured in the BT-IP under Settings Hardware ➔ Status/Remote Control ➔ Authentication Code.

For a 'BT-IP generation 2' device, the UDP code is configured in the BT-IP under Settings ➔ Relay Settings ➔ Relay Activation Code ➔ Web Interface.

For door opening via the UDP code to work, the IP address or host name of the BT-IP must also be specified and the UDP remote control protocol must be activated in the BT-IP.

DOOR OPENING VIA DTMF CODE

SIP door stations usually allow access to be opened during a connection when a specific DTMF code is received.

A code can be set that must be sent to the IP station to open access.

During an established connection with the IP station, this code is sent via DTMF. For devices of the 'BT-IP' type, a # is automatically appended.

If the opening of the IP station access is triggered at the indoor station during a connection, the DTMF code is sent to the IP station and a corresponding visualisation appears at the indoor station. After setup, you should check that the IP station actually opens the access. Since no feedback is received from the IP station, it is possible that the visualisation occurs even though the IP station does not open the access, for example because the wrong code is set.

Configuration by webinterface

The device can be configured with a web browser.

If a network connection to the device is possible from the computer used, the configuration can be carried out directly via the network. Otherwise, the device can also be configured via a special configuration WLAN.

Configuration via the network

To configure the device via the network, the IP address of the device is required.

In the delivery state, the device tries to obtain a dynamic IP address from a DHCP server. If no DHCP server is found in the network, the device assigns itself an IP address in the link-local network 169.254.0.0/16.

On devices in the delivery state, the IP address is announced as soon as it is known or shown in the display. Alternatively, the IP address can also be set by pressing the configuration button.

As soon as the IP address is known, the login to the web interface can take place.

Remember that if the device has assigned itself an IP address, that you must also assign your computer an IP address in the link-local network 169.254.0.0/16 in order to access the device. The device and the computer must be on the same network segment for a connection is possible.

With a faulty network configuration network access may no longer be possible. In this case you can regain access to the device as follows. Start the network configuration mode by pressing configuration button three times. The device then behaves with regard to the network configuration as in the delivery state. It either receives an IP address from the DHCP server or assigns one to itself.

Configuration via the configuration WLAN

The network configuration mode can be started by pressing the configuration button three times. In the network configuration mode, a configuration WLAN is provided in the immediate vicinity of the device (only for devices with WLAN antenna).

If you are in the immediate vicinity of the device, you can then use a computer, tablet or

mobile phone to connect to the configuration WLAN to configure the device.

The name and password of the WLAN are: behnke-station

When you are connected to the WLAN, open your browser and enter the IP address http://10.10.10.10 in the address line.

Then the login to the web interface can take place.

Login to the web interface

To get to the web interface, you enter the IP address of the device in the address line of the web browser.

Then you log in with the administrator password (default: admin).

After logging in, the web interface shows various sections for configuration on the left. The pre-selected section 'Basic configuration' shows the most important settings of all sections on one page. In many cases, a configuration of these settings is sufficient for commissioning. If not, the individual sections allow the access to all setting options.

The individual sections are explained below. Not all the settings listed are always displayed in the web interface. Depending on the device type and configuration, settings that are not required are hidden.

Secured connection

The web interface can be accessed using HTTP (unsecured connection) or HTTPS (secured connection).

To avoid security risks, the use of a secured connection, ie HTTPS, is recommended. A secured connection requires the installation of a certificate in the browser used.

If the device tries to install the certificate in the browser, it will probably display a warning and ask to allow the installation.

Global settings

If the device is operated as an IP intercom system, there are some settings that must be configured uniformly on all devices in the IP intercom system. This page is used to configure these global settings. When saved, they are automatically transferred to all devices in the IP intercom system. No changes can be made while this process is running.

Make sure that all devices are installed and ready for operation before changing global settings.

See manual under Implementation of an IP intercom system .

Transfer

Status: When the global settings are saved, the partial step carried out or the progress of the transfer is displayed here.

If the global settings could not be saved successfully, 'failed' is displayed here for a short time. In this case, you must check why the process failed, fix the problem and then restart the saving of the global settings.

The devices of the intercom system must use the same administrator password, otherwise the global settings cannot be transferred.

Saving global settings in all devices

General

Basic settings

Language:

- English
- German
- French

Default: English

Language used for voice announcements and display texts

If the configuration button is used in the delivery state, the desired language is requested first in order to set this setting accordingly. After that, the language can no longer be changed by the configuration button, unless the device is reset to the factory settings.

When accessing to the device by the web interface, the language of the web browser will be used. However, it is possible to change the language for the duration of the session by clicking the appropriate flag before logging in.

Name:

name that will be transmitted to the remote station in case of a connection or displayed in the web interface

Operation mode:

- SIP phone
- IP intercom

Default: IP intercom

The device can be operated as a SIP telephone or as an IP intercom.

SIP phone
operating mode if the device is connected to a SIP server (IP telephone system) as a SIP subscriber or if the device is to communicate directly with other SIP telephones (SIP direct calls)

IP intercom
operation mode if the device is operated as an IP intercom in connection with other devices

Hybrid mode:	• no • yes Default: no Simultaneous use of several operation modes The hybrid mode is intended for more complex application scenarios with different communication infrastructures. In hybrid mode, the device works in the selected operation mode SIP telephone or IP intercom. This is then the main operation mode, but it is also possible to use the other operation modes. Unless otherwise specified, the device always uses the main operation mode for an outgoing call. If one of the other operation modes is to be used, this can be specified in the call number as follows. If you want to call the number 123 as a SIP telephone via the SIP account for the IP telephone system (SIP server) with the address 192.168.16.199, then you enter the number as follows: sip:123@192.168.16.199 If you want to call in intercom mode the indoor station with intercom ID 1, enter the call number as follows: com:1
Installer / contact:	name with phone number or email address of the company, department or person who can be contacted in the event of a service case This information is displayed on the login screen of the web interface or when logging in as a user in the user configuration.

Basic settings for operating the device

Web interface	User password:	password for normal users without or with limited authorisation for configuration The following characters may be used in a password:

a-z A-Z o-9 ! ? # $ % & ( ) * + , - . / : ; = [] | { } ^ _

It is possible that several users log in with this password at the same time. If no user password is specified, logging in as a normal user is not possible.

Administrator password:

Default: admin

password with authorisation for configuration

The following characters may be used in a password:
a-z A-Z o-9 ! ? # $ % & ( ) * + , - . / : ; = [] | { } ^ _

It is possible that several users log in with this password at the same time. However, only one user can access the configuration. If another user tries to configure the device at the same time, he receives a message that he must wait until the other user has left the configuration.

If a user accesses the configuration but does not exit it correctly, for example by simply closing his browser or switching to another page without logging out, the access to the configuration is blocked and will be again possible after one minute.

Lock login in case of abuse:

- no
- yes

Default: yes

If an incorrect password is entered several times, the login will be blocked for a certain period of time.

At first, the registration will only be blocked for a short time. Further incorrect registration attempts will increase the blocking period up to a maximum of 24 hours.

If the correct password is entered after the blocking period, the blocking period is reset. The blocking period can also be reset by restarting the device.

Access to the web interface:

- HTTP allowed
- HTTP allowed if no certificate
- use HTTPS

Default: HTTP allowed

The web interface can be accessed using HTTP (unsecured connection) or HTTPS (secured connection).

To avoid security risks, the use of a secured connection, ie HTTPS, is recommended. A secured connection requires the installation of a certificate in the used browser.

If the device tries to install the certificate in the browser, it will probably display a warning and ask to allow the installation.

Access via HTTPS is always possible. This option can be used to set whether access via HTTP is also permitted or not.

This option does not affect the retrieval of images or video streams. This can be done via HTTP, even if HTTPS must be used for the web interface.

HTTPS security:

- default encryption
- stronger encryption
- strongest encryption

Default: default encryption

Access to the web interface via HTTPS (secure connection) uses TLS with various encryption methods. With stronger or strongest encryption, older TLS versions or weak encryption are no longer supported.

Stronger encryption increases security, but can mean that HTTPS access is no longer possible with older web browsers.

Web server certificate: information about the web server certificate, if such a certificate has been uploaded

Certificate: upload / remove

upload
The certificate of the web server can be uploaded in PEM format here. A file is required that contains exactly one certificate with an unencrypted private key.
Once uploaded, the certificate information will appear

under 'Web server certificate' above.

remove
The uploaded certificate can be removed here.

Show version and serial number at login:

- no
- yes

Default: yes

displaying the software version and serial number on the login screen

Settings for access to the web interface

Configuration by user

Allow:

- no
- only selected user settings
- all user settings

Default: no

In the delivery state, normal users have no authorisation to configure the device.

In certain cases it may still be useful to allow the user to change certain settings, such as the door opener code.

There is a selection of configuration settings that can be offered to the user for configuration if required.

This setting can be used to determine whether the user should be allowed all or only a certain selection of these user configuration settings.

Password:

- no
- yes

Default: no

changing the user password

Special periods and dates:

- no
- yes

Default: no

definition of periods such as company holidays in which the normal schedules are not valid

Direct call buttons:

- no
- yes

Default: no

configuration of the name, number, etc. of the direct call buttons

Phonebook entries:

- no
- yes

Default: no

creating, changing and deleting phone book entries

Codes for door opener relay:

- no
- yes

Default: no

creating, changing and deleting door opener codes

Numbers for call-triggered opening:

- no
- yes

Default: no

creating, changing and deleting call numbers for call-triggered opening

Schedules for continuous opening:

- no
- yes

Default: no

ajusting the schedule for continuous opening

Audio settings:

- no
- yes

Default: no

adjusting the volume and microphone sensitivity

Individual announcements:

- no

- yes

Default: no

Management of individual announcements

Configuration permissions for normal users

Subadministration

Allow:

- no
- yes

Default: no

This setting can be used to determine whether a subadministrator should be provided.

A subadministrator is a user who can be assigned rights to configure selected areas and functions and to use certain functionalities.

Important notes

- The following applies to the assignment of rights: Prohibiting is stronger than allowing. If one setting allows access and another prohibits it, access is not possible.
- To permit complete rights assignment, sections that are hidden due to the current configuration or non-existent hardware are also displayed. The areas in question are then marked with the x symbol.
- The subadministrator does not have access to subadministration and the administrator password.
- If the subadministrator is granted access to the 'basic Configuration' section, they will find the most important settings for the other areas on one page. However, the settings for sections or functions to which they do not have access will be hidden. Furthermore, only warnings and configuration problems relating to settings to which he has access are displayed. Please note that the device may be displayed to the sub-administrator as 'basically ready for operation', but further warnings and configuration problems may be displayed when logging in as an administrator.
- If the device is used as an IP intercom and the

subadministrator is granted access to the 'IP intercom' section, he can only access other devices in the intercom system via the topology view if a subadministrator with the same subadministrator password and corresponding permissions is configured in the device in question.

Subadministrator password:

Default: subadmin

password with selected authorisations for configuration

The following characters may be used in a password:
a-z A-Z 0-9 ! ? # $ % & ( ) * + , - . / : ; = [] | { } ^ _

As with the administrator password, it is possible for several users to log in with this password at the same time. However, only one user can access the configuration. If another user tries to configure the device at the same time, he receives a message that he must wait until the other user has left the configuration.

If a user accesses the configuration but does not exit it correctly, for example by simply closing his browser or switching to another page without logging out, the access to the configuration is blocked and will be again possible after one minute.

Basic configuration:

- no
- partially
- yes

Default: no

Global settings:

- no
- partially
- yes

Default: no

General:

- no
- partially
- yes

Default: no

Operation mode:	• no • yes Default: no
User configuration:	• no • yes Default: no
Configuration mode:	• no • yes Default: no
Network:	• no • partially • yes Default: no
Port authentication:	• no • yes Default: no
SNMP:	• no • yes Default: no
SIP phone:	• no • partially • yes Default: no
Direct SIP calls:	• no • yes Default: no
SIP account 1:	• no • yes Default: no

SIP account 2:	• no • yes Default: no
IP intercom:	• no • partially • yes Default: no
Network bridge:	• no • yes Default: no
Synchronisation:	• no • yes Default: no
Camera:	• no • partially • yes Default: no
Camera access:	• no • yes Default: no
IP camera:	• no • yes Default: no
Display:	• no • partially • yes Default: no
Functions:	• no • yes Default: no

Connection:	• no • partially • yes Default: no
Call answering:	• no • yes Default: no
Buttons:	• no • partially • yes Default: no
Handset:	• no • partially • yes Default: no
Keypad:	• no • partially • yes Default: no
Functions:	• no • yes Default: no
Phone book:	• no • partially • yes Default: no
Export & import:	• no • yes Default: no
LDAP:	• no • yes

Default: no

Relays:
- no
- partially
- yes

Default: no

Relay 1:
- no
- yes

Default: no

Relay 2:
- no
- yes

Default: no

Operation mode:
- no
- yes

Default: no

Door opener codes:
- no
- yes

Default: no

Continuous opening:
- no
- yes

Default: no

Allow opening by door opener button:
- no
- yes

Default: no

Call-triggered opening:
- no
- yes

Default: no

Webhook for activation:
- no
- yes

Default: no

Triggers:	• no • partially • yes Default: no
Alarm input:	• no • yes Default: no
Sabotage:	• no • yes Default: no
Radar sensor:	• no • yes Default: no
Scheduled calls:	• no • yes Default: no
System start:	• no • yes Default: no
Daily audio test:	• no • yes Default: no
Noise alarm:	• no • yes Default: no
Acoustics:	• no • partially • yes Default: no

Diagnostics:	• no • partially • yes Default: no
Log, syslog, weblog & network trace:	• no • yes Default: no
Test:	• no • yes Default: no
System:	• no • partially • yes Default: no
Save / restore / reset:	• no • yes Default: no
Firmware update:	• no • yes Default: no
Auto-provisioning:	• no • yes Default: no
API:	• no • yes Default: no
ControlCenter:	• no • yes Default: no
Special function:	• no

- yes

Default: no

ControlCenter:

- no
- partially
- yes

Default: no

Door opening as subadministrator:

- no
- partially
- yes

Default: yes

This setting can be used to grant or revoke the subadministrator's authorisation for door opening.

Without authorisation for door opening, the following adjustments are made when using the subadministrator password:

- no door opener buttons under 'visualisation'
- hide user password
- the 'door opening' action cannot be selected for buttons, phone book entries and triggers
- cmd:free1, cmd:free2, cmd:open1, cmd:open2, cmd:close1, cmd:close2, cmd:code1 ande cmd:code2 cannot be used as special parameters in the call number
- door opener relay operation mode cannot be changed
- hide the following settings for a door opener relay: door opener codes, continuous opening, opening by door opener button, webhooks
- hide the setting for the acoustical indication 'if invalid code entered at the indoor station'
- no button for triggering a door opener relay under 'Diagnostics'
- HTML API: no access to hidden settings, no triggering of door opener relays or events

Important note

To prevent abusive door opening by the subadministrator, access to the following functions or their sections should be blocked.

- General - configuration mode
- Network - SNMP

- Card reader
- Diagnostics - log, syslog, weblog & network trace
- System - save / restore / reset
- System - auto-provisioning

Furthermore, in the 'Acoustics' section, the acoustical indication 'if invalid code entered at the indoor station' should not be configured to 'play voice announcement with valid code'.

Administrator for certain sections and functions

Configuration mode

Allow:

- no
- yes, by phone, keypad or display
- only by phone

Default: yes, by phone, keypad or display

The configuration mode allows to configure the device either remotely using a tone dialing telephone or locally at the device using the keypad if available.

The configuration mode is protected by a 4-digit security code. If desired, it can also be deactivated.

On a device with a display, the configuration mode can also be activated and used via the virtual keypad of the code lock function, but only if the activation of the configuration mode via the keypad is permitted. If no code lock function is available on the display, the virtual keypad can also be displayed as follows: swipe with one finger horizontally quickly across the display from left to right.
When activating the configuration mode or as long as it is active, the virtual keypad is displayed in blue.

See manual under Configuration by phone, keypad or display.

Security code:

Default: oooo

4-digit code that must be entered in order to activate the configuration mode

Lock activation in case of abuse:

- no
- yes

Default: yes

If an incorrect security code is entered several times, the activation of the configuration mode is blocked for a certain period of time.

Initially, the activation is only blocked for a short time. Further incorrect activation attempts lead to an increase of the blocking period up to a maximum of 24 hours.

If the configuration mode will be activated correctly after the blocking period, the blocking period is reset. The blocking period can also be reset by restarting the device.

Configuration by phone, keypad or display

Schedules

Special periods and dates:

Periods such as company holidays in which the normal schedules are not valid

Normally, during a special period, a schedule is always evaluated as invalid and the corresponding action for invalid times is executed.

Alternatively, it is also possible to define other valid periods for special periods. To do this, you write after the existing valid periods in a schedule *** and then you specify the valid periods for special periods.

Example
If the schedule should normally be valid from 8 a.m. to 12 p.m. and from 2 p.m. to 6 p.m., but only from 9 a.m. to 12 p.m. during the special period, enter the following for the corresponding schedule:

8-12 14-18 *** 9-12

Treat holidays like:

- the corresponding day of the week
- in Germany (Baden-Württemberg)
- in Germany (Bayern)
- in Germany (Berlin)
- in Germany (Brandenburg)
- in Germany (Bremen)
- in Germany (Hamburg)

- in Germany (Hessen)
- in Germany (Mecklenburg-Vorpommern)
- in Germany (Niedersachsen)
- in Germany (Nordrhein-Westfalen)
- in Germany (Rheinland-Pfalz)
- in Germany (Saarland)
- in Germany (Sachsen)
- in Germany (Sachsen-Anhalt)
- in Germany (Schleswig-Holstein)
- in Germany (Thüringen)
- in France
- in France (Alsace-Moselle)
- in Luxembourg
- self defined holidays

Default: the corresponding day of the week

Evaluation of schedules on public holidays

When evaluating time schedules, holidays can be ignored, i.e. treated like the corresponding weekday, or treated separately.

In order to treat holidays separately, they have to be specified. The easiest way to do this is to select that you want to treat the holidays as in a certain country or in a certain region.

If the country or region is not included in the selection, you can also define the public holidays yourself. The list of public holidays must be adjusted accordingly.

Important
Check the given dates for public holidays and adjust them if necessary!

New Years's Day: Default: 1.1.

Twelfth Day: Default: 6.1.

International Women's Day: Default: 8.3.

Good Friday: Default: 7.4.23 29.3.24 18.4.25 3.4.26 26.3.27 14.4.28 30.3.29 21.4.30 11.4.31 26.3.32 15.4.33 7.4.34 23.3.35 11.4.36 3.4.37

Easter Monday: Default: 10.4.23 1.4.24 21.4.25 7.4.26 29.3.27 17.4.28

	2.4.29 22.4.30 14.4.31 29.3.32 18.4.33 10.4.34 26.3.35 14.4.36 6.4.37
Labor Day:	Default: 1.5.
Allied victory:	Default: 8.5.
Europe Day:	Default: 9.5.
Ascension Day:	Default: 18.5.23 9.5.24 29.5.25 14.5.26 6.5.27 25.5.28 10.5.29 30.5.30 22.5.31 6.5.32 26.5.33 18.5.34 3.5.35 22.5.36 14.5.37
Whit Monday:	Default: 29.5.23 20.5.24 9.6.25 25.5.26 17.5.27 5.6.28 21.5.29 10.6.30 2.6.31 17.5.32 6.6.33 29.5.34 14.5.35 2.2.36 25.5.37
Corpus Christi Day:	Default: 8.6.23 30.5.24 19.6.25 4.6.26 27.5.27 15.6.28 31.5.29 20.5.30 12.6.31 27.5.32 16.6.33 8.6.34 24.5.35 12.6.36 4.6.37
Luxembourgish national holiday:	Default: 23.6.
French national holiday:	Default: 14.7.
Assumption Day:	Default: 15.8.
World Children's Day:	Default: 20.9.
Day of German Unity:	Default: 3.10.
Reformation Day:	Default: 31.10.
All Saints Day:	Default: 1.11.
Armistice:	Default: 11.11.
Day of Repentance and Prayer:	Default: 16.11.22 22.11.23 20.11.24 19.11.25 18.11.26 17.11.27 22.11.28 21.11.29 20.11.30 19.11.31 17.11.32 16.11.33 22.11.34 21.11.35 19.11.36 18.11.37
Christmas Day:	Default: 25.12.

Boxing Day:	Default: 26.12.

Settings for the use of schedules

Cooling Strategy:	• activate fan earlier • standard • activate fan later • fan off • level 1 • level 2 • level 3 • level 4 Default: standard

Settings for cooling the device

Network

If settings of this sections are changed and saved, the network configuration will be updated. You are automatically logged out. After that, it may take a moment before the device is reachable again.

If the device is detected, you will be automatically logged in again. If the device receives a different IP address, it cannot be detected automatically. In this case, you must determine the new IP address yourself, for example by querying the IP address by pressing twice the configuration button on the connection board.

Address MAC:	display of the device's MAC address The MAC address is required, for example, if a specific IP address is to be assigned to the device via DHCP or when the device is auto-provisioned.
Hostname:	unique designation of the device in the network The host name is transmitted to the DNS server and enables the device to be addressed using the host name instead of its IP address. This is particularly useful in networks with dynamic IP address assignment, as the device can still be reached under the host name even if the IP address changes. The host name must be unique, i.e. there cannot be any other device in the same network domain with the same name.
Network connection:	• **wired Ethernet** • **VLAN** • **WLAN** **Default: wired Ethernet** way how the device is connected to the IP network Normally, the device is connected to the Ethernet port of a PoE switch via a network cable. This supplies it with energy (Power over Ethernet) and connects it to the network. Optionally, the device can also be connected to a wireless network (WLAN). wired Ethernet connection to a LAN or an untagged VLAN

	VLAN connection to a tagged VLAN WLAN connection to a wireless network In this case, the power supply of the device must be ensured either by using a plug-in power supply or by additionally connecting the device to a PoE port. In order to achieve a sufficient quality of the wireless connection, an external antenna module is usually required.

WLAN	**Name:**	name of the wireless network (SSID) Access to wireless networks using the WPA2 encryption standard is supported. The WEP and WAP encryption standards are not supported for security reasons. Detected wireless networks are shown below. By clicking on a detected name, this can be transferred to the input field and only the associated password needs to be entered.
	Password:	password required to connect to the wireless network

Settings for the connection to a wireless network

Device	**Current IP address:**	display of the IP address of the device In case of static address assignment, it is the configured IP address. In case of dynamic address assignment, it is the IP address assigned by the DHCP server. In case of link-local, the IP address assigned by the device to itself is shown, unless the device was assigned an IP address by a DHCP server. In this case, the IP address assigned by the DHCP server is shown. Then, the address assignment should then be changed to 'dynamic'.

Assignation of IP address:

- static
- dynamic
- link-local

Default: dynamic

way the device gets an IP address

static= manual address assignment
The network administrator manages the IP addresses of the network. You have received an IP address from the network administrator that you enter here. In this case, the associated net mask and the gateway must also be specified. If domain names are to be used, the search domain and at least one DNS server must also be specified. All this information can be obtained from the network administrator.

dynamic= automatic address assignment
There is a DHCP server in the network that manages and distributes the IP addresses. The device automatically tries to obtain an IP address from this DHCP server. The IP address assigned in this way can be queried by pressing the configuration button twice. In the case of a device with a display, it is displayed briefly after it has been assigned.
A dynamically assigned address can change, for example if the device was disconnected from the network for a certain time. The network administrator can create a reservation in the DHCP server so that the device always receives the same IP address. For this, he needs the MAC address of this device.

link-local= self-assignment of an address
This address assignment is intended for networks without a DHCP server. The device assigns itself a free IP address in the 169.254.0.0/16 network. The assigned IP address can be queried by pressing the configuration button twice. For a device with a display it will also be displayed briefly after assignment.
This type of address assignment is used when several devices are operated as an IP intercom in an independent network.
If there is a DHCP server in the network that assigns an IP address, this will be used. In this case, the address assignment should be set to 'dynamic'!

Important
In networks with a DHCP server, 'dynamic' should be

selected as the address assignment!

Allow fallback to link-local:

- no
- yes

Default: yes

If the device with dynamic address assignment has not received an address from the DHCP server after a certain period of time, it can assign itself a free IP address in the link-local network 169.254.0.0/16 if this setting allows the fallback to link-local.

This means that the device always receives an IP address, regardless of whether a DHCP server is available or not.

Important
The fallback to link-local makes it easier to access the device for the first time because it always receives an IP address. In networks with a DHCP server, the fallback is not required and should be switched off. In networks without a DHCP server, however, the address assignment 'link-local' must be set.

Fallback after:

10 - 90 s

Default: 15 s

This setting determines how long to wait after activating the network connection before performing the fallback to link-local.

IP address:

Default: 192.168.100.100

IP address assigned by the network administrator

In the case of static IP address assignment, you receive an IP address and the associated net mask and gateway address from the network administrator.

Net mask:

Default: 255.255.255.0

net mask received from the network administrator

In the case of static IP address assignment, you receive an IP address and the associated net mask and gateway address from the network administrator.

Gateway: gateway address received from the network administrator

In the case of static IP address assignment, you receive an IP address and the associated net mask and gateway address from the network administrator.

DNS settings:
- set manually
- obtain automatically

Default: obtain automatically

In case of dynamic address assignment, the DHCP server usually also transmits the search domain and the DNS server(s). This information can also be set manually if desired.

Search domain: name of the local domain

If a host name is to be resolved into an IP address, the search domain is appended to the host name in order to obtain a fully specified computer name (FQHN = full-qualified host name). Then the IP address for this name will be requested from the DNS server.

Primary DNS server: IP address of the DNS server

Secondary DNS server: IP address of another DNS server

VLAN tag: 1 - 4094

Default: 1

ID or number of the VLAN

Priority:
- 0 = background
- 1 = best effort
- 2 = excellent effort
- 3 = critical applications
- 4 = video
- 5 = voice
- 6 = internetwork control
- 7 = network control

Default: 5 = voice

priority of the network packets sent by the device

IP network settings of the device

NTP

Current time:

display of the current time of the device

In order that the device has a valid time, a time-server must be configured to request the valid time and to synchronize with it.

The device regularly synchronizes its time with the time-server. If the time is synchronized, it is displayed in grey.

If it is not possible to retrieve the valid time from the time-server, the time is displayed in red with the message 'not synchronized, invalid'. If the time is invalid, all schedules are evaluated as invalid.

If the time could already be retrieved from the time-server, but the server is no longer reachable, then the time is displayed in yellow with the message 'not synchronized but valid'. The device has a valid time, but of course inaccuracies can occur because the time is no longer synchronized. In this case, schedules are further evaluated.

When the device restarts, it may take a moment before the first synchronization with the time-server takes place.

Timezone:

Default: Europe/Berlin

time zone in which the device is located

With NTP, the coordinated universal time (UTC) is obtained from the time-server. Using the time zone, the universal time is then converted to the time in the region / zone in which the device is installed.

Configure time-server:

- **set manually**
- **receive via DHCP**

Default: set manually

The device can obtain the valid time from a time server.

The time server can either be specified manually or, if the IP address assignment is dynamic, transmitted by the DHCP server via option 42.

Not all DHCP servers transmit a time server via option 42. This requires a corresponding configuration of the DHCP server!

If the device does not have a valid time, all schedules are evaluated as invalid.

Time-server obtained via DHCP: display of the time server that was transmitted via DHCP option 42

Time-server: Default: pool.ntp.org

The device can obtain the valid time from a time-server.

The default is a public time-server on the Internet. If the device cannot reach the time-server, for example because Internet access is not permitted or the DNS settings are incorrect, then the device does not have a valid time.

If the device does not have a valid time, all schedules are evaluated as invalid.

If no internet access is possible, the address of a time-server in the local network can of course also be given.

Settings for the synchronization with a time-server

E-mail

Allow sending e-mails:

- no
- yes, via SMTP
- yes, via SMTP/SMTPS
- yes, via SMTPS (SSL/TLS)

Default: no

It is possible to send an e-mail in certain situations, for example to log the access control or as a message if no one could be reached by telephone with a direct call.

This setting determines whether sending e-mails is allowed or not.

If e-mails are to be sent, then an e-mail account must be specified via the following settings, which can be used for sending.

E-mail address: e-mail address from which the e-mails are sent

Outgoing e-mail server: IP address or host name of the outgoing e-mail server

Port:
- standard
- 25
- 465
- 587
- 2525
- define

Default: standard

port of the outgoing e-mail server

Port 587 is currently the standard port for SMTP transmission. It supports both SMTP and SMTPS.

In the past, port 25 was also used for SMTP and port 465 for SMTPS.

Port 2525 is not an official SMTP port. However, it is sometimes used as an alternative to port 587.

Defined port: 1 - 65535

Default: 587

port of the outgoing e-mail server

If the outgoing e-mail server uses a different port than the ones normally used, you can set it here.

Username: username for logging into the outgoing e-mail server

Password: password for logging into the outgoing e-mail server

Verify server certificate:
- no
- yes

Default: yes

When using SMPTS as the transmission protocol, the outgoing email server transmits a certificate with information on the encryption.

Here you can set whether or not the validity of this server certificate is checked before use. If the server certificate is invalid, the communication with the server will fail.

In addition, the server certificate contains the name or the IP address of the server (CN=common name). In order for the certificate to be valid, the CN must correspond to the entry in the 'Outgoing email server' field.

Verify server CN:

- no
- yes

Default: yes

A server certificate contains the name or the IP address of the server (CN=common name). In order for the certificate to be valid, the CN must correspond to the entry in the 'Outgoing email server' field.

Here you can set whether or not the CN of the server is checked when checking a server certificate.

Test mail: send

Here you can send a test mail to test the settings for sending e-mails.

A window opens in which you can enter the address to which the test mail should be sent.

If the configuration has been changed, the changes must be saved or discarded before a test mail can be sent.

Settings for sending e-mails

Services

Publish own services by MDNS:

- no
- yes

Default: yes

The device can publish its services via MDNS. This allows that the device can be automatically detected by other devices in the network or by the IP video software.

The IP intercom system requires the publication of MDNS services.

Detect services:

- no
- by MDNS
- by UDP
- per MDNS and UDP

Default: per MDNS and UDP

The device can automatically detect a supported camera connected to the extension port if it publishes its services via MDNS or UDP.

The IP intercom system requires the detection of MDNS services.

Settings for the publication and discovery of services

USB extension port

Operation mode:

- ethernet port
- absorption port

Default: absorption port

The USB extension port is available on a device with AIF IP when a USB extension port adapter is connected. It can be used as an Ethernet port or as an absorption port.

Ethernet port
The device connected to the USB extension port is integrated into the incoming network at the main port. If DHCP is used, the device also gets its IP address from the DHCP server in this network.
If an IP camera is connected to the USB extension port, it can also be accessed directly from the network in this operation mode.

As an Ethernet port, the USB extension port is

integrated into the incoming network depending on the configured network connection.
If a VLAN is used for the Webcam, the USB extension port is integrated into the VLAN of the Webcam.
If only a VLAN is used for the device, the USB extension port is integrated into the VLAN of the device.
If no VLANs are used, the USB extension port is integrated into the untagged network.
The USB extension port itself is always untagged.

absorption port
The device connected to the USB extension port is integrated into a absorption LAN of the Behnke station. If DHCP is used, the device receives an IP address from the Behnke station.
If an IP camera is connected to the USB extension port, it cannot be accessed directly from the network in this operation mode. Supported cameras can be automatically detected and integrated by the Behnke station.

Absorption network: 0 - 255

Default: 2

address range for the assignment of an IP address via DHCP to a device connected to the absorption port

The specified address range should normally not be used in a local network. If this is not the case, another, unused address range can be selected here.

Settings for the usage of the USB extension port

UDP communication

Activate:

- no
- yes

Default: yes

The IP video software requires that the monitored devices transmit and receive data via UDP. If the UDP communication is deactivated, the IP video software cannot be used for this device.

See manual under UDP communication.

Destination IP address for status messages:

Default: 255.255.255.255

The status messages are usually sent to the address 255.255.255.255, i.e. all participants in the same IP network (broadcast).

Destination port for status messages:

1024 - 65534

Default: 8112

Local port for remote control messages:

1024 - 65534

Default: 8113

Character encoding:

- UTF-8
- ANSI

Default: ANSI

This setting can be used to set the character encoding used by the LDAP server so that special characters are displayed correctly.

Windows® systems usually use ANSI as the character encoding.

Activate reflector:

- no
- yes

Default: yes

The Behnke IP video software can automatically detect devices that are installed in the same IP network as the PC with IP video software based on the UDP status messages sent.

If the devices and the PC with the IP video software are in different IP networks, this automatic detection does not work because the UDP status messages are normally implemented as broadcast messages and broadcasts are not forwarded to other networks.

In this case it is possible to connect the IP video software to a server (reflector) that forwards the status messages to the IP video software.

A reflector can either be implemented by installing the IP video server software on a PC. Alternatively, this device can also take on the role of a reflector if

this is activated via this setting.

If the reflector is activated, then you configure the IP address of this device as the server IP address in the IP video software under 'Common setup' and the port specified below for reflector clients, normally 8255, as the port. Then you activate 'Use server' to use the reflector.

After saving the configuration, a green or red box appears in the IP video software behind 'Use server', which shows whether the connection to the server is established (green) or not (red).

Up to 50 PCs with IP video software can be connected to one reflector. For larger installations, the IP video server software should be used.

If a device is used as a reflector, it should be ensured that its IP address does not change. Therefore, in networks with dynamic address assignment, an IP address should be reserved for the device in the DHCP server.

The communication between the IP video software and the reflector takes place via a TCP connection via the set port, usually 8255. The PC's firewall must be set so that it allows TCP connections to the reflector via the set port.

Local port for reflector clients: 1024 - 65534

Default: 8255

Settings for the communication with IP video / other software

TCP communication

Activate:

- no
- yes

Default: no

This setting can be used to specify whether TCP status messages should be sent to an alarm server or not.

A separate TCP connection is established for each status message. The TCP connection is terminated by the Behnke station after the status message has been

	sent. If the alarm server is not available, any status messages are discarded. If the Behnke station has no network connection, status messages are buffered and sent as soon as the network connection is available again. If the network connection is down for too long, a buffer overflow may occur. In this case, the oldest messages are discarded and a discard message is generated. This interface is used exclusively for sending status messages. See manual under TCP communication.
Connection to the alarm server:	Indicates whether the last status message could be sent to the alarm server or not. OFFLINE The last status message could not be sent to the alarm server. ONLINE The last status message could be sent to the alarm server.
Alarm server:	host name or IP address of the alarm server
Destination port:	1024 - 65534 **Default: 25000**

Settings for the communication with an alarm server

Port authentication	**Method:**

- **none**
- **EAP-MD5**
- **EAP-TLS**
- **EAP-TTLS**
- **PEAP**

Default: none

The 802.1x protocol describes a process in which a terminal device such as this one can be authenticated before it can connect to the network.

To do this, the switch and the device must support the 802.1x protocol. The device first connects to the switch and this then forwards the information to a RADIUS server, which allows access to the network or not.

The 'Extensible Authentication Protocol' (EAP) is used between the device, the switch and the RADIUS server. There are various methods of EAP. This setting can be used to determine which method should be used.

none
Port authentication is disabled.

EAP-MD5
The password is compared via a challenge-response procedure using an MD5 hash function over an unencrypted connection.
This method is considered obsolete and no longer safe!

EAP-TLS
The device is authenticated using certificates through a secure TLS tunnel.

EAP-TTLS
The device is authenticated by transmitting the password over a secure TLS tunnel.

PEAP
The device is authenticated using a challenge-response method over a secure TLS tunnel.

Authentication:

- mandatory
- optional

Default: mandatory

This setting can be used to determine whether or not the network connection should be activated if the port authentication fails.

optional
If port authentication fails, network connection activation will continue.

mandatory

The network connection is only activated if the port authentication was successful before.

Identity: identity for authentication with the RADIUS server

Anonymous identity: anonymous identity that is used as the unencrypted identity for outer authentication

The username is used for inner authentication.

User certificate: information on the user certificate, if such a certificate has been uploaded

Certificate: upload / remove

upload
The user certificate can be uploaded in PEM or CRT format here. If the uploaded file contains several certificates, only the first certificate is installed. Once uploaded, the certificate information will appear under 'User certificate' above.

remove
The uploaded certificate can be removed here.

Trusted CA: information on the certificate of the trusted CA, if such a certificate has been uploaded

Certificate: upload / remove

upload
The certificate of a trustworthy CA can be uploaded in PEM format here. If the uploaded file contains several certificates, only the first certificate is installed. Once uploaded, the certificate information will appear under 'Additional trusted CA' above.

remove
The uploaded certificate can be removed here.

Secret key: information on the secret key certificate, if such a certificate has been uploaded

Certificate: upload / remove

upload

The secret (= private) key can be uploaded in PEM or KEY format here.
Once uploaded, it will be displayed under 'Secret Key' above whether the correct password for the secret key has been entered below.

remove
The uploaded certificate can be removed here.

Password for secret key: password to decrypt the secret key uploaded above

Inner authentication method:

- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- GTC
- MD5

Default: PAP

inner authentication method when using EAP-TTLS

PEAP version:

- automatic
- version 0
- version 1

Default: automatic

PEAP version to be used

automatic
The version specified by the RADIUS server is used.

version 0
Use of version 0 is being enforced.

version 1
Use of version 1 is being enforced.

Inner authentication method:

- MSCHAPv2
- GTC
- MD5

Default: MSCHAPv2

inner authentication method when using PEAP

Username:	identity for authentication with the RADIUS server
Password:	password for authentication with the RADIUS server

Settings for the 802.1x port authentication

LLDP	
Activate:	• no • yes Default: no This setting allows the LLDP (= Link Layer Discovery Protocol) to be activated. It applies when the device is no longer in the delivery state. LLDP is activated in the delivery state, even if this setting is configured to 'no'. The LLDP is a manufacturer-independent Layer 2 protocol that offers the possibility of exchanging information between neighboring devices, for example between this device and the switch to which it is connected. For this purpose, information is sent to and received by the neighboring device at periodic intervals, independently of one another. Such information can be: identification of the device, functions of the device or information on the device configuration.
Transmit interval:	1 - 3600 s Default: 30 s This setting defines the interval in seconds for sending LLDP packets.
Transmit hold factor:	2 - 10 Default: 4 The factor set here multiplied by the set transmission interval results in the hold time for LLDP packets.
Publish system functions:	• no

- yes

Default: yes

This setting determines whether the system function of the device should be published or not.

Publish management addresses:

- no
- yes

Default: yes

This setting specifies whether the management addresses, i.e. the IP addresses via which the device can be configured, should be published or not.

Activate LLDP-MED:

- no
- yes

Default: yes

LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Devices) is an extension of LLDP to support the interoperability of VoIP end devices with other devices in the network.

Fast start interval:

1 - 10 s

Default: 3 s

This setting defines the duration for which LLDP packets are sent when the LLDP-MED quick start mechanism is triggered.

Publish inventory:

- no
- yes

Default: yes

This setting determines whether inventory information (product name, product version, firmware version, operating system version, serial number, manufacturer, hardware ID) should be published or not.

Publish PoE information:

- no
- yes

Default: yes

This setting determines whether information about the PoE power supply should be published or not.

Publish network policy for voice:

- no
- yes

Default: yes

This setting determines whether the settings currently used by the device for telephony should be published as a network policy for voice or not.

Implement network policy for voice:

- no
- yes

Default: yes

This setting specifies if a network policy for voice is received whether or not it is to be implemented.

If so, when a corresponding policy is received, the configuration of the device is changed so that it complies with the policy. The device therefore automatically switches to the corresponding VLAN. The IP address assignment is set to dynamic.

Settings for LLDP

SNMP

Activate:

- no
- yes

Default: no

This setting allows the SNMP (= Simple Network Management Protocol) to be activated.

It applies if the device is no longer in the delivery state. SNMP is activated in the delivery state, even if this setting is configured to 'no'.

SNMP is a standardised network protocol for monitoring and controlling network devices such as switches, routers or IP door intercom systems.

It enables a central network management system to query information from the device (e.g. operating states, configuration parameters or statistics) and, if

configured accordingly, to make settings on the device.

Important note
This device only supports SNMPv3.
In contrast to older versions (v1 and v2c), SNMPv3 offers secure communication through authentication and encryption. This prevents unprotected access and the interception or manipulation of network data.
For security reasons, support for SNMPv1 and SNMPv2c was deliberately omitted.

Permitted access:

- read
- read & write

Default: read & write

Default settings (SNMP general) and runtime settings (TEMP settings) of the Behnke station may only be read.

This setting determines whether the configuration settings of the Behnke station may only be read or also written.

Authentication algorithm:

- SHA
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Default: SHA

SNMPv3 uses authentication (e.g. SHA) to check senders and prevent tampering.

Authentication user:

SNMPv3 user for authentication

Authentication password:

Default: snmpadmin

The SNMPv3 password is used to securely identify the user during authentication.

Encryption algorithm:

- AES
- AES128
- AES192
- AES256

Default: AES

SNMPv3 uses encryption (e.g. AES) to protect data from being read.

Encryption password: Default: snmpadmin

The encryption password for SNMPv3 is used to encrypt the data transmission and thus protect it from unauthorised access.

System location: installation location of the device

Contact person: contact information of the person or department responsible for the device, e.g. an e-mail address or telephone number

Management information base (MIB): The provided MIB (management information base) defines the manageable objects of the Behnke station with names, IDs and data types.

It provides information that standard MIBs do not contain.

Notes and examples: This device only supports SNMPv3.
The following examples use the command line programmes snmpget, snmpset and snmpwalk. They assume that the supplied BEHNKE-STATION MIB file has been installed and use the IP address 192.168.16.200 and the default values for authentication (SHA & snmpadmin) and encryption (AES & snmpadmin) as examples.

read the registration status of the first SIP account
snmpget -v3 -u admin -l authPriv -a SHA -A snmpadmin -x AES -X snmpadmin 192.168.16.200 BEHNKE-STATION::TEMP-IP-STATE-1

read the call number for button 1
snmpget -v3 -u admin -l authPriv -a SHA -A snmpadmin -x AES -X snmpadmin 192.168.16.200 BEHNKE-STATION::BUTTONS-NUMBER-1

set name and call number for button 1
snmpset -v3 -u admin -l authPriv -a SHA -A snmpadmin -x AES -X snmpadmin 192.168.16.200

BEHNKE-STATION::BUTTONS-NAME-1 s 'Reception'
BEHNKE-STATION::BUTTONS-NUMBER-1 s '123'

read all TEMP settings
snmpwalk -v3 -u admin -l authPriv -a SHA -A
snmpadmin -x AES -X snmpadmin 192.168.16.200
BEHNKE-STATION::TEMP

Settings for SNMP

Port forwarding

HTTP port of the web server (80):

1 - 65535

Default: 80

forwarded port for accessing the web interface via an unsecured connection (HTTP)

When accessing the device behind a NAT, the port that is forwarded to port 80 of the device can be set here.

Port forwarding is normally detected automatically and it is not necessary to specify the forwarded port.

For devices with a camera, port forwarding must also be set up for port 8080 so that the camera image can be displayed in the web interface when accessing the device behind a NAT. This port forwarding cannot be detected automatically and must therefore be specified.

Important note
Although possible, setting up port forwarding for accessing the web interface via an unsecured connection (HTTP) is not recommended. Only a secure connection (HTTPS) should be used to access the device behind a NAT.

HTTPS port of the web server (443):

1 - 65535

Default: 443

forwarded port for accessing the web interface via an secured connection (HTTPS)

When accessing the device behind a NAT, the port that is forwarded to port 443 of the device can be set

here.

Port forwarding is normally detected automatically and it is not necessary to specify the forwarded port.

For devices with a camera, port forwarding must also be set up for port 8443 so that the camera image can be displayed in the web interface when accessing the device behind a NAT. This port forwarding cannot be detected automatically and must therefore be specified.

HTTP port of the IP camera (8080):

1 - 65535

Default: 8080

forwarded port for accessing the camera image via an unsecured connection (HTTP)

When accessing the device behind a NAT, the port that is forwarded to port 8080 of the device can be set here.

This port forwarding must be set up so that the camera image can be displayed in the web interface when accessing the device behind a NAT.

Important note
Although possible, it is not recommended to set up port forwarding to access the device via an unsecured connection (HTTP). Only a secure connection (HTTPS) should be used to access the device behind a NAT.

HTTPS port of the IP camera (8443):

1 - 65535

Default: 8443

forwarded port for accessing the camera image via an secured connection (HTTPS)

When accessing the device behind a NAT, the port that is forwarded to port 8443 of the device can be set here.

This port forwarding must be set up so that the camera image can be displayed in the web interface when accessing the device behind a NAT.

Settings for accessing the device behind a NAT

SIP	Network settings:	see section SIP phone

Network settings for SIP communication

SIP phone

see wiki

Direct SIP calls

Allow direct SIP calls:

- no
- yes

Default: no

This setting allows or forbids SIP direct calls.

With a SIP direct call, a SIP telephone calls another SIP telephone directly. To establish the connection, it is not the remote station's number that is required, but its IP address or host name. An IP telephone system (SIP server) is not required for this.

If, for example, a SIP telephone with the IP address 192.168.16.199 is to be called directly, configure the number for the desired button:

sip:192.168.16.199

If the remote station does not use the standard port 5060 but, for example, port 5070, then enter this in the call number as follows:

sip:192.168.16.199:5070

If a DNS server is available, you can also directly call the host name of the remote station. If this is, for example, phone.behnke-online.com, then configure the phone number:

sip:phone.behnke-online.com

If the device and remote station are in the same domain, it is sufficient to configure the following number:

sip:phone

When using host names, a port other than the standard port 5060 can also be specified.

pseudo SIP registration

Some SIP phones can only place a SIP call if they have previously performed SIP registration. So in such a case, direct SIP calls are not actually possible.

However, it is possible to register such a SIP phone at the Behnke station (pseudo SIP registration). To do this, one simply enters the IP address or host name of the Behnke station as the SIP server in the SIP account of the SIP telephone. Call number, user name, ID and password can be chosen as desired.

Pseudo SIP registration is only possible if direct SIP direct are allowed.

If the SIP telephone is then to be called from the Behnke station, the call number used for the pseudo SIP registration must be specified for the direct SIP call.

For example, if the SIP phone has the IP address 192.168.16.199 and you used 123 as the call number for the pseudo SIP registration of the SIP phone, then you configure the following as the call number:

sip:123@192.168.16.199

Accept incoming direct SIP calls:

- no
- only known call numbers
- only following numbers
- only known and following numbers
- yes

Default: yes

This setting determines whether an incoming direct SIP call may be accepted or not. It is possible to restrict call acceptance to known or specified numbers.

A call number is known if it is stored in the configuration for a call button, the i button of the keypad, a quick dialling number, a trigger or a phone book entry and if it triggers a direct SIP call.

Only the IP address or the host name is used to

	evaluate whether a direct SIP call number is known. Any user specified in the address is irrelevant for the evaluation. When using schedules, a call number is only considered known if it could also be dialled by the button or trigger at the time of the incoming call. schedule is valid when receiving a call The call number for the time periods of the schedule is considered known, but not the call number for the other time periods. schedule is invalid when receiving a call The call number for the other time periods of the schedule is considered known, but not the call number for the time periods of the schedule.
Direct SIP call numbers:	For an incoming direct SIP call, calls from the phone numbers specified here may be accepted. A direct SIP call number consists of the prefix sip: and the IP address or host name. A user can be specified in the address but is not required. To evaluate whether a direct SIP call number is known, only the IP address or host name is used. Any user specified in the address is irrelevant for the evaluation. It is possible to specify multiple phone numbers by separating each with a comma.

Settings for the direct connection with other SIP telephones

SIP account 1	Register:	• no • yes Default: no If the device is to be operated on a SIP server (IP telephone system), it must first register with it. To do this, a user with a phone number or name, ID and password is usually created in the SIP server. To register, the IP address of the SIP server is also required. You can obtain all this information from the administrator of the SIP server.

The administrator of the SIP server can also provide information about which port and which transmission protocol must be used to connect to the SIP server. In most cases, port 5060 and the UDP protocol are used.

If the transmission to the SIP server is to be encrypted, the TLS protocol and normally port 5061 are used. In this case, you may have to upload a certificate that identifies the SIP server as a trustworthy remote station.

The registration with the IP telephone system is repeated at regular intervals. This can be influenced by the registration timeout.

Registration state:

- unknown
- wait
- unregistered
- registration in progress
- registration failed
- registered

display of the registration state of the SIP account

In certain situations, for example if the device has just started or the settings have been saved in the 'SIP telephone' section, the device tries to establish a connection to the SIP server specified for this account and to register with it.

When the device tries to register, the registration state is displayed as 'registration in progress'. As soon as the result is known, the registration state is either 'registered' if the registration was successful or 'registration failed' otherwise.

If the settings for the SIP account are edited in the web interface, the registration state 'unknown' is displayed during editing until the settings are either saved or the changes are discarded.

When the SIP stack is started, the SIP accounts are in the 'wait' registration state for a brief moment, so briefly that this registration state is usually not visible in the web interface.

The registration status is 'not registered' if the setting 'Register' of the SIP account is set to 'no'.

Server: If a SIP server and a substitute SIP server are specified or if the domain is specified so that the SIP server to be used is queried via DNS, then the SIP server used is displayed here.

Phone number / user name : call number under which the device can be reached on the SIP server

User id: If the SIP server requires authentication during registration, the user ID and password are used.

Password: password for the registration at the SIP server

Communication:

- specify SIP server
- specify SIP server and substitute SIP server
- specify SIP registrar and SIP proxy
- specify SIP domain and request server via DNS

Default: specify SIP server

This setting defines how the connection to the IP telephone system should be made.

specify SIP server
A SIP server is specified with which the device registers and with which it communicates in the event of a call in order to establish the connection.

specify SIP server and substitute SIP server
Two SIP servers are specified, a main SIP server and a substitute SIP server.
The device first registers with the main SIP server and also communicates with it in the event of a call.
If communication with the main SIP server fails (no registration or connection error), the device registers with the substitute SIP server and also communicates with it in the event of a call.
If communication with the substitute SIP server also fails, then an attempt is made to switch back to the main SIP server.

specify SIP registrar and SIP proxy
Two servers are specified, a SIP registrar and a SIP proxy.
The device registers with the SIP registrar. When a call is made, communication takes place with the SIP proxy.

specify SIP domain and request server via DNS
A SIP domain is specified. During registration, a query is made via DNS NAPTR / SRV which SIP server is to be used for the specified domain.
The device then registers with this SIP server and also communicates with it in the event of a call.
If communication fails (no registration or connection error), the SIP servers available for the specified domain are queried again and an attempt is made to switch to another SIP server.

Domain: Domain name

Server: host name or IP address of the SIP server

Port: 1 - 65535

Default: 5060

port of the SIP server that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Substitute server: host name or IP address of the substiture SIP server

Port: 1 - 65535

Default: 5060

port of the SIP registrar that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Other user for substitute server:

- no
- yes

Default: no

This setting determines which user is to be used to

	register with the substitute SIP server. It is possible to use the same user as when registering on the main SIP server, or to specify another user with its own user ID and password.
Phone number / user name :	call number under which the device can be reached on the substitute SIP server
User id:	If the substitute SIP server requires authentication during registration, the user ID and password are used.
Password:	password for the registration at the substitute SIP server
Registrar:	host name or IP address of the SIP registrar
Port:	1 - 65535 **Default: 5060** port of the SIP registrar that is used for the SIP communication The following ports are normally used depending on the transmission protocol used: 5060 for UDP or TCP 5061 for TLS
Proxy:	host name or IP address of the SIP proxy
Port:	1 - 65535 **Default: 5060** port of the SIP proxy that is used for the SIP communication The following ports are normally used depending on the transmission protocol used: 5060 for UDP or TCP 5061 for TLS
Transmission protocol:	• **UDP** • **TCP** • **TLS**

Default: UDP

transmission protocol for the SIP communication

Port 5060 is normally used for SIP communication via the UDP or TCP protocol.

If the transmission to the SIP server is to be encrypted, the TLS protocol and normally port 5061 are used.

The encryption only affects the SIP protocol. Whether and how the audio and video data is encrypted during a SIP call can be set under 'Media encryption'.

Use SIPS:

- no
- yes

Default: no

This setting can be used to specify whether SIPS URIs are to be used or not.

A call to a SIPS URI is guaranteed to be encrypted from end to end. All SIP traffic within the call is secured with TLS from the sender to the domain of the final recipient. Once a SIP message reaches the final recipient's domain, it is securely sent to the final destination. The security mechanism for this final hop is determined by the domain of the final destination, and the use of TLS is not mandatory.

Use Behnke Station client certificate:

- no
- yes

Default: no

When registering via TLS, the SIP server proves its identity to the client (Behnke station) by means of a certificate.

The SIP server also has the option of verifying the identity of the client (mTLS) by requesting that it send its certificate.

This setting determines whether the Behnke station's certificate should be used as the client certificate. If this is not the case, you can upload your own

certificate, which will then become the client certificate.

Important note
Retrieving the client certificate by the SIP server is not standard, but an optional additional security measure to allow only trusted devices to access the SIP service.
Many SIP servers do not request a client certificate, so it is irrelevant whether a client certificate is stored or not.

Client certificate: information about the client certificate, if such a certificate has been uploaded

Certificate: upload / remove

upload
In most cases, authentication with the SIP server takes place via a user ID and password. An alternative option for authentication is that the SIP server requests the transmission of a client certificate.

If the SIP server needs a client certificate for authentication, such a certificate can be uploaded here in PEM format. A file is required that contains exactly one certificate with an unencrypted private key.
Once uploaded, the certificate information will appear under 'client certificate' above.

remove
The uploaded certificate can be removed here.

Registration timeout: 5 - 100000 s

Default: 3600 s

The registration at the SIP server is repeated shortly before the registration timeout expires.

NAT policy:

- use default NAT policy
- none
- use public IP address
- ICE with STUN server
- ICE with TURN server
- UPNP

Default: use default NAT policy

The NAT strategy can be specified individually for outgoing calls via this SIP account or the standard NAT strategy specified under 'NAT and firewall' can be used.

For incoming calls, the setting specified under 'NAT and firewall' is used.

STUN server: Default: stun.linphone.org

With the help of a STUN server, the device can determine the public IP address of the NAT router, as well as the public, externally used port that was assigned to a local port by the NAT.

This information is required when setting up a call.

TURN server: A TURN server acts as a relay server for the participants to enable communication across NAT or firewall boundaries.

TURN is used when solutions like STUN cannot be used. A TURN server normally requires authentication with a username and password.

TURN user: username for logging into the TURN server

TURN password: password for logging into the TURN server

AVPF mode:

- use default AVPF mode
- disabled
- enabled

Default: use default AVPF mode

The AVPF mode can be specified individually for outgoing calls via this SIP account or the setting specified under 'AVPF mode' can be used.

For incoming calls, the setting specified under 'AVPF mode' is used.

Avpf report interval: 0 - 5 s

Default: 1 s

Interval between RTCP reports when using AVPF/SAVPF

Accept incoming calls via this account:

- no
- only known call numbers
- only following numbers
- only known and following numbers
- yes

Default: yes

This setting determines whether an incoming call via this SIP account may be accepted or not. It is possible to restrict call acceptance to known or specified numbers.

A call number is known if it is stored in the configuration for a call button, the i button of the keypad, a quick dialling number, a trigger or a phone book entry and if it triggers a call via this SIP account.

When using schedules, a call number is only considered known if it could also be dialled by the button or trigger at the time of the incoming call.

schedule is valid when receiving a call
The call number for the time periods of the schedule is considered known, but not the call number for the other time periods.

schedule is invalid when receiving a call
The call number for the other time periods of the schedule is considered known, but not the call number for the time periods of the schedule.

Call numbers:

For an incoming call via this SIP account, calls from the phone numbers specified here may be accepted.

Only the plain phone number or username is specified without sip: and without appending the server or domain.

It is possible to specify multiple phone numbers by separating each with a comma.

Special configuration:

- none
- mediasec / 3ge2ae

Default: none

This setting allows the SIP communication for this account to be expanded with special functionalities.

This is only required for very special applications and should only be activated for these.

mediasec / 3ge2ae
When registering, the SIP server is informed of the use of the encryption type. When calling, the encryption type and the range of the encryption (end to access edge, encryption between device and registration server) is communicated.

Settings for the connection to a SIP server

SIP account 2

Register:

- no
- yes

Default: no

If the device is to be operated on a SIP server (IP telephone system), it must first register with it. To do this, a user with a phone number or name, ID and password is usually created in the SIP server. To register, the IP address of the SIP server is also required. You can obtain all this information from the administrator of the SIP server.

The administrator of the SIP server can also provide information about which port and which transmission protocol must be used to connect to the SIP server. In most cases, port 5060 and the UDP protocol are used.

If the transmission to the SIP server is to be encrypted, the TLS protocol and normally port 5061 are used. In this case, you may have to upload a certificate that identifies the SIP server as a trustworthy remote station.

The registration with the IP telephone system is repeated at regular intervals. This can be influenced by the registration timeout.

Registration state:

- unknown
- wait

- unregistered
- registration in progress
- registration failed
- registered

display of the registration state of the SIP account

In certain situations, for example if the device has just started or the settings have been saved in the 'SIP telephone' section, the device tries to establish a connection to the SIP server specified for this account and to register with it.

When the device tries to register, the registration state is displayed as 'registration in progress'. As soon as the result is known, the registration state is either 'registered' if the registration was successful or 'registration failed' otherwise.

If the settings for the SIP account are edited in the web interface, the registration state 'unknown' is displayed during editing until the settings are either saved or the changes are discarded.

When the SIP stack is started, the SIP accounts are in the 'wait' registration state for a brief moment, so briefly that this registration state is usually not visible in the web interface.

The registration status is 'not registered' if the setting 'Register' of the SIP account is set to 'no'.

Server: If a SIP server and a substitute SIP server are specified or if the domain is specified so that the SIP server to be used is queried via DNS, then the SIP server used is displayed here.

Phone number / user name: call number under which the device can be reached on the SIP server

User id: If the SIP server requires authentication during registration, the user ID and password are used.

Password: password for the registration at the SIP server

Communication:

- specify SIP server
- specify SIP server and substitute SIP server
- specify SIP registrar and SIP proxy

- specify SIP domain and request server via DNS

Default: specify SIP server

This setting defines how the connection to the IP telephone system should be made.

specify SIP server
A SIP server is specified with which the device registers and with which it communicates in the event of a call in order to establish the connection.

specify SIP server and substitute SIP server
Two SIP servers are specified, a main SIP server and a substitute SIP server.
The device first registers with the main SIP server and also communicates with it in the event of a call.
If communication with the main SIP server fails (no registration or connection error), the device registers with the substitute SIP server and also communicates with it in the event of a call.
If communication with the substitute SIP server also fails, then an attempt is made to switch back to the main SIP server.

specify SIP registrar and SIP proxy
Two servers are specified, a SIP registrar and a SIP proxy.
The device registers with the SIP registrar. When a call is made, communication takes place with the SIP proxy.

specify SIP domain and request server via DNS
A SIP domain is specified. During registration, a query is made via DNS NAPTR / SRV which SIP server is to be used for the specified domain.
The device then registers with this SIP server and also communicates with it in the event of a call.
If communication fails (no registration or connection error), the SIP servers available for the specified domain are queried again and an attempt is made to switch to another SIP server.

Domain: Domain name

Server: host name or IP address of the SIP server

Port: 1 - 65535

Default: 5060

port of the SIP server that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Substitute server: host name or IP address of the substiture SIP server

Port: 1 - 65535

Default: 5060

port of the SIP registrar that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Other user for substitute server:

- no
- yes

Default: no

This setting determines which user is to be used to register with the substitute SIP server.

It is possible to use the same user as when registering on the main SIP server, or to specify another user with its own user ID and password.

Phone number / user name : call number under which the device can be reached on the substitute SIP server

User id: If the substitute SIP server requires authentication during registration, the user ID and password are used.

Password: password for the registration at the substitute SIP server

Registrar: host name or IP address of the SIP registrar

Port: 1 - 65535

Default: 5060

port of the SIP registrar that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Proxy: host name or IP address of the SIP proxy

Port: 1 - 65535

Default: 5060

port of the SIP proxy that is used for the SIP communication

The following ports are normally used depending on the transmission protocol used:
5060 for UDP or TCP
5061 for TLS

Transmission protocol:

- UDP
- TCP
- TLS

Default: UDP

transmission protocol for the SIP communication

Port 5060 is normally used for SIP communication via the UDP or TCP protocol.

If the transmission to the SIP server is to be encrypted, the TLS protocol and normally port 5061 are used.

The encryption only affects the SIP protocol. Whether and how the audio and video data is encrypted during a SIP call can be set under 'Media encryption'.

Use SIPS:

- no

- yes

Default: no

This setting can be used to specify whether SIPS URIs are to be used or not.

A call to a SIPS URI is guaranteed to be encrypted from end to end. All SIP traffic within the call is secured with TLS from the sender to the domain of the final recipient. Once a SIP message reaches the final recipient's domain, it is securely sent to the final destination. The security mechanism for this final hop is determined by the domain of the final destination, and the use of TLS is not mandatory.

Use Behnke Station client certificate:

- no
- yes

Default: no

When registering via TLS, the SIP server proves its identity to the client (Behnke station) by means of a certificate.

The SIP server also has the option of verifying the identity of the client (mTLS) by requesting that it send its certificate.

This setting determines whether the Behnke station's certificate should be used as the client certificate. If this is not the case, you can upload your own certificate, which will then become the client certificate.

Important note
Retrieving the client certificate by the SIP server is not standard, but an optional additional security measure to allow only trusted devices to access the SIP service.
Many SIP servers do not request a client certificate, so it is irrelevant whether a client certificate is stored or not.

Client certificate: information about the client certificate, if such a certificate has been uploaded

Certificate: upload / remove

upload
In most cases, authentication with the SIP server takes place via a user ID and password. An alternative option for authentication is that the SIP server requests the transmission of a client certificate.

If the SIP server needs a client certificate for authentication, such a certificate can be uploaded here in PEM format. A file is required that contains exactly one certificate with an unencrypted private key.
Once uploaded, the certificate information will appear under 'client certificate' above.

remove
The uploaded certificate can be removed here.

Registration timeout:

5 - 100000 s

Default: 3600 s

The registration at the SIP server is repeated shortly before the registration timeout expires.

NAT policy:

- use default NAT policy
- none
- use public IP address
- ICE with STUN server
- ICE with TURN server
- UPNP

Default: use default NAT policy

The NAT strategy can be specified individually for outgoing calls via this SIP account or the standard NAT strategy specified under 'NAT and firewall' can be used.

For incoming calls, the setting specified under 'NAT and firewall' is used.

STUN server:

Default: stun.linphone.org

With the help of a STUN server, the device can determine the public IP address of the NAT router, as well as the public, externally used port that was assigned to a local port by the NAT.

This information is required when setting up a call.

TURN server: A TURN server acts as a relay server for the participants to enable communication across NAT or firewall boundaries.

TURN is used when solutions like STUN cannot be used. A TURN server normally requires authentication with a username and password.

TURN user: username for logging into the TURN server

TURN password: password for logging into the TURN server

AVPF mode:

- use default AVPF mode
- disabled
- enabled

Default: use default AVPF mode

The AVPF mode can be specified individually for outgoing calls via this SIP account or the setting specified under 'AVPF mode' can be used.

For incoming calls, the setting specified under 'AVPF mode' is used.

Avpf report interval: 0 - 5 s

Default: 1 s

Interval between RTCP reports when using AVPF/SAVPF

Accept incoming calls via this account:

- no
- only known call numbers
- only following numbers
- only known and following numbers
- yes

Default: yes

This setting determines whether an incoming call via this SIP account may be accepted or not. It is possible to restrict call acceptance to known or specified numbers.

A call number is known if it is stored in the configuration for a call button, the i button of the

keypad, a quick dialling number, a trigger or a phone book entry and if it triggers a call via this SIP account.

When using schedules, a call number is only considered known if it could also be dialled by the button or trigger at the time of the incoming call.

schedule is valid when receiving a call
The call number for the time periods of the schedule is considered known, but not the call number for the other time periods.

schedule is invalid when receiving a call
The call number for the other time periods of the schedule is considered known, but not the call number for the time periods of the schedule.

Call numbers: For an incoming call via this SIP account, calls from the phone numbers specified here may be accepted.

Only the plain phone number or username is specified without sip: and without appending the server or domain.

It is possible to specify multiple phone numbers by separating each with a comma.

Special configuration:

- none
- mediasec / 3ge2ae

Default: none

This setting allows the SIP communication for this account to be expanded with special functionalities.

This is only required for very special applications and should only be activated for these.

mediasec / 3ge2ae
When registering, the SIP server is informed of the use of the encryption type. When calling, the encryption type and the range of the encryption (end to access edge, encryption between device and registration server) is communicated.

Settings for the connection to a second SIP server

Encryption

Media encryption:

- none
- SRTP
- ZRTP
- DTLS

Default: none

After a SIP connection has been established, the participants exchange media data (audio and possibly video). Here you can set whether and how this media data should be encrypted.

Force media encryption:

- no
- yes

Default: no

In the case of forced media encryption, the connection setup fails if the remote station does not support the selected media encryption.

Verify server certificates:

- no
- yes

Default: yes

When using TLS as the transmission protocol, the SIP server transmits a certificate with information on the encryption.

Here you can set whether or not the validity of this server certificate is checked before use. If the server certificate is invalid, the registration with the SIP server will fail.

In order for a server certificate to be valid, it must be signed by a known, trusted authority (CA=certified authority). If the server certificate was signed by an unknown CA, the certificate of this CA can be installed in the device, so that the validity of the server certificate can be checked.

In addition, the server certificate contains the name or the IP address of the server (CN=common name). In order for the certificate to be valid, the CN must correspond to the entry in the 'Server' field of the corresponding SIP account.

Verify server CN:

- no

- yes

Default: yes

A server certificate contains the name or the IP address of the server (CN=common name). In order for the certificate to be valid, the CN must correspond to the entry in the 'Server' field of the corresponding SIP account.

Here you can set whether or not the CN of the server is checked when checking a server certificate.

Install additional trusted CAs:

- no
- yes

Default: no

If a connection is to be established to a SIP server with TLS as the transmission protocol, and this SIP server uses a certificate that was signed by a trustworthy authority (CA=certified authority) that is not known, then the registration at the SIP server fails.

So that the validity of the server certificate can be checked correctly, it is possible to make the device aware of additional CAs by uploading their certificate.

Additional trusted CA: information on the certificate of the trusted CA, if such a certificate has been uploaded

Certificate: upload / remove

upload
The certificate of a trustworthy CA can be uploaded in PEM format here. If the uploaded file contains several certificates, only the first certificate is installed. Once uploaded, the certificate information will appear under 'Additional trusted CA' above.

remove
The uploaded certificate can be removed here.

Additional trusted CA: additional trusted CA

Certificate: certificate

Settings for encrypted connections

NAT and firewall	
NAT policy:	• none • use public IP address • ICE with STUN server • ICE with TURN server • UPNP Default: none A separate NAT strategy can be defined for each SIP account, which is then used for outgoing calls via this SIP account. The NAT strategy specified here is used for all other calls.
STUN server:	Default: stun.linphone.org With the help of a STUN server, the device can determine the public IP address of the NAT router, as well as the public, externally used port that was assigned to a local port by the NAT. This information is required when setting up a call.
TURN server:	A TURN server acts as a relay server for the participants to enable communication across NAT or firewall boundaries. TURN is used when solutions like STUN cannot be used. A TURN server normally requires authentication with a username and password.
TURN user:	username for logging into the TURN server
TURN password:	password for logging into the TURN server
Public IP address:	public IP address of the NAT router

Settings for operation behind a NAT or firewall

AVPF	AVPF mode:	• disabled • enabled Default: disabled AVPF increases the reliability of video connections because it allows quick error correction when transmission errors occur. A separate setting for the AVPF mode can be defined for each SIP account, which is then used for outgoing calls via this SIP account. The setting specified here for the AVPF mode is used for all other calls.
	Avpf report interval:	0 - 5 s Default: 1 s interval between RTCP reports when using AVPF/SAVPF

Settings for the AVPF mode

Voice codecs	#1:	• none • G.711 A-law (PCMA) • G.711 µ-law (PCMU) • G.722 • G.729 • GSM • iLBC • Speex (8 kHz) • Speex (16 kHz) Default: G.711 µ-law (PCMU)
	#2:	• none • G.711 A-law (PCMA) • G.711 µ-law (PCMU) • G.722 • G.729 • GSM • iLBC • Speex (8 kHz) • Speex (16 kHz) Default: G.711 A-law (PCMA)

#3:
- none
- G.711 A-law (PCMA)
- G.711 µ-law (PCMU)
- G.722
- G.729
- GSM
- iLBC
- Speex (8 kHz)
- Speex (16 kHz)

Default: G.729

Preference list of supported voice codecs

Video codecs

#1:
- none
- H.264
- VP8

Default: H.264

#2:
- none
- H.264
- VP8

Default: VP8

Preference list of supported video codecs

Cipher suites

#1:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: AEAD_AES_128_GCM

#2:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: AES_CM_128_HMAC_SHA1_80

#3:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: AEAD_AES_256_GCM

#4:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: AES_256_CM_HMAC_SHA1_80

#5:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: none

#6:
- none
- AES_CM_128_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

Default: none

Preference list of supported cipher suites

Payload types

Telephone-event:

96 - 127

Default: 101

H.264:
- set manually
- set automatically

Default: set automatically

96 - 127

Default: 96

VP8:

- set manually
- set automatically

Default: set automatically

96 - 127

Default: 96

Setting of the preferred payload types

Early Media

For outgoing calls:

- refuse
- allow

Default: allow

If the called remote station supports and requests 'early media', the microphone signal and the video from the camera can be transmitted to the remote station on an outgoing call before it has accepted the connection.

This allows the remote station to identify the caller before accepting the connection.

If the connection is established via a SIP server, the SIP server must also support 'early media'.

For group calls:

- refuse
- allow

Default: refuse

This setting determines whether Early Media is also sent during group calls.

Important note
Early Media group calls require a lot of system resources depending on the SIP video resolution and the number of called parties and can cause delays in other processes (sound output, recognition of keystrokes, ...).

Audio and video transmission before accepting a connection

Media management

For outgoing calls:

- early offer / SDP in INVITE
- late offer / SDP in ACK

Default: early offer / SDP in INVITE

In a SIP call, a participant describes the codecs and the media he supports in the SDP. This SDP is then exchanged with the remote station in order to determine the codec or the codecs or media that are to be used for the connection.

There are two options for outgoing connections:

early offer / SDP in INVITE
With 'early offer', the SDP is sent to the remote station when the connection is established in the INVITE. The remote station then decides which codecs or media should be used for the connection and then sends its SDP when the connection is accepted.

late offer / SDP in ACK
With the 'late offer' an INVITE without SDP is sent to the remote site when the connection is established. If the remote site wants to accept the connection, it sends back its SDP. The caller uses this to decide which codecs or media should be used for the connection and sends then its SDP in the ACK back to the remote station.

Negotiation of codecs and media for a connection

Packetization

Transmission ptime:

- use the default value of the codec
- 10 ms
- 20 ms
- 30 ms
- 40 ms
- 50 ms
- 60 ms
- 70 ms
- 80 ms
- 90 ms
- 100 ms
- 110 ms
- 120 ms
- 130 ms
- 140 ms
- 150 ms

	• 160 ms • 170 ms • 180 ms • 190 ms • 200 ms Default: use the default value of the codec
Reception ptime:	• do not specify • 10 ms • 20 ms • 30 ms • 40 ms • 50 ms • 60 ms • 70 ms • 80 ms • 90 ms • 100 ms • 110 ms • 120 ms • 130 ms • 140 ms • 150 ms • 160 ms • 170 ms • 180 ms • 190 ms • 200 ms Default: do not specify

Setting the package size for voice and video transmission

SIP video	Video transmission:	• no • show only incoming video Default: show only incoming video
	Preferred video resolution:	• QCIF = 176x144 • QVGA = 320x240 • CIF = 352x288 • VGA = 640x480 • 4CIF = 704x576 • SVGA = 800x600 • XGA = 1024x768 • 720P = 1280x720

Default: CIF = 352x288

Important notice
The use of a high SIP video resolution requires a lot of system resources and can lead to the delay of other processes (sound outputs, recognition of keystrokes, ...). In this case, the SIP video resolution or the maximum framerate should be reduced.

Maximum framerate:

1 - 30 fps

Default: 15 fps

This setting can be used to limit the number of images that are transmitted to the remote station per second during a SIP video connection.

Keyframe rate:

- use the default value of the codec
- high
- automatic

Default: automatic

SIP video codecs transmit a complete picture (keyframe) from time to time and only the picture changes in between.

For most cases, the default of the codec can and should be used. However, some systems require the transmission of keyframes at short intervals. This can then be achieved using this setting.

When set to 'automatic', the default codec is used unless it is detected that a SIP account is connected to a SIP server that is known to require a high keyframe rate. In such a case, a high keyframe rate is automatically used for all SIP accounts.

Adjust video direction:

- no
- yes

Default: yes

If it is configured that SIP video transmission should only be in one direction, then the video direction is adjusted and indicated in the SDP accordingly that video can only be sent or only received.

This setting can be used to specify whether or not to

		adjust the video direction. If the video direction is not adjusted, then in the case of a video connection, the SDP always indicates that video can be received and sent.
	General image settings:	see section Camera

Settings for SIP connections with video transmission

Network	MTU for RTP packets:	500 - 3000 bytes Default: 1500 bytes
	Sending DTMF tones:	• use SIP INFO • use RFC 2833 Default: use RFC 2833 method used to send DTMF tones This setting only affects DTMF tones that are sent from the device during a SIP connection, for example by after dialing via the keypad, if this is allowed. The remote station must support the set method so that it can recognize the sent DTMF tones.
	SIP over UDP/TCP:	• port disabled • random port • selected port Default: selected port local port of the device for the SIP communication via UDP/TCP Here the port is set that is used for incoming and outgoing SIP communication if UDP or TCP is used as the transmission protocol. Port 5060 is normally used for this. If this device is to be called by a SIP direct call via UDP/TCP, the port set here must also be specified if it differs from the standard value 5060. With UDP/TCP, the port used by a SIP server (IP telephone system) to which the device is connected is

normally also 5060. The port of the SIP server is not specified here, but in the corresponding SIP account under 'Port'.

Important notice
If incoming SIP direct calls are to be accepted with this device, a defined port must be selected.

Port: 1 - 65535

Default: 5060

SIP over TLS:
- port disabled
- random port
- selected port

Default: selected port

local port of the device for the SIP communication via TLS

The port that is used for incoming and outgoing SIP communication is set here if TLS is used as the transmission protocol. Port 5061 is normally used for this.

If this device is to be called using a SIP direct call via TLS, the port set here must also be specified if it differs from the standard value 5061.

With TLS, the port that a SIP server (IP telephone system) to with which the device is connected is usually also 5061. The port of the SIP server is not specified here, but in the corresponding SIP account under 'Port '.

Port: 1 - 65535

Default: 5061

Port or port range for audio streaming: Default: 7078

local port of the device for sending and receiving audio via RTP

With a SIP call, the audio data is transmitted from this port to the remote station and the audio data from the remote station is received on this port.

A single port, for example 7078, can be specified or a port range, for example 7078-7080. If a port range is specified, a port from this range is selected when a call is made.

Port or port range for video streaming:

Default: 9078

local port of the device for sending and receiving video via RTP

With a SIP call, the video data is transmitted from this port to the remote station and the video data from the remote station is received on this port.

A single port, for example 9078, can be specified or a port range, for example 9078-9080. If a port range is specified, a port from this range is selected when a call is made.

DSCP for SIP:

- 0x00 = BE
- 0x0a = AF11
- 0x0c = AF12
- 0x0e = AF13
- 0x12 = AF21
- 0x14 = AF22
- 0x16 = AF23
- 0x1a = AF31
- 0x1c = AF32
- 0x1e = AF33
- 0x22 = AF41
- 0x24 = AF42
- 0x26 = AF43
- 0x2e = EF

Default: 0x1a = AF31

classification for IP packets sent with the SIP protocol

With such a classification, it can be achieved in network infrastructures that support this that certain IP packets are forwarded with priority.

The classification AF31 (multimedia streaming) is normally used for the SIP protocol.

DSCP for audio streaming:

- 0x00 = BE
- 0x0a = AF11
- 0x0c = AF12

- 0x0e = AF13
- 0x12 = AF21
- 0x14 = AF22
- 0x16 = AF23
- 0x1a = AF31
- 0x1c = AF32
- 0x1e = AF33
- 0x22 = AF41
- 0x24 = AF42
- 0x26 = AF43
- 0x2e = EF

Default: 0x2e = EF

classification of the IP packets sent during audio transmission

With such a classification, it can be achieved in network infrastructures that support this that certain IP packets are forwarded with priority.

The highest classification EF (expedited forwarding) is normally used for audio transmission in order to forward the packets as quickly as possible.

DSCP for video streaming:

- 0x00 = BE
- 0x0a = AF11
- 0x0c = AF12
- 0x0e = AF13
- 0x12 = AF21
- 0x14 = AF22
- 0x16 = AF23
- 0x1a = AF31
- 0x1c = AF32
- 0x1e = AF33
- 0x22 = AF41
- 0x24 = AF42
- 0x26 = AF43
- 0x2e = EF

Default: 0x00 = BE

classification of the IP packets sent during video transmission

With such a classification, it can be achieved in network infrastructures that support this that certain IP packets are forwarded with priority.

The lowest classification BE (best effort) is normally used for video transmission. This means that the packets are forwarded as well as possible. This ensures that more important packets, for example audio data, can be forwarded first.

Audio jitter compensation:

0 - 200 ms

Default: 60 ms

If the audio data sent by the remote station arrives late due to a fluctuating network bandwidth, then there is jitter, a drop in the audio signal.

Jitter compensation can prevent such disruptive dropouts by keeping the audio signal transmitted by the remote station available for a certain time. This means that the audio signal from the remote station is output with a slight delay, which enables jitter to be compensated for within the set duration.

Video jitter compensation:

0 - 200 ms

Default: 60 ms

If the video data sent by the remote station arrives late due to a fluctuating network bandwidth, then there is jitter, a drop in the video signal.

Jitter compensation can prevent such disruptive dropouts by keeping the video signal transmitted by the remote station available for a certain time. This means that the video signal from the remote station is output with a slight delay, which enables jitter to be compensated for within the set duration.

Maximum available download bandwidth:

- do not specify
- 100 kBit/s
- 200 kBit/s
- 300 kBit/s
- 400 kBit/s
- 500 kBit/s
- 600 kBit/s
- 700 kBit/s
- 800 kBit/s
- 900 kBit/s
- 1 MBit/s
- 2 MBit/s

- 3 MBit/s
- 4 MBit/s
- 5 MBit/s
- 6 MBit/s
- 7 MBit/s
- 8 MBit/s
- 9 MBit/s
- 10 MBit/s
- 20 MBit/s
- 30 MBit/s
- 40 MBit/s
- 50 MBit/s
- 60 MBit/s
- 70 MBit/s
- 80 MBit/s
- 90 MBit/s
- 100 MBit/s

Default: 300 kBit/s

This information is passed on to the remote station during the call so that the remote station has sufficient information to configure its audio and video codec output bit rate correctly so that the available bandwidth is not exceeded.

Maximum available upload bandwidth:

- do not specify
- 100 kBit/s
- 200 kBit/s
- 300 kBit/s
- 400 kBit/s
- 500 kBit/s
- 600 kBit/s
- 700 kBit/s
- 800 kBit/s
- 900 kBit/s
- 1 MBit/s
- 2 MBit/s
- 3 MBit/s
- 4 MBit/s
- 5 MBit/s
- 6 MBit/s
- 7 MBit/s
- 8 MBit/s
- 9 MBit/s
- 10 MBit/s
- 20 MBit/s
- 30 MBit/s
- 40 MBit/s

	• 50 MBit/s • 60 MBit/s • 70 MBit/s • 80 MBit/s • 90 MBit/s • 100 MBit/s Default: 1 MBit/s This information, together with the signalled remote side available bandwidth, is used to properly configure the output bit rate of the audio and video codec.
Adaptive bitrate control:	• no • yes Default: yes Adaptive bitrate control uses RTCP feedback information to dynamically control the output bitrate of the audio and video encoders, allowing them to adapt to network conditions and available bandwidth.
General network settings:	see section Network

Network settings for SIP communication

SIP communication	Expert settings:	• use default settings • set individually Default: use default settings Change expert settings only after consulting the hotline!
	Omit unique route:	• no • yes Default: yes
	Normalize call number:	• no • yes Default: no

Custom size of keep-alive packets:

1 - 727 x CRLF

Default: 2 x CRLF

This setting allows a user-defined size for keep-alive packets. If the value x is set, the keep-alive packets consist of x repeated CRLF sequences.

Care must be taken to ensure that the total size of the keep-alive packets, including the offset, does not exceed the MTU.

Important note
With SIP over UDP, keep-alive packets are used to keep NAT bindings open and are typically very small. According to RFC 5626, a keep-alive consists of a double CRLF, i.e. 4 bytes. Any other size may cause technical problems simply because it is not RFC-compliant.

Identify incoming calls by Via:

- no
- yes

Default: no

IP video call number:

- default number
- number of the remote station
- contact of the remote station

Default: default number

call number that is transmitted to the IP video software

By default, the dialled number is transmitted for an outgoing call and the number of the remote station for an incoming call. This setting determines whether the call number or contact information of the remote station transmitted via the SIP protocol should be transmitted to the IP video software after a connection has PBX, the evaluation of the contact information provides a better result.

Important note
The function cannot be guaranteed in all cases. When using the function, a check of the various call scenarios (group call, pick-up, forwarding, ...) should be carried out with the SIP PBX used.

Use sip.instance:

- no
- yes

Default: yes

Special settings for the SIP communication

IP intercom

To use Behnke stations as an IP intercom system, observe the following points:

- The administrator password is a global setting and must be the same for all intercom devices.
- Each device belongs to a group. An intercom system can be divided into up to 9 groups.
- Outdoor stations have no ID. Indoor stations have an ID between 1 and 99.
- All outdoor stations of the same group are displayed in the phone book of an indoor station.
- An outdoor station can call indoor stations in the same group by dialling the ID as the call number.
- In the 'IP intercom' operation mode, buttons for which no call number is configured dial their button number: button 1 calls ID 1, button 2 calls ID 2 and so on. As a result, the buttons of an outdoor station are already assigned to the indoor stations of the same group in delivery state.
- A door opener code can be configured for each indoor station. This code can then be used at all outdoor stations in the same group that have a code lock function.
- All intercom devices require firmware version 5.85 or newer. Ideally, the firmware is synchronised, i.e. all devices use the same version.

See manual under Implementation of an IP intercom system .

Device:	display of the device type with name
Group:	1 - 9 **Default: 1** This setting defines the intercom group for this device. Outdoor and indoor stations of the same group can establish directly a connection with each other.All detected outdoor stations of the same intercom group are automatically displayed in the phone book of an indoor station. In the delivery state, the buttons of an outdoor station are already assigned to the indoor stations of the same group. Button 1 of an outdoor station therefore calls the indoor station(s) with ID 1 of the same group, button 2 calls the indoor station(s) with ID 2 and so on.
ID:	1 - 99

Default: 1

This setting defines the intercom ID of this indoor station.

The intercom ID is used to determine the call number under which the indoor station(s) can be reached in intercom mode.

Calling an indoor station of the same group
Within the same intercom group, the ID can be dialled directly as the call number. For example, if an outdoor station calls 2, all indoor stations in the same intercom group with ID 2 are called.

Button assignment in delivery state
If no call number is configured for an outdoor station button, it calls in intercom mode the ID that corresponds to the button number.
If no call number is configured, button 1 of an outdoor station calls the indoor station(s) with ID 1 of the same group, button 2 calls the indoor station(s) with ID 2 and so on.

Calling an indoor station of another group
To call indoor stations of another group, a 3-digit call number is used. This starts with the intercom group followed by the two-digit intercom ID.
For example, to call the indoor stations of group 2 with ID 1, use the call number 201.

Calling an indoor station in hybrid mode
If an outdoor station is used in hybrid mode, indoor stations can be called in intercom mode by specifying com: before the call number.
So if the indoor stations with ID 1 are to be called, configure the following as the call number:
com:1

Media encryption:

- none
- SRTP
- ZRTP
- DTLS

Default: ZRTP

After a connection has been established, the participants exchange media data (audio and possibly video). Here you can set whether and how

this media data should be encrypted.

Changing global settings: see section Global settings

Indoor station

Reset selection after: 3 - 30 s

Default: 5 s

If the user starts searching in the phone book but does not continue the search, i.e. no longer presses a display key, the phone book will be reset to the main selection after the time set here and the first entry will be displayed again.

Search of the initial letter:

- no
- if 10 or more entries
- if 15 or more entries
- if 20 or more entries
- if 25 or more entries
- if 30 or more entries
- yes

Default: if 10 or more entries

The user can restrict the displayed entries to a certain initial letter in order to find the desired entry more quickly in a telephone book with many entries.

For this purpose, a button with a magnifying glass and the character A is shown on the display to the right of the arrow keys  , if this is allowed by this setting.

If the user presses the magnifying glass key, a screen is displayed with all the initial letters that appear in the telephone book. The user can then press one of the initial letters to display a restricted phone book that only consists of entries that begin with this initial letter.

The user can then select one of these entries or use 'return' to go to the main selection of the phone book.

Skipping from the last to the first entry and vice versa:

- refuse
- allow

Default: allow

If the last entry in the phone book is reached when scrolling down with ↓, it is possible to jump back to the first entry by pressing ↓ again, if this setting allows this.

The same applies to scrolling up with ↑ when the first entry is reached. If you press ↑ again, you can jump to the last entry.

If you keep one of the arrow keys ↓ or ↑ pressed, you will continue to scroll in the corresponding direction until the end or the beginning is reached. By pressing the arrow key again, you can jump to the beginning or end, if this is allowed.

Set preferred device:

- refuse
- allow

Default: allow

This setting determines whether or not a preferred device can be specified.

If a preferred device may be specified, the star key is displayed on the main screen.

The entries in the phone book are sorted alphabetically. It is possible to designate a device of particular interest, such as the main entrance, as the preferred device. The preferred device is then displayed as the first entry in the telephone book for quick and easy access.

To set a device as the preferred device, first select it using the arrow keys and then press the star key. The device is then placed at the top of the phone book and a yellow star indicates that it is the preferred device.

To set a different device as the preferred device, simply select it and then press the star key. To remove a preferred device, select the preferred device and then press the yellow star key.

In addition to sorting the phone book, the preferred device can also be used for the 'automatic preview' function.

Toggle ringtone volume:

- refuse
- allow

Default: allow

This setting determines whether the ringtone volume can be switched via the main screen.

If so, a corresponding icon will be displayed in the upper right corner of the main screen.

It is always possible to change the ringtone volume via the web interface in the 'Acoustics' section.

Preview when leaving the screensaver:

- no
- yes

Default: no

In the case that the phone book only contains a single station, this setting determines whether or not the preview of this station should be displayed directly when exiting the screen saver.

Show station name:

- no
- yes

Default: yes

This setting determines whether or not the station name of the indoor station should be displayed at the top of the main screen of the indoor station.

Show station information:

- no
- yes

Default: yes

This setting determines whether or not the station information (ID, group and station name) should be displayed when the configuration is called up on the indoor station.

User login:

- refuse
- allow

Default: allow

This setting determines whether users are allowed to

log in to the indoor station to change the user settings.

The user password is empty on delivery. Each user can log in to their indoor station and set their own user password for their indoor station.

Display synchronised time:

- no
- yes

Default: yes

This setting determines whether the current time is displayed or not.

Important note
The time is only displayed if time synchronisation with the NTP time server configured in the 'network' section has been successful.
After restarting the indoor station, it may take a short time for synchronisation with the time server to be completed and the time to be displayed.

Settings of the main screen of the indoor station function

Interior door

Connection:

- no
- yes, bell button
- yes, door opener
- yes, bell button & door opener

Default: no

An interior door is the access to the area in which the indoor station is installed and where no Behnke-Station is installed.

If the interior door has a bell button and/or a door opener, it is possible to connect these to the indoor station. If the bell button is pressed, a signal is sent to the indoor station and it is possible to activate the door opener of the interior door to open it.

This setting can be used to specify whether and how an internal door is connected.

bell button
When the bell button is pressed, an acoustic and

visual signal is emitted at the indoor station.
The ringtone used can be set in the 'acoustics' area.

door opener
When a door opener is connected, a door opener button for the interior door is displayed on the indoor station.
If this is pressed, relay 1 is activated if it has been configured as a door opener relay.

Signaling duration of a bell button press:	5 - 60 s Default: 15 s When the bell button of the interior door is pressed, the indoor station is signalled. This setting can be used to specify how long this signalling takes place.

Integration of an additional access door without Behnke station

Code lock function	Code for relay 1:	Default: 2580 The code defined here can then be used at all outdoor stations in the same group that have a code lock function with relay 1 as the door release relay. If an outdoor station of another group is assigned to this indoor station via a button or a phone book entry, the code also applies to its code lock function.
	Code for relay 2:	The code defined here can then be used at all outdoor stations in the same group that have a code lock function with relay 2 as the door release relay. If an outdoor station of another group is assigned to this indoor station via a button or a phone book entry, the code also applies to its code lock function.

Codes for the code lock function of then outdoor stations

Video surveillance	Automatic preview:	• no • preferred device • yes

Default: no

An indoor station can request an automatic preview from a specific or all Behnke outdoor stations in its intercom group, provided that these have a camera and motion detection is enabled.

With automatic preview, the outdoor station informs the indoor station about any detected movement.

An acoustic signal is then emitted at the indoor station and the preview of the outdoor station is automatically displayed.

To request an automatic preview of a specific outdoor station, use the 'preferred device' setting and select the relevant outdoor station as the preferred device.

The automatic preview can also be switched via the main screen of the indoor station, provided that this is permitted via the 'toggle automatic preview' setting.

Important note
Check whether the use of the automatic preview is possible and permissible under the legal regulations of your country or your company.

Toggle automatic preview:

- refuse
- allow

Default: allow

This setting determines whether the automatic preview can be switched via the main screen.

If so, a corresponding icon will be displayed in the upper left corner of the main screen.

It is always possible to switch the automatic preview via the web interface.

Event history duration:

- disabled
- 1 min
- 2 min
- 3 min
- 4 min

- 5 min
- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 45 min
- 1 h
- 2 h
- 3 h
- 4 h
- 5 h
- 6 h
- 7 h
- 8 h
- unlimited

Default: 3 min

When an automatic preview is triggered, the device that triggered it is recorded in an event history.

This can contain a maximum of 3 different devices. If more devices trigger an automatic preview, older entries are removed and only the 3 most recent ones are retained.

This setting determines how long an entry remains in the event history. After the set period has elapsed, older entries are automatically removed from the event history.

As soon as there are entries in the event history, a corresponding icon is displayed at the top left of the main screen of the indoor station and the names of the devices are listed below it.

Pressing the icon displays the preview of all devices in the event history. If there are multiple devices, the video from the device that last triggered the automatic preview is displayed in full size and the other videos are displayed in small size.

Important note

The event history is not stored permanently and will therefore be lost if the device is restarted or fundamentally reconfigured.

Delete history after viewing:

- no
- yes

Default: yes

This setting determines whether the event history should be deleted after being called up or not.

Video preview when motion is detected

Call history

Call history duration:

- disabled
- 1 min
- 2 min
- 3 min
- 4 min
- 5 min
- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 45 min
- 1 h
- 2 h
- 3 h
- 4 h
- 5 h
- 6 h
- 7 h
- 8 h
- unlimited

Default: 3 min

The last incoming call is recorded in the call history.

If further calls are received, only the last incoming call is retained in the call history.

This setting determines how long the entry remains in the call history. Once the set period has expired, the entry is automatically removed from the call history.

As soon as there is an entry in the call history, a corresponding icon is displayed in the top right-hand corner of the main screen of the indoor station and the name of the device is displayed below it.

Pressing the icon displays a preview of the device in the call history.

Important note

The event history is not stored permanently and will therefore be lost if the device is restarted or fundamentally reconfigured.

Delete history after viewing:

- no
- yes

Default: yes

This setting determines whether the call history should be deleted after being called up or not.

Settings for the last incoming call

Network bridge

Remote station:

Intercom devices can automatically find each other within the same network and exchange information.

If the devices are distributed across several networks, it is necessary to connect the networks with each other by setting up network bridges.

To set up a network bridge, use this setting to specify the IP address or host name of a device in another network.

This makes this device the active bridgehead. It attempts to establish a connection to the remote station, the passive bridgehead. If this is successful, the bridge goes 'online' and information is regularly exchanged in both directions.

If the devices are distributed across more than two networks, additional network bridges can be set up.

Important notes

- For a multi-network intercom system to function reliably, every device in the intercom system must be able to reach every other device directly via the network - regardless of which network it is in.
- If the passive bridgehead is specified via an IP address that it has received via DHCP, it is

essential to create a reservation for this address so that it does not change.
- The same device can take on the role of one active bridgehead and up to 3 passive bridgeheads.
- If a bridgehead fails, it can take up to 3 minutes before this is recognised and the devices previously transmitted via the bridge are removed.
- A network bridge always works in both directions. It is not necessary to set up a network bridge for the return path.
- If you set up a bridge between A and B and another one between B and C for networks A, B and C, then A is also connected to C. It is not necessary to set up a network bridge between A and C.
- To avoid unnecessary network traffic, you should refrain from setting up unnecessary network bridges.

Bridge: display for a network bridge whether the device (active bridgehead) is connected to the remote station (passive bridgehead)

OFFLINE
There is currently no connection to the remote station.

ONLINE
The device is currently connected to the remote station.

If a bridgehead fails, it can take up to 3 minutes before this is recognised and the bridge is displayed as 'offline'.

Settings and information for a multi-network intercom system

Synchronisation

Firmware status:
- not synchronised
- synchronised

display of the firmware status of the intercom system

not synchronised

There are devices with different firmware versions. Synchronisation to the latest firmware version should be performed.

synchronised
All detected devices use the same firmware version.

Version of this device: display of the installed firmware version

The changes between each firmware version are described in the Technical Manual.

See manual under Version History.

Firmware: synchronise / update / check for update

synchronise
By 'synchronising', the firmware version of this device can be installed on all other devices of the intercom system.

Important notes:

- In the delivery state or after a hardware reset, synchronisation is not possible because no firmware file is available. In these cases, the firmware of the device must be updated first, even if it is the same version.
- If devices from different platforms (P1, P2 and so on) are part of the intercom system, at least one device for each platform must have the firmware version to be synchronized to.
- While synchronisation is in progress, no firmware updates or synchronisation on another device may be performed, otherwise the synchronisation will be aborted and fail.

update
A new firmware can be uploaded here in order to install it on the system.
A firmware is required that is suitable for the platform (P1, P2 and so on) of the system.

check for update
A connection to the support server will be established to check whether there is new firmware for this device.
If so, the new firmware can be downloaded from the link provided. When the firmware file has been

downloaded completely, it can then be installed using 'update'.
If the computer cannot or is not allowed to establish an Internet connection, then it is not possible to contact the support server and thus check the firmware version.

Firmware synchronisation:

If a firmware synchronisation is carried out, the partial step carried out or the progress of the installation are displayed here.

If a firmware synchronisation could not be completed successfully, 'failed' is displayed here for a short time. In this case, the firmware synchronisation must be restarted.

Firmware update:

If a firmware update is carried out, the partial step carried out or the progress of the installation are displayed here.

If a firmware update could not be completed successfully, 'failed' is displayed here for a short time. In this case, the firmware update must be restarted.

Installing the same firmware version on all devices

IP stations

Number: 0 - 10

Default: 0

Using Behnke stations (=BS, Generation 3) as intercom devices is very easy, as they can communicate directly with each other via the IP network.

In addition, a Behnke indoor station also allows the integration of IP stations. IP stations are other SIP telephones with IP cameras, such as Behnke SIP telephones (=BT-IP) of generations 1 and 2, or IP cameras.

This setting determines how many of these IP stations are to be integrated. A group is then displayed for each IP station, which can be used to specify the necessary information.

The specified IP stations only apply to this indoor station.Please note that functionality is not guaranteed when integrating SIP telephones from other manufacturers.

The functionality of the indoor station in conjunction with IP stations is limited to preview, connection and door opening or only to video preview when an IP camera is integrated. IP stations are not displayed in the topology, are not included in firmware synchronisation, and the codes set in the indoor station for the code lock function do not apply to IP stations.

Station: **remove**

remove
If several IP stations have been created and one is no longer needed, it can be deleted using 'remove'. If there are subsequent IP stations, they will move up one position.

Inclusion of non-Behnke stations in the indoor station

IP station 1

Type:

- **BT-IP generation 1**
- **BT-IP generation 2**
- **other SIP phone**
- **IP camera**

Default: BT-IP generation 2

type of SIP phone to be integrated

BT-IP Generation 1
First-generation Behnke SIP phone. These devices usually have a 'Behnke type B' IP camera.

BT-IP Generation 2
Second-generation Behnke SIP telephone. These devices have a 'Behnke type A' or 'Behnke type B' IP camera.

Other SIP telephone
Please note that functionality is not guaranteed when integrating SIP telephones from other manufacturers.

IP camera
IP camera that provides a suitable MJPG video stream.

Name: This name is displayed in the indoor station's phone book or during preview or connection with the device.

Call number: Calls to and from IP stations can be made either as direct SIP calls or via a SIP account.

direct SIP calls
Direct SIP calls can be made directly in 'IP intercom' mode. Hybrid mode is not required.

calls via a SIP account
The indoor station must be operated in hybrid mode so that intercom and SIP telephone functionality can be used, and the indoor station must be connected to a SIP telephone system via a SIP account.
The phone number of the IP station must always be specified with the prefix sip1: for the first SIP account or sip2: for the second SIP account.

IP address or host name: IP address or host name of the SIP telephone

If an IP address is specified, it must be ensured that it does not change in the future. This is the case in a network with static IP address assignment. If, on the other hand, the SIP telephone receives an address from a DHCP server, a reservation of a fixed IP address can be created in the DHCP server for the SIP phone so that it does not change.

If a DHCP reservation is not possible, the unique host name of the SIP telephone can also be specified.

Access type:

- access
- door
- wicket
- gate
- car access
- barrier
- access with own designation
- car access with own designation

Default: access

This setting indicates which type of access should be opened.

Depending on this setting, the pictograms and texts displayed when opening the access are adapted.

UDP code to open access:

IP stations of the 'BT-IP' type allow doors to be opened via the UDP remote control protocol, regardless of whether a connection exists or not.

This setting specifies the code that must be sent to the IP station via the UDP remote control protocol in order to open access.

For a 'BT-IP generation 1' device, the UDP code is configured in the BT-IP under Settings Hardware → Status/Remote Control → Authentication Code.

For a 'BT-IP generation 2' device, the UDP code is configured in the BT-IP under Settings → Relay Settings → Relay Activation Code → Web Interface.

For door opening via the UDP code to work, the IP address or host name of the BT-IP must also be specified and the UDP remote control protocol must be activated in the BT-IP.

DTMF code to open access:

SIP door stations usually allow access to be opened during a connection when a specific DTMF code is received.

This setting specifies the code that must be sent to the IP station to open access.

During an established connection with the IP station, this code is sent via DTMF. For devices of the 'BT-IP' type, a # is automatically appended.

If the opening of the IP station access is triggered at the indoor station during a connection, the DTMF code is sent to the IP station and a corresponding visualisation appears at the indoor station. After setup, you should check that the IP station actually opens the access. Since no feedback is received from the IP station, it is possible that the visualisation occurs even though the IP station does not open the access, for example because the wrong code is set.

Webhook to open access:

If the opening of the access is triggered at the indoor station during a preview of an IP camera, the webhook specified in this setting is sent and a corresponding

visualisation is displayed on the indoor station. After setup, you should check that access is actually opened by sending the webhook.

Body:

The data transmitted in the request body of the webhook will be specified here.

Visualised opening duration:

1 - 90 s

Default: 5 s

When the opening of the IP station access is triggered at the indoor station, a corresponding visualisation is displayed at the indoor station.

This setting determines how long this visualisation is displayed. It should be set so that it corresponds to the activation duration of the door opener relay of the IP station.

Camera type:

- Behnke type A
- Behnke type B
- other

Default: Behnke type A

type of the IP camera

Behnke type A
This type applies to Behnke IP camera modules that are equipped with camera electronics from another manufacturer. If the web interface of the camera is accessed directly, these cameras can be recognized by the fact that they do not show a Behnke logo but the logo of the manufacturer of the camera electronics.

Behnke type B
This type applies to Behnke IP camera modules that are equipped with a Behnke camera electronic. If the web interface of the camera is accessed directly, these cameras can be recognized by the Behnke logo.

other
This type may allow the use of an IP camera that does not come from Behnke. Please note that the functionality of third-party cameras is not guaranteed. This type requires the specification of the URL to receive the camera's MJPG stream.

IP address or host name of the camera:

IP address or host name of the IP camera to be used

If an IP address is specified, it must be ensured that it does not change in the future. This is the case in a network with static IP address assignment. If, on the other hand, the camera receives an address from a DHCP server, a reservation of a fixed IP address can be created in the DHCP server for the camera so that it does not change.

If a DHCP reservation is not possible, the unique host name of the camera can also be specified.

URL to receive MJPG stream:

When using an IP camera from a third-party provider, the URL must be specified via which the device can request the MJPG stream of the IP camera.

Camera user:

username that is specified when the IP camera requires authentication to retrieve video streams

Cameras of the type 'Behnke type A' use 'root' as the user name in the delivery state.

Camera password:

password that will be transmitted when the IP camera requires an authentication to retrieve video streams

Cameras of the type 'Behnke type A' use the password 'Admin' in the delivery state, cameras of the type 'Behnke type B' use the password 'admin'.

Preferred view:

- top left
- top center
- top right
- center left
- center
- center right
- bottom left
- bottom center
- bottom right

Default: center

This setting can be used to specify the preferred view of the camera image. If the video image is transmitted to an indoor station in 'IP intercom' mode, the indoor station can use this setting as the default for the

image section displayed.

Display

Type:

- no display detected
- small display
- medium display

display of the detected display

Functions:

- disabled
- 1 button
- 1 button & telephone
- 1 button & code lock
- 1 button & information text
- 1 button & logo
- 1 button & telephone & code lock
- 1 button & telephone & information text
- 1 button & telephone & logo
- 1 button & code lock & information text
- 1 button & code lock & logo
- 1 button & telephone & code lock & info text
- 1 button & telephone & code lock & logo
- 2 buttons
- 2 buttons & code lock
- 2 buttons & information text
- 2 buttons & logo
- 3 buttons
- 3 buttons & code lock
- 4 buttons
- 4 buttons & code lock
- 5 buttons
- 5 buttons & code lock
- 6 buttons
- 6 buttons & code lock
- 7 buttons
- 7 buttons & code lock
- 8 buttons
- 8 buttons & code lock
- 9 buttons
- 9 buttons & code lock
- 10 buttons
- 10 buttons & code lock
- 11 buttons
- 11 buttons & code lock
- 12 buttons
- 12 buttons & code lock
- 13 buttons

- 13 buttons & code lock
- 14 buttons
- 14 buttons & code lock
- 15 buttons
- 15 buttons & code lock
- 16 buttons
- 16 buttons & code lock
- 17 buttons
- 17 buttons & code lock
- 18 buttons
- 18 buttons & code lock
- 19 buttons
- 19 buttons & code lock
- 20 buttons
- 20 buttons & code lock
- 21 buttons
- 21 buttons & code lock
- 22 buttons
- 23 buttons & code lock
- 24 buttons
- 24 buttons & code lock
- 25 buttons
- 26 buttons & code lock
- 27 buttons
- 27 buttons & code lock
- 28 buttons
- 29 buttons & code lock
- 30 buttons
- 31 buttons & code lock
- 32 buttons
- 35 buttons & code lock
- 36 buttons
- 39 buttons & code lock
- 40 buttons
- 44 buttons & code lock
- 45 buttons
- 49 buttons & code lock
- 50 buttons
- telephone
- code lock
- information text
- logo
- logo & phone book
- logo & phone book & telephone
- logo & phone book & code lock
- logo & phone book & telephone & code lock
- phone book
- phone book & code lock
- buttons automatically

- buttons automatically & code lock
- indoor station

Default: indoor station

Here you can specify which function or which combination of functions should be shown and made available on the display. The following functions are available:

disabled
No function is provided and only a blank screen is displayed. If the display is to be switched off completely, this can be achieved using the 'Brightness' setting.

button(s)
Depending on the selection, one or more call buttons are shown on the display. The labelling and the call number or action of the individual buttons are specified in the section 'Buttons'. If someone presses such a (virtual) button, the configured call number will be called or the configured action will be executed.
If there are several buttons, the buttons on the display are numbered from bottom to top, and if there are several columns, from left to right. Button 1 is therefore at the bottom left.
Real buttons, if available, and virtual display buttons are connected in parallel. This means that it does not matter whether the virtual button x is pressed on the display or the real call button x. The configured number for the button x will be called or the configured action will be executed.

telephone
This function allows you to dial an arbitrary number. A keypad for entering the number and a handset key for starting and ending the call are shown on the display. If this function is combined with others, a button with a handset symbol is displayed. This button must then be pressed in order to display the actual telephone function.
If a real keypad is available, the phone number can also be entered via this. However, starting a call via the handset key of the real keypad is only possible if the 'Telephone' function has been allowed in the 'Keypad' area.
In hybrid mode, the number is dialled in the set main operation mode.

code lock

This function allows you to enter a code in order to control a relay, for example to open the door. To do this, a keypad is shown on the display for entering the code.
If this function is combined with others, a button with a key is displayed. This must then be pressed to display the actual code lock function.
If a real keypad is available, the code lock function can also be called up using the key button if the 'code lock' function has been allowed in the section 'Keypad'.
The code entry is completed by pressing the # key. If the set code for a relay is 2580, for example, then you enter 2580 #.
If the automatic code checking is switched on in the section 'Relay', the code can also be entered without a #.
It is possible to activate the configuration mode via the virtual keypad of the code lock function and to enter configuration steps, if the activation of the configuration mode via keypad has been allowed in the section 'General'. When activating the configuration mode or as long as it is active, the keypad is displayed in blue.

information text

An arbitrary text can be entered and designed under 'Information text', which is then shown on the display. This could be, for example, a welcome message or the opening times.
A function can be assigned to the information text, for example triggering button 1, which is executed when someone presses the information text on the display.

logo

Under 'Logo' an image file, for example a company logo, can be uploaded and adjusted, which is then shown on the display. Supported image formats are JPG, PNG, GIF and BMP with a maximum file size of 10 MB.
A function can be assigned to the logo, for example triggering button 1, which is executed when someone presses the logo on the display.

phonebook

A phone book is shown on the display that can hold up to 300 entries. These are entered in the section

'Phone book'.
An entry can be selected using the arrow keys that are shown on the display. Then the call or the configured action can be triggered by pressing OK or by pressing the entry.
In order to ensure that many entries are easy to handle, entries can be grouped, for example by department. There is also a search function that allows entries to be found using the first letter.

Function of the physical button:

- activate button 1
- play an explanatory announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play an explanatory announcement

An all-in-one communication station has a physical button below the display. If several virtual buttons are shown on the display, you can set what happens when a visitor presses the physical button.

Either the physical button is treated like the virtual button 1, that is, button 1 is triggered and the configured number is dialled or the configured action is executed.

Alternatively, a voice announcement can be issued. You can choose between a predefined voice message or your own voice message. The predefined voice message explains that the visitor should press one of the virtual buttons on the display.

Design:

- white
- grey
- dark grey
- aluminium
- stainless steel
- brass
- silver
- set individually

Default: silver

colour adaptation of the display background and the displayed buttons

You can choose between different predefined designs

or the design can be individually determined using the corresponding settings.

Display elements:

- show all
- set individually

Default: show all

When a connection is established, the display informs the visitor about the status of the connection. In addition, pictograms, an explanatory text and the call destination or the remote station are shown.

Normally, all of these display elements are shown. If desired, the display can be configured individually and individual or all elements can be hidden.

Automatic revitalisation:

- no
- after 10 min
- after 30 min
- after 1 h
- yes

Default: no

Touching the display can lead to electrostatic discharges. Strong discharges can disrupt the display electronics and lead to the display content no longer being displayed correctly.

In such a case, the display electronics must be restarted in order to rectify the fault.

This setting can be used to determine whether the display electronics should be automatically restarted, i.e. revitalised, at regular intervals.

When the display electronics are restarted, the display content disappears for a very brief moment.

ESD detection:

- no
- yes

Default: yes

Touching the display can lead to electrostatic discharges. Strong discharges can disrupt the display electronics and lead to the display content no longer being displayed correctly.

In such a case, the display electronics must be restarted in order to rectify the fault.

This setting can be used to determine whether and how a detected electrostatic discharge should be handled.

Connection

Acoustical indications / voice announcements:	see section Acoustics

Buttons

Code lock function via buttons

Allow:

- no
- yes

Default: no

The code lock function is normally provided via the keypad. If there is no keypad but several direct call buttons are available, this setting can be used to activate the simple code lock function via direct call buttons.

A code can be entered by pressing a sequence of direct call buttons, whereby the digit entered corresponds to the number of the direct call button pressed.

Codes for the simple code lock are defined in the 'Relay' section, just like the codes for the normal code lock. However, there are the following restrictions:
- a code must have at least 2 digits
- permitted digits: 1 to number of direct call buttons
- a code may not begin with 2 identical digits

If, for example, the code 16322 is to be entered, the buttons 1, 6, 3, 2 and 2 must be pressed in succession.

After the time set under 'Timeout for code entry' has elapsed, the code is validated. For this reason, this is the maximum time that may elapse between the individual button presses when entering the code.

Important note
In order to achieve a sufficient number of codes and thus security, at least 4 direct call buttons should be available and correspondingly long codes with 7 or 8 digits should be used.

Timeout for code entry: 500 - 3000 ms

Default: 1000 ms

After the time set here, the code is validated. For this reason, this is the maximum time that may elapse

between the individual button presses when entering the code.

Simple code lock for devices without keypad

Special parameters

General:

The telephone number that is to be dialed is usually entered in the 'Call number' field.

This is absolutely sufficient for the vast majority of cases. However, there are also special cases in which special parameters can or must be inserted in the call number in order to generate the desired behavior.

Such special cases are explained in the help for the following options.

SIP direct calls:

If, for example, a SIP telephone with the IP address 192.168.16.199 is to be called directly, configure the number:

sip:192.168.16.199

You can find further information on SIP direct calls in the section 'SIP phone' in the help for the setting 'Allow SIP direct calls'.

SIP calls over a specific SIP account:

In order to make a call via a specific SIP account, the IP address or the host name of the server that is entered in the 'Server' field of the corresponding SIP account must also be specified. For example, if the number 123 is to be used via the SIP account with the server 192.168.1.199, then configure the number:

sip:123@192.168.1.199

Alternatively, you can specify sip1: or sip2: in front of the number in order to make the call via the corresponding SIP account. For example, if the number 123 is to be called via the second SIP account, then configure the number:

sip2:123

Calls in IP intercom mode:

In 'IP intercom' mode, buttons that have not been configured with a call number dial their button number: button 1 calls ID 1, button 2 calls ID 2, and so

on. This means that when the system is delivered, the buttons on an outdoor station are already assigned to the indoor stations in the same group.

However, it is also possible to configure a call number. If hybrid mode is used and 'IP intercom' is not the main operating mode, the prefix com: must be added to the call numbers given in the examples to indicate that it is an intercom call.

For example, if you want to call the indoor station with intercom ID 1 of your own intercom group, configure the following as the call number:

1

It is also possible to call the intercom ID of another intercom group by dialling a 3-digit call number. The first digit is the intercom group (1-9) followed by the 2-digit intercom ID (01-99).

To call intercom ID 1 of intercom group 2, configure the following as the call number:

201

In intercom mode, Behnke stations that belong to the intercom system can also be reached via their IP address, host name or serial number.

To call a Behnke station with the IP address 192.168.1.199, configure the following as the call number:

192.168.1.199

If you want to call the Behnke station with the serial number 12345, configure the call number as follows:

#12345

Important note
If a button is individually configured in intercom mode, the corresponding button name should also be configured accordingly.

Calls in a specific operation mode:

In hybrid mode, calls are usually made in the set main operation mode. If you want to call in a different or a specific operation mode, this must be specified

accordingly.

If, for example, the number 123 is to be called as a SIP telephone via the SIP account with the server 192.168.1.199, then configure the number:

sip:123@192.168.16.199

If you want to call in intercom mode the indoor station with intercom ID 1, enter the call number as follows:

com:1

For more information about calling in hybrid mode, see in the section 'General' the 'Hybrid mode' setting help.

Group calls: Group calls are normally implemented using the appropriate selection of the 'Action' field. A corresponding number of fields for entering the phone numbers are then displayed.

Alternatively, several phone numbers can be entered directly in a call number field in order to call them simultaneously as a group call.

If, for example, the numbers 11, 22 and 33 are to be called at the same time, i.e. as a group call, then configure the number:

11,22,33

Call chains: Call chains are normally implemented using the appropriate selection of the 'Action' field. A corresponding number of fields for entering the phone numbers are then displayed.

Alternatively, several phone numbers can be entered directly in a phone number field in order to call them one after the other as a call chain.

If, for example, the numbers 11, 22 and 33 are to be called one after the other, i.e. as a call chain, then configure the number:

11;22;33

Commands: It is possible to enter commands in the call number.

To do this, enter cmd: followed by the desired command.

This allows the realisation of very individual functions for special cases.

The possible commands and their use are explained here as well as in the following settings. If you need help in using them, please contact our service hotline (see the 'Help' section).

command chains with and without phone number
It is possible to specify several commands or an additional phone number to be dialed by separating the individual commands or the phone number with ; as for a call chain.

If, for example, the individual voice announcement 1 is to be played first and then the door opener relay 1 is to be activated, you configure:

cmd:play1;cmd:free1

If the individual voice announcement 2 is to be played first and then the number 123 is to be dialed, you configure:

cmd:play2;123

wait time between commands in a command chain
To wait a short time (1 to 9 s) before executing the next command, the following commands can be used.

cmd:wait1 (wait 1 s)
:
cmd:wait9 (wait 9 s)

If, for example, the voice announcement 'Please wait' is to be played first and then door opener relay 1 is to be activated after 3 seconds, then configure:

cmd:play_wait;cmd:wait3;cmd:free1

executing a command at a specific time
Normally, a command is always executed immediately. It is also possible to execute a command

at a later point in time, for example after the remote terminal has picked up. The desired time can be specified using /.
The following examples explain the execution of commands at different times using the example of the play1 command.

cmd:play1 (immediately)
cmd:/play1 (after the remote station has picked up)
cmd://play1 (after the remote station has hung up)
cmd:///play1 (after the end of the call)

It is possible to execute several commands at different times. If, for example, the call number 123 is to be called and the individual voice announcement 1 it to be played immediately (locally on the device), the voice announcement 2 after the remote station has picked up (to the remote station) and voice announcement 3 after the remote station has hung up (locally on the device), this is done by configuring:

cmd:play1/send2/play3;123

The specified time via / only applies to the next call that follows the command. In the case of a call chain, the desired time can also be specified using |. Then it applies to the call chain that follows the command. Example:

cmd:|play1 (after a remote station has picked up)
cmd:||play1 (after a remote station has hung up)
cmd:|||play1 (after the end of the call chain)

If, for example, the numbers 11, 12 and 13 are to be called in a call chain and announcement 1 is played to the remote station after one of the remote stations has picked up, you configure:

cmd:|send1;11;12;13

Connection related commands:

terminate connection
With the following command it is possible to end a connection directly by the command.

cmd:hangup (terminate connection)

If, for example, the call number 11 is to be called and the connection is to be terminated automatically 5 seconds after going off-hook, configure:

cmd:/wait5;cmd:/hangup;11

do not allow canceling the connection
Depending on the settings in the 'Connection' section under 'Cancel connection', it is normally possible to cancel an outgoing connection by pressing the same or also another call button again.
If cancelling the connection is not to be allowed for a specific call button, this can be achieved with the following command.

cmd:no_cancel (cancelling the connection not allowed)

For call chains, the no_cancel command applies until the end of the call chain.

For example, if call numbers 11, 12 and 13 in a call chain are to be called without the call being cancelled by pressing a call button again, configure:

cmd:no_cancel;11;12;13

Relays and door opening related commands:

activation of a door opener relay
If a relay is configured as a door opener relay, the following commands can be used to activate the relay for the set opening time.

cmd:free1 (for relay 1)
cmd:free2 (for relay 2)
cmd:free1&2 (for relays 1 and 2)

activation/deactivation of permanent opening
If a relay is configured as a door opener relay and permanent opening of the access is permitted, then the following commands can be used to activate or deactivate permanent opening.

cmd:open1 (activate opening for relay 1)
cmd:close1 (deactivate opening for relay 1)
cmd:open2 (activate opening for relay 2)
cmd:close2 (deactivate opening for relay 2)

activation/deactivation of the connection indication
If a relay is used in 'connection indication' operation

mode, the following commands can be used to activate or deactivate the relay.

cmd:on1 (activate relay 1)
cmd:off1 (deactivate relay 1)
cmd:on2 (activate relay 2)
cmd:off2 (deactivate relay 2)

individual door opener code

Normally, the codes set in the 'Relay' area apply to a door opener relay. However, it is possible to use a command to define a code that is valid for the indoor station and that only applies to the subsequent connection and replaces all other codes for this relay. The use of the command requires that the relevant relay is configured as a door opener relay.

The command to define an individual door opener code for relay 1 is cmd:code1= followed by the desired code and accordingly cmd:code2= for relay 2. If no code is specified, door opening is not possible in the following connection for the corresponding relay.

If, for example, the number 123 is to be called and the door opening via relay 1 should be possible with the code 99, you configure:

cmd:code1=99;123

If, for example, the number 123 is to be called and the door opening via relay is not allowed, you configure:

cmd:code1=;123

select door opener relay for card reader via call button

For a device with card reader, it is possible to define in the authorisation profile which door opener relay (1, 2 or 1 & 2) should switch a card of this profile. For most cases this is sufficient.

In the special case where both relays are used as door opener relays, and depending on the situation sometimes one and sometimes the other relay is to be switched via the same card, this can be achieved as follows.

In the authorisation profile, 1 / 2 is selected as the setting for the door opener relay. This allows to select via a call button which door opener relay is to be switched by the cards of the profile.

Normally, relay 1 is switched. If the second relay or both relays are to be switched, before presenting the card, an appropriately configured call button must be pressed, which selects the relay to be switched. There is then 5 seconds to present an authorised card and switch the selected relay.

To use the call button to select the door opener relay, configure:

cmd:set1 (select relay 1)
cmd:set2 (select relay 2)
cmd:set1&2 (select relay 1 & 2)

send DTMF code to remote station
When the connection is established, a DTMF code can be sent to the remote station. If the Behnke station has established a connection to another Behnke station, the door opener relay of the remote Behnke station can be activated in this way, for example.

In order to call the Behnke station with the call number 123 and to send the door opener code o# after the connection is established, configure:

cmd:/dtmf=o#;123

Acoustics and voice announcements related commands:

play an individual voice announcement
If individual voice announcements have been uploaded or generated in the section 'Acoustics', the following commands can be used to play them.

cmd:play1 (play voice announcement 1)
:
cmd:play9 (play voice announcement 9)

The command play always plays the voice announcement locally on the device. If instead a voice announcement is to be played during a connection (see 'executing a command at a specific time' below) to the remote station, the following commands can be used for this.

cmd:/send1 (play voice announcement 1 to the remote station)
:
cmd:/send9 (play voice announcement 9 to the remote station)

play standard voice announcement
Some voice announcements are already in the device and can be played using the following commands.

cmd:play_welcome (play 'welcome')
cmd:play_start (play 'connection will be established')
cmd:play_wait (play 'please wait')
cmd:play_free (play 'free access')
cmd:play_end (play 'connection terminated')

disable preset acoustic indications
In the 'Acoustics' area, various acoustic indications can be activated, which are then automatically emitted, for example, when the connection is established or the access is opened. Sometimes these preset acoustic indications are to be disabled for a certain button in order to possibly also replace them with an individual voice announcement. For this purpose, the preset acoustic indications can be disabled via the following commands.

cmd:quiet_start (indication 'at the start of a connection' off)
cmd:quiet_wait (indication 'while establishing the connection' off)
cmd:quiet_audio (no indication when an audio problem has been detected)
cmd:quiet_free (indication 'when/during opening the access' off)
cmd:quiet_end (indication 'at the end of a connection' off)
cmd:quiet_error (indication 'on connection error' off)

cmd:quiet (all acoustic indications for this action off)
cmd:unquiet (all acoustic indications for this action on)

For command chains, the quiet/unquiet commands always apply until the end of the command chain.

For example, if the call number 11 is to be called and

the indication at the start of the connection is to be replaced by the individual voice announcement 1, configure:

cmd:quiet_start;cmd:play1;11

If, for example, the call numbers 11, 12 and 13 are to be called in a call chain and no acoustic indications are to be output, configure:

cmd:quiet;11;12;13

disable key click

In the 'Acoustics' area, you can generally set whether or not a button click is emitted when a direct call button is pressed or when a trigger is released.
If the key click is to be deactivated only for a specific key or a specific trigger, this is possible via the following command.

cmd:no_click (disable key click)

To do this, the no_click command must be at the very beginning of the call number and it only refers to the first keystroke when the device is at rest.

mute loudspeaker

Using the following commands, the loudspeaker can be muted or the mute function can be deactivated again.

cmd:mute (mute on)
cmd:unmute (mute off)

If, for example, the call number 11 is to be called without the dialling being audible, configure:

cmd:mute/unmute;11

If, for example, the call number 11 is to be called, the individual voice announcement 1 is to be played after going off-hook to the remote station and the connection is then to be terminated without this being audible at the device, then configure:

cmd:no_click;cmd:mute/send1;cmd:/hangup;11

In the 'Acoustics' section, you can set the acoustic indications that are given after activating mute (announcement 'muted' / double beep) or before deactivating (announcement 'audible' / beep).

Important note
Muting the loudspeaker provides a way to listen to the device environment. If this command is to be used, please check that this function is possible and takes place within the legal regulations of your country or company.

Video related commands:

display IP video
The IP video software can display the video image from a Behnke station with camera when the telephone next to the PC is called from the Behnke station.
Normally, when the telephone receices a call from a Behnke station, a window with the video image opens automatically for the duration of the call.
Using the command cmd:video= followed by the station ID, it is also possible to display the video image for a few seconds at a remote station without triggering a call. How long the video image is displayed in this case can be set in the IP video software.
For example, the person at the remote station can be informed of the presence of a visitor. The person can then either call back the Behnke station or open the door directly via the IP video software, provided a licence to open the door is available.
This command requires IP video software version 2.0.87 or newer.

If, for example, the video image is to be displayed on the PC with the station ID 123, configure:

cmd:video=123

If the voice announcement 'Please wait' is also to be played, configure:

cmd:video=123;cmd:play_wait

Keypad related commands:

It is possible to activate one of the keypad functions (telephone, code lock, quick dialling) via a direct call button. Of course, this only makes sense if a keypad or alternatively (except quick dialling function) a

display is available. In addition, the function must be permitted by the 'setting' functions in the 'keypad' section. This also applies if a direct call button on the display is used to activate the function.

activating keypad function
cmd:telephone (activate telephone function)
cmd:code_lock (activate code lock function)
cmd:quick_dialling (activate quick dialling function)

Important note
If one of the above commands is used, the device hangs up and triggers the corresponding function. Other commands or call numbers following the command execution are ignored.

Display related commands:

name shown on the display
On devices with a display, the configured name is shown on the display when a button is pressed or a phone book entry is selected.
It is possible to change the name displayed after pressing/selecting using the command cmd:name=.

If the name 'Reception' and the call number 123 are configured for button 1, both the display button 1 and the physical button 1 dial this call number and display the name.
If physical button 1 is to dial another call number, e.g. 456, and display the name 'Stock', configure:

if:button;cmd:name=Stock;456;if:else;123

Conditions:

It is possible to check in the phone number whether a certain condition is fulfilled or not, in order to then dial a certain phone number or execute a command depending on the situation. To check a condition, enter if: followed by the desired condition. Via if:else an execution can take place if the last if-condition was not fulfilled. The if:else part can also be omitted.

available conditions
if:net (if there is a valid network connection)
if:sip1 (if SIP account 1 is registered)
if:sip2 (if SIP account 2 is registered)
if:cloud (if cloud account is registered)
if:open1 (if permanent opening by relay 1)
if:open2 (if permanent opening by relay 2)
if:alarm (if status of alarm input is 1)
if:action (if triggered as action button)

if:touch (if triggered as virtual button)
if:button (if triggered as physical button
if:else (else)

example 1
If the first SIP account is registered, the number 123 should be dialed, otherwise the individual voice announcement 1 should be played.

if:sip1;123;if:else;cmd:play1

example 2
If access via door opener relay 1 is permanently open, visitors should be informed that access is possible. Otherwise, the number 123 should be called.

if:open1;cmd:free1;if:else;123

action button
A direct call button can be used as an action button. If an action button is pressed during an established connection, the stored commands are executed. If the action button is pressed again during command execution or outside a connection, the behaviour is the same as for a normal direct call button.
To make a call button an action button, start the call number with the condition if:action followed by the commands that the action button should execute. If the button is also to be used as a direct call button, add the condition if:else followed by the call number to be called.
For commands that follow the condition if:action, no time can be specified via / or |, since the time of their execution is already specified, namely within an established connection.

For example, if button 2 is to be used as an action button to send the door opener code 0# via DTMF to another Behnke station with which a connection has been established, configure:

if:action;cmd:dtmf=0#

If the same key is also to call the Behnke station with the call number 123 when it is pressed outside of a connection, configure:

if:action;cmd:dtmf=0#;if:else;123

differentiation between physical button and display button
If buttons are shown on the display and physical buttons are also available, these are connected in parallel, i.e. display button 1 and physical button 1 both use the call number configured under button 1, display button 2 and physical button 2 use the call number configured under button 2 and so on.
The if:touch and if:button conditions allow different phone numbers to be configured for the display button and physical button.

For example, if the display button is to call the number 123 and the physical button 456, you configure:

if:touch;123;if:button;456

Sending e-mails:

It is possible to send an e-mail via a special command in the call number (see commands) when a button is pressed. The prerequisite for this is that sending e-mails is allowed and correctly configured in the 'Network' area.

To send an e-mail, enter cmd: followed by the e-mail address to which the e-mail should be sent.

The e-mail contains information about the button pressed and a camera image, if a camera is available.

example 1
An e-mail should be sent to info@behnke-online.com.

cmd:info@behnke-online.com

example 2
An e-mail should be sent to info@behnke-online.com and the number 123 should be called.

cmd:info@behnke-online.com;123

example 3
The number 123 should be called. If the call is not accepted, an e-mail should be sent to the address

Explication of the special parameters for call numbers

info@behnke-online.com.

123;cmd:info@behnke-online.com

alarm input

The command to send an e-mail can also be used in the call number of the alarm input. The sent e-mail then contains a corresponding message depending on the status of the alarm input. It is sent without a camera image.

sabotage / noise alarm

The command for sending an e-mail can also be used in the call number for a detected sabotage or for a noise alarm. The sent e-mail then contains a corresponding message. Sending is done with camera image, if allowed.

Handset

Operation mode:

- disabled
- handset
- handset & direct call button
- handset & telephone function

Default: handset

When connecting a handset as an extension module, this setting can be used to specify how it should be operated.

disabled
The handset is disabled. It cannot be used for communication or to trigger a function.

handset
You can switch from handsfree mode to handset by picking up the handset.
Hanging up the handset switches back to handsfree mode.
In addition, an existing connection is cancelled when the handset is hung up if this is specified in the setting 'Cancel connection when hanging up the handset'.

handset & direct call button
The functionality is identical to the 'handset' operation mode.
In addition, the fork switch of the handset functions like a direct call button that is triggered when the handset is picked up.
This means that picking up the handset can trigger a call or an action.

handset & telephone function
This operation mode requires a device with keypad or display.
The functionality is identical to the 'handset' operation mode.
In addition, the telephone function is activated when the handset is picked up and a telephone number can be dialled via the keypad or the virtual keypad of the display.
When using this operation mode, it makes sense to allow the telephone function in the 'Keypad' area or,

in the case of a display, to activate the telephone function as a display function.

Functions of the keypad: see section Keypad

Volume: 0 - 100 %

Default: 80 %

Microphone sensitivity: 0 - 100 %

Default: 60 %

Cancel connection when hanging up the handset:

- no
- yes

Default: yes

This setting determines whether an existing connection or function should be cancelled when the handset is hung up.

Handset direct call button

Name: Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is used to label the corresponding virtual call button or is shown on the display as the call destination when the connection is established.

Action:

- none
- call
- group call with 2 numbers
- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers
- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1

:

- play voice announcement #9

Default: call

Action to be performed when the button is pressed

The following actions are possible:

none
The keystroke is ignored.

call
A connection is established to the remote station specified under 'Call number'.

group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains' can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Periods of time are specified in a schedule and a telephone number is specified that is called if the button is pressed within one of the specified (valid) periods of time.
In addition, an action can be specified that is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the button is pressed. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to a schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice announcement.

play voice announcement
An individual voice announcement can be set which is issued when the button is pressed.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the button is pressed within one of the (valid) periods specified in the schedule.

Door opener relay:

- 1
- 2
- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in the section 'Relay'.

Action for the other time periods:

- call
- announce opening hours
- announce availability
- announce personal availability
- play voice announcement #1
  :
- play voice announcement #9

Default: call

	This action is carried out if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.
Call number for the other time periods:	This number is called if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Triggering a call by picking up the handset

Phone book

Phone book: export / import

export
All entries of the current phone book are exported to a text file with the namephonebook.txt.

import
A phone book file that was previously exported can be re-imported here.
The current phone book will be lost when importing.
When the phone book is synchronised with an LDAP server, importing a phone book file is not possible.

Provisioning phone book as download:

- no
- yes

Default: no

It is possible to provide the phone book as a download. You get the same file as when you export the phone book.

If the IP address of the Behnke station is 192.168.16.200, for example, then the download can take place via the following URLs.

http://192.168.16.200/phonebook.txt
or
https://192.168.16.200/phonebook.txt

Downloading via HTTP is only possible if it was set in the section 'General' that web connections via HTTP are allowed.

If the phone book is made available as a download, other devices with a phone book function can automatically import the phone book.

If another device is to import the phone book, then the auto-provisioning in the section 'System' of the other device is used. Phonebook can be downloaded. The auto-provisioning must be activated and as the auto-provisioning URL you simply enter the URL under which the phone book can be downloaded. The

automatic import then takes place in the set auto-provisioning rhythm.

URL for: phone book

displaying the appropriate URL to download the phone book of this device

Options

Font size:

- smallest font size
- small font size
- medium font size
- big font size
- biggest font size

Default: big font size

font size with which names are displayed in the phone book

If a larger font size is set, fewer entries are visible on the display than with a smaller font size.

In addition, a larger font size can mean that long names cannot be displayed completely in one line. In this case, only the part of the name that fits on the screen is displayed and the rest is cut off.

A font should always be set as large as possible in order to improve readability and thus enable or facilitate barrier-free building access.

Adjustment:

- left left-justified
- centered

Default: centered

alignment with which names are displayed in the phone book

Inscription:

- as entered
- in uppercase

Default: as entered

the way in which entries are shown in the display

Reset selection after:

3 - 30 s

Default: 5 s

If someone starts searching in the phone book but does not continue the search, i.e. no longer presses a display key, the phone book will be reset to the main selection after the time set here and the first entry will be displayed again.

Operation indication:

- don't show
- show

Default: show

If the phone book is displayed and the selection has not yet been started, the following note can be displayed above the first entry to explain the use of the telephone book:

choose an entry with ↓ ↑
then press OK

This setting defines whether this information text should be displayed or not.

Display order:

- groupments first
- in alphabetical order

Default: in alphabetical order

Groupments allow a phone book with many entries to be divided into smaller sub-phone books in order to be able to find entries more quickly.

If this setting is set to 'groupments first', then when the phone book is displayed, the groupments are listed first and then the phone book entries that do not belong to any groupments. The groupments or the remaining entries are listed separately each in alphabetical order.

If you set this setting to 'in alphabetical order', then the groupments and the phone book entries without groupments are mixed and displayed together in alphabetical order.

Mark groupments with an arrow:

- no

- yes

Default: yes

If groupments are used, they can be marked with an arrow ⇢ below in order to differentiate them from normal entries and to suggest to the visitor that further entries can be displayed by selecting the groupment.

Action when pressing a non-selected entry:

- none
- scroll to the entry
- select the entry

Default: select the entry

A green stripe is shown in the middle of the display, which marks the currently selected entry in the phone book.

If the visitor presses 'OK' or directly on the selected entry in the green stripe, this entry is selected and the associated action is triggered.

Here you can set the action that should take place when the visitor clicks on an entry above or below the green stripe.

none
The keystroke is ignored.

scroll to the entry
The entry is scrolled so that it is then displayed in the green stripe. After that, the visitor still has to press 'OK' or directly on the entry to trigger the associated action.

select the entry
The entry is selected and the associated action is carried out directly.

Group entries with same initial letter:

- no
- if 10 or more entries
- if 15 or more entries
- if 20 or more entries
- if 25 or more entries
- if 30 or more entries
- yes

Default: if 10 or more entries

In a phone book with many entries, grouping entries with the same first letter can make it easier to find entries.

If entries with the same initial letter are grouped, when the entries are displayed, if an entry comes with a different initial letter, this entry is displayed with a greater distance to the previous entry. This makes it easier to find entries with the desired initial letter.

This setting can be used to determine whether such a grouping of entries with the same initial letter should be made, and if so, from what total number of entries in the phone book.

Search of the initial letter:

- no
- if 10 or more entries
- if 15 or more entries
- if 20 or more entries
- if 25 or more entries
- if 30 or more entries
- yes

Default: if 10 or more entries

A visitor can restrict the displayed entries to a certain initial letter in order to find the desired entry more quickly in a telephone book with many entries.

For this purpose, a button with a magnifying glass and the character A is shown on the display to the right of the arrow keys  , if this is allowed by this setting.

If the visitor presses the magnifying glass key, a screen is displayed with all the initial letters that appear in the telephone book. The visitor can then press one of the initial letters to display a restricted phone book that only consists of entries that begin with this initial letter.

The visitor can then select one of these entries or use 'return' to go to the main selection of the phone book.

End of phone book:

- don't show
- show

Default: show

So that a visitor can better recognize that he has scrolled through all entries, after the last entry in the telephone book

*** END ***

is displayed if this is allowed by this setting.

Skipping from the last to the first entry and vice versa:

- refuse
- allow

Default: allow

If the last entry in the phone book is reached when scrolling down with  , it is possible to jump back to the first entry by pressing  again, if this setting allows this.

The same applies to scrolling up with  when the first entry is reached. If you press  again, you can jump to the last entry.

If you keep one of the arrow keys  or  pressed, you will continue to scroll in the corresponding direction until the end or the beginning is reached. By pressing the arrow key again, you can jump to the beginning or end, if this is allowed.

Multilanguage phone book:

- no
- English & German
- English & French
- German & French
- yes

Default: no

Normally, the phone book is displayed in the language set for the device under 'General'.

This setting allows you to switch to a multilanguage phone book. With a multilanguage phone book, a visitor first selects one of the permitted languages by pressing the corresponding flag. The phone book is then displayed and voice prompts are issued in the language selected by the visitor.

Use physical button as OK:

- no
- yes

Default: no

An all-in-one communication station has a physical button below the display.

This setting allows you to specify that the physical button can be used as the OK button for the phone book as long as the phone book is displayed. Outside of the phone book display, the button retains its normal function.

Settings for display and utilization

LDAP

Phone book synchronisation:

- disabled
- every 5 minutes
- every 30 minutes
- every 60 minutes
- during the night

Default: disabled

It is possible to synchronise the phone book with another system (LDAP server).

For this, the phone book entries are regularly requested and the phone book is automatically updated when changes are made.

For example, a Windows® server can be configured as an LDAP server so that users or contacts can be retrieved from the Active Directory.

This setting determines whether a phone book synchronization should be carried out and at what frequency.

State:

display of the state of the phone book synchronisation

wait
The configuration has just been changed. The state will be updated soon.

synchronisation in progress
An attempt is being made to contact the LDAP server to synchronise the phone book.

no connection to the server
The connection to the LDAP server could not be established successfully.
This error occurs if the entries for the server, port or transmission protocol are incorrect, if the network routing does not work or a firewall is blocking communication.
Another possibility is that the username or password you entered is incorrect.
When using ldaps:// it occurs if the certificate of the LDAP server is not valid. In this case, the connection should be possible if the setting 'Verify server certificate' is configured to 'no' as a test.

search failed
The connection to the LDAP server could be established and information retrieved, but there was an error when transferring the data found to the phone book.
This error can occur with incorrect or incompatible data in the LDAP directory.

synchronisation failed
The connection to the LDAP server could be established and information retrieved, but there was an error when transferring the data found to the phone book.
This error can occur with incorrect or incompatible data in the LDAP directory.

partially synchronised
The phone book entries supplied by the LDAP server could not all be accepted.
Either more entries were found than fit in the phone book or invalid phone numbers were transferred.

synchronised
The phone book entries supplied by the LDAP server could all be transferred correctly.
The phone book synchronisation was carried out successfully.

LDAP server: IP address or host name of the LDAP server

The supported protocols are ldap:// and the encrypted variant ldaps://. If no protocol is specified,

ldap:// is used.

Verify server certificate:

- no
- yes

Default: yes

This setting determines whether or not the LDAP server's certificate is checked when using ldaps://.

If so, the server must transmit a valid certificate that contains the name or the IP address of the server (CN=common name). Otherwise the connection to the server will fail.

User: username for logging into the LDAP server

Password: password for logging into the LDAP server

DN of the search base: The DN (=distinguished name) describes a unique position in an LDAP directory.

The position in the LDAP directory at which the search for telephone book entries is to be carried out is specified here.

If, for example, the synchronisation with the LDAP server ldap://behnke-server.local is to take place for the Behnke domain, the DN of the search base is:

ou=Behnke,dc=behnke-server,dc=local

Search filter: If no search filter is specified, all objects in the search base that have a name and a telephone number are transferred to the phone book.

By specifying a search filter, the search can be restricted to objects that match the search filter. The other objects are then ignored.

For example, if only users are to be added to the phone book, the search filter is:

objectClass=user

If only users and contacts are to be included, the search filter is:

(|(objectClass=user)(objectClass=contact))

Include subunits in the search:

- no
- yes

Default: yes

The setting determines whether only the search base itself should be searched, or all of its subunits (subtrees, organizational units).

Call number:

- phone number
- other number

Default: phone number

This setting defines which field (attribute) of an object in the LDAP directory is to be used as the phone number for the telephone book entry.

If the field is available several times for an object, for example several 'other numbers', then the last entry is adopted as the phone number.

Groupment:

- no
- by department
- by company

Default: no

If the 'department' or 'company' attributes are available for objects, these can be adopted as groupment and the phone book entries grouped accordingly.

Character encoding:

- UTF-8
- ANSI

Default: ANSI

This setting can be used to set the character encoding used by the LDAP server so that special characters are displayed correctly.

Windows® servers usually use ANSI as the character encoding.

System number:

If the device is operated on a telephone system and the telephone numbers are entered in the LDAP directory including the system number, then the system number can be entered in this field.

When transferring to the phone book, the system number is removed so that only the extension number is transferred.

Example: If the system number is 068418177 and an object with the call number 06841/8177-777 is found, the call number 777 is adopted.

Extension number length:

0 - 5

Default: 4

If the device is operated on a telephone system, the length of the extension numbers can be set here.

If a phone number is added to the phone book that is longer than an extension number, the entry in the 'Outside line' field is placed in front of the phone number.

Outside line:

Default: 0

If the device is operated on a telephone system, you can set here which number must be dialed in order to make an external call. Otherwise this field should remain empty.

If a phone number is added to the phone book that is longer than an extension number, the 'outside line' set here is placed in front of the phone number.

Synchronise phone book with an LDAP server

Entries:

The total number of entries in the phone book is displayed here. A maximum of 300 entries are possible. You can also create new phone book entries, edit existing ones or delete the entire phone book.

new entry
Here you can create a new phone book entry.

Entries that can be selected in the phone book

edit entry
Click on the entry you want to edit.

remove entry
First click on the entry you want to edit. Then click on 'remove this entry' to remove the entry.

remove all entries
deleting the entire phone book

edit / remove the displayed phone book entry

remove this entry
remove the displayed phone book entry

Groupment:

- none
- new groupment

Default: none

A groupment, for example sales or production, can be assigned to a phone book entry.

Groupments allow a phone book with many entries to be divided into smaller sub-phone books in order to be able to find entries more quickly.

Groupments are displayed in the main selection of the phone book, but not the entries that are assigned to this groupment. These are only displayed when someone selects the groupment in the phone book.

Here you can, if you wish, assign a certain groupment to this entry, provided that it already exists. Simply select the appropriate groupment.

If the groupment does not yet exist, then select 'new groupment'. A 'Denomination' field is then displayed in which you can specify the name of the new groupment. The new groupment is then automatically assigned to this entry.

An existing groupment is automatically deleted when there are no more phone book entries assigned to it.

If this entry is to be displayed in the main selection of the telephone book, then do not assign it to any groupment.

Denomination: denomination of the new groupment

Entry

Name: name of the remote station to be called or the action to be carried out

The name entered here is displayed for selection in the phone book or is shown on the display as the call destination when the connection is established.

If the name of a person with first and last name is to be used, then enter the name in the format 'last name first name' so that the display order is correct when the phone book is displayed in alphabetical order.

Action:

- none
- call
- group call with 2 numbers
- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers
- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1
  :
- play voice announcement #9

Default: call

Action to be taken when the phone book entry is selected

The following actions are possible:

none
The selection is ignored and the phone book is redisplayed.

call
A connection is established to the remote station specified under 'Call number'.

Group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

Call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains' can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Time periods are specified in a schedule and a phone number is specified that is called if the entry is selected within one of the specified (valid) time periods.
In addition, an action can be specified that is carried out if the entry is selected at a different point in time, ie outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the entry is selected. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to the schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the entry is selected at a different point in time, ie outside

the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice announcement.

play voice announcement
An individual voice announcement can be set, which is issued when the entry is selected.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the entry is selected within one of the (valid) periods specified of the schedule.

Door opener relay:

- 1
- 2
- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in the section 'Relay'.

Action for the other time periods:

- call
- announce opening hours
- announce availability
- announce personal availability
- play voice announcement #1
  :
- play voice announcement #9

Default: call

This action is carried out if the entry is selected outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Call number for the other time periods: This number is called if the entry is selected outside of one of the (valid) periods specified in the schedule or if the device does not have a valid time.

Relays

Very important notice

Both relays are voltage-free switching contacts. The specified maximum values for the switching voltage (max. 30VDC / 30VAC), the switching current (max. 2A) and the switching capacity (max. 60W / 60VA) must all be respected.

Door module relay	Switch:	• like relay 1 • like relay 2 Default: like relay 1 A delocalised electronic has two relays (relay 1 and relay 2) whose function can be set separately. If a door module is connected to the delocalised electronics, there is another relay on the connection board of the door module. This setting determines whether the relay of the door module is to be switched as relay 1 or as relay 2.

Settings for the switching contact of the door module

Relay 1	Contact:	• closed • open • error on closing • error on opening display of the current status of the switching contact
	Operation mode:	• disabled • door opener relay with make contact • door opener relay with break contact • connection indication with make contact • connection indication with break contact • additional bell with make contact • additional bell with break contact • fault indication with make contact • fault indication with break contact Default: door opener relay with make contact This setting defines how the relay is to be operated. The following operation modes are possible:

disabled
The relay is not used and is deactivated. In this case, the switching contact is open.

door opener relay with make contact
The relay is used to control a door opener, whereby a normally open contact (NO) is required.
In this case, the switching contact is normally open and is only closed when the door is to be opened.
How long the contact is closed, i.e. how long the door is opened, can be set using the 'opening duration' setting.
One or more codes can be defined to trigger the door opening at an indoor station or via the code lock function of the keypad, if available.

door opener relay with break contact
The relay is used to control a door opener, whereby a normally closed contact (NC) is required.
In this case, the switching contact is normally closed and is only opened when the door is to be opened.
How long the contact is opened, and thus also the door, can be set using the 'opening duration' setting.
One or more codes can be defined to trigger the door opening at an indoor station or via the code lock function of the keypad, if available.

connection indicator with make contact
The switching contact is normally open (= no connection) and is closed when a connection is to be displayed.
You can use additional settings to specify which connections are to be displayed exactly: incoming connections, outgoing connections, outgoing connections after the remote terminal has been accepted the call, ...

connection indicator with break contact
The switching contact is normally closed (= no connection) and is opened when a connection is to be displayed.
You can use additional settings to specify which connections are to be displayed exactly: incoming connections, outgoing connections, outgoing connections after the remote terminal has been accepted the call, ...

additional bell with make contact

The switching contact is normally open (= no ringing) and is closed when the additional bell is to be activated.
Additional settings can be used to set when and, if necessary, how long the additional bell should be activated: for an incoming connection while the doorbell is ringing, at the beginning of a direct call, while a direct call is being established, ...

additional bell with break contact
The switching contact is normally closed (= no ringing) and is opened when the additional bell is to be activated.
Additional settings can be used to set when and, if necessary, how long the additional bell should be activated: for an incoming connection while the doorbell is ringing, at the beginning of a direct call, while a direct call is being established, ...

fault indication with make contact
The switching contact is normally open (= no fault) and is closed when a fault is detected on the device. A fault can be recognized when the device no longer has a valid network connection or when the registration with the SIP server has failed.
If the daily audio test is activated in the 'triggers' area, an audio problem can also be identified as a fault.

fault indication with break contact
The switching contact is normally closed (= no fault) and is opened when a fault is detected on the device. A fault can be recognized when the device no longer has a valid network connection or when the registration with the SIP server has failed.
If the daily audio test is activated in the 'triggers' area, an audio problem can also be identified as a fault.

Access:

- **closed**
- **free**

display of the current status of the access, if the relay is used as a door opener relay

closed
The door opener relay is not activated at the moment. This means that the connected door opener is not active and therefore does not allow the entrance to be

opened.

free
The door opener relay is activated at the moment. This means that the connected door opener is active and thus allows the entrance to be opened.

Access type:

- access
- door
- wicket
- gate
- car access
- barrier
- access with own designation
- car access with own designation

Default: access

This setting indicates which type of access should be opened with the switching contact.

Depending on this setting, the labelling of buttons for opening the access in the web interface, voice announcements when opening the access and, for devices with a display, the pictograms and texts displayed when opening the access are adapted.

Own designation:

For an access type with its own designation, this setting can be used to specify the designation.

Opening duration:

1 - 90 s

Default: 5 s

If a valid code is entered for this door opener relay, then this setting determines how long the access is opened.

In order to enable or facilitate barrier-free building access, the opening duration should be set so that people with walking disabilities or in wheelchairs also have sufficient time to enter the building.

Required codes:

- 0
- 1
- 2
- 3
- 4

- 5
- 6
- 7
- 8
- 9
- 10

Default: 2

The activation of the door opener relay and thus the opening of the access takes place via a code that can either be sent from the indoor station during a connection or that can be entered using the code lock function of the keypad, if available.

For each code it can be determined whether it is valid for the indoor station or the code lock function, and whether it is always valid or only at certain times, provided the device has a correct time.
This setting determines how many codes are required in total for this door opener relay.

If the same code is to be specified for the indoor station and for the code lock function, then 2 codes are required, one for the indoor station and one for the code lock function, whereby the same code is specified in both cases.

Allow code 1:

- no
- for indoor station
- for indoor station according to simple schedule
- for indoor station according to schedule
- for code lock
- for code lock according to simple schedule
- for code lock according to schedule
- once for code lock
- once for code lock according to simple schedule
- once for code lock according to schedule

Default: for indoor station

A code can either be sent from an indoor station as a DTMF tone sequence or entered using the code lock function of the keypad, provided the device has a keypad. For devices with a display, the code lock function can also be enabled via the display.

Here you can set whether the following code should apply for inside (indoor station/telephone) or outside (code lock/keypad).

It is also possible to set that a code can only be used once for the code lock. Such a one-time code is automatically deleted after successful use.

You can also specify whether the code should always be accepted or only at certain times. If you want to limit the code to certain times, you specify the valid time periods in a schedule, i.e. the times at which the code should be accepted.
For codes that are only to be accepted according to the schedule, the device must have the correct time, see NTP in the section 'Network'. If this is not the case, the code will not be accepted.

If you want the same code to apply to the indoor station and the code lock, then 2 codes are required, one that is allowed for the indoor station and one with the same code that is allowed for the code lock.

Code 1: Default: 0

A code consists of 1 to 8 digits.

If the code is entered, the entry is terminated with #. For example, if the stored code is 2580, then you enter 2580 #.

If the 'automatic code check' is switched on, the code can also be entered without a #.

Allow code 2:

- no
- for indoor station
- for indoor station according to simple schedule
- for indoor station according to schedule
- for code lock
- for code lock according to simple schedule
- for code lock according to schedule
- once for code lock
- once for code lock according to simple schedule
- once for code lock according to schedule

Default: for code lock

A code can either be sent from an indoor station as a DTMF tone sequence or entered using the code lock function of the keypad, provided the device has a keypad. For devices with a display, the code lock

function can also be enabled via the display.

Here you can set whether the following code should apply for inside (indoor station/telephone) or outside (code lock/keypad).

It is also possible to set that a code can only be used once for the code lock. Such a one-time code is automatically deleted after successful use.

You can also specify whether the code should always be accepted or only at certain times. If you want to limit the code to certain times, you specify the valid time periods in a schedule, i.e. the times at which the code should be accepted.
For codes that are only to be accepted according to the schedule, the device must have the correct time, see NTP in the section 'Network'. If this is not the case, the code will not be accepted.

If you want the same code to apply to the indoor station and the code lock, then 2 codes are required, one that is allowed for the indoor station and one with the same code that is allowed for the code lock.

Code 2: Default: 2580

A code consists of 1 to 8 digits.

If the code is entered, the entry is terminated with #. For example, if the stored code is 2580, then you enter 2580 #.

If the 'automatic code check' is switched on, the code can also be entered without a #.

Current state of the access:

- closed
- opened

Default: closed

This setting shows the current status of the access if permanent manual opening is permitted using the appropriate code.

Permanent opening can be started with the appropriate opening code (access remains permanently open) or ended using the closing code

(access is closed) or by changing this setting accordingly.

Code to close: Default: oooo

This code terminates the permanent opening of the access to, i.e. the access is closed.

The code for opening and the code for closing must be different and both codes should logically differ from codes for opening this access for a short time.

Code to open: Default: 1111

This code starts the permanent opening of the access to, i.e. the access is opened permanently.

The code for opening and the code for closing must be different and both codes should logically differ from codes for opening this access for a short time.

Time limit:

- none
- 1 min
- 2 min
- 3 min
- 4 min
- 5 min
- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 45 min
- 1 h
- 2 h
- 3 h
- 4 h
- 5 h
- 6 h
- 7 h
- 8 h
- 9 h
- 10 h
- 11 h
- 12 h

Default: none

This setting can be used to set a time limit for manual continuous opening.

If the access is opened manually continuously and is not closed again within the time limit, it will be closed automatically after the time limit has expired.

If the access is already open and is then manually opened continuously again, the time limit will start again.

Important note
If a time limit is set, the access will be automatically closed after restarting the device for security reasons if it is manually opened continuously.

Allow opening by door opener button:

- no
- according to simple schedule
- according to schedule
- yes

Default: yes

If an additional door opener button is connected to the device, this setting can be used to determine whether this door opener relay is activated and access is opened when this door opener button is pressed.

In addition to the options of ignoring the door opener button or always opening access when it is pressed, it is also possible to use the door opener button according to the schedule. In this case, the valid time periods are specified in a schedule, i.e. the times during which the opening of the entrance via the door opener button should be allowed.

Activate while incoming connection:

- no
- yes

Default: yes

This setting determines whether the switching contact of this relay should be closed during an incoming connection.

The switching contact is closed when an incoming connection is accepted automatically or manually. The switching contact remains closed for the entire

duration of the connection and is opened again when the connection is terminated.

Activate when outgoing connection:

- no
- after the called answered the call
- yes

Default: yes

This setting determines whether the switching contact of this relay should be closed during an outgoing connection.

The switching contact can be closed directly at the beginning of an outgoing connection, i.e. before the connection is established, or only after the connection has been established, i.e. when the called party has answered the call.

If the switching contact has been closed, it remains closed for the rest of the connection time and is opened again when the connection is ended.

Activate:

- while ringing
- at the beginning of a direct call
- during the establishment of a direct call

Default: while ringing

In the 'additional bell' operation mode, this setting specifies when the additional bell should be activated, i.e. the switching contact should be closed. Different modes of operation are possible.

If incoming calls are to be signalled via the additional bell, this can be done using the setting 'while ringing'.

If, on the other hand, a visitor who has pressed a button is to be signalled via the additional bell, this is possible via the settings 'at the beginning of a direct call' or 'during the establishment of a direct call'.

<u>while ringing</u>
The switching contact is closed as soon as an incoming connection is detected. It then remains closed until either the connection has been accepted automatically or manually or it is determined that there is no more incoming connection.

If it is set in the section 'Connection' that incoming calls are to be rejected, the additional bell has no function.

at the beginning of a direct call
The switching contact is closed as soon as a direct call button has been pressed and a connection is to be established. The setting 'Activation time' can be used to set how long the switching contact should remain closed. The switching contact is opened again when the activation duration is over or when the direct call is terminated beforehand.

during the establishment of a direct call
The switching contact is closed as soon as a direct call button has been pressed and a connection is to be established. The switching contact is opened again when the called party has picked up or if the direct call is terminated beforehand.

Activation time:

1 - 90 s

Default: 5 s

This setting defines the duration that an additional bell is activated at the beginning of a direct call.

Webhook for activation:

This setting can be used to specify a webhook to be sent when the relay is activated.

A webhook is a URL used to notify another device over the network that a certain event has occurred.

For example, a webhook can be used to control a network relay to open the door or trigger other functions.

The protocol to be used (HTTP or HTTPS) must be specified in the URL. It may also be necessary to specify authentication (username or username and password) in the URL if the device receiving the webhook requires it.

For example, if the command relay=1 is to be sent to a network relay with the IP address 192.168.16.200 and the user 'user' with the password 'password' is to be used as authorisation, the following URL results: http://user:password@192.168.16.200/?relay=1

If the network relay does not require authentication, the following is sufficient:
http://192.168.16.200/?relay=1

By default, a webhook uses the HTTP GET method.

However, if the URL is prefixed with json- or urlencoded-, the webhook switches to data transfer in the request body via the HTTP POST method. In this case, an additional input field 'body' appears, in which the data to be sent can be entered.

Here are two examples of such webhooks:
json-http://192.168.16.200
urlencoded-http://192.168.16.200

Important note
Sending webhooks requires a functional network connection.

Body: The data transmitted in the request body of the webhook will be specified here.

Webhook for deactivation: This setting can be used to specify a webhook to be sent when the relay is deactivated.

Body: The data transmitted in the request body of the webhook will be specified here.

Verify webhook identity:

- no
- certificate
- certificate & hostname

Default: certificate & hostname

This setting determines whether the identity of an https webhook should be verified when communicating with it.

To ensure secure communication, the certificate and host name should be verified.

The certificate can only be verified if the device has a valid time.

Required numbers for call-triggered opening: 0 - 20

Default: 0

When an incoming call is accepted, it is possible to automatically trigger access for certain authorised phone numbers.

This setting can be used to set the number of authorised phone numbers for such call-triggered opening.

For better manageability, a name or other comment can be added to each call number.

Important notes
This functionality requires that the call number be transmitted when an incoming call is received.
The authorised call numbers must be entered exactly as they are transmitted.
As it is not possible to verify the authenticity of the transmitted call number, it is the responsibility of the installer or user to ensure that the use of this function does not result in unauthorised call-triggered opening in their application.

Sluice function:

- no
- via relay 2

Default: no

The sluice function allows, after opening the access via relay 1 a little later, to automatically open another access via relay 2.

Activate sluice relay after: 1 - 90 s

Default: 10 s

This setting determines the length of time to wait in the sluice function before relay 2 is activated.

The set duration starts with the activation of relay 1.

Settings for the first switching contact

Relay 2

Contact:

- closed
- open
- error on closing

- error on opening

display of the current status of the switching contact

Operation mode:

- disabled
- door opener relay with make contact
- door opener relay with break contact
- connection indication with make contact
- connection indication with break contact
- additional bell with make contact
- additional bell with break contact
- fault indication with make contact
- fault indication with break contact

Default: additional bell with make contact

This setting defines how the relay is to be operated.
The following operation modes are possible:

<u>disabled</u>
The relay is not used and is deactivated. In this case, the switching contact is open.

<u>door opener relay with make contact</u>
The relay is used to control a door opener, whereby a normally open contact (NO) is required.
In this case, the switching contact is normally open and is only closed when the door is to be opened.
How long the contact is closed, i.e. how long the door is opened, can be set using the 'opening duration' setting.
One or more codes can be defined to trigger the door opening at an indoor station or via the code lock function of the keypad, if available.

<u>door opener relay with break contact</u>
The relay is used to control a door opener, whereby a normally closed contact (NC) is required.
In this case, the switching contact is normally closed and is only opened when the door is to be opened.
How long the contact is opened, and thus also the door, can be set using the 'opening duration' setting.
One or more codes can be defined to trigger the door opening at an indoor station or via the code lock function of the keypad, if available.

<u>connection indicator with make contact</u>
The switching contact is normally open (= no connection) and is closed when a connection is to be displayed.

You can use additional settings to specify which connections are to be displayed exactly: incoming connections, outgoing connections, outgoing connections after the remote terminal has been accepted the call, ...

connection indicator with break contact
The switching contact is normally closed (= no connection) and is opened when a connection is to be displayed.
You can use additional settings to specify which connections are to be displayed exactly: incoming connections, outgoing connections, outgoing connections after the remote terminal has been accepted the call, ...

additional bell with make contact
The switching contact is normally open (= no ringing) and is closed when the additional bell is to be activated.
Additional settings can be used to set when and, if necessary, how long the additional bell should be activated: for an incoming connection while the doorbell is ringing, at the beginning of a direct call, while a direct call is being established, ...

additional bell with break contact
The switching contact is normally closed (= no ringing) and is opened when the additional bell is to be activated.
Additional settings can be used to set when and, if necessary, how long the additional bell should be activated: for an incoming connection while the doorbell is ringing, at the beginning of a direct call, while a direct call is being established, ...

fault indication with make contact
The switching contact is normally open (= no fault) and is closed when a fault is detected on the device. A fault can be recognized when the device no longer has a valid network connection or when the registration with the SIP server has failed.
If the daily audio test is activated in the 'triggers' area, an audio problem can also be identified as a fault.

fault indication with break contact
The switching contact is normally closed (= no fault) and is opened when a fault is detected on the device.

A fault can be recognized when the device no longer has a valid network connection or when the registration with the SIP server has failed.
If the daily audio test is activated in the 'triggers' area, an audio problem can also be identified as a fault.

Access:

- closed
- free

display of the current status of the access, if the relay is used as a door opener relay

closed
The door opener relay is not activated at the moment. This means that the connected door opener is not active and therefore does not allow the entrance to be opened.

free
The door opener relay is activated at the moment. This means that the connected door opener is active and thus allows the entrance to be opened.

Access type:

- access
- door
- wicket
- gate
- car access
- barrier
- access with own designation
- car access with own designation

Default: access

This setting indicates which type of access should be opened with the switching contact.

Depending on this setting, the labelling of buttons for opening the access in the web interface, voice announcements when opening the access and, for devices with a display, the pictograms and texts displayed when opening the access are adapted.

Individual designation:

For an access type with its own designation, this setting can be used to specify the designation.

Opening time:

1 - 90 s

Default: 5 s

If a valid code is entered for this door opener relay, then this setting determines how long the access is opened.

In order to enable or facilitate barrier-free building access, the opening duration should be set so that people with walking disabilities or in wheelchairs also have sufficient time to enter the building.

Required codes:

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

Default: 2

The activation of the door opener relay and thus the opening of the access takes place via a code that can either be sent from the indoor station during a connection or that can be entered using the code lock function of the keypad, if available.

For each code it can be determined whether it is valid for the indoor station or the code lock function, and whether it is always valid or only at certain times, provided the device has a correct time.
This setting determines how many codes are required in total for this door opener relay.

If the same code is to be specified for the indoor station and for the code lock function, then 2 codes are required, one for the indoor station and one for the code lock function, whereby the same code is specified in both cases.

Allow code 1:

- no
- for indoor station
- for indoor station according to simple schedule
- for indoor station according to schedule

- for code lock
- for code lock according to simple schedule
- for code lock according to schedule
- once for code lock
- once for code lock according to simple schedule
- once for code lock according to schedule

Default: for indoor station

A code can either be sent from an indoor station as a DTMF tone sequence or entered using the code lock function of the keypad, provided the device has a keypad. For devices with a display, the code lock function can also be enabled via the display.

Here you can set whether the following code should apply for inside (indoor station/telephone) or outside (code lock/keypad).

It is also possible to set that a code can only be used once for the code lock. Such a one-time code is automatically deleted after successful use.

You can also specify whether the code should always be accepted or only at certain times. If you want to limit the code to certain times, you specify the valid time periods in a schedule, i.e. the times at which the code should be accepted.
For codes that are only to be accepted according to the schedule, the device must have the correct time, see NTP in the section 'Network'. If this is not the case, the code will not be accepted.

If you want the same code to apply to the indoor station and the code lock, then 2 codes are required, one that is allowed for the indoor station and one with the same code that is allowed for the code lock.

Code 1: Default: 0

A code consists of 1 to 8 digits.

If the code is entered, the entry is terminated with #. For example, if the stored code is 2580, then you enter 2580 #.

If the 'automatic code check' is switched on, the code can also be entered without a #.

Allow code 2:

- no
- for indoor station
- for indoor station according to simple schedule
- for indoor station according to schedule
- for code lock
- for code lock according to simple schedule
- for code lock according to schedule
- once for code lock
- once for code lock according to simple schedule
- once for code lock according to schedule

Default: for code lock

A code can either be sent from an indoor station as a DTMF tone sequence or entered using the code lock function of the keypad, provided the device has a keypad. For devices with a display, the code lock function can also be enabled via the display.

Here you can set whether the following code should apply for inside (indoor station/telephone) or outside (code lock/keypad).

It is also possible to set that a code can only be used once for the code lock. Such a one-time code is automatically deleted after successful use.

You can also specify whether the code should always be accepted or only at certain times. If you want to limit the code to certain times, you specify the valid time periods in a schedule, i.e. the times at which the code should be accepted.
For codes that are only to be accepted according to the schedule, the device must have the correct time, see NTP in the section 'Network'. If this is not the case, the code will not be accepted.

If you want the same code to apply to the indoor station and the code lock, then 2 codes are required, one that is allowed for the indoor station and one with the same code that is allowed for the code lock.

Code 2:

Default: 2580

A code consists of 1 to 8 digits.

If the code is entered, the entry is terminated with #. For example, if the stored code is 2580, then you

enter 2580 #.

If the 'automatic code check' is switched on, the code can also be entered without a #.

Current state of the access:

- closed
- opened

Default: closed

This setting shows the current status of the access if permanent manual opening is permitted using the appropriate code.

Permanent opening can be started with the appropriate opening code (access remains permanently open) or ended using the closing code (access is closed) or by changing this setting accordingly.

Code to close:

Default: oooo

This code terminates the permanent opening of the access to, i.e. the access is closed.

The code for opening and the code for closing must be different and both codes should logically differ from codes for opening this access for a short time.

Code to open:

Default: 1111

This code starts the permanent opening of the access to, i.e. the access is opened permanently.

The code for opening and the code for closing must be different and both codes should logically differ from codes for opening this access for a short time.

Time limit:

- none
- 1 min
- 2 min
- 3 min
- 4 min
- 5 min
- 10 min
- 15 min
- 20 min
- 25 min

- 30 min
- 45 min
- 1 h
- 2 h
- 3 h
- 4 h
- 5 h
- 6 h
- 7 h
- 8 h
- 9 h
- 10 h
- 11 h
- 12 h

Default: none

This setting can be used to set a time limit for manual continuous opening.

If the access is opened manually continuously and is not closed again within the time limit, it will be closed automatically after the time limit has expired.

If the access is already open and is then manually opened continuously again, the time limit will start again.

Important note
If a time limit is set, the access will be automatically closed after restarting the device for security reasons if it is manually opened continuously.

Allow opening by door opener button:

- no
- according to simple schedule
- according to schedule
- yes

Default: yes

If an additional door opener button is connected to the device, this setting can be used to determine whether this door opener relay is activated and access is opened when this door opener button is pressed.

In addition to the options of ignoring the door opener button or always opening access when it is pressed, it is also possible to use the door opener button according to the schedule. In this case, the valid time

periods are specified in a schedule, i.e. the times during which the opening of the entrance via the door opener button should be allowed.

Activate while incoming connection:

- no
- yes

Default: yes

This setting determines whether the switching contact of this relay should be closed during an incoming connection.

The switching contact is closed when an incoming connection is accepted automatically or manually. The switching contact remains closed for the entire duration of the connection and is opened again when the connection is terminated.

Activate when outgoing connection:

- no
- after the called answered the call
- yes

Default: yes

This setting determines whether the switching contact of this relay should be closed during an outgoing connection.

The switching contact can be closed directly at the beginning of an outgoing connection, i.e. before the connection is established, or only after the connection has been established, i.e. when the called party has answered the call.

If the switching contact has been closed, it remains closed for the rest of the connection time and is opened again when the connection is ended.

Activate:

- while ringing
- at the beginning of a direct call
- during the establishment of a direct call

Default: while ringing

In the 'additional bell' operation mode, this setting specifies when the additional bell should be activated, i.e. the switching contact should be closed.

Different modes of operation are possible.

If incoming calls are to be signalled via the additional bell, this can be done using the setting 'while ringing'.

If, on the other hand, a visitor who has pressed a button is to be signalled via the additional bell, this is possible via the settings 'at the beginning of a direct call' or 'during the establishment of a direct call'.

while ringing
The switching contact is closed as soon as an incoming connection is detected. It then remains closed until either the connection has been accepted automatically or manually or it is determined that there is no more incoming connection.
If it is set in the section 'Connection' that incoming calls are to be rejected, the additional bell has no function.

at the beginning of a direct call
The switching contact is closed as soon as a direct call button has been pressed and a connection is to be established. The setting 'Activation time' can be used to set how long the switching contact should remain closed. The switching contact is opened again when the activation duration is over or when the direct call is terminated beforehand.

during the establishment of a direct call
The switching contact is closed as soon as a direct call button has been pressed and a connection is to be established. The switching contact is opened again when the called party has picked up or if the direct call is terminated beforehand.

Activation time:

1 - 90 s

Default: 5 s

This setting defines the duration that an additional bell is activated at the beginning of a direct call.

Webhook for activation:

This setting can be used to specify a webhook to be sent when the relay is activated.

A webhook is a URL used to notify another device over the network that a certain event has occurred.

For example, a webhook can be used to control a network relay to open the door or trigger other functions.

The protocol to be used (HTTP or HTTPS) must be specified in the URL. It may also be necessary to specify authentication (username or username and password) in the URL if the device receiving the webhook requires it.

For example, if the command relay=1 is to be sent to a network relay with the IP address 192.168.16.200 and the user 'user' with the password 'password' is to be used as authorisation, the following URL results:
http://user:password@192.168.16.200/?relay=1

If the network relay does not require authentication, the following is sufficient:
http://192.168.16.200/?relay=1

By default, a webhook uses the HTTP GET method.

However, if the URL is prefixed with json- or urlencoded-, the webhook switches to data transfer in the request body via the HTTP POST method. In this case, an additional input field 'body' appears, in which the data to be sent can be entered.

Here are two examples of such webhooks:
json-http://192.168.16.200
urlencoded-http://192.168.16.200

Important note
Sending webhooks requires a functional network connection.

Body: The data transmitted in the request body of the webhook will be specified here.

Webhook for deactivation: This setting can be used to specify a webhook to be sent when the relay is deactivated.

Body: The data transmitted in the request body of the webhook will be specified here.

Verify webhook identity:

- no
- certificate

- certificate & hostname

Default: certificate & hostname

This setting determines whether the identity of an https webhook should be verified when communicating with it.

To ensure secure communication, the certificate and host name should be verified.

The certificate can only be verified if the device has a valid time.

Required numbers for call-triggered opening: 0 - 20

Default: 0

When an incoming call is accepted, it is possible to automatically trigger access for certain authorised phone numbers.

This setting can be used to set the number of authorised phone numbers for such call-triggered opening.

For better manageability, a name or other comment can be added to each call number.

Important notes
This functionality requires that the call number be transmitted when an incoming call is received.
The authorised call numbers must be entered exactly as they are transmitted.
As it is not possible to verify the authenticity of the transmitted call number, it is the responsibility of the installer or user to ensure that the use of this function does not result in unauthorised call-triggered opening in their application.

Settings for the second switching contact

Codes

Automatic code checking:

- on
- off

Default: on

If a code for a door release relay is entered, the entry

must normally be completed with #. If the set code is 2580, for example, then 2580 # is entered.

If the automatic code checking is switched on, when you enter a code, the device automatically checks after the set time whether the code entered is valid. If so, the code entry is automatically completed and you do not have to complete the entry with #.

Without an automatic code check, you must complete the code entry with #.

If you start entering a code and then no further digits are entered for 5 seconds, the code entry is discarded.

After:

500 - 3000 ms

Default: 1000 ms

time after which an entered code is automatically checked

If you set the automatic code checking to a short duration of time, problems can arise if there is a longer code (e.g. 1234) whose beginning corresponds exactly to a shorter code (e.g. 12). If a longer code is entered too slowly, the shorter code may be recognized.

In this case you can either use this setting to increase the time after which codes are automatically checked or to switch off the automatic code check. Another option is to select the codes so that no code corresponds to the beginning of another code.

Accept codes from indoor stations:

- no
- only known call numbers
- only following numbers
- only known and following numbers
- yes

Default: yes

This setting determines whether or not codes are accepted from the indoor station to control relays during a connection as a SIP phone. It is possible to limit the acceptance of codes to known or specified numbers.

A call number is known if it is stored in the configuration for a call button, the i button of the keypad, a quick dialling number, a trigger or a phone book entry and if it triggers a call via this SIP account.

When using schedules, a call number is only considered known if it could also be dialled by the button or trigger at the time of the incoming call.

schedule is valid when receiving a call
The call number for the time periods of the schedule is considered known, but not the call number for the other time periods.

schedule is invalid when receiving a call
The call number for the other time periods of the schedule is considered known, but not the call number for the time periods of the schedule.

Important note
This setting only applies to connections as a SIP phone.
When a code is received, the remote phone number transmitted by the SIP PBX is determined. Some SIP PBXs do not update the phone number when a call is forwarded or picked up. The evaluation can only be done correctly if the SIP PBX transmits the correct call number. For some SIP PBXs, evaluating the contact information provides a better result.
The function can therefore not be guaranteed in all cases. When using the function, a check of the different call scenarios (pick-up, forwarding, ...) should be carried out with the SIP PBX used.

Call numbers: Only codes from the phone numbers given here will be accepted.

If only the plain phone number is specified, it applies to the default SIP account. Otherwise, the SIP account can be specified by specifying the prefix sip: before the number and appending the server of the account with @. Alternatively, the prefix sip1: or sip2: can be used before the call number to assign the call number to the first or second SIP account. It is also possible to specify a direct SIP number if direct SIP calls are allowed.

It is possible to specify multiple phone numbers by

separating each with a comma.

Use contact information as call number:

- no
- yes

Default: no

When a code is received, the remote phone number transmitted by the SIP PBX is determined. Some SIP PBXs do not update the phone number when a call is forwarded or picked up. The evaluation can only be done correctly if the SIP PBX transmits the correct call number. For some SIP PBXs, evaluating the contact information provides a better result.

Important note
The function can therefore not be guaranteed in all cases. When using the function, a check of the different call scenarios (pick-up, forwarding, ...) should be carried out with the SIP PBX used.

Settings for entering the code

Access control

Send e-mail:

- no
- when access is granted
- when access is refused
- when access granted or refused

Default: no

It is possible to send an e-mail in order to log if an attempt is made to open the access via the code lock function, the card reader or from an indoor station.

This setting defines whether and in which cases such logging should take place.

Devices with a camera can be set so that a picture is taken at the moment of the access attempt and sent as an e-mail attachment.

This functionality requires that the sending of e-mails in the section 'Network' in the group 'E-Mail' has been allowed and configured correctly.

Important notice
If you would like to use the logging of the access

	control via e-mail, please check that the sending and storage of these e-mails is possible and takes place within the framework of the legal regulations of your country or your company, especially if camera images are also sent.
Send e-mail to:	e-mail address to which the log should be sent
With camera image:	• no • yes Default: yes Devices with a camera can be set so that a picture is taken at the moment of the access attempt and sent as an e-mail attachment. <u>Important notice</u> If you would like to use the logging of the access control via e-mail, please check that the sending and storage of these e-mails is possible and takes place within the framework of the legal regulations of your country or your company, especially if camera images are also sent.

Logging of access control via e-mail

Play tone while opening of the access:	see section Acoustics
Terminate connection after opening of the access:	see section Connection
Use door opener button:	see section Triggers

Triggers

Alarm input

Status: display of the current status of the alarm input

Detection:

- disabled
- by rising edge
- by falling edge
- by rising or falling edge

Default: by rising edge

The alarm input allows information to be transmitted to the device using a voltage and then an alarm to be triggered. The following options are available for the detection of an alarm:

disabled
The alarm input is deactivated. A voltage connected to the alarm input is ignored and no alarm is recognized.

by rising edge
If there is no voltage at the alarm input (state 0) and a voltage is then detected (state 1), a rising edge is recognized and an alarm is triggered.
If the voltage drops again (state 0), it is a falling edge. This is ignored and no alarm is triggered.

by falling edge
If a voltage is present at the alarm input (state 1) and it then drops out (state 0), a falling edge is detected and an alarm is triggered.
If the voltage comes back (state 1), it is a rising edge. This is ignored and no alarm is triggered.

by rising or falling edge
If there is no voltage at the alarm input (state 0) and then a voltage is detected (state 1), then a rising edge is recognized. If there is a voltage at the alarm input (state 1) and then it drops out (state 0), then a falling edge is recognized.
In both cases, ie whenever the status changes, an alarm is triggered.

Debounce time: 50 - 1500 ms

Default: 100 ms

Here you can set how long the alarm input must change its state (0 = no voltage or 1 = voltage present) at least before this change is recognized as valid.

If there is strong interference in the vicinity of the device, it can radiate into the connection cable of the alarm input and lead to voltage fluctuations. Such interference can trigger false alarms. In this case, increasing the debounce time can help.

If the debounce duration is set very high, it is possible that brief changes in status are no longer correctly recognized.

Minimum duration rising edge:

- none
- 1 s
- 2 s
- 3 s
- 4 s
- 5 s
- 6 s
- 7 s
- 8 s
- 9 s
- 10 s
- 15 s
- 20 s
- 25 s
- 30 s
- 35 s
- 40 s
- 45 s
- 50 s
- 55 s
- 60 s
- 70 s
- 80 s
- 90 s
- 2 min
- 3 min
- 4 min
- 5 min
- 6 min
- 7 min
- 8 min
- 9 min

- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 35 min
- 40 min
- 45 min
- 50 min
- 55 min
- 60 min

Default: none

In certain cases, the alarm should not be triggered immediately when the edge changes, but only when the new state has been present for a certain time.

This setting determines how long state 1 must be present on a rising edge before the alarm is triggered.

If the minimum duration of the rising edge is not reached, no alarm is triggered. In this case, falling back to state 0 is not interpreted as a falling edge.

Minimum duration falling edge:

- none
- 1 s
- 2 s
- 3 s
- 4 s
- 5 s
- 6 s
- 7 s
- 8 s
- 9 s
- 10 s
- 15 s
- 20 s
- 25 s
- 30 s
- 35 s
- 40 s
- 45 s
- 50 s
- 55 s
- 60 s
- 70 s
- 80 s

- 90 s
- 2 min
- 3 min
- 4 min
- 5 min
- 6 min
- 7 min
- 8 min
- 9 min
- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 35 min
- 40 min
- 45 min
- 50 min
- 55 min
- 60 min

Default: none

In certain cases, the alarm should not be triggered immediately when the edge changes, but only when the new state has been present for a certain time.

This setting determines how long state 0 must be present on a falling edge before the alarm is triggered.

If the minimum duration of the falling edge is not reached, no alarm is triggered. In this case, falling back to state 1 is not interpreted as a rising edge.

Treat alarm:

- like a button
- like a message
- like a sabotage

Default: like a button

A recognized alarm is like a direct call button (alarm button) that has been pressed, and an action can be set that is triggered when the alarm key is pressed, i.e. when an alarm is recognized.

If an alarm is detected, this setting can be used to define how exactly it is treated, like a button or a message.

like a button
If the device is idle and an alarm is detected, the set action is triggered.
If, on the other hand, the device is in a connection and an alarm is detected, it is treated like a button press. What happens then depends on the settings 'Cancel connection with initiating button' or 'Cancel connection with other button' in the section 'Connection'.
Depending on the setting and the situation, it may be that the connection is terminated and the action set for the alarm input is triggered. However, it is also possible that the alarm cannot cancel the connection, or it can cancel it, but not triggering another function (button) is not permitted. In both cases, the function specified for the alarm input is not carried out, so the alarm is lost.

like a message
If the device is idle and an alarm is detected, the set action is triggered.
If, on the other hand, the device is in a connection and an alarm is detected, it is stored and the set action is triggered as soon as the connection is terminated and the device is idle again.

like a sabotage
When an alarm is detected, a sabotage is triggered. Further processing takes place according to the settings made below under 'Sabotage'

Message for status 0: This message is displayed when there is no voltage present at the alarm input (status 0).

It is used when an alarm is triggered by a falling edge and an e-mail is sent.

Message for status 1: This message is displayed when there is a voltage present at the alarm input (status 1).

It is used when an alarm is triggered by a rising edge and an e-mail is sent.

Name: Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is

used to label the corresponding virtual call button or is shown on the display as the call destination when the connection is established.

Action:

- none
- call
- group call with 2 numbers
- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers
- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1
  :
- play voice announcement #9

Default: call

Action to be performed when the button is pressed

The following actions are possible:

none
The keystroke is ignored.

call
A connection is established to the remote station specified under 'Call number'.

group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains'

can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Periods of time are specified in a schedule and a telephone number is specified that is called if the button is pressed within one of the specified (valid) periods of time.
In addition, an action can be specified that is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the button is pressed. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to a schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice announcement.

play voice announcement
An individual voice announcement can be set which is issued when the button is pressed.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the button is pressed within one of the (valid) periods specified in the schedule.

Door opener relay:
- 1
- 2

- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in the section 'Relay'.

Action for the other time periods:

- call
- announce opening hours
- announce availability
- announce personal availability
- play voice announcement #1
  :
- play voice announcement #9

Default: call

This action is carried out if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Call number for the other time periods:

This number is called if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Triggering a call or alarm by a voltage

Sabotage

Safety shutdown:

display of the current state of the safety shutdown

In the case of a safety shutdown, the extension port network is deactivated.

An activated safety shutdown can be deactivated via the web interface. With delocalised electronics, deactivation can also be done via the configuration button.

activate / deactivate

activate
activate the safety shutdown

deactivate
deactivate the safety shutdown

Contact for door opener button / sabotage:

- use for door opener button
- use as sabotage contact

Default: use for door opener button

This setting determines how the contact for door opener button / sabotage is to be used.

use for door opener button
A door opener button can directly trigger the opening of the door, i.e. the triggering of the door opener relay, see section 'Relay' for this.

use as sabotage contact
In the event of sabotage, an action can be triggered, for example sending an e-mail or activating the safety shutdown.

A door opener button or a sabotage contact is a normally open contact.

Safety shutdown in case of sabotage:

- no
- yes

Default: yes

This setting determines whether or not the safety shutdown should be activated when a sabotage is detected.

Message in case of sabotage:

This message is displayed when a sabotage is detected.

Name:

Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is used to label the corresponding virtual call button or is shown on the display as the call destination when the connection is established.

Action:

- none
- call
- group call with 2 numbers
- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers

- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1
  :
- play voice announcement #9

Default: call

Action to be performed when the button is pressed

The following actions are possible:

none
The keystroke is ignored.

call
A connection is established to the remote station specified under 'Call number'.

group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains' can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Periods of time are specified in a schedule and a telephone number is specified that is called if the button is pressed within one of the specified (valid)

periods of time.
In addition, an action can be specified that is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the button is pressed. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to a schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice announcement.

play voice announcement
An individual voice announcement can be set which is issued when the button is pressed.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the button is pressed within one of the (valid) periods specified in the schedule.

Door opener relay:
- 1
- 2
- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in the section 'Relay'.

Action for the other time periods:
- call

- announce opening hours
- announce availability
- announce personal availability
- play voice announcement #1
  :
- play voice announcement #9

Default: call

This action is carried out if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Call number for the other time periods:

This number is called if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Settings for handling a detected sabotage

Radar sensor

Detection:

- disabled
- arriving persons/objects
- leaving persons/objects
- arriving or leaving persons/objects

Default: arriving persons/objects

The radar sensor allows people or objects in front of the device to be detected and reported. The following options are available for detection:

<u>disabled</u>
The radar sensor is deactivated. No people or objects are reported.

<u>arriving persons/objects</u>
If the radar sensor detects people or objects that are approaching, i.e. moving towards the radar sensor, it reports this.
People or objects that move away from the radar sensor are ignored and no message is triggered.

<u>leaving persons/objects</u>
If the radar sensor detects people or objects that are moving away, i.e. moving away from the radar sensor, it reports this.
People or objects that approach, that is, moving towards the radar sensor, are ignored and no

message is triggered.

<u>arriving or leaving persons/objects</u>
If the radar sensor detects people or objects that are approaching or moving away, it reports this in both cases.

Maximum detection range:

1 - 100 %

Default: 20 %

The radar sensor can detect moving objects in an area of up to 10 meters in front of the sensor. The sensor is more sensitive in the frontal direction than in the edge areas. The sensitivity (range) decreases to the side compared to the frontal direction.

By reducing the detection area, the radar sensor can be set so that it only detects and reports approaching people, for example, when they are just in front of the device.

Detection pause:

1 - 25 s

Default: 10 s

If the radar sensor has detected and reported people or objects, further detection can be paused for a moment so that there are no multiple reports.

This duration, for which the detection is paused, can be specified via this setting.

Operation mode of the radar sensor relay:

- make contact
- break contact

Default: make contact

There is a relay on the radar sensor board that is switched when movement is detected.

Here you can set whether this relay should function like a normally open contact (NO) or like a normally closed contact (NC).

As a normally open contact, the relay contact is normally open and it is closed for the set activation period as soon as movement is detected.

As a normally closed contact, it is exactly the opposite. Normally the relay contact is closed and it is opened for the set activation duration when movement is detected.

Activation time of the radar sensor relay:

1 - 255 s

Default: 5 s

When movement is detected, the relay on the radar sensor board is switched for the duration set here.

Name:

Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is used to label the corresponding virtual call button or is shown on the display as the call destination when the connection is established.

Action:

- none
- call
- group call with 2 numbers
- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers
- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1
  :
- play voice announcement #9

Default: call

Action to be performed when the button is pressed

The following actions are possible:

<u>none</u>
The keystroke is ignored.

<u>call</u>
A connection is established to the remote station

specified under 'Call number'.

group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains' can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Periods of time are specified in a schedule and a telephone number is specified that is called if the button is pressed within one of the specified (valid) periods of time.
In addition, an action can be specified that is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the button is pressed. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to a schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice

announcement.

play voice announcement
An individual voice announcement can be set which is issued when the button is pressed.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the button is pressed within one of the (valid) periods specified in the schedule.

Door opener relay:

- 1
- 2
- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in the section 'Relay'.

Action for the other time periods:

- call
- announce opening hours
- announce availability
- announce personal availability
- play voice announcement #1
  :
- play voice announcement #9

Default: call

This action is carried out if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Call number for the other time periods: This number is called if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Settings for the detection of persons or objects

Schedule	Scheduled calls:	• no • according to simple schedule • according to schedule • according to simple schedule with initialisation • according to schedule with initialisation Default: no It is possible to automatically initiate a call at a specific time. Periods of time are specified in a schedule and two numbers are specified. The first number is called at the beginning of a valid period and the second at the end. If only one of the two numbers is given, only one call is triggered at the beginning or at the end of a valid period of time. The time-controlled calls are triggered when the device is in the idle state. If the device is in use, it will not be triggered until use has ended. with initialisation The time-controlled calls are triggered at the beginning or end of a valid period of time. With the setting 'with initialisation', a call is also triggered after a restart or after a configuration change to ensure that the device is in the correct state.
	Name:	Name of the remote station to be called or the action to be carried out For devices with a display, the name entered here is shown on the display as the call destination when the connection is established.
	Call number at the beginning of a valid period:	This number will be called at the beginning of the (valid) periods specified in the schedule.
	Call number at the end of a valid period:	This number will be called at the end of the (valid) periods specified in the schedule.

Settings for scheduled calls

System start

Call after system start:

- no
- yes

Default: no

It is possible to automatically trigger a call after starting the device.

The call is triggered as soon as the device is in idle mode for the first time after start-up and the set delay time has elapsed.

After:

0 - 120 s

Default: 5 s

This setting allows the call to be delayed slightly after system start-up to give the device sufficient time to perform SIP registration, for example.

The call is triggered as soon as the device is in idle mode for the first time after start-up and the delay time set here has elapsed.

Message:

This message is displayed when the system has been started.

Name:

Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is shown on the display as the call destination when the connection is established.

Call number:

number of the remote station to be called

Triggering a call after starting the device

Daily audio test

Perform:

- no
- yes

Default: no

The daily audio test allows the functionality of the loudspeaker and microphone to be checked regularly.

For this purpose, various tones are emitted via the loudspeaker, which then have to be recognised again via the microphone.

If the audio test fails, a call or an action can be triggered, for example to inform a remote station by voice announcement or email.

If the last audio test has failed, the remote station is informed of the audio problem by voice announcement when a call is made after the connection is established.

The audio test can also be triggered manually, for example via the web interface. If a manually triggered audio test fails, a call is only triggered if the previously known test result was ok.

If a relay is used in the operating mode 'fault indication', a fault is detected in case of a failed audio test and the relay is switched accordingly.

At: 0 - 23 h

Default: 10 h

time at which the automatic audio test should be carried out

If it has been set in the 'Network' section that the time of the device is synchronised with an NTP time server, the audio test is performed daily at the set time as soon as the device is in idle mode.

Without synchronised time, the audio test is performed daily at an unspecified time.

Audio test for:

- hands-free
- handset
- handset & speaker
- hands-free & handset

Setting of the audio units to be tested: see section Acoustics

Audio test: trigger

trigger audio test to check loudspeaker and microphone

Message: This message is displayed when the the audio test has failed.

Name: Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is shown on the display as the call destination when the connection is established.

Call number: number of the remote station to be called

Regular check of loudspeaker and microphone

Noise alarm

Detection:

- disabled
- high ambient noises

Default: disabled

The noise detection function allows you to monitor the ambient noise and to trigger a noise alarm in certain situations. For this purpose, noise detection must be switched on in the 'Acoustics' area. The following options are available for the detection of a noise alarm:

disabled
Noise alarm detection is deactivated and no noise alarms are detected.

high ambient noise
If the ambient noise exceeds an adjustable noise threshold for an adjustable duration, then a noise alarm is detected.

Ambient noises: display of the current volume of the environment in dB

Important notice
Since the Behnke station is not a calibrated dB measuring device, the dB values displayed are not absolute but tendential.

Minimum noise level: 70 - 95 dB

Default: 80 dB

This setting determines the noise level that must be exceeded for a noise alarm to be detected.

Important notice
Since the Behnke station is not a calibrated dB measuring device, the adjustable dB values are not absolute but tendential, which are also subject to a certain range of fluctuation from device to device.
If the tendential values do not meet the requirements, the setting of the minimum noise level should be checked with a calibrated dB meter during set-up, changes and at regular intervals.

Minimum duration of high noise level:

0 - 120 s

Default: 30 s

This setting determines how long the minimum noise level must be exceeded before a noise alarm is triggered.

Minimum duration of non-high noise level:

0 - 120 s

Default: 30 s

If a noise alarm is detected, this setting specifies how long the noise level must fall below the minimum noise level before the high ambient noise is considered to have ended and a noise alarm can be detected again.

Alarm suppression:

- none
- 1 s
- 2 s
- 3 s
- 4 s
- 5 s
- 6 s
- 7 s
- 8 s
- 9 s
- 10 s
- 15 s
- 20 s
- 25 s
- 30 s
- 35 s

- 40 s
- 45 s
- 50 s
- 55 s
- 60 s
- 70 s
- 80 s
- 90 s
- 2 min
- 3 min
- 4 min
- 5 min
- 6 min
- 7 min
- 8 min
- 9 min
- 10 min
- 15 min
- 20 min
- 25 min
- 30 min
- 35 min
- 40 min
- 45 min
- 50 min
- 55 min
- 60 min

Default: none

To avoid triggering too many noise alarms in succession, the reporting of further alarms can be suppressed for a certain duration after a detected noise alarm. If alarms are detected during this period, they are no longer reported and are therefore lost.

The duration can be set via this setting.

When the device is restarted, for whatever reason, the alarm suppression is reset and a detected alarm is reported again.

Treat noise alarm:

- like a button
- like a message

Default: like a button

A recognized noise alarm is like a direct call button (noise alarm button) that has been pressed, and an

action can be set that is triggered when the noise alarm key is pressed, i.e. when a noise alarm is recognized.

If a noise alarm is detected, this setting can be used to define how exactly it is treated, like a button or a message.

<u>like a button</u>
If the device is idle and a noise alarm is detected, the set action is triggered.
If, on the other hand, the device is in a connection and a noise alarm is detected, it is treated like a button press. What happens then depends on the settings 'Cancel connection with initiating button' or 'Cancel connection with other button' in the section 'Connection'.
Depending on the setting and the situation, it may be that the connection is terminated and the action set for the noise alarm is triggered. However, it is also possible that the noise alarm cannot cancel the connection, or it can cancel it, but not triggering another function (button) is not permitted. In both cases, the function specified for the noise alarm is not carried out, so the noise alarm is lost.

<u>like a message</u>
If the device is idle and a noise alarm is detected, the set action is triggered.
If, on the other hand, the device is in a connection and a noise alarm is detected, it is stored and the set action is triggered as soon as the connection is terminated and the device is idle again.

Message: This message is displayed when a noise alarm is detected.

Name: Name of the remote station to be called or the action to be carried out

For devices with a display, the name entered here is used to label the corresponding virtual call button or is shown on the display as the call destination when the connection is established.

Action:
- **none**
- **call**
- **group call with 2 numbers**

- group call with 3 numbers
- group call with 4 numbers
- call chain with 2 numbers
- call chain with 3 numbers
- call chain with 4 numbers
- call according to simple schedule
- call according to schedule
- door opening
- door opening according to simple schedule
- door opening according to schedule
- play voice announcement #1
  :
- play voice announcement #9

Default: call

Action to be performed when the button is pressed

The following actions are possible:

none
The keystroke is ignored.

call
A connection is established to the remote station specified under 'Call number'.

group call
A connection to 2, 3 or 4 remote stations is established at the same time. If one of the remote stations accepts the connection, the connections to the remaining remote stations are terminated.
When calling via a SIP server (IP telephone system), it must allow a corresponding number of simultaneous calls for the registered SIP subscriber.

call chain
A connection to 2, 3 or 4 remote stations is established one after the other until one of the remote stations accepts the connection or all remote stations have been called.
In the section 'Connection', the setting 'Maximum duration of connection establishment for call chains' can be used to specify how long the attempt is made to reach the first remote stations in the chain.
The duration of the connection to the last remote station is determined by the setting 'Maximum duration of connection establishment'.

call according to schedule
Periods of time are specified in a schedule and a telephone number is specified that is called if the button is pressed within one of the specified (valid) periods of time.
In addition, an action can be specified that is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a different number, announce the opening times or availability, or play your own voice announcement.

door opening
A door opener relay is specified, which is activated when the button is pressed. The specified relay must of course be configured as a door opener in the section 'Relay'.
When the door is opened according to a schedule, the door is only opened at the (valid) times specified in the schedule.
An action can be specified which is carried out if the button is pressed at a different point in time, i.e. outside of the valid time periods.
You can either call a number, announce the opening times or availability, or play your own voice announcement.

play voice announcement
An individual voice announcement can be set which is issued when the button is pressed.
The selected voice announcement must of course have been uploaded or generated in the section 'Acoustics'.

Call number: number of the remote station to be called

Call number for the time periods of the planning: This number will be called if the button is pressed within one of the (valid) periods specified in the schedule.

Door opener relay:

- 1
- 2
- 1 & 2

Default: 1

Here, the door opener relay is specified that is activated in order to open the access. The specified relay must of course be configured as a door opener in

	the section 'Relay'.
Action for the other time periods:	• call • announce opening hours • announce availability • announce personal availability • play voice announcement #1 : • play voice announcement #9 Default: call This action is carried out if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.
Call number for the other time periods:	This number is called if the button is pressed outside of the (valid) periods specified in the schedule or if the device does not have a valid time.

Settings for the detection of high ambient noise

Special parameters for call numbers:	see section Buttons

Acoustics

Noise detection:

- on
- off

Default: on

The device can measure the ambient noise and analyze how loud the environment is.

For this purpose, the environment of the last 15 minutes is evaluated and then the volume class (1-5) is given. The higher the volume class, the louder the environment.

Depending on the environment, a device should be used that is suitable for this volume class.

Important note
The functions 'audio test', 'daily audio test' and 'noise alarm' require the activation of noise detection.

Hands-free microphone:

- not connected
- connected

Default: connected

Normally, the devices have a microphone. In exceptional cases, for example if the device is equipped with a handset, there may be no hands-free microphone.

In this case, this setting can be used to specify that no hands-free microphone is connected so that the missing microphone signal is not displayed as an error. For a device with a handset, the handset microphone is then also used for noise detection and voice connections.

Microphone:

display of the current microphone state

If a functioning microphone is connected to the microphone connection, its signal is detected and displayed accordingly.

If no microphone is connected, no signal is normally

detected.

If the loudspeaker is accidentally connected to the microphone connection instead of the microphone, it also supplies a signal and it is not possible to distinguish from the signal whether it is a loudspeaker or a microphone.

Ambient noises: display of the current volume of the environment in dB

Important notice
Since the Behnke station is not a calibrated dB measuring device, the dB values displayed are not absolute but tendential.

Volume class / environment:

- quiet environment
- normal environment
- noisy environment
- very noisy environment
- extremely noisy environment

When the noise detection is activated, the device continuously measures the ambient noise and uses this to determine a volume class and an assessment of how loud the environment is.

The higher the volume class, the louder the environment.

Evaluation: reset

resetting the rating of the volume class / environment

Expert settings:

- use default settings
- set individually

Default: use default settings

Change expert settings only after consulting the hotline!

DB correction: 70 - 130 %

Default: 100 %

Since the Behnke station is not a calibrated dB measuring device, the dB values displayed are not

absolute but tendential.

If the ambient noises displayed are generally too high or too low, this setting can be used to make a correction. Even after the correction has been made, the displayed values are tendential.

DB offset:

-10 - 10 dB

Default: 0 dB

Since the Behnke station is not a calibrated dB measuring device, the dB values displayed are not absolute but tendential.

If the ambient noises displayed are generally too high or too low, this setting can be used to adjust the offset. Even after the correction has been made, the displayed values are tendential.

Microphone_detection:

- no
- yes

Default: yes

When microphone detection is enabled, noise detection first attempts to determine whether a microphone is connected or not.

If no microphone is detected, ambient noise cannot be determined and 0 dB is displayed.

Without microphone detection, ambient noise is always determined and displayed. Due to system noise, ambient noise may be detected even though no microphone is connected.

Log microphone signal computation:

- no
- yes

Default: no

This setting determines whether the calculation of the microphone signal should be logged.

This usually generates a large number of log entries and should therefore only be activated for a short time for debugging purposes.

Audio

Audio test for:

- hands-free
- handset
- handset & speaker
- hands-free & handset

Default: hands-free

For a device with handset, this setting can be used to specify whether the loudspeaker and microphone of the device (= hands-free) or the handset or both should be tested during an audio test.

The hands-free communication cannot be tested on a device with a handset but without a microphone. Instead, the device loudspeaker built into the handset module can also be tested during the audio test.

A newly selected setting must first be saved before an audio test can be triggered with this setting.

Audio test: trigger

trigger audio test to check loudspeaker and microphone

Current volume: display of the currently used volume

If noise detection is used, the volume used by the device can be automatically increased in a noisy environment. The volume displayed here may then differ from the volume set below.

Volume: 0 - 100 %

Default: 80 %

Increase volume automatically:

- no
- from volume class 1 = quiet enviroment
- from volume class 2 = normal enviroment
- from volume class 3 = noisy environment
- from volume class 4 = very noisy environment
- from volume class 5 = extremely noisy environment

Default: from volume class 3 = noisy environment

The volume used by the device can be increased

automatically in a noisy environment.

The volume class determined by the noise detection is used to evaluate the environment.

The volume is increased from the volume class set here. In a quieter environment, the set volume is used.

Microphone sensitivity: 0 - 100 %

Default: 70 %

Notification tone volume:

- very low
- low
- standard

Default: standard

This setting can be used to reduce the volume of the notification tones emitted at the device, such as when starting up, pressing a button or scrolling.

The setting has an effect relative to the generally used volume.

Daily audio test: see section Triggers

Audio settings of the handset: see section Handset

Adjustments of the audio signals

IP audio

Expert settings:

- use default settings
- set individually

Default: use default settings

Change expert settings only after consulting the hotline!

Receive amplification: -10 - 10 dB

Default: 3 dB

Ddigital amplification/attenuation of the audio

signals received from the remote station during a SIP connection

Transmit amplification:

-10 - 10 dB

Default: 3 dB

digital amplification/attenuation of the audio signals sent to the remote station during a SIP connection

Echo suppression:

- off
- very light
- light
- medium
- strong
- very strong

Default: strong

The echo suppressor tries to attenuate the microphone signal as soon as the person on the other side speaks in order to improve hands-free communication and further reduce any residual echo.

This setting can be used to determine whether and how much the microphone signal should be attenuated when the other party speaks.

Echo cancellation:

- on
- off

Default: on

Echo cancellation tries to recognize and reduce audio signals that are output via the loudspeaker of the device and are then picked up again after being reflected by the microphone.

Without echo compensation, when the person on the other side speaks, they hear what they have just said with a delay (echo). This can be very annoying.

Adjustments of the audio signals for IP connections

Ringtone

Ringtone volume:

- off
- low
- high

Default: high

This setting determines whether a low, high or no ring tone should be emitted.

It applies when using the 'indoor station' display function to signal an incoming call and for the indoor door bell button.

The setting can also be changed via the bell icon in the upper right corner of the indoor station's main screen.

Low ringtone volume:

10 - 50 %

Default: 30 %

volume of the low ringtone

High ringtone volume:

60 - 100 %

Default: 80 %

volume of the high ringtone

Variant:

- Ding Dong
- Echo Bells
- Hypnotic
- Pulsing

Default: Pulsing

This setting defines the ringtone that is played when an incoming connection is received.

It is only available if the call answering is configured to 'accecpt manually' and the acoustical indication of an incoming connection is configured to 'play tone'.

Pause between ringtones:

0 - 30 s

Default: 0 s

This setting defines the time that the system waits after the ringtone has been played before playing it again.

Variant for interior door:

- Ding Dong
- Echo Bells
- Hypnotic
- Pulsing

Default: Ding Dong

This setting defines the ringtone that is emitted when the doorbell button on the interior door is pressed.

It is only available if it is configured in the 'Intercom' section that a bell button for the interior door is connected.

Variant for automatic preview:

- play nothing
- Droplets
- Echoes
- Radar
- Sonar

Default: Echoes

This setting determines the ringtone that is played when the automatic preview is displayed.

Signalling an incoming connection

Indications

In case of a hardware error:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If the device is starting:

- play nothing
- play tone

Default: play tone

If the device has reveiced an IP address:

- play nothing
- play tone

Default: play tone

Announcements for barrier-free access: compliance / activate

In the case of barrier-free access, a visitor must be informed of important events (start of a connection, door opening, ...) both visually via pictograms or display outputs and acoustically via voice announcements.

The necessary acoustic indications are marked with the symbol ♿ and are to be set to voice announcement for barrier-free access.

If an acoustic indication is not appropriately set, its symbol ♿ shall be outlined in red (non-compliant) or yellow (conditionally compliant).

compliant / conditionally compliant / non-compliant
This indicates whether all necessary acoustic indications are set to emit a voice announcement (compliant) or not (non-compliant).
If individual voice announcements are to be used, appropriate voice announcements must be uploaded or generated accordingly (conditionally compliant).

activate
All acoustic indications required for barrier-free access shall be set to emit a voice announcement.

Important notice
The notices for barrier-free access provided here are only recommendations of a purely informative nature. Please check which legal regulations for barrier-free access apply in your country or company and that these are fully complied with.

When triggering a trigger:
- play nothing
- play tone

Default: play nothing

When pressing a direct call button:
- play nothing
- play tone

Default: play tone

When pressing a keypad key:
- play nothing
- play tone

Default: play tone

When pressing the door opener button:	• play nothing • play tone Default: play tone
When picking up or hanging up the handset:	• play nothing • play tone Default: play nothing
When handset is to be hung up:	• play nothing • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
If activating a blocked function:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
At an incoming connection:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play tone
At the start of a connection:	• play nothing • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play nothing
While establishing the connection:	• play nothing • play voice announcement • play voice announcement #1 :

- play voice announcement #9

Default: play voice announcement

At the end of a connection:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play tone

If the connection can not be established:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If the connection duration has expired:

- play nothing
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If the called station doesn't answer:

- play nothing
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If the called station is busy:

- play nothing
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

When activating the telephone function:

- play nothing
- play voice announcement

- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

When activating the code lock function:

- play nothing
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

When activating the quick dialling function:

- play nothing
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If no valid quick dialling entered:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

If invalid code entered at the code lock:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

When opening the access:

- play nothing
- play tone
- play voice announcement
- play voice announcement #1
  :
- play voice announcement #9

Default: play voice announcement

While opening of the access:	• play nothing • play tone • play buzzer tone Default: play tone
If continuous opening has been enabled:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
If continuous opening has been disabled:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
If card is accepted by the card reader:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play tone
If card is refused by the card reader:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play tone
When activating door opener 1:	• play default announcement • play voice announcement #1 : • play voice announcement #9 Default: play default announcement

When activating door opener 2:	• play default announcement • play voice announcement #1 : • play voice announcement #9 Default: play default announcement
When using the phone book:	• play nothing • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
After answering an analogue call:	• play nothing • play tone Default: play tone
After answering an IP call:	• play nothing • play tone Default: play tone
For the called station after answering the call:	• play nothing • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play nothing
If invalid code entered at the indoor station:	• play nothing • play tone • play voice announcement • play voice announcement with valid code • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement with valid code
After the mute function has been activated:	• play nothing • play tone • play voice announcement • play voice announcement #1 :

	• play voice announcement #9 Default: play voice announcement
Before the mute function will be deactivated:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement
If a call chain has been confirmed:	• play nothing • play tone • play voice announcement • play voice announcement #1 : • play voice announcement #9 Default: play voice announcement

Adjustments for the acoustic indications

Individual announcements	Announcement:	play / upload / remove / generate play The selected voice announcement is played through the loudspeaker of the computer. upload An announcement in the WAV file format can be uploaded here for the selected voice announcement. The required format of the WAV file is 16 kHz, 16 bit, mono and the maximum file size is 1 MB. remove The selected voice announcement will be removed. generate The selected voice announcement is generated. A window opens in which you can enter the desired text for the announcement. The device then contacts the support server to receive the desired voice announcement file. If the computer cannot or is not allowed to establish an Internet connection, it is not possible to contact

Management of individual announcements

the support server and thus generate voice announcements.

The generation of voice announcements via the support server is a service that is currently (05/2026) provided free of charge. The service is subject to change, i.e. the service may be one day modified, discontinued or replaced by a service for which a charge is made.

Diagnostics

So that we can provide you with optimal support in the event of support, you can download diagnostic data and network traces here and send them to us or transfer them directly to our support server. After consulting our support, you can also use the setting 'activate online-log and allow online-support' to enable remote access to your device.

Very important notice
Diagnostic data, network traces, the online log, the weblog and the syslog contain, among other things, data on the device, the configuration, the network, connections, audio, video and errors that have occurred. If you transmit this data to us, you give your agreement that we may use this data for support purposes. If you allow us remote access, you also agree that we may change the configuration of the device for support purposes.

Serial number:	display of the serial number of the device In certain cases we need the serial number shown here, for example if you transfer diagnostic or trace files to the support or for the online support. The support can identify the device via the serial number.
Support:	display in case of online support whether the device is connected to the support server OFFLINE There is currently no connection to the support server. ONLINE The device is currently connected to the support server.

Log	**Run level:**	• COM • AIF • CFG • HAL • HAL-NOISE • DSP • NET • WEB • CAM • PHO • PHO-SIP

- PHO-MSG
- PHO-IP
- PHO-IC
- APP
- all

Default: all

The software of the device is divided into run levels, each of which takes care of the tasks of a specific sub-area.

When the software is started, the COM level starts first. This then starts the other run levels one after the other. If the configuration is changed, the run levels may be terminated in reverse order up to a certain level and then restarted.

If there is an event in an run level, a log entry for this event is created in the log.

Usually the events of all run levels are logged. However, it is also possible to log only the events of a specific run level.

COM initial run level
starting/stopping/ monitoring the other levels, system logging, firmware update

AIF connection interface
monitoring/control of the hardware on the connection board (buttons, keypad, relays, alarm input, LED, USB switch, network switch), management of the extension interface and the connected modules

CFG configuration
loading/saving/ managing all configuration settings

HAL hardware abstraction level
monitoring/control of the high-performance board (CPU frequency, temperature, memory), detection/management of the connected USB hardware, detection/management of events (keystrokes, keyboard entries), output of tones and voice announcements in the loudspeaker, management of the audio adapter (HAL-SND), noise detection (HAL-NOISE)

DSP display

display detection, control of display outputs, management of the touch screen, filter for displaying SIP video, reception/display of the stream of a video web server

NET network
creation/administration/monitoring of network connections, administration/monitoring of NTP and syslog settings, sending/receiving of UDP messages (status/remote control), detection and publication of MDNS services, detection and integration of IP cameras, network traces, auto-provisioning

WEB webserver
control/monitoring of the web server, communication with the web server application, administration of the users of the web interface, transfer of data to the support server (log, traces, online support)

CAM camera
integration of USB cameras, detection/configuration of the connected USB or IP camera and distribution of the video image, video web server for retrieving videos/images from the camera, filter for SIP video transmission, analysis of the camera image (motion detection, brightness, darkness)

PHO phone
provision of a SIP telephone (PHO-SIP), provision of an IP intercom device (PHO-IP), evaluation of SIP messages (PHO-MSG), administration/control of telephone connections, output of tones and voice announcements to the remote station

APP application
top run level, provision of the core functionalities (door phone, code lock, card reader, telephone, configuration)

Application:

- off
- errors
- warnings
- messages
- debugging

Default: messages

Here you can set the level up to which (1=errors, 2=warnings, 3=messages, 4=debug) events are to be saved in the log.

If, for example, you select 'messages' as the setting, errors, warnings and messages are saved in the log.

The 'debug' setting generates many entries and should only be selected in very special diagnostic cases.

SIP stack:

- off
- errors
- warnings
- messages
- debugging

Default: errors

The SIP stack is an essential and extensive component of the software. It consists of various parts that can enter the corresponding events in the log.

Here you can set the level up to which (1=errors, 2=warnings, 3=messages, 4=debug) events of the SIP stack should be saved in the log.

For example, if you select 'warnings' as the setting, errors and warnings are saved in the log.

The 'messages' and 'debug' settings generate many entries and should only be selected in special diagnostic cases.

SIP messages:

- no
- yes

Default: yes

When used as a SIP telephone or as an IP intercom, communication between the participants takes place via SIP messages.

This setting determines whether SIP messages should be saved in the log.

SIP messages can contain a lot of information. If a SIP message is logged, this is done in the SIP run level, more precisely SIP-MSG.

First, it is specified by whom the message was received or to whom it was sent. Then several lines are logged that begin with - and log the information of the SIP message.

Intercom topology:

- no
- yes

Default: yes

This setting determines whether all intercom devices are logged when a change in the intercom topology is detected.

LDAP messages:

- no
- yes

Default: no

If the phone book synchronisation via LDAP is activated, this setting can be used to determine whether LDAP messages are saved in the log.

This usually generates many log entries and should therefore only be activated briefly for debugging purposes.

Memory:

- standard
- intensive
- debugging

Default: standard

This setting determines how intensively memory changes are logged in the log.

The 'intensive' and 'debug' settings generate many entries and should only be selected in very special diagnostic cases.

System load:

- standard
- intensive
- debugging

Default: standard

This setting determines how intensively system load changes are logged in the log.

The 'intensive' and 'debug' settings generate many entries and should only be selected in very special diagnostic cases.

Diagnostics: download / transfer to support

download
The diagnostic file will be downloaded and can be saved on the computer.

transfer to support
If you are in contact with our support, you can transfer the diagnostic file directly to the support server here. Only transfer the diagnosis if the support has asked you to do so and if you agree that we may use the data contained in the diagnosis file for diagnosis purposes.
If the computer cannot or is not allowed to establish an Internet connection, then contacting the support server and thus transmitting the diagnosis is not possible.

Activate online-log and allow online-support:

- no
- no, disabled by support
- no, support server not reachable
- yes, without permission for remote configuration
- yes

Default: no

So that we can provide you with the best possible support in the event of support, you can, after consultation, make the log available to our support team online, ie transfer it to our support server and enable remote access to your device.

The online log contains, among other things, data on the device, the configuration, the network, connections, audio, video and errors that have occurred.

If you activate the online log via this setting and allow us to provide online support, you agree that we can use the online log for support purposes and that we can change the configuration of the device for support purposes.

If online support is enabled without permission for remote configuration, the support can see and analyse the configuration of the device but does not have the ability to change it.

With the online log or online support, the device establishes encrypted Internet connections to our support server. If the device is not allowed to establish Internet connections, for example because a firewall is blocking them, then the online log or the Online support not possible.

Before activating online support via this setting, our support team must allow online support for this device. The serial number of this device is required for this.

Online-support via configuration button:

- refuse
- allow

Default: allow

This setting determines whether online support can be activated or deactivated by pressing the configuration button 5 times.

Logging of event messages from the software

Network trace

Activate trace:

- no
- yes

Default: yes

The device can record the network traffic and make it available in a file (network trace) for further analysis.

A trace can be downloaded, for example, to forward it to the support, or it can be transferred directly to our support server. In both cases, this should only be done on request from the support.

A trace contains, among other things, data on the device, the configuration, the network, connections, audio, video and errors that have occurred.

If you send us a trace, you agree that we can use it for support purposes.

Interface:

- any
- device

Default: device

This setting can be used to set the network interface on which the trace is to be carried out.

Size:

- small
- medium
- big

Default: small

This setting defines the size of the ring buffer of the trace.

A larger buffer allows more network traffic to be recorded, so you can look back into the past longer. However, the trace file can then become very large, which may make transmission more difficult.

Filter:

- none
- SIP
- SIP and RTP streams
- SIP and syslog
- SIP, RTP streams and syslog
- define

Default: SIP, RTP streams and syslog

The trace can record the entire network traffic or filter out certain interesting packets and only record these.

This setting can be used to determine whether a filter should be used and, if so, for which network packets.

Filter expression:

own filter for the network trace

Information on PCAP filter expressions can be found at https://www.tcpdump.org

Trace:

download / transfer to support

download
The trace file will be downloaded and can be saved on

the computer.

transfer to support
If you are in contact with our support, you can transfer the trace file directly to the support server here.
Only transmit the diagnosis if the support has asked you to do so and if you agree that we may use the data contained in the trace file for diagnosis purposes.
If the computer cannot or is not allowed to establish an Internet connection, contacting the support server and thus transferring the trace is not possible.

Setting for recording network traffic

Weblog

Activate weblog:

- no
- yes

Default: no

This setting determines whether the log can be called up with a web browser.

Password:

Default: weblog

password that must be entered when logging on to the device's web interface in order to call up the weblog, if it is activated

Providing the log for retrieval with a web browser

Syslog

Activate syslog:

- no
- yes

Default: no

The log can be sent as syslog messages over the network to a syslog server if the syslog is activated via this setting.

In addition to the software log, the syslog also contains the log messages for the entire system.

Syslog server:

IP address or host name

Sending the log to a syslog server

Test	State:	display of the current state of the system, see also the section 'System'
	Contact of relay 1:	display of the current state of the first switching contact and the state of the access
	Contact of relay 2:	display of the current state of the second switching contact
	Audio test:	trigger trigger audio test to check loudspeaker and microphone
	SIP registration:	trigger trigger new registration of all configured SIP accounts
	Door opener relay 1:	trigger trigger activation of door opener relay 1 if relay 1 is configured as door opener relay
	Door opener relay 2:	trigger trigger activation of door opener relay 2 if relay 2 is configured as door opener relay
	Button:	trigger trigger the selected button
	Outdoor station:	call call the selected outdoor station
	Call number:	call call the specified number

IP address or host name:	ping / resolve / arp ping or resolve the specified IP address or host name or display arp cache entries

Remote triggering/testing of certain device functions

System

Information

Device type:

- unknown device
- all-in-one communication station
- compact communication station
- modular communication station
- delocalised communication station
- indoor communication station

The device automatically detects the device type based on the connection board and the connected components.

If the recognized device type displayed here is not correct, please contact the support.

Version:

display of the installed firmware version

The changes between each firmware version are described in the Technical Manual.

See manual under Version History.

Platform:

- P1
- P2

display of the platform

Mainboard:

- unknown
- Dragonboard® 410c
- Geniatech® DB4
- Geniatech® DB4 V2
- Geniatech® DB11

display of the used mainboard

Connection board:

- unknown AIF
- AIF hybrid
- AIF indoor, variant 1
- AIF indoor, variant 2
- AIF IP, variant A
- AIF IP, variant B
- AIF IP, variant C
- AIF IP, variant D

display of the used connection board

System: display of the used operating system

SIP stack version: display of the version of the SIP stack

Serial number: display of the serial number of the device

Address MAC: display of the device's MAC address

The MAC address is required, for example, if a specific IP address is to be assigned to the device via DHCP or when the device is auto-provisioned.

IP address: display of the IP address of the device

In case of static address assignment, it is the configured IP address.

In case of dynamic address assignment, it is the IP address assigned by the DHCP server.

In case of link-local, the IP address assigned by the device to itself is shown, unless the device was assigned an IP address by a DHCP server. In this case, the IP address assigned by the DHCP server is shown. Then, the address assignment should then be changed to 'dynamic'.

IP address of the webcam: display of the IP address of the webcam if it uses a different IP address than the device

Power supply:

- PoE
- PoE+

The energy supply that is available to the device is displayed here.

If the device is not supplied via the network cable but via a 48V plug-in power supply unit, PoE+ is displayed as the power supply.

For devices with a hearing loop module, PoE + is absolutely necessary for the hearing loop module to work.

USB extension port:

- no
- yes

display if a USB extension port adapter is connected (if AIF IP)

Microphone: display of the current microphone state

If a functioning microphone is connected to the microphone connection, its signal is detected and displayed accordingly.

If no microphone is connected, no signal is normally detected.

If the loudspeaker is accidentally connected to the microphone connection instead of the microphone, it also supplies a signal and it is not possible to distinguish from the signal whether it is a loudspeaker or a microphone.

Current volume: display of the currently used volume

Camera:

- no camera detected
- Behnke USB (HD01)
- Behnke USB (HD04)
- AXIS® IP camera
- Behnke B-Smart (M1054)
- Behnke HD (M3005)
- Behnke HD (M3007)
- Behnke HD (M3045)
- Behnke HD (M3065)
- Behnke HD (M3066)
- Behnke HD (M3067)
- Behnke HD (M3086)
- Behnke HD (M4327)
- Behnke IP camera
- Behnke IP
- Behnke Smart
- IP camera

display of the detected USB or IP camera

Display:

- no display detected
- small display
- medium display

display of the detected display

Card reader:

- no card reader detected
- Behnke USB (T4BO)

	display of the detected card reader
SIP account 1:	display of the current registration state if the SIP account 1 is to be registered
SIP account 2:	display of the current registration state if the SIP account 2 is to be registered
Behnke cloud:	display of the current registration state if the device is to be registered with the Behnke cloud server
Phone book:	display of the state of the phone book synchronisation
Relay 1:	display of the current state of the first switching contact or the state of the access if the relay is used as a door opener relay
Relay 2:	display of the current state of the second switching contact or the state of the access if the relay is used as a door opener relay
Alarm input:	display of the current state of the alarm input
Safety shutdown:	display of the current state of the safety shutdown
Extension module 1 - 10:	• unknown • buttons • LEDs • LEDs S10 • radar sensor • delocalised electronic • door module • fan module • I/O module • handset
Current time:	display of the current time of the device In order that the device has a valid time, a time-server must be configured to request the valid time and to synchronize with it. The device regularly synchronizes its time with the

time-server. If the time is synchronized, it is displayed in grey.

If it is not possible to retrieve the valid time from the time-server, the time is displayed in red with the message 'not synchronized, invalid'. If the time is invalid, all schedules are evaluated as invalid.

If the time could already be retrieved from the time-server, but the server is no longer reachable, then the time is displayed in yellow with the message 'not synchronized but valid'. The device has a valid time, but of course inaccuracies can occur because the time is no longer synchronized. In this case, schedules are further evaluated.

When the device restarts, it may take a moment before the first synchronization with the time-server takes place.

Slot:

- unknown
- slot A
- slot B

The device has 2 slots for installing the firmware, a slot A and a slot B. One slot is active, the other inactive.
The system is always started from the active slot. When the firmware is updated, the new firmware is first installed on the inactive slot. If the update has been carried out successfully, the slots are swapped. The inactive slot is activated and the active one deactivated. Then the device restarts with the new firmware from the formerly inactive, now active slot.

State:

- out of service
- device not reachable
- partially ready
- ready
- call
- firmware update
- sabotage detected / safety shutdown
- update of extension module

out of service
The device is not ready for operation. The device is typically in this state when settings have been changed and saved. Parts of the software are then

restarted in order to apply the changes. After a brief moment, the device should return to the state 'ready' or 'partially ready'.

device not reachable
This status is displayed in the web interface when the browser can no longer reach the device. In this case, the device may no longer be in operation, for example because it has been disconnected from the network or the power supply. However, it can it could also be that the network connection to the device is not working because the device is just restarting or perhaps has received a different IP address or there is a network problem.

partially ready
In this state, some functions can be used without any problems, but there are also functions that are configured but not available. Typically, the device is in this state if not all configured SIP accounts could be successfully registered. In this case, calls over the corresponding SIP account can not be made, but other functions such as code lock or card reader can be used if available.

ready
The device is ready for operation.

call
The device is currently in communication. If settings are changed in the web interface in this state and then saved, the call may be ended.

firmware update
A firmware update is currently being carried out. If this is successfully completed, the device will restart.

update of extension module
The firmware of an extension module is currently being updated. The device can continue to be used during the update, but the extension modules are not available.

Important information about the system

System: restart / activate slot A/B

restart
The device will restart.

activate slot A/B
The device has 2 slots for installing the firmware, a slot A and a slot B. One slot is active, the other inactive.
The system is always started from the active slot. During a firmware update, the new firmware is first installed on the inactive slot. If the update has been carried out successfully, the slots are swapped. The inactive slot is activated and the active one deactivated the device restarts with the new firmware from the formerly inactive, now active slot.
The firmware on the old slot is retained. You can switch back to the old, i.e. inactive slot in order to work with the previous firmware again.
Please note that the system on the inactive slot may be damaged, for example because a firmware update was interrupted. If switching to the inactive slot fails because the system is damaged, the device usually restarts and uses the slot with the functional firmware again.

Configuration: save / restore / reset

save
The configuration of the device is saved in a text file called behnke-station.ini. In addition to the settings, the file may also contain data such as certificates, logos or individual voice announcements.
To protect sensitive information, the configuration file behnke-station.ini is stored in a ZIP file named behnke-station.zip and encrypted with the administrator password.

restore
A configuration file (behnke-station.ini or behnke-station.zip) that was previously saved can be reloaded here.
In the case of a ZIP file, the administrator password must first be set to the password used to encrypt the ZIP file.
When restoring the current configuration is lost and is replaced by the configuration in the configuration file. The device is restarted for this.

reset
The configuration of the device is reset to the factory settings. The current configuration is lost. After the

reset, the device is restarted.

Firmware: update / check for update

update
A new firmware can be uploaded here in order to install it on the system.
A firmware is required that is suitable for the platform (P1, P2 and so on) of the system.
The device has 2 slots for installing the firmware, a slot A and a slot B. One slot is active, the other inactive.
The system is always started from the active slot. During a firmware update, the new firmware is first installed on the inactive slot. If the update has been carried out successfully, the slots are swapped. The inactive slot is activated and the active one deactivated the device restarts with the new firmware from the formerly inactive, now active slot.

check for update
A connection to the support server will be established to check whether there is new firmware for this device.
If so, the new firmware can be downloaded from the link provided. When the firmware file has been downloaded completely, it can then be installed using 'update'.
If the computer cannot or is not allowed to establish an Internet connection, then it is not possible to contact the support server and thus check the firmware version.

Firmware update:

- preparation
- downloading
- verification
- copying
- decryption
- decompression
- firmware too old
- preparations
- reboot required
- installation
- terminated
- failed

If a firmware update is carried out, the partial step carried out or the progress of the installation are

displayed here.

If a firmware update could not be completed successfully, 'failed' is displayed here for a short time. In this case, the firmware update must be restarted.

License information: download

The firmware of the device contains components that are under different licenses. The ZIP file, which you can download here, contains a complete overview of all components and their licenses.

Auto provisioning

Provisioning:

- disabled
- at starting
- every 5 minutes
- every 30 minutes
- every 60 minutes
- during the night

Default: disabled

As an alternative to the option of specifying the device's configuration via the web interface, the device can also receive its configuration via the network. This is called auto-provisioning.

For auto-provisioning, the device contacts a server (auto-provisioning server) in the defined auto-provisioning rhythm to receive the configuration.

This setting allows auto-provisioning to be activated. It applies when the device is no longer in the delivery state. In the delivery state, auto-provisioning is activated with a rhythm of 5 minutes, even if this setting is configured to 'disabled'.

URL of the auto-provisioning server
In order for the device to be able to contact the auto-provisioning server, it needs its URL. This URL can be configured using the 'URL' setting or, for devices with a dynamic IP address (DHCP), can be transmitted by the DHCP server, if this is configured in the right way in the DHCP server.
To do this, the DHCP server needs the MAC address of

this device so that it then transmits the auto-provisioning URL in DHCP option 66 or in DHCP option 43 when assigning the IP address.
The help for the 'URL' setting explains how the URL must be structured.

configuration file
To get a configuration file for a device that can be saved on the auto-provisioning server, you can, for example, save the configuration of a device in the section 'System'. Then you get a file behnke-station.ini
The configuration file is a text file that can be adapted if necessary.
The configuration file must be saved under a specific name on the auto-provisioning server. This name consists of the MAC address of the device (12 digits, without colons) and the extension .ini
If a device finds a new or changed configuration file during the auto-provisioning process, it is loaded and activated. The old configuration is replaced by the new one.

additional configuration
Normally, a configuration obtained via auto-provisioning completely replaces the old configuration. However, it is also possible to mix the configurations.
First the local configuration is loaded and then the settings of the auto-provisioning configuration are also adopted. Settings that do not yet exist are created and settings that already exist are replaced. Phone book entries are an exception here. If phone book entries are found in the auto-provisioning file, only these are accepted. Any existing phone book entries are discarded.
To adopt a configuration as an additional configuration, the first line of the file must be adapted so that it reads:
BEHNKE STATION INCLUDE CONFIGURATION FILE

phone book
The phone book can either be transmitted in a configuration file or in a separate phone book file.
To get a phone book file, you can, for example, export the phone book of a device in the section 'Phone book'. Then you get a file phonebook.txt
The phone book file is a text file that can be adapted if necessary.

The phone book file with the name phonebook.txt is saved on the auto-provisioning server and is then available for all devices.
If a device finds a new or changed phone book file during the auto-provisioning process, it is imported. The old phone book is replaced by the new one.

phone book synchronisation with an LDAP server
If the phone book is synchronised with an LDAP server and a configuration file is to be transferred via auto-provisioning, then the configuration file should be transferred as an additional configuration without phone book entries.
In addition, when the telephone book is synchronised via LDAP, it is not possible to transfer a telephone book file via auto-provisioning.

firmware
New firmware for the device can also be sent via auto-provisioning.
For this purpose, the firmware file is saved on the auto-provisioning server. In addition, the version that is to be installed by the devices is specified in a firmware version file with the name firmware.txt.
To install the firmware firmware-1.23, you enter 1.23 in the firmware version file.
If a device detects during the auto-provisioning process that the firmware version file indicates a different version than the one installed, the corresponding firmware is downloaded and installed.

URL: The configuration file can be requested from the auto-provisioning server using different protocols (TFTP, FTP, HTTP, HTTPS) depending on the type of server. The protocol used by the server must be specified in the URL.

It may also be necessary to specify an authentication (user name or user name and password) in the URL, if the server requires one.

If the configuration file is in a subdirectory of the server, the corresponding path must of course also be specified.

If, for example, the configuration file in the subdirectory /path/to/files is to be requested from the TFTP server with the address 192.168.1.1 as the

	user 'user' with the password 'password', the following URL results: tftp://user:password@192.168.1.1/path/to/files If the server does not require a password, then it is sufficient: tftp://user@192.168.1.1/path/to/files If it does not require any authentication at all, then it is sufficient: tftp://192.168.1.1/path/to/files And if the data is in the main directory, then the URL is: tftp://192.168.1.1 With a different server type, instead of tftp:// use ftp:// http:// or https://
Provisioning of:	• configuration • firmware • phone book • configuration & firmware • configuration & phone book • firmware & phone book • configuration & firmware & phone book Default: configuration & firmware & phone book This setting determines which elements are to be retrieved during auto-provisioning.

Provision of the configuration via network

API	Access to HTML API:	• refuse • allow Default: refuse The HTML API allows the configuration of the device to be queried or changed via HTML requests, for example with a web browser. Events can also be triggered. This setting determines whether such HTML requests should be allowed or not.

Access to the HTML API requires the entry of the administrator password, an API command and possibly other parameters. The general scheme is:

https://[IP address]/?key=[administrator password]&api=[command]

If the administrator password contains special characters, these must be URL-encoded.

It is recommended to always use HTTPS so that the information is transmitted in encrypted form. HTTP requests are also possible, provided this is allowed by the 'Web connections' setting in the section 'General'.

More information on using the HTML API can be found using the help command.

https://[IP address]/?key=[administrator password]&api=help

See manual under HTML API.

Access to SSE:

- refuse
- allow

Default: refuse

With Server-Sent Events (SSE), a client, such as a web browser, sends an HTTP request to the Behnke station (=server). The connection established in this process remains open and the Behnke station repeatedly sends new events, such as recognised keystrokes, to the client.

This setting determines whether such SSE requests should be allowed or not.

Access to SSE requires the administrator password and possibly other parameters. The general scheme is:

http://[IP address]:8080/?key=[administrator password]&sse
https://[IP address]:8443/?key=[administrator password]&sse

If the administrator password contains special characters, these must be URL-encoded.

It is recommended to always use HTTPS so that the information is transmitted in encrypted form. However, HTTP requests are also possible if this has been enabled in the 'Web connections' setting in the 'General' section.

Further information on using SSE can be obtained using the help command.

https://[IP address]:8443/?key=[administrator password]&sse

The [IP address] is usually the IP address of the Behnke station, unless a VLAN has been configured for the webcam in the 'Network' section. In this case, it is the IP address of the webcam.

See manual under SSE.

URL for: API help / SSE help

API help
display the appropriate URL to request the API help

SSE help
display the appropriate URL to request the SSE help

Interface for configuration and control of the device

ControlCenter

Connect to a ControlCenter:

- no
- yes

Default: no

A Behnke ControlCenter is a remote management system for the central configuration of Behnke stations.

This setting determines whether this device should be connected to a ControlCenter.

Status: OFFLINE
There is currently no connection to the ControlCenter.

ONLINE
The device is currently connected to the ControlCenter.

ControlCenter: host name or IP address of the ControlCenter

Password: password for logging into the ControlCenter

Verify identity:

- no
- certificate
- certificate & hostname

Default: certificate

This setting determines whether the identity of the ControlCentre should be verified when communicating with it.

To ensure secure communication, the certificate and host name should be verified.

The certificate can only be verified if the device has a valid time.

Local configuration:

- refuse
- allow

Default: allow

When connected to a ControlCenter, this setting determines whether or not local configuration of the device via the web interface is permitted when logging in with the administrator password.

If local configuration is not permitted, the device can only be configured via the ControlCenter.

Important note
Configuration via the web interface when logging in with the user password, via configuration mode, via the HTML API, via LDAP or via auto-provisioning are not affected by this setting, as the permission to configure them can be controlled via the corresponding settings.

Special function

Secure system:

- no
- yes

Default: yes

It is strongly recommended to secure the system. It should only be switched off in exceptional cases, for example for diagnostic purposes.

With a secured system, you can only log in via the web interface.

Supervise system:

- no
- yes

Default: yes

When the system is monitored, the functionality of important components, such as the web server, is checked at regular intervals. In the event of a malfunction, suitable measures are taken to remedy the malfunction.

Reset via configuration button:

- refuse
- allow

Default: allow

This setting determines whether the configuration of the device can be reset to the factory settings using the configuration button.

A reset via the web interface after logging in with the administrator password is always possible.

Automatic restart:

- no
- every day
- every week
- every 2 weeks
- every 4 weeks

Default: every 4 weeks

To increase stability, we recommend restarting the system at regular intervals, for example every 4 weeks.

This setting can be used to define such automatic

restarts.

If the device has a correct time (see NTP in the section 'Network'), the restart will be carried out on the specified day at the specified time in the specified restart rhythm.

If the time is not correct, the automatic restart is carried out when the operating time of the device reaches the set restart rhythm.

If the device is in use at the time of restart, it will wait until the device is idle again.

At: 0 - 23 h

Default: 1 h

time at which the automatic restart should be carried out

On:
- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Default: Monday

day of the week on which the automatic restart should be carried out

Limit maximum frequency:
- no
- yes

Default: no

Expert settings:
- use default settings
- set individually

Default: use default settings

Change expert settings only after consulting the hotline!

Shutdown temperature threshold:

- extremely high
- very high
- high
- standard
- low
- very low

Default: standard

Prolonged direct exposure to sunlight may cause the device to heat up considerably, especially on devices with a dark front panel or when the device is installed in an insulated wall.

When the temperature threshold set here is reached, the device is shut down for the time specified in the 'shutdown duration' setting.

During the shutdown, the device cannot be used. However, certain events terminate a shutdown prematurely to restore the device's operational readiness.

The following events terminate a shutdown:
- pressing the configuration button
- pressing a direct call button
- pressing a key on the keypad
- touching the display

Events from direct call buttons or a key of the keypad can only be detected if they are connected directly, i.e. not via an extension module.

Shutdown duration:

15 - 90 min

Default: 60 min

When the shutdown temperature threshold is reached, the device is shut down for the time set here.

Switch off PoE of the extension port:

- no
- yes

Default: yes

This setting determines whether the PoE supply of the extension port should be switched off during a shutdown.

Reboot after shutdown phase:

- no
- yes

Default: no

This setting determines whether the device should be rebooted after a shutdown phase.

Increase the system security and stability

ControlCenter

Status:	OFFLINE There is currently no connection to the ControlCenter. ONLINE The device is currently connected to the ControlCenter.
System:	**restart / reset** restart The device will restart. reset The configuration of the device is reset to the factory settings. The current configuration is lost. After the reset, the device is restarted.

Help

Important
First read the technical manual or, as explained below, the help for the corresponding settings! If you still cannot solve the problem with these explanations, contact the hotline.

Hotline: +49 (0) 6841 8177-777

Technical Manual
- click on Technical Manual=› the manual is opened

Help for a section
If you move the mouse over one of the sections shown on the left, a question mark appears behind it.
- Click on the question mark =› the technical manual with information for this section is opened

Help for a setting
If you move the mouse over a setting, a question mark appears behind it.
- mouse over the question mark =› the help text is displayed
- click on the question mark =› the help text is displayed permanently
- click again on the question mark =› the help text is hidden again
- double click on the question mark =› the setting is reset to the default value
- for password fields: mouse over the question mark =› the password is displayed in plain text

The following settings allow you to test the help.

Example	Example:	• move the mouse over this field • this is not the default value Default: move the mouse over this field This is the help text for this example. It is displayed as long as the mouse is over the question mark. You can also show it permanently by clicking on the question mark. Clicking the question mark again hides it again. Also test resetting to the default value: change the field and then double-click on the question mark to reset the field to the default value.

Password:	Default: admin The password is displayed in plain text as long as the mouse is over the question mark.

Configuration by phone or display

Configuration mode

The device can be configured remotely using a telephone that can send DTMF tones or directly on the device with the virtual keypad.

If desired, the configuration option on the device can be deactivated so that configuration is only possible remotely. The configuration via the configuration mode can also be completely forbidden, so that the device can then only be configured via the web interface.

To get into the configuration mode, a 4-digit security code must be entered. The configuration itself is done by entering so-called configuration steps, each of which sets a specific function.

Step 1: activate configuration mode

REMOTELY WITH A TELEPHONE

- call Behnke station and wait until it picks up and emits a beep
  [beep]
- press key * briefly within 2 seconds after the beep
  [beep]
- enter the security code (default: 0000)
  [beep] [beep]

If the entered security code is wrong, the connection will be terminated.
If more than 2 seconds have passed since the beep after picking up the phone, the configuration mode can be activated by pressing the * key twice.

ON THE DEVICE VIA THE DISPLAY

- press the display button with the key to display the virtual keypad
- briefly press the button *
  [beep]The virtual keypad is displayed in blue.
- enter the security code (default: 0000)
  [beep] [beep]

If the entered security code is wrong, the device emits a deep, somewhat longer error tone.
If no key button is available on the display, the virtual keypad can also be displayed as follows: you swipe with one finger quickly and horizontally across the display from left to right.

Step 2: enter configuration steps

- enter a configuration step (see section Configuration steps)
  [beep] [beep]
- enter parameter and complete with # key
  [beep] [beep] [beep]

If, for example, the number 123 is to be configured for button 1 (configuration step 21), you enter:

21 [beep] [beep] 123 #[beep] [beep] [beep]

Several configuration steps can be entered one after the other. The order of the configuration steps is arbitrary. If an incorrect entry is made in the configuration mode, a dark, somewhat longer error tone is emitted. After the error tone has sounded, the entry can be continued with the next configuration step. The configuration mode ends automatically if no entry is made for 30 seconds.

Step 3: terminate configuration mode

- press the button * briefly or no entry for 30 seconds

Configuration steps

Reset the device and restore delivery status

00 * * * * #

With a reset, the complete configuration is deleted and all parameters are set to the defaults in the delivery state. A reset takes a few seconds. During this time, a high-pitched beep can be heard.

Change security code — default: oooo

01 new code [beep] new code #

The security code has four digits and only consists of digits. Enter the new code twice in a row. In order to prevent unauthorized configuration, it is essential to change the specified security code.

Allow configuration — default: o

02
- 0 # yes, by phone, keypad or display
- 1 # only by phone
- 2 # no

The configuration mode allows the device to be configured either remotely using a telephone with tone dialing or locally on the device using an existing keypad or display.
It is possible to switch off the configuration on the device, i.e. using the keypad or display, and only allow remote configuration, i.e. via telephone. Alternatively, the configuration via the configuration mode can be switched off completely.

Call acceptance — default: o

03
- 0 # accept manually
- 1 # accept automatically
- 2 # decline
- 3 # accept automatically & mute

An incoming call can be accepted automatically as soon as it is signalled or manually by the press of a button.
With manual call acceptance, a person in front of the device can accept the call as long as the call is pending by pressing a call button or a key on the keypad.
If it is set that incoming calls are to be rejected, incoming calls are ended immediately when they are signalled, without an acoustic signal being given on the device.

Duration of actuation of call buttons default: 0

04

0 #	minimal
1 #	1 second
:	:
5 #	5 seconds

Here you can set how long a real, physical direct call button must be pressed before the button press is recognized as valid and the call number configured for the button is called.
By increasing the duration of actuation, false tripping can be reduced. For the vast majority of applications, however, a minimum actuation duration is the correct setting.
This setting does not apply to direct call buttons that are connected via an extension module. Their actuation time is fixed and cannot be changed.

Maximum connection duration default: 9

05

0 #	unlimited
1 #	1 minute
:	:
9 #	9 minutes

The maximum duration for a connection is set here. The connection duration begins for an outgoing call after the remote station has picked up and for an incoming call after the call has been accepted.
After the maximum connection time has expired, the connection is automatically terminated.

Volume default: *80

06

0 #	level 0 (0 %)
1 #	level 1 (11 %)
2 #	level 2 (22 %)
:	:
9 #	level 9 (99 %)
*0 #	0 %
:	:
*100 #	100 %

The volume of the loudspeaker output can be set in steps from 0 (=quiet) to 9 (=loud).
Alternatively, it is possible to specify the desired volume in percent (*0 to *100).

Microphone sensitivity default: *60

07

0 #	level 0 (0 %)

1 #	level 1 (11 %)
2 #	level 2 (22 %)
:	:
9 #	level 9 (99 %)
*0 #	0 %
:	:
*100 #	100 %

The sensitivity of the microphone can be set in steps from 0 (=insensitive) to 9 (=sensitive). Alternatively, it is possible to specify the desired microphone sensitivity in percent (*0 to *100).

Operation mode of relay 1 **default: 6**

08	0 #	disabled
	1 #	door opener relay with break contact, 2 codes for indoor station
	2 #	door opener relay with break contact, 2 codes for code lock
	3 #	door opener relay with break contact, 1 code for indoor station, 1 code for code lock
	4 #	door opener relay with break contact, 2 codes for indoor station
	5 #	door opener relay with break contact, 2 codes for code lock
	6 #	door opener relay with break contact, 1 code for indoor station, 1 code for code lock
	7 #	connection indication with make contact for outgoing connections
	8 #	connection indication with make contact for incoming connections
	9 #	connection indication with make contact for outgoing and incoming connections
	10 #	additional bell with make contact at the beginning of a direct call
	11 #	additional bell with make contact during the establishment of a direct call
	12 #	additional bell with make contact while ringing
	13 #	fault indication with make contact
	14 #	connection indication with break contact for outgoing connections
	15 #	connection indication with break contact for incoming connections
	16 #	connection indication with break contact for outgoing and incoming connections
	17 #	additional bell with break contact at the beginning of a direct call
	18 #	additional bell with break contact during the establishment of a direct call
	19 #	additional bell with break contact while ringing
	20 #	fault indication with break contact

With operation modes 1 to 6, the relay is operated as a door opener relay. You can choose between normally open and normally closed contact. With the normally open contact, the switching contact is normally open and is only closed when the door is to be opened it. In case of a normally closed contact is exactly the other way round: the switching contact is normally closed and is only opened when the door is to be opened. How long the switching contact is switched can be set in configuration step 09. Using configuration steps 10 and 11, two codes can be set, which, depending on the selected operation mode, apply to the indoor station (telephone that receives the call) or the code lock (available via keypad or display).
For operation modes 10 an 17, configuration step 09 can be used to define how long the

additional bell is activated at the beginning of the direct call.
In the 'fault indication' operation mode, a fault occurs when the device no longer has a valid network connection or when registration with the SIP server has failed.

Attention: Other operation modes can be set via the web interface, for example with more than 2 activation codes or with activation codes that are only valid according to a schedule.

If the operation mode is set via this configuration step and additional activation codes have been enabled via configuration step 818, these will be automatically disabled.

Activation time of relay 1 default: 5

09

1 #	1 second
:	:
90 #	90 seconds

This configuration step defines the activation time when operating as a door opener relay (operation modes 1 to 6) or the activation time for an additional bell at the beginning of a direct call (operation mode 10).

Activation codes of relay 1

10 1st activation code # default: 0

11 2nd activation code # default: 2580

The activation codes only consist of digits and have a maximum of eight digits.
In the delivery state, the second activation code applies to the code lock function, which is available on devices with a keypad or display. For security reasons, the specified code should therefore be changed.

When entering the activation code, the following special symbols are permitted at the beginning:
*1 = activation code applies to indoor station
*2 = activation code applies to code lock
If no special symbol is entered, the activation code applies to the last setting made.

Attention: The operation mode set via configuration step 08 determines the validity (for indoor station or for code lock) of the activation codes. Using *1 or *2 can lead to a change in the operation mode previously set via configuration step 08. Likewise, setting the operation mode again via configuration step 08 will overwrite any validity previously set via *1 or *2.

Operation mode of relay 2 default: 12

12

0 #	disabled
1 #	door opener relay with break contact, 2 codes for indoor station

2 # door opener relay with break contact, 2 codes for code lock
3 # door opener relay with break contact, 1 code for indoor station, 1 code for code lock
4 # door opener relay with break contact, 2 codes for indoor station
5 # door opener relay with break contact, 2 codes for code lock
6 # door opener relay with break contact, 1 code for indoor station, 1 code for code lock
7 # connection indication with make contact for outgoing connections
8 # connection indication with make contact for incoming connections
9 # connection indication with make contact for outgoing and incoming connections
10 # additional bell with make contact at the beginning of a direct call
11 # additional bell with make contact during the establishment of a direct call
12 # additional bell with make contact while ringing
13 # fault indication with make contact
14 # connection indication with break contact for outgoing connections
15 # connection indication with break contact for incoming connections
16 # connection indication with break contact for outgoing and incoming connections
17 # additional bell with break contact at the beginning of a direct call
18 # additional bell with break contact during the establishment of a direct call
19 # additional bell with break contact while ringing
20 # fault indication with break contact

With operation modes 1 to 6, the relay is operated as a door opener relay. You can choose between normally open and normally closed contact. With the normally open contact, the switching contact is normally open and is only closed when the door is to be opened it. In case of a normally closed contact is exactly the other way round: the switching contact is normally closed and is only opened when the door is to be opened. How long the switching contact is switched can be set in configuration step 09. Using configuration steps 10 and 11, two codes can be set, which, depending on the selected operation mode, apply to the indoor station (telephone that receives the call) or the code lock (available via keypad or display).
For operation modes 10 and 17, configuration step 13 can be used to define how long the additional bell is activated at the beginning of the direct call.
In the 'fault indication' operation mode, a fault occurs when the device no longer has a valid network connection or when registration with the SIP server has failed.

Attention: Other operation modes can be set via the web interface, for example with more than 2 activation codes or with activation codes that are only valid according to a schedule.

If the operation mode is set via this configuration step and additional activation codes have been enabled via configuration step 826, these will be automatically disabled.

Activation time of relay 2 default: 5

13 1 # 1 second
: :
90 # 90 seconds

This configuration step defines the activation time when operating as a door opener relay (operation modes 1 to 6) or the activation time for an additional bell at the beginning of a direct

call (operation mode 10).

Activation codes of relay 2

14 1st activation code #
15 2nd activation code #

The activation codes only consist of digits and have a maximum of eight digits.
In the delivery state, no activation codes are specified for relay 2.

When entering the activation code, the following special symbols are permitted at the beginning:
*1 = activation code applies to indoor station
*2 = activation code applies to code lock
If no special symbol is entered, the activation code applies to the last setting made.

Attention: The operation mode set via configuration step 12 determines the validity (for indoor station or for code lock) of the activation codes. Using *1 or *2 can lead to a change in the operation mode previously set via configuration step 12. Likewise, setting the operation mode again via configuration step 12 will overwrite any validity previously set via *1 or *2.

Operation mode alarm input default: 1

17 0 # disabled
1 # alarm on rising edge & treat like a button
2 # alarm on rising edge & treat like a message
3 # alarm on rising edge & treat like a sabotage
4 # alarm on falling edge & treat like a button
5 # alarm on falling edge & treat like a message
6 # alarm on falling edge & treat like a sabotage
7 # alarm on rising or falling edge & treat like a button
8 # alarm on rising or falling edge & treat like a message
9 # alarm on rising or falling edge & treat like a sabotage

The alarm input allows information to be transmitted to the device using a voltage and then an alarm to be triggered. You can set whether an alarm is triggered on a rising edge (change from 'no voltage at the alarm input' to 'voltage at the alarm input') or a falling edge (change from 'voltage at alarm input' to 'no voltage at alarm input') or should be triggered in both cases.
A recognized alarm is like a direct call button (alarm button) that has been pressed, and a call number can be specified via configuration step 18 that is called when the alarm key is pressed, i.e. when an alarm is recognized this setting determines how exactly it is treated, like a button or like a message.

<u>treat like a button</u>
If the device is idle and an alarm is detected, the set action is triggered. If, on the other hand, the device is in a connection and an alarm is detected, then this is treated like a button press.

If the disconnection is permitted the connection is terminated and the action set for the alarm input is triggered. If the connection is not allowed to be cancelled or the triggering another function (button) is not allowed, the function defined for the alarm input is not executed, so the alarm is lost.

treat like a message
If the device is idle and an alarm is detected, the set action is triggered. If, on the other hand, the device is connected and an alarm is detected, it is stored and the set action is triggered as soon as the connection is finished and the device is idle again.

Call number for the alarm input

18 call number #

The phone number that is called when an alarm is detected can be specified here.

Call number for direct call button

20	call number #	button i of the keypad
21	call number #	button 1
22	call number #	button 2
23	call number #	button 3
24	call number #	button 4
25	call number #	button 5
26	call number #	button 6
27	call number #	button 7
28	call number #	button 8
29	call number #	button 9
2*10	call number #	button 10
2*11	call number #	button 11
:		
2*50	call number #	button 50

The phone numbers only consist of digits and have a maximum of 50 digits.

When entering the phone numbers, the following special symbols are permitted:
*0 = dial *
*1 = dial #
*2 = P = 2 seconds pause
*3 = p = 1 second pause
*4 = R = flash function
*5 = ; = call chain
*6 = , = group call
*8 = sip: = SIP call
*90 = com: = intercom call
*951 = cmd:play1

:
*959 = cmd:play9
*971 = cmd:free1
*972 = cmd:free2
*973 = cmd:free1&2
*974 = cmd:close1
*975 = cmd:open1
*976 = cmd:close2
*977 = cmd:open2
** = .
*# = @

Reset voice announcements

50 * * * * #

A reset deletes all individual voice announcements and resets configuration steps 53 to 59 to the default settings.

Record individual voice announcement

51 1 # record announcement #1
: :
9 # record announcement #1

After entering configuration step 51 and the number of the announcement to be recorded, a beep sounds and recording begins. The recording will end automatically after the maximum recording time has elapsed. It can also be ended manually by pressing #.

Please note: Recording voice announcements when configuring remotely with a telephone is currently only possible in 'analogue telephone' mode.

Play individual voice announcement

52 1 # play announcement #1
: :
9 # play announcement #1

After entering configuration step 52 and the number of the announcement to be played, the announcement is played. Playback ends automatically after the voice announcement has been finished. It can also be ended manually by pressing #.

Voice announcement for door opener relay 1 default: 10

53

1 # play announcement #1
:
9 # play announcement #1

10 # play standard announcement

This configuration step allows you to specify the voice message that will be played when relay 1 is activated.

The input can only be made or only has an effect if both relays are used in 'door opener relay' mode and configuration step 59 has been configure to 10, that a voice announcement should generally be played when the access is opened.

Voice announcement for door opener relay 2 default: 10

54

1 # play announcement #1
:
9 # play announcement #1
10 # play standard announcement

This configuration step allows you to specify the voice message that will be played when relay 2 is activated.

The input can only be made or only has an effect if both relays are used in 'door opener relay' mode and configuration step 59 has been configure to 10, that a voice announcement should generally be played when the access is opened.

Voice announcement for telephone function default: 10

55

0 # do not play announcement
1 # play announcement #1
:
9 # play announcement #1
10 # play standard announcement

This configuration step allows you to set a voice announcement that will be played when using the telephone function until you start dialling the number.

Voice announcement for code lock function default: 10

56

0 # do not play announcement
1 # play announcement #1
:
9 # play announcement #1
10 # play standard announcement

This configuration step allows you to set a voice message that is played when the code lock

function is used until the code is entered.

Voice announcement for quick dialling function default: 10

57

0 #	do not play announcement
1 #	play announcement #1
:	:
9 #	play announcement #1
10 #	play standard announcement

This configuration step allows you to set a voice announcement that is played when using the quick dialling function until you start entering the two-digit quick dialling code.

Voice announcements for direct calls default: * * *

58 x [beep] y [beep] z [beep] #

x = voice announcement before dialling the number
y = voice announcement while waiting for the call to be answered
z = voice announcement after the call is answered for the called person

where the following input values are permitted for x, y and z:

0 = do not play voice announcement
1 = play voice announcement #1
:
9 = play voice announcement #9
* = play standard voice announcement

This configuration step allows you to set up three voice announcements that will be played during direct calls (dialing a stored phone number). The configuration step requires you to enter three digits between 0 and 9 or an * to specify the desired voice announcement.

The first digit specifies the voice announcement that is played before dialling the number, e.g. a message such as 'Key press detected'. The second digit specifies the voice announcement that is played cyclically while waiting for the call to be answered, e.g. a message such as 'Please wait. Connection is being established'. The third digit specifies the voice announcement that is played as soon as it is detected that the called party has answered the call, whereby this message is only audible to the called party, e.g. a message such as 'Call from door phone' or a location specification when used as an emergency telephone.

This configuration step applies to all direct calls, including quick dialling function, and to all calls initiated via the phone book.

Example:
Let's assume that the following voice announcements were recorded with configuration step 51:

1st voice announcement (51-1): 'Key press detected.'
5th voice announcement (51-5): 'Please wait. Connection is being established.'
6th voice announcement (51-6): 'Call from door phone.'

The voice announcements for direct calls are played by entering the following:

58 1 [beep] 5 [beep] 6 [beep] #

If you do not want the announcement 'Key press detected' to be played, you can achieve this by entering the following:

58 0 [beep] 5 [beep] 6 [beep] #

If you want to use the standard voice announcements, you can do so by entering the following:

58 * [beep] * [beep] * [beep] #

Output when opening access default: 10

59

0 #	play nothing
1 #	play announcement #1
:	:
9 #	play announcement #1
10 #	play standard announcement
11 #	play tone

This configuration step allows you to specify what is output when access is granted via a door opener relay.

If the configuration step is set to 10 and both relays are used as door opener relays, then configuration steps 53 (relay 1) and 54 (relay 2) can be used to set which voice announcement is to be played for each relay.

Network configuration mode default: 0

70

0 #	terminate
1 #	start

If the network configuration is incorrect, network access may no longer be possible. In this case, you can regain access to the device as follows. Start the network configuration mode by entering configuration step 70 1 #. The device then behaves with regard to the network configuration as in the delivery state. It either receives an IP address from the DHCP server or assigns one to itself.

While the network configuration mode is active, the configuration WLAN is also available in the immediate vicinity of the device (only for devices with WLAN antenna). The name and password of the WLAN are behnke-station. When you are connected to the WLAN, open your browser and

enter http://behnke-station or alternatively the IP address 10.10.10.10 in the address line.

The network configuration mode is automatically terminated after 10 minutes or after changing the network configuration.

Language default: 4

71
2 # German
3 # French
4 # English

The language that is used for voice announcements and display output can be set here.

Operation mode default: 1

1 # sip phone
2 # IP intercom

The device can be operated as a SIP telephone or as an IP intercom.

SIP phone
operation mode if the device is connected to a SIP server (IP telephone system) as a SIP subscriber or if the device is to communicate directly with other SIP telephones (direct SIP calls)

IP intercom
operation mode if the device is operated as an IP intercom in connection with other devices

Reset the administrator password for the web interface default: admin

73

If the administrator password for configuring the device via the web interface is no longer known, it can be reset to the default value using this configuration step.

You can then log in to the web interface with the specified administrator password.

Network connection default: 0

74
0 # wired Ethernet
1 # VLAN
2 # VLAN for Webcam only
3 # VLANs for device and Webcam
4 # WLAN

Here you can set how the device is connected to the IP network.

Normally, the device is connected to the Ethernet port of a PoE switch via a network cable. This supplies it with energy (Power over Ethernet) and connects it to the network. Optionally, the device can also be connected to a wireless network (WLAN).

wired Ethernet
connection to a LAN or an untagged VLAN

VLAN
connection with a tagged VLAN
The VLAN tag can be set with configuration step 79.

VLAN for webcam only
untagged connection for the device and provision of a second network connection with a tagged VLAN only for access to the webcam
The network connection for the webcam can only be configured via the web interface.

VLANs for device and webcam
connection with a tagged VLAN and provision of a second network connection with a tagged VLAN only for access to the webcam
The VLAN tag for the VLAN of the device can be set with configuration step 79. The network connection for the webcam can only be configured via the web interface.

WLAN
connection to a wireless network
In this case, the power supply of the device must be ensured either by using a Behnke PoE injector or by additionally connecting it to a PoE port. In order to achieve a sufficient quality of the radio connection, an external antenna module is usually required.

Assignation of IP address **default: 1**

75
0 # static
1 # dynamic
2 # link-local

Here you can set how the device receives an IP address.

static = manual address assignment
The network administrator manages the IP addresses of the network. You have received an IP address from the network administrator that is entered with configuration step 76. In this case, you must also use configuration steps 77 and 78 to enter the associated net mask and the gateway.

dynamic = automatic address assignment
There is a DHCP server in the network that manages and distributes the IP addresses. The device automatically tries to obtain an IP address from this DHCP server.

link-local = self-assignment of an address
This address assignment is intended for networks without a DHCP server. The device assigns itself a free IP address in the 169.254.0.0/16 network. The assigned IP address can be queried by pressing the configuration button twice. This type of address assignment is used when several devices are operated as an IP intercom in an independent network.
If there is a DHCP server in the network that assigns an IP address, this will be used. In this case, the address assignment should be set to 'dynamic'!

Important
In networks with a DHCP server, 'dynamic' should be selected as the address assignment!

IP configuration in case of static address assignment — default: 192.168.100.100

76 IP address # — default: 192.168.100.100
77 net mask # — default: 255.255.255.0
78 gateway #

The IP configuration that the device uses when the IP address assignment is set to static can be set here.

When entering, points are entered using the * key.

VLAN tag — default: 1

79
1 # tag 1
: :
4094 # tag 4094

Here you can set the VLAN tag that is used for the VLAN of the device if 'VLAN' or 'VLANs for device and webcam' is set as the network connection.

Trigger an action — default: 0

97
0 # deactivate online-log and online-support
1 # activate online-log and allow online-support
2 # transmit diagnostic data to support
3 # transmit trace to support
4 # restart system
5 # activate inactive slot

Various actions can be triggered via this configuration step.

So that we can provide you with optimal support in the event of support, you can transfer diagnostic data and network traces directly to our support server. After consulting our support, you can also enable us to remotely access your device using configuration step 97 1 #.

Very important notice

Diagnostic data and network traces contain, among other things, data about the device, the configuration, the network, connections, audio, video and errors that have occurred. If you submit this data to us, you agree that we may use it for support purposes. If you allow us remote access, you also agree that we may change the configuration of the device for support purposes.

Announce an information

98 0 # device type
1 # firmware version
2 # system
3 # serial number
4 # MAC address
5 # IP address
6 # power supply
7 # detected hardware
8 # SIP registration
9 # relay 1
10 # relay 2
11 # alarm input
12 # current date
13 # current time

This configuration step allows various information about the device to be queried in the form of a voice output.

Announce configuration

99 configuration step #

This configuration step allows other configuration steps to be announced in order to query the current setting. For example, the call number set for button 1 can be queried via 99 21 #.

Additional configuration steps

The additional configuration steps allow a more refined configuration, which is only required in rare cases.

Handset operation mode default: 1

810 **0 #** disabled
1 # handset
2 # handset & direct call button
3 # handset & telephone function

When connecting a handset as an extension module, this setting can be used to specify how it should be operated.

disabled
The handset is disabled. It cannot be used for communication or to trigger a function.

handset
You can switch from handsfree mode to handset by picking up the handset.
Hanging up the handset switches back to handsfree mode.
In addition, an existing connection is cancelled when the handset is hung up if this is specified in the setting 'Cancel connection when hanging up the handset'.

handset & direct call button
The functionality is identical to the 'handset' operation mode.
In addition, the fork switch of the handset functions like a direct call button that is triggered when the handset is picked up.
This means that picking up the handset can trigger a call or an action.

handset & telephone function
This operation mode requires a device with keypad or display.
The functionality is identical to the 'handset' operation mode.
In addition, the telephone function is activated when the handset is picked up and a telephone number can be dialled via the keypad or the virtual keypad of the display.
When using this operation mode, it makes sense to allow the telephone function with configuration step 16 or, in the case of a display, to activate the telephone function as a display function.

Call number for handset direct call button

811 **call number #**

Here you can configure the call number that is dialled when the handset is picked up on a device with a handset in the 'handset & direct call button' operation mode.

Handset volume default: *80

812
0 #	level 0 (0 %)
1 #	level 1 (11 %)
2 #	level 2 (22 %)
:	:
9 #	level 9 (99 %)
*0 #	0 %
:	:
*100 #	100 %

The volume of the handset volume can be set in steps from 0 (=quiet) to 9 (=loud). Alternatively, it is possible to specify the desired volume in percent (*0 to *100).

Handset microphone sensitivity default: *60

813
0 #	level 0 (0 %)
1 #	level 1 (11 %)
2 #	level 2 (22 %)
:	:
9 #	level 9 (99 %)
*0 #	0 %
:	:
*100 #	100 %

The sensitivity of the handset microphone can be set in steps from 0 (=insensitive) to 9 (=sensitive). Alternatively, it is possible to specify the desired microphone sensitivity in percent (*0 to *100).

Cancel connection when hanging up the handset default: 1

814
0 #	no
1 #	yes

This setting determines whether an existing connection or function should be cancelled when the handset is hung up.

Activate Push-To-Talk default: 0

815
0 #	no
1 #	yes

During a call, a full-duplex voice connection is normally established in which both parties can speak and listen at the same time.

In rare cases, for example in extremely noisy environments or for hands-free to hands-free connections, the intelligibility of the full-duplex voice connection may not be sufficient.

If it is not possible to increase the volume or microphone sensitivity in such a case due to feedback, this setting can be used to activate Push-To-Talk.

With Push-To-Talk, a button is used as a Push-To-Talk button.

During a call, you can switch between talking (press and hold the Push-To-Talk button) and listening (release the Push-To-Talk button).

With Push-To-Talk, the volume and microphone sensitivity can be increased to the maximum without causing feedback.

Push-To-Talk button default: 1

816
1 # button 1
2 # button 2

This setting defines which physical button is to be used as the Push-To-Talk button.

Allow direct call via Push-To-Talk button default: 0

817
0 # no
1 # yes

During a call, the Push-To-Talk button is used to switch between talking and listening.

This setting can be used to specify whether or not the Push-To-Talk button can be used as a direct call button outside of a call.

Allow additional activation codes of relay 1 default: 0

818
0 # no
1 # yes

If relay 1 is operated as a door opener relay via configuration step 08, 2 activation codes are available, which are set via configuration steps 10 and 11.

If necessary, additional activation codes (activation codes 3 to 10) can be allowed via this configuration step.

Attention: During this process, all additional activation codes are reset and the validity of the individual codes is configured to code lock.

The additional activation codes can then be configured using configuration steps 819 to 826, whereby the explanation of configuration steps 10 and 11 applies.

The validity can then also be changed by using the special symbols *1 or *2. Without a special symbol, the validity last set for the corresponding code always applies.

Attention: If the operation mode of relay 1 is set via configuration step 08, the additional activation codes, if enabled, will be automatically disabled.

Additional activation codes of relay 1

819 activation code 3 #
:
826 activation code 10 #

Allow additional activation codes of relay 2 default: 0

827 0 # no
1 # yes

If relay 2 is operated as a door opener relay via configuration step 12, 2 activation codes are available, which are set via configuration steps 14 and 15.

If necessary, additional activation codes (activation codes 3 to 10) can be allowed via this configuration step.

Attention: During this process, all additional activation codes are reset and the validity of the individual codes is configured to code lock.

The additional activation codes can then be configured using configuration steps 828 to 835, whereby the explanation of configuration steps 14 and 15 applies.

The validity can then also be changed by using the special symbols *1 or *2. Without a special symbol, the validity last set for the corresponding code always applies.

Attention: If the operation mode of relay 2 is set via configuration step 12, the additional activation codes, if enabled, will be automatically disabled.

Additional activation codes of relay 2

828 activation code 3 #
:
835 activation code 10 #

HTML API

Access to the HTML API

In the 'System' section of the web interface, access to the HTML API can be allowed.

The HTML API allows the configuration of the device to be queried or changed via HTML requests, for example with a web browser. Events can also be triggered.

This setting determines whether such HTML requests should be allowed or not.

Access to the HTML API requires the entry of the administrator password, an API command and possibly other parameters. The general scheme is:

https://[IP address]/?key=[administrator password]&api=[command]

If the administrator password contains special characters, these must be URL-encoded.

It is recommended to always use HTTPS so that the information is transmitted in encrypted form. HTTP requests are also possible, provided this is allowed by the 'Web connections' setting in the section 'General'.

More information on using the HTML API can be found using the help command.

https://[IP address]/?key=[administrator password]&api=help

See manual under HTML API.

API help

[HELP]
general usage: https://[IP address]/?key=[administrator password]&api=[command]

If the administrator password contains special characters, these must be URL-encoded.

show this help: &api=help

get a list of all configuration sections: &api=get&sections
get a list of all configuration groups: &api=get&groups
get a list of all configuration groups of a section: &api=get&groups=[section]
get a list of all configuration groups of all sections: &api=get&groups=all
get a list of all events: &api=get&events

get values of all configuration options: &api=get&options
get values of all configuration options of a section: &api=get&[section]
get values of all configuration options of a group: &api=get&[group]
get values of all configuration options containing a search word: &api=get&[search word]
get value of a configuration option: &api=get&[option]
get values of 2 or more configuration options: &api=get&[option #1]&[option #2] (you can add further options)

default values of all configuration options: &api=default&options
default values of all configuration options of a section: &api=default&[section]
default values of all configuration options of a group: &api=default&[group]
default values of all configuration options containing a search word: &api=default&[search word]
default value of a configuration option: &api=default&[option]

type of all configuration options: &api=type&options
type of all configuration options of a section: &api=type&[section]
type of all configuration options of a group: &api=type&[group]
type of all configuration options containing a search word: &api=type&[search word]
type of a configuration option: &api=type&[option]

set a new value for a configuration option: &api=set&[option]=[new value]
set new values for 2 or more configuration options: &api=set&[option #1]=[new value]&[option #2]=[new value] (you can add further options)

trigger register of the SIP accounts: &api=trigger&register
trigger a certain call button: &api=trigger&button=[number of button]
trigger a certain door opener relay: &api=trigger&relay=[number of relay]
trigger a certain event: &api=trigger&event=[event]
trigger several events: &api=trigger&events=\"[events]\"
trigger a reboot of the system: &api=trigger&reboot
trigger a change of the system slot: &api=trigger&change_slot
trigger a reset of the system: &api=trigger&reset

The user password can also be used instead of the administrator password to trigger a door opener relay. If

the user password contains special characters, these must be URL-encoded.

A subadministrator can be granted access to the API. Access is then granted using the subadministrator password and is only possible for the sections and functions permitted to the subadministrator. Triggering functions also requires access authorisation for the corresponding function. The subadministrator cannot trigger events.

first line of returned information
OK: success
NOT AVAILABLE: the current configuration of the device does not allow the use of the API
NOT ALLOWED: the administrator password passed by &key= is wrong
LOCKED: the access to the device is currently locked
ERROR: one or more errors occured and are listed

If an error occured, the parameters that caused errors are listed and/or one or more of the following messages.
NO DATA: get without parameter which data to get, set without an option to be set or &trigger without an action to be triggered
IN USE: set could not be performed because another user is actually configurating the device
SAVE: set could not be performed because saving of the configuration failed

If the result has several lines, they are separated by LF (ASCII code 10).
If the lines are to be separated by CR (ASCII code 13) or CR LF instead of LF, this can be achieved by adding the parameter &cr or &crlf to the request.
If you use a web browser to regard the result, you can add the parameter &html to the request to make the result better readable.

examples (for IP address 192.168.16.200 and administrator password admin)
get the call number of button 1: https://192.168.16.200/?key=admin&api=get&buttons_number_1
set the call number of button 1 to 1234: https://192.168.16.200/?key=admin&api=set&buttons_number_1=1234
trigger the door opener relay 1: https://192.168.16.200/?key=admin&api=trigger&relay=1

SSE

Access to SSE

In the 'System' section of the web interface, access to SSE can be allowed.

With Server-Sent Events (SSE), a client, such as a web browser, sends an HTTP request to the Behnke station (=server). The connection established in this process remains open and the Behnke station repeatedly sends new events, such as recognised keystrokes, to the client.

This setting determines whether such SSE requests should be allowed or not.

Access to SSE requires the administrator password and possibly other parameters. The general scheme is:

http://[IP address]:8080/?key=[administrator password]&sse
https://[IP address]:8443/?key=[administrator password]&sse

If the administrator password contains special characters, these must be URL-encoded.

It is recommended to always use HTTPS so that the information is transmitted in encrypted form. However, HTTP requests are also possible if this has been enabled in the 'Web connections' setting in the 'General' section.

Further information on using SSE can be obtained using the help command.

https://[IP address]:8443/?key=[administrator password]&sse

The [IP address] is usually the IP address of the Behnke station, unless a VLAN has been configured for the webcam in the 'Network' section. In this case, it is the IP address of the webcam.

See manual under SSE.

SSE help

[HELP]
General use: https://[IP address]:8443/?key=[administrator password]&sse&[parameter/s]
or for http: http://[IP address]:8080/?key=[Aadministrator password]&sse&[parameter/s]

The [IP address] is usually the IP address of the Behnke station, unless a VLAN has been configured for the webcam in the 'Network' section. In this case, it is the IP address of the webcam.

If the administrator password contains special characters, these must be URL-encoded.

show this help: &sse=help

SSE first sends a welcome message (SSE_WELCOME) with the serial number of the device. Finally, events are sent, such as recognised keystrokes, or if there are no events, keep-alives (SSE_KEEP_ALIVE). If the connection is terminated by the device, a termination message (SSE_BYE) is sent beforehand.

If there are too many simultaneous SSE connections, the message SSE_TOO_MANY_CONNECTIONS is sent after SSE_WELCOME and the connection is terminated.

retrieve SSE: &sse
retrieve SSE in browser: &sse&html
SSE without keep-alive messages: &sse&no_keep_alive
SSE with access for all origins: &cors
SSE as eventsource: &eventsource

retrieve detected key presses: &sse&key
retrieve detected DTMF tones: &sse&dtmf
retrieve changed TEMP options: &sse&temp
retrieve application status changes: &sse&state
retrieve specific detected key press: &sse&[key]
retrieve specific detected DTMF tone: &sse&[DTMF tone]
retrieve specific changed TEMP variable: &sse&[TEMP option]
retrieve all events: &sse&all

The individual events/lines are separated by LF (ASCII code 10).
If the lines are to be separated by CR (ASCII code 13) or CR LF instead of LF, this can be achieved by adding the parameter &cr or &crlf to the request.

examples (for IP address 192.168.16.200 and administrator password admin)
retrieve recognised keystroke from call button 1: https://192.168.16.200:8443/?

key=admin&sse&key_button_1
retrieve status changes of the application: https://192.168.16.200:8443/?
key=admin&sse&state
retrieve status changes of access 1: https://192.168.16.200:8443/?
key=admin&sse&access_state_1
retrieve status changes of the relay contacts: https://192.168.16.200:8443/?
key=admin&sse&relay_contact_1&relay_contact_2

UDP communication

Using UDP communication

In the 'Network' area, UDP communication can be activated or deactivated. It is already activated in the delivery state.

If UDP communication is activated, the Behnke station regularly sends UDP status messages to provide information about the call status. In addition, sending UDP remote control messages to the Behnke station allows the activation of the integrated relays.

The IP video software requires UDP communication. If UDP communication is disabled, the IP video software cannot be used for this unit.

UDP status messages

UDP status messages are sent periodically to the IP address configured under 'Destination IP address for status messages' at the port configured under 'Destination port for status messages'.

A UDP status message consists of 32 characters and is structured as follows:

‹sequence number›#‹status›@‹parameter›‹checksum›

- sequence number
  Number of the current data set. Is always incremented by 1 up to 255 and then starts again at 0. In this way, multiple reception of a data set can be detected. The sequence number consists of a 2-byte hex string (for example: 01, FF, ...).

- status
  Indicates the current status or the type of data message. The status consists of a 2-byte hex string.

- parameter
  The parameter is the supplement to the status. It contains further information about the status, for example a call number or other refinement of the status. The parameter always consists of 24 characters (ASCII, no control characters). Unused digits are filled with blanks.

- checksum

The checksum is used to check whether the data packet is correct status data. The checksum consists of a 2-byte hex string and is formed over all data bytes as an addition modulo 256.

Status	Parameter	Description
0x0A	firmware version	idle In the case of a Behnke station, the first character of the parameter is a space and the other characters indicate the version. Otherwise, it is a different device generation.
0x01	caller number	incoming call
0x05	number of the remote station	connection state
0x07	number of the remote station	call setup of an outgoing call
0x14	device name	identification Max. 24 characters of the device name are transmitted.
0x4C	registration state	SIP registration parameter=1: SIP registration successful parameter=2: SIP registration failed
0x1E	see remote control messages	response to remote control message
0x5D	number of the remote station	show video

UDP remote control messages

UDP remote control messages to the IP address of the Behnke station are received on the port configured under 'Local port for remote control messages'.

A UDP remote control message consists of 24 characters and is structured as follows:

‹identifier›‹sender IP›‹sequence number›‹fill bytes›‹activation code›‹checksum›

- identifier
  Identification of the protocol: "BSREM" (5 characters - ASCII)

- sender IP
  Contains the IP address of the sender as a string of hex digits. 192.168.0.2 would then be "C0A80002".

- sequence number
  Used to identify the packet when a series of packets has been sent. This also allows duplicate packets received to be detected. The sequence number is represented

hexadecimally with two digits, range 0 to 255 => 00..FF.

- fill bytes
  Three fill bytes for backward compatibility with older products. Are filled with the string "100".

- activation code
  Matches a relay code configured in the 'Relay' section of the Behnke station and allowed for an indoor station. The relay is activated only if it matches. Unused digits of the activation code must be sent as "F". The activation code always consists of 4 digits (only DTMF characters '0123456789' and 'F').

- checksum
  The checksum is formed in the same way as for status messages. The Behnke station sends an acknowledgement after successfully checking and forwarding the request. The data packet has the status code 0x1E and as parameter the remote control data packet defined above is returned 1:1 (fills all 24 bytes of the parameter).

Extended UDP protocol

As previously described, the UDP protocol provides 4 digits for the transmission of the activation code. Therefore, a maximum of 4-digit codes can be transmitted.

There is an extension of the UDP protocol to transmit up to 8-digit codes. For this purpose, 8 instead of 4 digits are provided for the transmission of the activation code. The packet length of the UDP remote control message or of the UDP status message sent as feedback increases accordingly by 4 characters.

TCP communication

Using TCP communication

TCP communication can be enabled or disabled in the 'Network' section. It is disabled by default.

To use TCP communication, an alarm server must be specified to receive the TCP status messages.

When TCP communication is enabled, the Behnke station regularly sends TCP status messages to the alarm server to provide information about the device status.

Each TCP status message is terminated by CR LF, i.e. ASCII codes 13 & 10.

TCP status messages

Message	Description
call est [number]	connection established with subscriber [number]
call ring [number]	incoming connection from [number]
call ended [parameter]	connection ended / idle state parameter=1: SIP registration successful parameter=2: SIP registration failed
dial [number]	outgoing connection to [number]
key dir [parameter]	rirect call key pressed triggered via physical buttons 1..8 or virtual buttons parameter=1..75
key pad [parameter]	keypad key pressed parameter=0..9,*,#,A..D
key dis [parameter]	display key pressed parameter=up, down or ok
key mult [parameter]	button of a buttons extension modules pressed triggered via physical buttons 9..75 parameter=9..75
rel 1 [parameter]	status of relay 1 parameter=0: deactivated parameter=1: activated

rel 2 [parameter]	status of relay 2 parameter=0: deactivated parameter=1: activated
DTMF [Parameter]	DTMF tone detected parameter=0..9,*,#,A..D
discarded [parameter]	buffer overflow, messages discarded parameter=number of discarded messages

Annexe

Technical specifications, features and functions

Important notice

This manual describes the Behnke station in general. This means that it also describes technical specifications, features and functions that may not be available for your model or variant of the Behnke station or only if appropriate additional modules are connected.

General

language:	German, French or English
operation mode:	as SIP telephone or IP intercom
configuration:	with a web browser via HTTP or HTTPS via a tone dialing telephone or the display access protected by password or security code user types: administrator, subadministrator, normal user
scheduled functions:	schedules for each individual weekday or for Mon-Fri/Sat-Sun support for public holidays and special periods as company holidays predefined public holidays for Germany, France and Luxembourg freely adjustable public holidays

Network

connection:	Ethernet 100BaseT according to IEEE 802.3, RJ45 or terminals, or WLAN according to 802.11 b/g/ n with WPA2 (only with antenna module)
Energy supply:	PoE according to IEEE 802.3af or
IP address assignment:	static, dynamic or link-local
VLAN support:	support for tagged VLANs
time:	synchronization via NTP, version 4 with public time server (requires Internet access) or with local time server, if available
e-mail:	sending E-Mails via SMTP or SMTPS when a call button or the alarm input is triggered or when sabotage is detected for logging the access control
dervices:	detection and publication of services via mDNS
UDP communication:	status and remote control messages via UDP

TCP communication:	sending status messages via TCP to an alarm server
port authentication:	according to IEEE 802.1x with EAP EAP-MD5, EAP-TLS, EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPv2, GTC, MD5) or PEAP (MSCHAPv2, GTC, MD5)
LLDP:	according to IEEE 802.1AB support of LLDP-MED, CDP, EDP, SONMP
SNMP:	SNMPv3 SHA, SHA-224, SHA-256, SHA-384, SHA-512 AES, AES128, AES192, AES256

SIP phone

connections:	via SIP server (IP telephone system) or as direct SIP calls
accounts:	2 freely configurable SIP accounts
call acceptance:	separately adjustable for each SIP account or direct SIP calls restrictable to known or specified call numbers
transmission protocol:	UDP, TCP or TLS
Communication:	SIP server SIP server and substitute SIP server SIP registrar and SIP proxy request SIP server via DNS NAPTR/SRV
NAT strategy:	public IP address, ICE with STUN or TURN server, UPNP
AVPF support:	yes, 0-5 s report interval
media encryption:	SRTP, ZRTP or DTLS
voide codecs:	G.711 A-law (PCMA), G.711 µ-law (PCMU), G.722, G.729, GSM, iLBC, Speex (8 kHz) or Speex (16 kHz)
video codecs:	H.264 or VP8
cipher suites:	AES_CM_128_HMAC_SHA1_80, AES_256_CM_HMAC_SHA1_80, AEAD_AES_128_GCM or AEAD_AES_256_GCM
early media:	adjustable for outgoing calls
media management:	early offer or late offer
packetization:	ptime according to codec or adjustable, 10-200 ms
video:	incoming
video resolution:	QCIF = 176x144, QVGA = 320x240, CIF = 352x288, VGA = 640x480, 4CIF = 704x576, SVGA = 800x600, XGA = 1024x768 or 720P = 1280x720
DTMF transmission:	SIP INFO or RFC 2833

DSCP:	classification individually adjustable for SIP protocol, audio and video transmission
jitter compensation:	for audio and video, 0-200 ms

IP intercom system

technology:	peer-to-peer intercom system automatic device detection via mDNS secure data exchange via HTTPS communication via SIP direct calls without server video transmission via MJPG stream or SIP video
system capacity:	max. 100 Behnke stations max. 9 intercom groups max. 99 intercom IDs for indoor stations
configuration:	via the web interface (all settings) via a Behnke indoor station (important settings)
hybrid operation:	additional connection to a telephone system operation as a SIP telephone
multi-network intercom system:	max. 8 different networks per intercom system max. 1 active (outgoing) network bridge per device max. 3 passive (incoming) network bridges per device
firmware:	update via web interface easy distribution to all devices through synchronisation
non-Behnke stations:	integration of up to 9 IP stations (=non-Behnke stations) Behnke SIP phones (=BT-IP) of generations 1 and 2 Behnke IP cameras door opening via DTMF or UDP code other SIP phones and IP cameras (with reservation)
additional functions:	integration of an additional access door without Behnke station automatic video preview when motion is detected

Display

supported displays:	small (3.5") or medium (7") Behnke touch display
functions:	direct call buttons (small display: up to 10, medium display: up to 30), telephone function, code lock function, telephone book, logo, information text, display of pictograms, status texts and call destination
background lighting:	0-100%, switchable according to schedule
touchscreen:	resistive, adjustable pressure sensitivity, calibratable
screen saver:	after 5-90 s, can be deactivated when the display is touchedor the device is used

	device is used
telephone function:	dialing an arbitrary number
code lock function:	entering a code to control a relay
phone book:	max. 300 entries grouping of entries possible adjustable font size, text alignment and display sequence operating instructions grouping of entries with the same first letter search for the first letter export/import of the phone book and provision as download phone book synchronization with an LDAP server functions when selecting an entry: call, group call with 2-4 numbers, call chain with 2-4 numbers, call according to the schedule, door opening always or according to the schedule, output individual voice announcement
logo:	upload an image file in JPG, PNG, GIF or BMP format with max. 10 MB, adjustable display size, automatic image optimization, triggering a function when touched
information text:	up to 8 lines, adjustable font size, font color and text alignment, triggering of a function possible when touched

Connection

call acceptance:	automatically after 0-60 s, manually by pressing a button or rejecting incoming calls silent call acceptance with muting possible code interrogation possible to release the connection
connection establishment:	unlimited or max. 5 s - 5 min separately adjustable for individual calls and call chains
connection duration:	unlimited or max. 1-9 min
disconnection:	adjustable: allowed, allowed after 1-30 s, not allowed

Buttons

display buttons:	small display: max. 10 medium display: max. 30
functions:	fall, group call with 2-4 numbers, call chain with 2-4 numbers, call according to schedule, door opening always or according to schedule, output individual voice message

Relays

number:	2

number:	2
operating mode:	adjustable per relay: door opener relay, connection indication, additional bell or fault indication
switching voltage:	max. 30 VDC / 30 VAC
switching current:	max. 2 A
switching capacity:	max. 60 W / 60 VA
cable length:	max. 30 m
switching contact:	when operating as a door opener relay: normally open or normally closed contact otherwise: normally open contact
door opener relay:	control of a door opener to open an access opening time: 1-90 s codes: max. 9, valid for indoor station or code lock, always or according to a schedule manual, permanent opening (can be activated via codes) or automatic opening according to a schedule possible activation via door release button possible, always or according to schedule logging of access control via e-mail
connection indication:	control of the relay when the device is connected, can be activated for incoming connection, outgoing connection or outgoing connection after picking up the remote station
additional bell:	actuation of the relay while ringing for an incoming call, at the beginning of a direct call (1-90 s) or while a direct call is being set up
fault indication:	actuation of the relay if there is a fault (network connection, SIP registration) on the device
sluice function:	automatic, time-delayed opening of a second access delay time: 1-90 s
webhooks:	sending a URL over the network when the relay is activated or deactivated

Triggers

triggerable functions:	call, group call with 2-4 numbers, call chain with 2-4 numbers, call according to schedule, door opening always or according to schedule, output individual voice announcement
alarm input:	5-24 VDC triggering: with rising and/or falling edge debounce time: 50-1500 ms minimum rising/falling edge duration: none, 1 s - 60 min cable length: max. 30 m
schedule:	executing calls or commands at a specified time

	triggering: at the beginning and / or at the end of a valid period of the schedule
system start:	execute calls or commands after starting the device
daily audio test:	regular check of the functioning of the loudspeaker and microphone trigger a call or a command or indicate a fault in case of a detected audio problem
noise alarm:	available when noise detection is activated minimum noise level: 70-95 dB (tendential) minimum duration of high/not high noise level: 0-120 s

Acoustics

audio test:	function test for loudspeaker and microphone
noise detection:	switchable: measuring and evaluating ambient noise
volume:	0-100 % automatic increase of the volume in a noisy environment: off or from a certain volume class (1-5)
audio amplifier:	1 W output power
microphone sensitivity:	0-100 %
IP audio:	transmit/receive amplification: -10-10 dB echo suppression echo cancellation
acoustic indications:	adjustable, sound or voice output
individual voice announcements:	9 à max. 30 s upload a WAV file (16 KHz, 16 Bit, mono) with max. 1 MB generate voice announcements from text (requires Internet connection, currently (05/2026) free of charge, subject to alterations)

System

configuration:	save/restore configuration
firmware:	2 slot system update via the web interface or via auto-provisioning signed and encrypted firmware files
auto provisioning:	possible: at startup, every 5/30/60 minutes or during the night setting the URL or transmitting via DHCP option 66 or 43 supported protocols: TFTP, FTP, HTTP, HTTPS receive a configuration file (complete or partial), a phone book or a firmware update
API:	HTML-API over HTTP or HTTPS

	requesting/modifying the configuration requesting status information triggering events
SSE:	connection over HTTP or HTTPS requesting detected keys, DTMF tones and changed status information
special functions:	system securisation system supervision automatic restarts temperature supervision with shutdown
operating temperature:	-20 to 50 °C
Conformity:	CE, RoHS EN55035, EN55032, EN62368-1

System startup problems

If there is an error, the device may not start, as described in the section Startup.

Problem after firmware update

If the device no longer starts correctly after a firmware update, you can switch back to the previously used firmware version as follows.

- disconnect the device from the power supply (network cable / PoE injector)
- wait briefly and then reconnect the power supply
- immediately press and hold the configuration button before the status LED lights up
- status LED lights up red
- immediately release the configuration button and then briefly press it twice
- status LED lights up yellow
- device starts, activates the firmware on the inactive slot and then restarts

Problem after configuration change

If the device no longer starts correctly due to a faulty configuration, it should be reset to factory settings as follows.

- disconnect the device from the power supply (network cable / PoE injector)
- wait briefly and then reconnect the power supply
- immediately press and hold the configuration button before the status LED lights up
- status LED lights up red
- keep the configuration button pressed
- for at least 5 seconds
- status LED lights up white
- immediately release the configuration button and then briefly press it twice
- device starts and resets the configuration to factory settings

Hardware error

If there is a hardware error, the device tries, if still possible, to output an error number via the status LED, the loudspeaker or the display, if available.

2 initialisation error
3 IO error
4 network hardware error
5 network device error
6 audio device error
7 line device error
8 USB hardware error

9 AIF error
10 no delocalised electronic detected

The error number is displayed by the status LED as follows.

- status LED lights up red
- for about 20 seconds
- status LED goes out briefly
- status-LED flashes yellow several times
- :
- to display the error number
- device is restarting

In the event of a hardware error, please contact our

Service hotline: +49 6841 / 8177-777

Version history

version 2.90 29/11/2022

- first firmware version

version 3.00 1/1/2023

SIP phone
- Change: automatic appending of the SIP server when creating the SIP identity only if no SIP server is specified in the 'phone number / user name' field

version 3.63 21/8/2023

Basic configuration
- New: jump to the relevant setting by clicking on a warning or error message
- New: display of a hardware problem if no microphone signal is detected
- New: display of a configuration problem when the fallback to link-local should be turned off or the IP address assignment should be changed
- New: display of appropriate messages if the device or configuration is not suitable for barrier-free access

General
- New: creating/modifying of individual voice announcements in the user configuration
- New: displaying a contact information (installer/service) on the login screen and in the user configuration
- Change: allow special characters for the administrator or user password
- New: indications for a barrier-free access
- Change: support for up to 10 time periods for schedules
- Change: setting option to grant a user access to schedules for continuous opening
- New: setting option whether or not the video direction in the SDP should be adjusted for SIP video connections in one direction

Network
- Change: removal of support for the USB extension port adapter on the AIF hybrid
- New: support of the USB extension port adapter on the USB hub
- New: settings whether the certificate or the CN of the outgoing e-mail server should be verified or not
- Change: sending the dialled call number via UDP status message also for calls via the telephone function
- Change: support of net masks instead of subnet masks

Analogue phone

- New: extended configuration steps for adjusting the expert settings for analogue audio, DTMF, busy tone detection and connection detection

SIP phone

- Change: checking port 5059 when a failed SIP registration returns response code 501
- Change: delayed output of the voice announcement to the remote station if the connection is in the hold state directly after activation of a door opener relay
- New: setting the maximum available bandwidth for SIP connections and adaptive bitrate control
- New: setting the maximum framerate for SIP video connections
- New: acceptation of incoming calls separately adjustable for each SIP account or direct SIP calls with the option to only accept calls from known or specified call numbers
- New: customisable keyframe rate for SIP video transmissions
- Change: update of the validity check of an FQDN
- Change: support of the special configuration of a SIP account also for calls via the telephone function
- New: support of SIPS for TLS
- New: setting option for the preferred payload type for telephone-event, H.264 and VP8
- New: retrying the registration process when a SIP domain is given to query the server via DNS and the NAPTR request fails

Camera

- Change: display of the HTTP URLs when displaying the URLs for camera access if access to the web interface is only allowed via HTTPS, but access to the camera is allowed via HTTP
- Change: adapt webcam resolution also for IP cameras
- Change: adjustable brightness threshold above which an environment previously evaluated as dark is again evaluated as bright
- Change: increase the maximum length of door opener codes that can be transmitted by the IP video software from 4 to 8
- New: provide an XML file to retrieve the video image via action URL for Snom® phones that support this

Display

- New: using reduced display brightness instead of switching off the display when screen saver is active
- New: ESD detection to remedy malfunctions of the display due to electrostatic discharges

Connection

- New: accepting incoming calls with code entry to unlock the connection
- New: silent acceptance of incoming calls with muting
- New: DTMF commands for the remote station: hang up, mute on/off
- New: DTMF confirmation for call chains

Buttons
- New: additional commands for use in the call number: wait, play voice announcements to the remote party, hang up, disconnect not allowed, play standard voice announcements, disable voice announcements for the call, mute call, disable key click
- Change: increase the maximum length of a call number to 100 characters so that longer e-mail addresses can also be used

Relays
- New: sluice function for automatic and delayed opening of a second access
- Change: skipping the webhook for deactivation of a relay if the relay is already deactivated
- New: during a call as a SIP telephone, the acceptance of a code sent by the remote station can be restricted to known or specified call numbers
- New: support of operation as break contact in addition to operation as make contact for all operation modes

Triggers
- New: delayed triggering of the alarm input by setting the minimum edge duration
- New: noise alarm for detection of high ambient noise

Acoustics
- New: display of the detected microphone signal
- New: audio test for loudspeaker and microphone
- New: key click for direct call buttons, keypad keys, door opener button or when triggering a trigger can be individually set
- New: playing the voice announcement set for an acoustical indication in the web interface
- Change: correct output of a configured individual voice announcement for the called party after answering the call
- New: conformity check and activation of language outputs for a barrier-free access
- Change: general on/off switching of the IP echo suppression instead of in the connection
- Change: increasing the echo cancellation duration
- Change: adjusting the analogue audio settings

Diagnostics
- Change: improved handling of malformed SIP messages
- Change: improved handling of log messages with special characters

System
- Change: display of an error message when restoring a configuration file if it could not be decrypted
- Change: keeping the PoE supply of the extension port switched on during a shutdown with the appropriate setting
- New: possibility of setting which elements are to be retrieved during auto-provisioning
- New: support of the hardware version V2 of the Geniatech® DB4 mainboard

Web interface
- Change: scrollable configuration sidebar for browser windows with low height

version 3.74 31/9/2023

Network
- Change: support for the integration of an IP camera as a display camera also with an AIF hybrid
- Change: increase the maximum length of the URL for integrating an other IP camera to 200 characters

SIP phone
- Change: adjusted handling on failover to another SIP server
- Change: analysis of the correct SIP server used for registration in case of registration failure

Camera
- New: displaying the IP video window when motion is detected without triggering a call
- New: support for the M3067 IP camera

Display
- Change: reduced brightness must not be set higher than the normal brightness
- Change: adjusting the default calibration of the medium display with resistive touchscreen
- Change: unlocking ESD detection for medium display with resistive touchscreen

Buttons
- New: new command to display the IP video window without triggering a call
- New: new command for sending DTMF codes to the remote station within a connection
- New: new condition to use a direct call button as an action button and execute commands within a connection via it

Acoustics
- New: setting option whether or not a tone should be emitted to the remote station after an incoming call is accepted

System
- Change: improved configuration of the serial interfaces
- Change: improved display of the validity period of uploaded certificates

version 4.00 1/1/2024

Network
- Change: deactivating the network during the start-up phase for devices with AIF IP

- Change: deactivating the LLDP service when it is not required
- New: possibility to disable the fallback to link-local by pressing the configuration button 6 times
- Change: support for port authentication with tagged VLAN
- Change: setting the VLAN priority when receiving a corresponding LLDP-MED policy

SIP phone
- New: support of SIP accounts on the same SIP server with different users
- Change: using the SIP domain, if specified, instead of the SIP server to assign the SIP account via sip1:, sip2:, sip3:

Buttons
- New: new command to disable the voice announcement in case of a detected audio problem

Phone book
- Change: correction when removing all phone book entries when using the web interface in French

Triggers
- New: automatic triggering of a call or action after system start-up
- New: daily audio test to regularly check the functionality of the loudspeaker and microphone

Diagnostics
- New: display of the current state of the relay contacts when testing the device
- New: display of the arp-cache for diagnostic purposes

version 5.15 25/2/2025

General
- Change: automatic saving of the configuration if the configuration mode is terminated by hanging up and not with *

Network
- New: setting the NTP time server to be used via DHCP option 42
- Change: integration of the extension port into the VLAN of the Webcam if the extension port is used as an Ethernet port and a VLAN for the Webcam is used
- New: support for port forwarding to access the device behind a NAT
- Change: change regarding TLS in the email sending settings: smtp does not use TLS, smtp/smtps uses TLS if possible, and smtps uses TLS

Analogue phone
- Change: hanging up on a call via the analogue telephone line if no line is connected

SIP phone
- New: options to set the preferred cipher suites for media encryption
- New: integration of the cipher suites AEAD_AES_128_GCM and AEAD_AES_256_GCM
- New: setting option for the call number that is transmitted to the IP video software
- Change: increasing the timeout for calls on hold

Camera
- New: support for the M4327 IP camera
- New: permanent display of the IP video window without triggering a call

Display
- New: new display functions: logo & phone book, logo & phone book & telephone, logo & phone book & code lock, logo & phone book & telephone & code lock

Buttons
- New: code lock function via buttons for devices without keypad

Handset
- New: support for a handset extension module

Phone book
- Change: allow the user to change phone book entries

Relays
- Change: deactivating a relay in the 'connection indication' operating mode if the connection is cancelled or if the relay was activated manually via a command before the connection, but no connection was established
- New: support for one-time codes for the code lock function

Triggers
- Change: correct deactivation of the noise alarm

Acoustics
- New: support for Push-To-Talk

System
- Change: adaptation when using passwords with special characters
- New: remote management via connection to a Behnke ControlCenter

ControlCenter
- New: one-off or regular transmission of selected configuration options

version 5.26 7/4/2025

General
- Change: correction for resetting the administrator password via configuration step 73

Network
- Change: ANSI character encoding for UDP status messages

SIP phone
- Change: setting option for normalising the call number
- Change: appending the missing domain to a number to be dialled

Display
- Change: correction when scrolling/triggering when using the phone book function

Phone book
- Change: faster scrolling in the phone book

Acoustics
- New: setting for microphone correction for noise detection

Diagnostics
- New: setting option for the network interface for the network trace

version 5.91 3/12/2025

General
- Change: correction when programming buttons via configuration mode in the case of 30 or more buttons
- New: introduction of a subadministrator with access rights for selected sections and functions

Network
- New: SNMP support

SIP phone
- Change: providing SIP video images with a timestamp
- Change: enabling VP8 as second video codec by default
- New: setting option for disabling the local port for SIP via UDP/TCP or TLS
- New: new setting to individually define the size of keep-alive packets
- New: new setting to allow early media for group calls
- New: using the Behnke Station certificate as client certificate for mTLS
- Change: automatic adjustment of the keyframe rate for SIP video transmissions
- Change: increasing the maximum length of the 'Phone number / user name' and 'User ID' fields to 100 characters

IP intercom
- New: support for network bridges to implement a multi-network intercom system
- New: firmware synchronisation of all devices in the intercom system
- New: integration option for other SIP phones or IP cameras as IP stations

- New: use of G.722 as the preferred codec for calls in intercom mode
- New: new setting for the volume of the ringtone
- New: automatic video preview when motion is detected
- New: history function for automatic preview and calls

Camera
- Change: correction when saving camera settings in case of manual definition of an IP camera
- Change: granting camera access for outgoing calls while the call is being established

Display
- New: option to deactivate the visualisation of keystrokes for the code lock function
- New: option of randomly distributing the digits of the code lock function

Buttons
- New: new conditions to configure virtual and physical buttons differently
- New: additional commands for use in the call number to activate one of the keypad functions
- New: additional command for use in the call number to change the name show in the display
- New: additional command for use in the call number to activate the phone book function

Phone book
- Change: encoding of LDAP search base and search filter depending on the set character encoding
- New: multilanguage phone book
- New: setting option to use the physical button as OK on an all-in-one communication station

Relays
- New: setting option for checking the identity of https webhooks

Acoustics
- New: setting option to operate the device without hands-free microphone

System
- Change: migration to Kirkstone
- New: triggering a door opener relay via the API with the user password
- Change: correction when saving/restoring the configuration if the administrator password contains a $ character
- Change: repeating detection when extension modules are missing

version 6.12 14/2/2026

General

- New: editing and setting voice announcements via configuration mode
- New: new special symbols (relays/voice announcement) for entering phone numbers via configuration mode
- New: configuring additional activation codes via configuration mode

Network
- New: sending TCP messages to an alarm server

IP intercom
- New: setting a preferred view for video display on the indoor station

Relays
- New: time limit for manually opening access continuously
- New: extension of webhook functionality to include the option of sending data as JSON or urlencoded
- New: own designation for door opener relay
- New: automatic opening of access in case of an incoming call of an authorised call number

Acoustics
- Change: improved evaluation of ambient noise

System
- New: SSE (server-sent events) for retrieving events such as detected key presses, DTMF tones or status changes via an HTTP or HTTPS connection

version 6.33 3/5/2026

SIP phone
- Change: updating the SIP stack

IP intercom
- Change: troubleshooting passwords containing special characters

License information and copyright notices

The software of the Behnke station and the associated firmware version offered for download are hereinafter referred to as „Behnke station software 6.33“.

License information

The Behnke station software 6.33 contains components that are under different licenses. You can get a complete overview of all components and their licenses either via the Behnke station's web interface in the section 'System' under 'License information' or download it under https://behnke.support/firmware/licenses-6.33.zip for platform P1 devices or under https://behnke.support/firmware/P2-licenses-6.33.zip for platform P2 devices.

Open source software

The Behnke station software 6.33 contains components that are licensed under the GNU Affero General Public License version 3, the GNU General Public License versions 2 or 3, or the GNU Lesser General Public License versions 2.1 or 3, respectively.
Anyone can receive the source code of these components from us on a data carrier for a refund of 5 euros for the cost of the data carrier and its shipping.
This offer is valid for a period of three years from delivery of the Behnke station with software version 6.33 or from the download of firmware version 6.33.

Please send your request, specifying the serial number and version 6.33 to:

Telecom Behnke GmbH
Robert-Jungk-Strasse 3
66459 Kirkel
Germany

As a precaution, it is pointed out that the use of the right guaranteed in the license agreement to replace the open source components with your own versions leads to the expiry of the certification or guarantee. The operation of the corresponding product is at your own risk.

Copyright notices

The Behnke station software contains components that require copyright notices. These are listed below.

For the components under license BSD- or BSD-Clause-4:

> Copyright © 1990 Regents of the University of California. All rights reserved.
>
> This product includes software developed by the University of California, Berkeley.

For the components under the ICU license:

Copyright © 1995-2014 International Business Machines Corporation and others. All rights reserved.

Permission free of charge to anyone who receives a copy of this software and associated documentation files (the "Software") grants to trade in the software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute and / or sell copies of the software, and to persons to whom the software is made available Permit to do so provided that the above copyright notices and this permission notice appear on all copies of the software and that both the above copyright notices and this permission notice appear in the accompanying documentation.

For the components under the license openssl:

Copyright © 1998-2008, The OpenSSL-Project. All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. https://www.openssl.org/

For the components under license PHP-3.0:

Copyright © 1999-2006, The PHP Group. All rights reserved.

This product includes PHP, available free of charge from https://www.php.net/

For the components under the FreeType license:

Copyright © 1996-2002, 2006, David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved.

This product includes software developed by the Free-Type team.

For the components under the Info-ZIP license:

Info-ZIP License

Copyright © 1990-2009 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly,

Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

- Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
- Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. Additional documentation is not needed for executables where a command line license option provides these and a note regarding this option is in the executable's startup banner. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
- Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
- Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

For the components under the libtiff license:

For the components under the Net-SNMP license:

Legal notices

- We reserve the right to make changes to our products in the interest of technical progress. In the course of ongoing development, the products shown may also differ optically from the products supplied.
- Reprints or adoption of texts, images and photos in any media from these instructions - even in part - are only permitted with our express written consent.
- The design of this manual is subject to copyright protection. We accept no liability for any errors, content or printing errors (including technical data or within graphics and technical sketches).
- AXIS is registered trademark or trademark application of Axis AB in various jurisdictions.
- Windows is a registered trademark of the Microsoft Corporation.
- Snom is a registered trademark of Snom Technology GmbH.
- All other company and product names may be trademarks of the respective companies with which they are associated.

Information on the product liability act

- All products from this manual may only be used for the specified purpose. If there are any doubts, this must be clarified with a competent specialist or our service department (see hotline numbers).
- Products that are powered (especially 230 V mains voltage) must be disconnected from the power supply before opening or connecting cables.
- Damage and consequential damage caused by interventions in or changes to our products as well as improper handling are excluded from liability. The same applies to improper storage or external influences.
- When working with 230 V mains voltage or with products operated on the mains or with batteries, the relevant guidelines must be observed, e.g. guidelines for compliance with electromagnetic compatibility or low voltage guidelines. Corresponding work should only be carried out by a specialist who is familiar with it.
- Our products comply with all the technical guidelines and telecommunications regulations applicable in Germany and the EU.

Electromagnetic Compatibility
Low Voltage Directive

Telecom Behnke GmbH
Robert-Jungk-Straße 3
66459 Kirkel
Deutschland / Germany

Info-Hotline: +49 6841 / 8177-700
Service-Hotline: +49 6841 / 8177-777

info@behnke-online.de
www.behnke-online.de

Télécom Behnke sàrl
15, rue du Parc
57600 FORBACH
France

Infoligne : +33 3 87 84 99 50
Hotline SAV : +33 3 87 84 99 55

info@behnke.fr
www.behnke.fr